TREK

DATA

USER GUIDE

April 2019

Approved for Public Release; Distribution is Unlimited.

TABLE OF CONTENTS

PARAGRAPH PAGE

1 Welcome ... 1

1.1 Getting Started ... 1

2 Technical Support ... 1

3 Introduction ... 1

4 Overview of the User Interface ... 2

4.1 Main Window ... 2
4.2 Menus ... 4

5 Quick Start Guides ... 5

5.1 How to Add a Service ... 6
5.2 How to Activate a Service ... 6
5.3 How to Deactivate a Service ... 6
5.4 How to View Processed Data ... 7
5.5 How to Change the Data Store ... 7

6 Details ... 7

6.1 Service ... 7
6.1.1 Service Dialog (Data Source Tab) ... 8
6.1.2 Service Dialog (Data Description Tab) ... 16
6.1.3 Service Dialog (Process Tab) ... 19
6.1.4 Service Dialog (Record Tab) ... 20
6.1.5 Service Dialog (Forward Tab) ... 27
6.2 Parameters ... 31
6.3 Displays ... 32
6.4 Manage Custom Displays ... 35
6.4.1 Add Custom Display Dialog ... 37
6.4.2 Modify Custom Display Dialog ... 38
6.4.3 Export Display Dialog ... 38
6.5 Manage Monitor Sets Dialog ... 38
6.5.1 Add Monitor Set Dialog ... 39
6.5.2 Modify Monitor Set Dialog ... 40
6.5.3 Export Monitor Set Dialog ... 40
6.6 Manage Monitoring Dialog ... 41
6.7 Monitor Messages Dialog ... 42
6.8 Configure Monitor Message Logging Dialog ... 42
6.9 Statistics ... 43
6.9.1 Configure Statistics Dialog ... 50
6.10 Configure Statistics Snapshot Recording Dialog ... 54
6.11 View Packet Dialog ... 55
6.12 Change Data Store Dialog ... 57
6.13 Manage Cryptography Settings Dialog ... 58
6.14 Application Messages ... 59
6.15 Application Configuration File ... 61
6.16 Application Settings ... 61

7 FAQ and Troubleshooting ... 62

FIGURES

FIGURE PAGE

Figure 1 Main Window 3
Figure 2 Service Menu Context Specific Menu Items 5
Figure 3 Add Service Dialog 8
Figure 4 Service Dialog (Data Source General Tab) 9
Figure 5 Service Dialog (Bundle Protocol Configuration) 10
Figure 6 Service Dialog (Multicast Configuration) 11
Figure 7 Service Dialog (TCP Client Configuration) 12
Figure 8 Service Dialog (TCP Listener Configuration) 13
Figure 9 Service Dialog (UDP Configuration) 14
Figure 10 Service Dialog (UNIX Domain Socket Configuration) 14
Figure 11 Service Dialog (Data Source Queues Tab) 15
Figure 12 Service Dialog (Data Source Cryptography Tab) 16
Figure 13 Service Dialog (Data Description Tab) 17
Figure 14 Pattern Match Using Packet Type 18
Figure 15 Service Dialog (Processing Tab) 19
Figure 16 Service Dialog Processing Tab Modify Properties Dialog 20
Figure 17 Service Dialog (Record Tab) 21
Figure 18 Service Dialog Record Tab (General Tab) 22
Figure 19 Multiple Record Directories Auto-Generated on Incoming Data 23
Figure 20 Auto-Generated Folders for Recorded Data Files 24
Figure 21 User Specified Record Directories and Base Filenames 24
Figure 22 Service Dialog Record Tab (Advanced Tab) 25
Figure 23 Service Dialog (Forward Tab) 27
Figure 24 Forward Destinations 28
Figure 25 Service Dialog Forward Tab Packet List 29
Figure 26 Service Dialog Forward Tab Transform 30
Figure 27 Service Dialog Forward Tab Encrypt 30
Figure 28 Parameters Dialog 31
Figure 29 Parameter Details Dialog 32
Figure 30 Displays Dialog 33
Figure 31 Predefined Display 34
Figure 32 Status Characters Dialog 35
Figure 33 Manage Custom Displays Dialog 36
Figure 34 Add Custom Display Dialog 37
Figure 35 Export Display Dialog 38
Figure 36 Manage Monitor Sets Dialog 39
Figure 37 Add Monitor Set Dialog 40
Figure 38 Export Monitor Set Dialog 41
Figure 39 Manage Monitoring Dialog 41
Figure 40 Monitor Messages Dialog 42
Figure 41 Configure Monitor Message Logging Dialog 43
Figure 42 Statistics in the Main Window 44
Figure 43 Statistics Dialog 44
Figure 44 Statistics Pop-Up Menu 45
Figure 45 Device Statistics View 46
Figure 46 Device and Packet Statistics 46
Figure 47 Device Receiving Unexpected Packets 47
Figure 48 Snapshot Statistics 47
Figure 49 Debug Statistics View for Packet 7 Service 48
Figure 50 Debug Statistics Expanded View for Packet 7 Service 49
Figure 51 Configure Statistics Dialog 50

Figure 52 Configure Statistics Snapshot Recording Dialog 54
Figure 53 View Packet Dialog.....55
Figure 54 View Configure Dialog 56
Figure 55 View Packet Example 57
Figure 56 Change Data Store Dialog.....58
Figure 57 Manage Cryptography Settings Dialog 58
Figure 58 Messages Dialog 60
Figure 59 Configure Messages Dialog 60
Figure 60 Clear Messages Dialog.....61

1 Welcome

The Telescience Resource Kit (TReK) is a suite of software applications and libraries that can be used to monitor and control assets in space or on the ground.

The TReK Data application provides the capability to manage data services such as receiving data, processing data, recording data, forwarding data, and displaying data.

The topics in this user guide require an understanding of the topics covered in the TReK Concepts document. Please be sure you have read the TReK Concepts document before reading this user guide.

1.1 Getting Started

Start with the Introduction which provides an application overview. Next, try the Quick Start Guides for "How Tos" for common functions. For help with details, reference the Details section. See the FAQ and Troubleshooting section for helpful hints and solutions to the common "gotchas".

2 Technical Support

If you are having trouble installing the TReK software or using any of the TReK software, please contact us for technical assistance:

TReK Help Desk E-Mail, Phone & Fax:

E-Mail: trek.help@nasa.gov
Telephone: 256-544-3521 (8:00 a.m. - 4:00 p.m. Central Time)
Fax: 256-544-9353

If you call the TReK Help Desk and you get a recording please leave a message and someone will return your call. E-mail is the preferred contact method for help. The e-mail message is automatically forwarded to the TReK developers and helps cut the response time. The HOSC Help Desk (256-544-5066) can provide assistance as needed and is available 24x7.

3 Introduction

The TReK Data application provides the capability to manage data services such as receiving data, processing data, recording data, forwarding data, and displaying data. It can be configured to receive different types of data from multiple sources simultaneously. The configuration can be saved.

The Data application creates a TReK data store on application initialization. The data store is used by the application to store incoming data so it can be accessed using the

TReK Telemetry Application Programming Interface (API). When using the TReK Telemetry API, you will need the data store name. The Data application uses "DefaultDataStore" as the default data store name. If you start another instance of the TReK Data application, and the "DefaultDataStore" name is already in use, the application will prompt you to enter a new and unique name. There is also an option within the application to change the data store name.

4 Overview of the User Interface

4.1 Main Window

The main window consists of three main areas as shown in Figure 1. The top part of the main window contains the list of services. A Service is used to identify one or more incoming data streams and what type of services should be applied to the incoming data. When you start the Data application the list will be empty. The middle part of the window is the Statistics area. Once you start receiving data, the Statistics area will display statistics information about the incoming data streams. It will also provide information about the services being performed like how many packets were recorded, how many packets were forwarded, etc. The Statistics area can be reconfigured to show several different views. The bottom part of the window is a message area that is used to display important status and information messages about the activities in progress.

You may have noticed that each service row has a color associated with it. The color provides information about the service. For example, when using the default colors, if the packet row is black, this indicates that the packet has not been activated. If the packet row is purple, this indicates that the service is initializing. If the packet row is blue, this indicates the packet has been activated but no data has arrived. If the packet row is green, this indicates that data packets are arriving. The colors are helpful in providing immediate information about the general configuration and status of each packet in the list.

Figure 1 shows two services in the Service area. The first service in the list is named **Science Data**. The Science Data service is configured to receive a data stream containing science data. The status is Active and the color is green to indicate that data is arriving. The second service in the list is named Health and Status Data. The status is Inactive and the color is black. This indicates that the service has been configured but not activated. Until the service is active, the Data application is not prepared to handle the incoming data. When a service is activated, it creates all the network sockets and other support needed to support the services requested. As soon as a service goes Active, the application will start applying the configured services to support any data that arrives (processing, recording, etc.).

The Statistics area and the Message Area are dock windows that you can float or dock. To float a dock window, use your left mouse button to click and hold the title area while

dragging the window to another area of the screen. To dock, use the title bar to drag the dock window over the main window and drop.

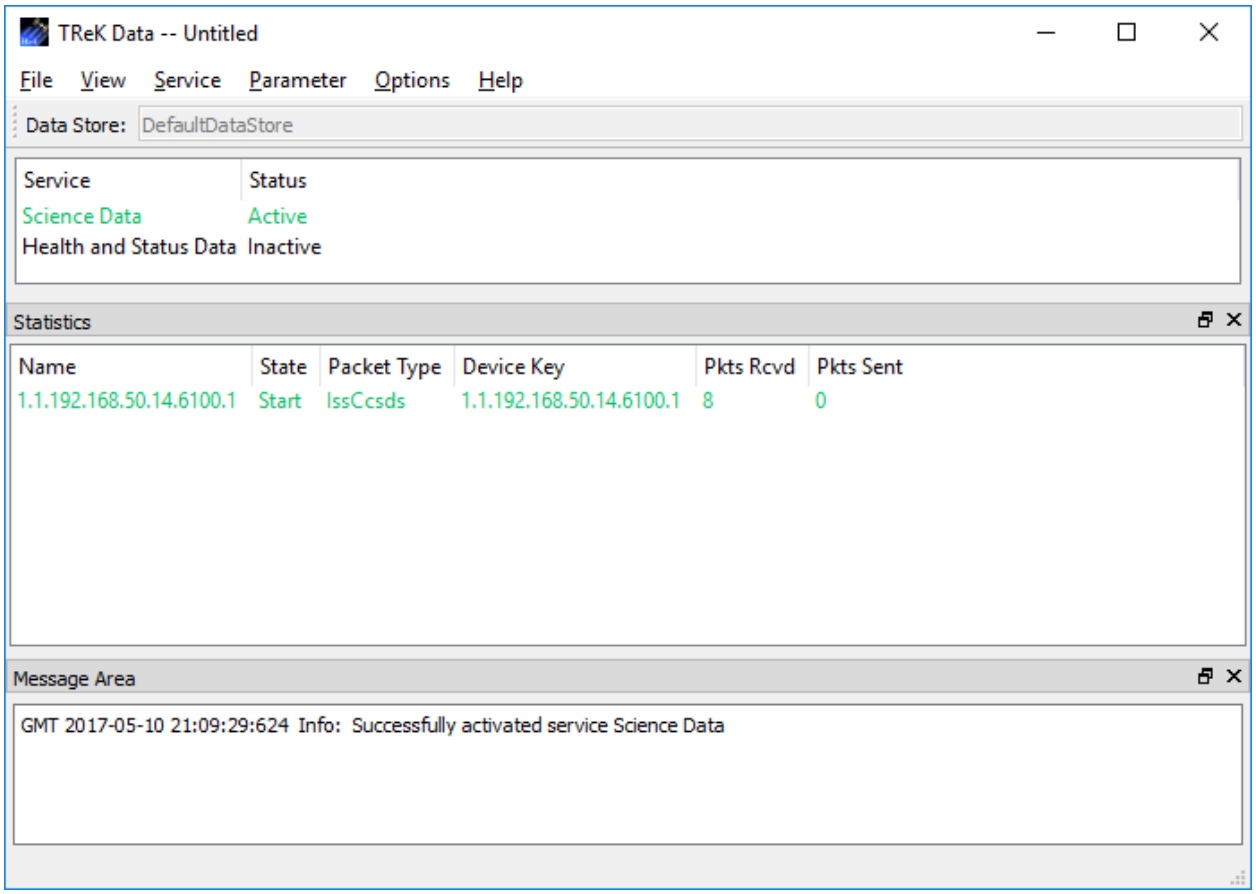


Figure 1 Main Window

Data Store Toolbar

The Data Store toolbar displays the name of the data store created by the application.

Service Area

The Service area provides a list of "Services". A Service is used to identify one or more incoming data streams and the services to be applied to the incoming data.

Statistics Area

The Statistics area provides real time statistics information for active services.

Message Area

The Message Area displays important information, warning and error messages. The message area can be cleared using the View menu.

4.2 Menus

The application menus are: File, View, Service, Parameter, Options, and Help. Each of these menus is described in more detail below.

File Menu

The File menu provides the capability to create a new configuration, open a configuration, save a configuration, and exit the application.

View Menu

The View menu provides the capability to clear the main window message area and show and hide the main window statistics and message area.

Service Menu

The Service menu provides the capability to perform functions associated with services such as adding a service, activating a service, or deleting a service. The service menu also shows context dependent menu items corresponding to the configuration of the service. The context menu items will only appear when the service is active. For example in Figure 2 there is a service selected that is configured to record data. Therefore, when the service is active and selected there will be additional service menu items to control recording. There are no additional menu items for Processing and Forwarding.

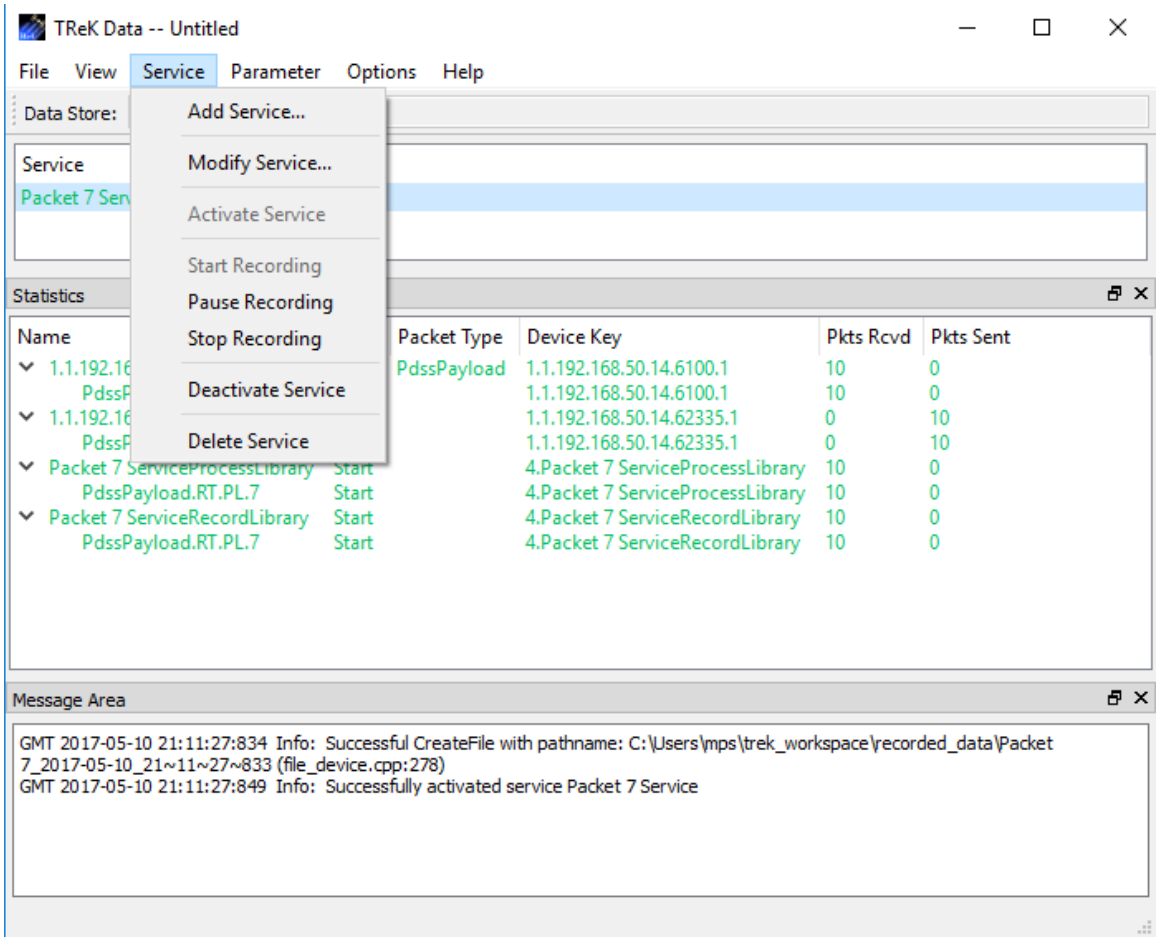


Figure 2 Service Menu Context Specific Menu Items

Parameter Menu

The Parameter menu provides access to parameter type capabilities such as displays and parameter monitoring.

Options Menu

The Options menu provides the capability to access statistics, reset statistics, configure statistics snapshot recording, and change the data store. It also provides access to the Messages dialog which can be used to display and filter application messages.

Help Menu

The Help menu provides access to on-line help and application version information.

5 Quick Start Guides

This section provides “How Tos” for common functions.

5.1 How to Add a Service

This section describes how to add a service. For additional information and details about the Add Service dialog please reference section 6.1.

1. To add a service, go to the Service menu and select Add Service.
2. Enter a service name unique to this instance of the Data application.
3. To configure the application to receive incoming data, enter the information about how the data will arrive on the Data Source tab. Using this tab you can configure to receive data using a specific communication protocol such as UDP.
4. To define what data the service should accept, enter a description of the data on the Data Description tab. This tab provides a way to control what data will be accepted for processing, recording, or forwarding.
5. To process incoming data, enter the processing information on the Process Tab. You can identify which packets you would like to process along with configuration information such as the number of buffers to use and the length of the buffers.
6. To record incoming data, enter the recording information on the Record Tab. You can specify to record data in a single directory or multiple directories.
7. To forward incoming data, enter the forwarding information on the Forward Tab. You can specify to forward data to one or more destinations selecting the communication protocol to use for each destination.

5.2 How to Activate a Service

This section describes how to activate a service.

1. To activate a service, select the service in the Main Window Service Area. Then go to the Service menu and select Activate Service.

Note: There is also a context sensitive pop-up menu available in the Main Window Service Area. Select the service in the list and then use the right mouse button to access the pop-up menu and select Activate Service.

5.3 How to Deactivate a Service

This section describes how to deactivate a service.

1. To deactivate a service, select the service in the Main Window Service Area. Then go to the Service menu and select Deactivate Service.

Note: There is also a context sensitive pop-up menu available in the Main Window Service Area. Select the service in the list and then use the right mouse button to access the pop-up menu and select Deactivate Service.

5.4 How to View Processed Data

The following steps describe how to view processed data. For additional information and details please reference section 6.3 and section 6.4. When a service is configured with processing turned on, the Data application will auto-generate pre-defined displays to view the processed data. The predefined displays can be accessed using the Show Displays menu item on the Parameter menu. Custom Displays can also be defined. See section 6.4 for details.

1. Add a service with Processing set to on.
2. Activate the service.
3. Go to the Parameter menu and select Show Displays.
4. Select a display in the list and push the Start button. The display is automatically started and will display data if data is being received.

5.5 How to Change the Data Store

The following steps describe how to change the data store. For additional information and details about the Data Store dialog please reference section 6.12. The data store name can only be changed when all data processing services are off. If there are any active services that are processing data, the data store cannot be changed.

1. On the Options menu select Change Data Store.
2. Enter a valid Data Store name. It must be unique and not in use by any other instances of the TReK Data application.
3. Push the OK button to save the data store name and exit the dialog.

If successful, the Data Store toolbar will be updated to reflect the new data store name.

6 Details

This section covers various application details.

6.1 Service

The Service dialog is used to define the services that should be applied to one or more incoming data streams. The Service configuration can only be modified when the Service is inactive. The Add Service dialog is show in Figure 3. Details are provided below.

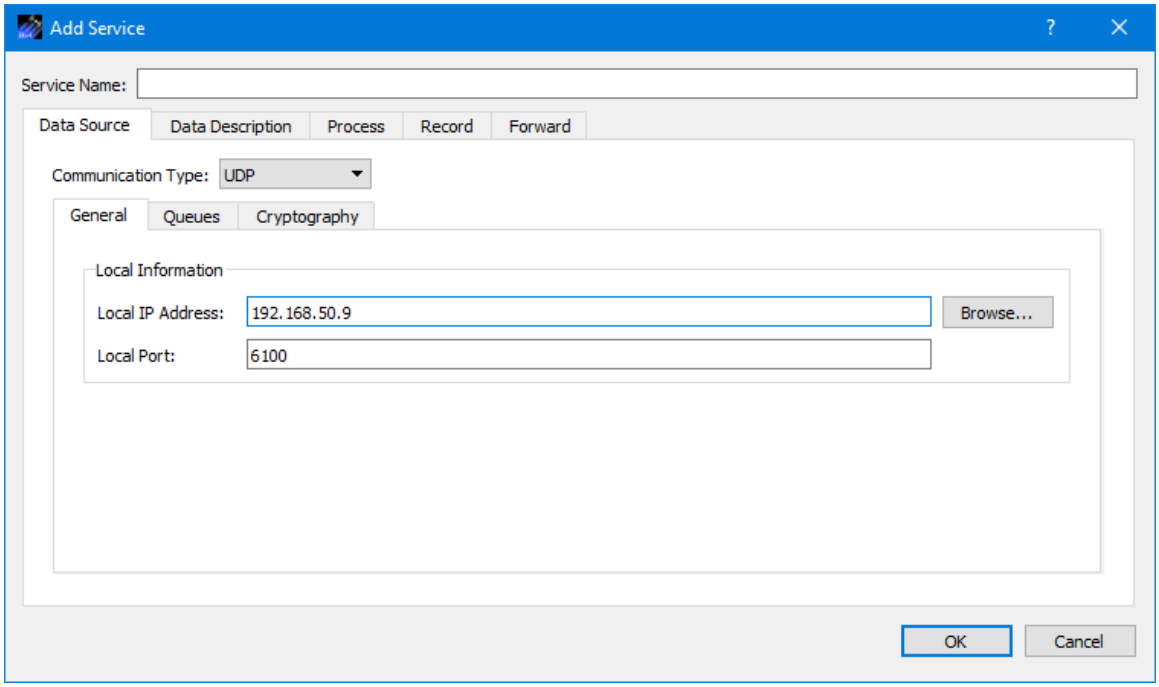


Figure 3 Add Service Dialog

<u>Service Name</u>
Each Service must have a unique name.

6.1.1 Service Dialog (Data Source Tab)

The Service Dialog Data Source tab is shown in Figure 4.

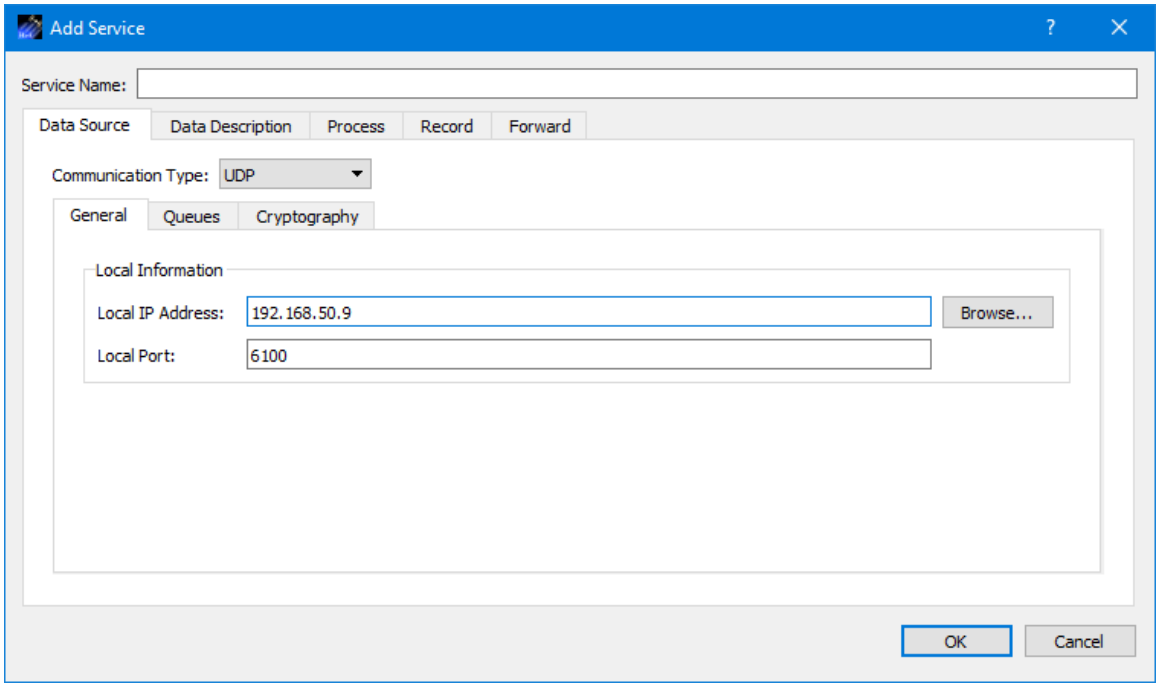


Figure 4 Service Dialog (Data Source General Tab)

6.1.1.1 Data Source General Tab

The Data Source General tab is used to enter information about how the data will be received. The fields that are displayed depend on the Communication Type setting. Communication Types include Bundle Protocol, Multicast, TCP Client, TCP Listener, UDP, and Unix Domain Socket (only available on Linux).

Each communication type configuration is described below.

6.1.1.1.1 Bundle Protocol Configuration

The Bundle Protocol Configuration is shown in Figure 5.

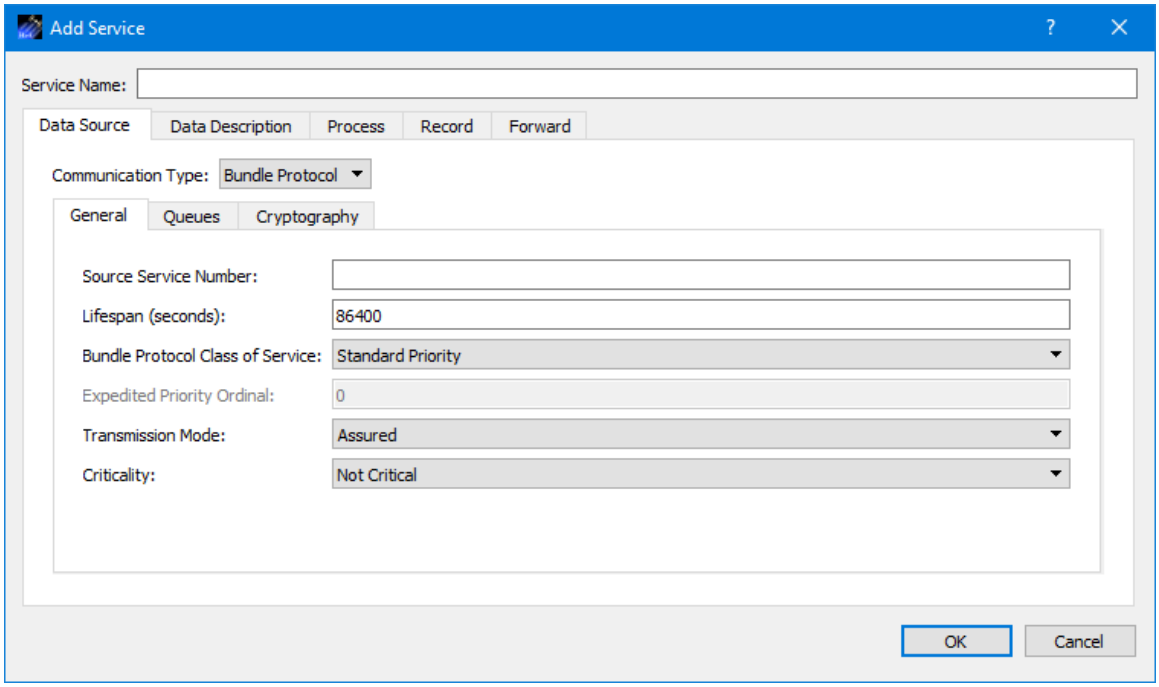


Figure 5 Service Dialog (Bundle Protocol Configuration)

Each field is described below.

Source Service Number

The source service number is ION's configured BP service number. This number is used to receive packets from ION.

Lifespan

The lifespan is the bundle's "time to live" (TTL) in seconds. The bundle is destroyed if its TTL has expired and it has not reached its destination. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 86400.

Bundle Protocol Class of Service

The BP class of service defines the transmission priority of outbound bundles from three ION priority queues corresponding to *Bulk Priority*, *Standard Priority*, and *Expedited Priority*. The expedited priority queue must be empty before bundles in the standard or bulk queues are serviced by ION. Therefore, bundles with *Expedited Priority* should only be sent in critical/emergency situations. The default value is *Standard Priority*.

Expedited Priority Ordinal

The expedited priority ordinal is only associated with the *Expedited Priority* class of service. Ordinal values range from 0 (lowest priority) to 254 (highest priority). The default value is 0.

Transmission Mode

The transmission mode defines the reliability of bundle delivery to a destination. The three transmission mode parameter values are *Best Effort*, *Assured*, and *Assured with Custody Transfer*. *Best Effort* relies upon the underlying convergence-layer protocol (e.g., Transmission Control Protocol or TCP) to retransmit missing bundles. *Assured* is a step up in reliability and includes BP support in detecting a lost TCP connection and re-forwarding of bundles assumed aborted by the convergence-layer protocol failure. *Assured with Custody Transfer* requires the reception, by the sending node, of a custody acceptance or refusal signal (packaged in a bundle) from the receiving node. The default value is *Assured*.

Criticality

A critical bundle is one that has to reach its destination as soon as is physically possible. For this reason, bundles flagged as critical may not include custody transfer and require an ION configuration with contact graph routing. In some cases, a critical bundle may be sent over multiple routes to ensure delivery to its final destination. Critical bundles are placed in the expedited priority queue and should only be used in emergency situations. The two criticality parameters are *Not Critical* and *Critical*. The default value is *Not Critical*.

6.1.1.1.2 Multicast Configuration

The Multicast Configuration is shown in Figure 6.

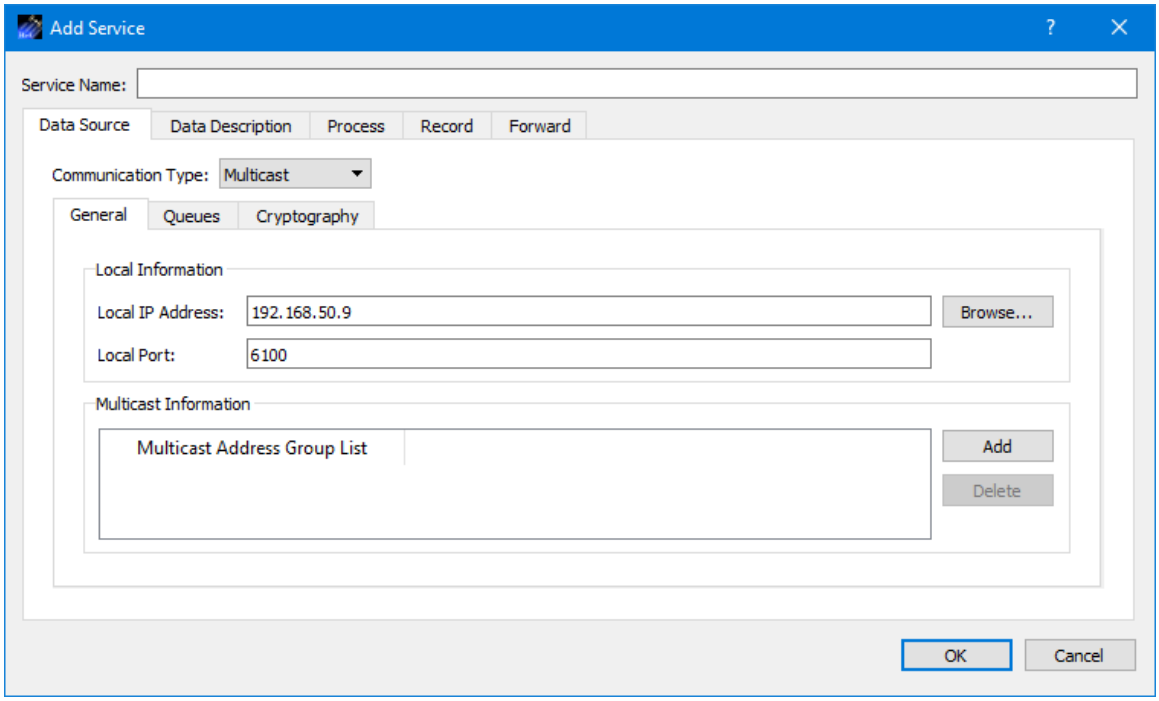


Figure 6 Service Dialog (Multicast Configuration)

Each field is described below.

Local IP Address
This is the local IP address used for the UDP socket used for the multicast communication.

Local Port
This is the local port used for the UDP socket used for the multicast communication.

Multicast Information
Use the + and – buttons to add and delete multicast address groups to the Multicast Address Group List.

6.1.1.1.3 TCP Client Configuration

The TCP Client Configuration is shown in Figure 7.

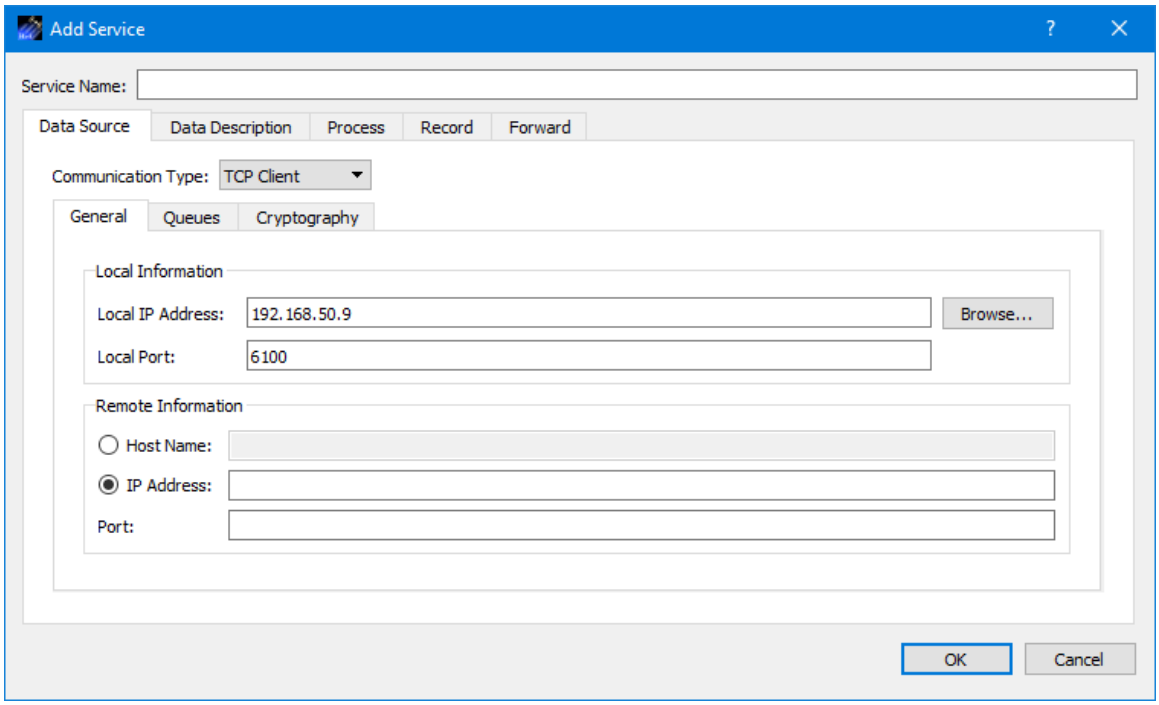


Figure 7 Service Dialog (TCP Client Configuration)

Each field is described below.

Local IP Address
This is the local IP address used for the TCP Client socket.

Local Port
This is the local port used for the TCP Client socket.

Host Name
This is the host name of the remote computer.

IP Address
This is the IP address of the remote computer.

Port
This is the port of the remote computer.

6.1.1.1.4 TCP Listener Configuration

The TCP Listener Configuration is shown in Figure 8.

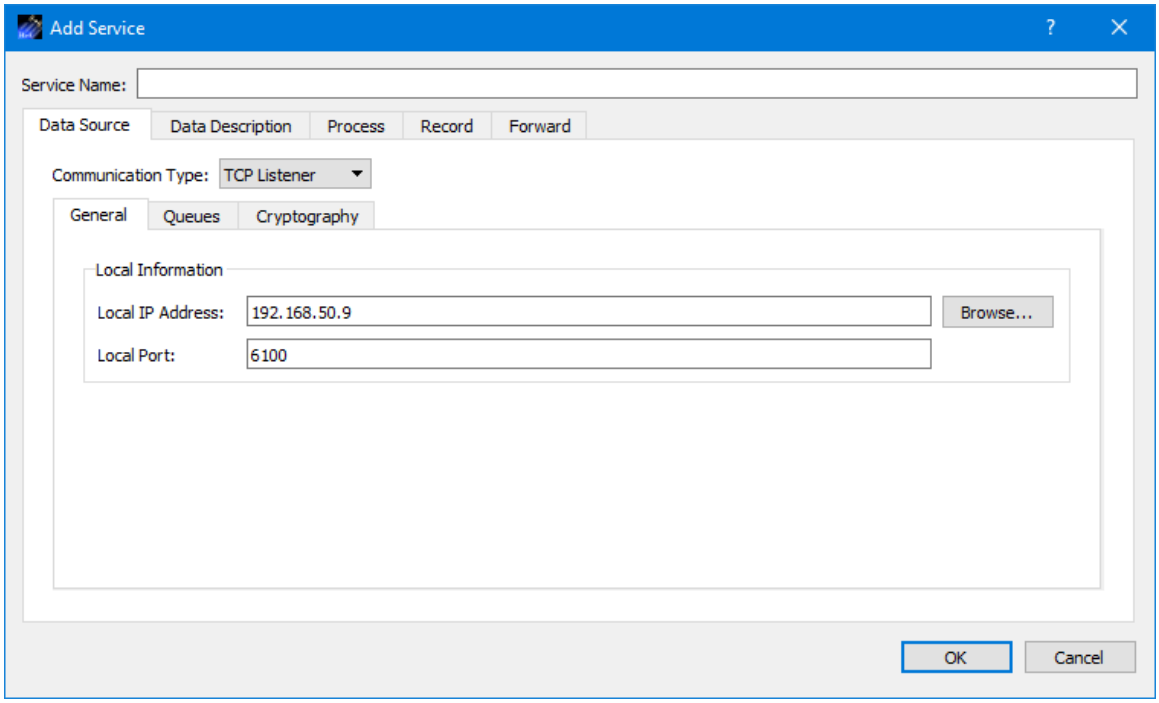


Figure 8 Service Dialog (TCP Listener Configuration)

Each field is described below.

Local IP Address
This is the local IP address used for the TCP Listener socket.

Local Port
This is the local port used for the TCP Listener socket.

6.1.1.1.5 UDP Configuration

The UDP Configuration is shown in Figure 9.

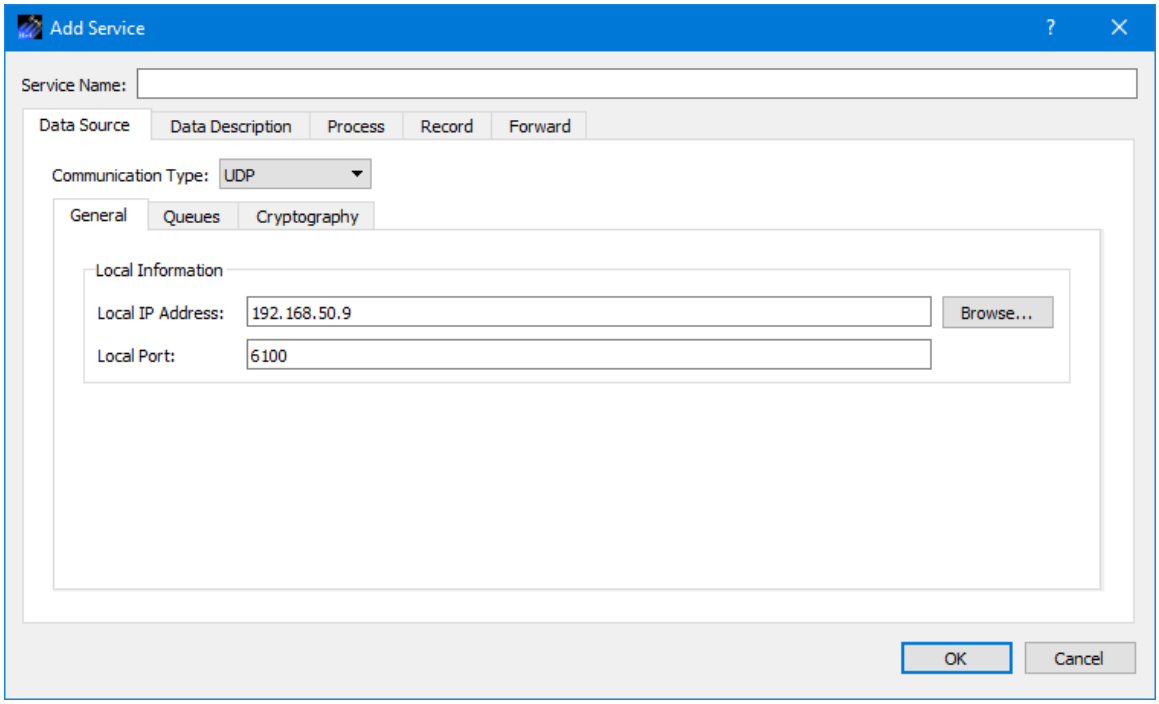


Figure 9 Service Dialog (UDP Configuration)

Each field is described below.

<u>Local IP Address</u>
This is the local IP address used for the UDP socket.

<u>Local Port</u>
This is the local port used for the UDP socket.

6.1.1.1.6 Unix Domain Socket Configuration

The UNIX Domain Socket Configuration is shown in Figure 10.

Figure 10 Service Dialog (UNIX Domain Socket Configuration)

Each field is described below.

<u>UNIX Domain Socket Name</u>
This is the name to use when creating the UNIX Domain socket. The name will be NUL (\0) prefixed when the socket is created to use an abstract namespace.

6.1.1.2 Data Source Queues Tab

Each configuration includes the capability to configure properties associated with the memory queue used to hold incoming data. The Queues Tab is shown in Figure 11. Settings on the Queues tab are available for each communication type and provide the capability to size the queue and the buffer size of the queue. A queue size of zero implies no buffer for incoming data.

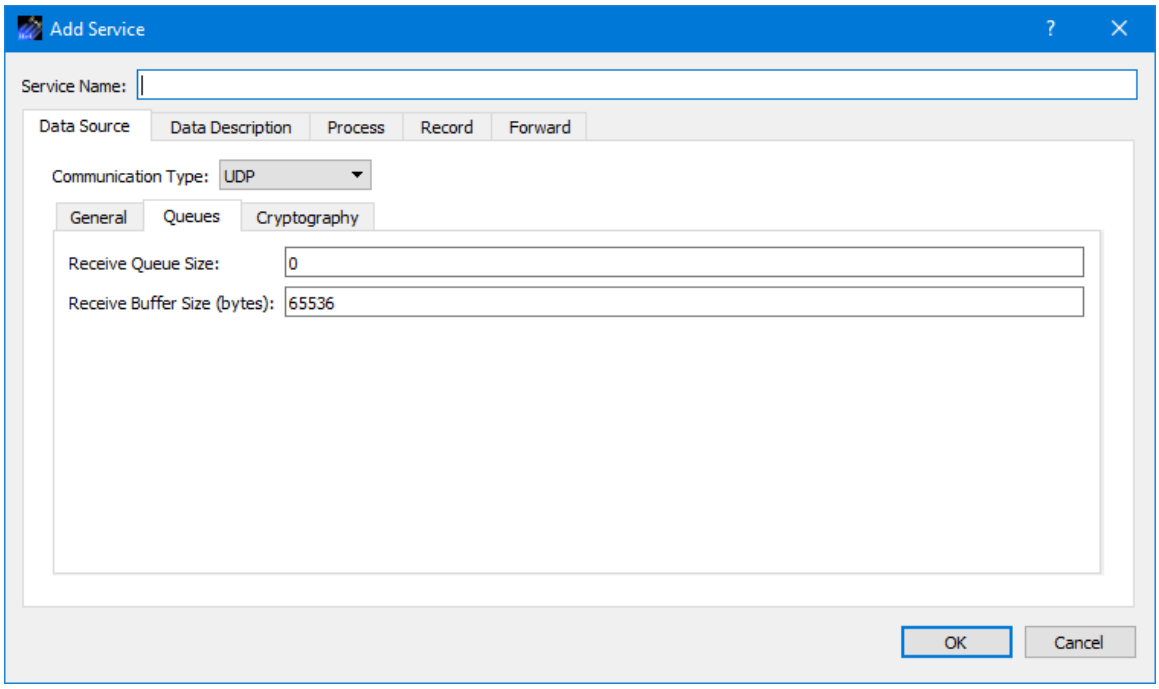


Figure 11 Service Dialog (Data Source Queues Tab)

6.1.1.3 Data Source Cryptography Tab

The Cryptography Tab is shown in Figure 12. If the incoming data is encrypted, information provided on the Cryptography tab can be used to decrypt the data. To decrypt incoming data, the TReK software needs the Peer Public Key for the encrypted data. If all incoming encrypted data being received by the decryption service was encrypted using the same source Public and Private key pair, set the Sender IP Address or Sender Node Number to N/A (the default setting) and identify the absolute path to the one and only Peer Public Key (i.e., the Public key that was used to encrypt all the data). If the incoming encrypted data is being sent from sources with different IP addresses or

node numbers, and the encryption sources are using different Public and Private key pairs, the decryption service may decrypt the various encrypted data streams by associating the correct Peer Public Key with the IP address or node number of the source that is sending the encrypted data. To decrypt incoming data, the Decrypt Incoming Data checkbox should be checked and the Peer Public Key Pathname Information should be populated. The Add button is used to add an entry. The Delete button is used to Delete an entry. The Peer Public Key button is used to browse the local disk for a peer public key file. One or more rows must be selected to use the Delete and Set Peer Public Key buttons.

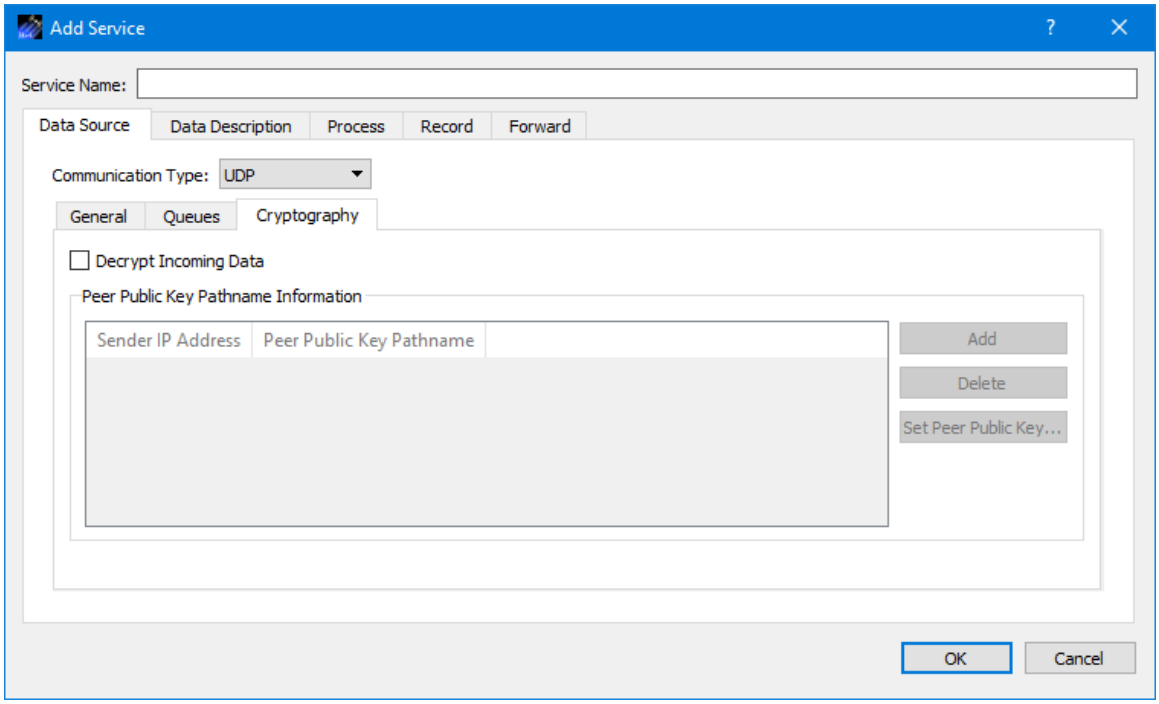


Figure 12 Service Dialog (Data Source Cryptography Tab)

6.1.2 Service Dialog (Data Description Tab)

The Data Description tab is shown in Figure 13. The Data Description tab provides a way to filter incoming data that will be processed, recorded, or forwarded.

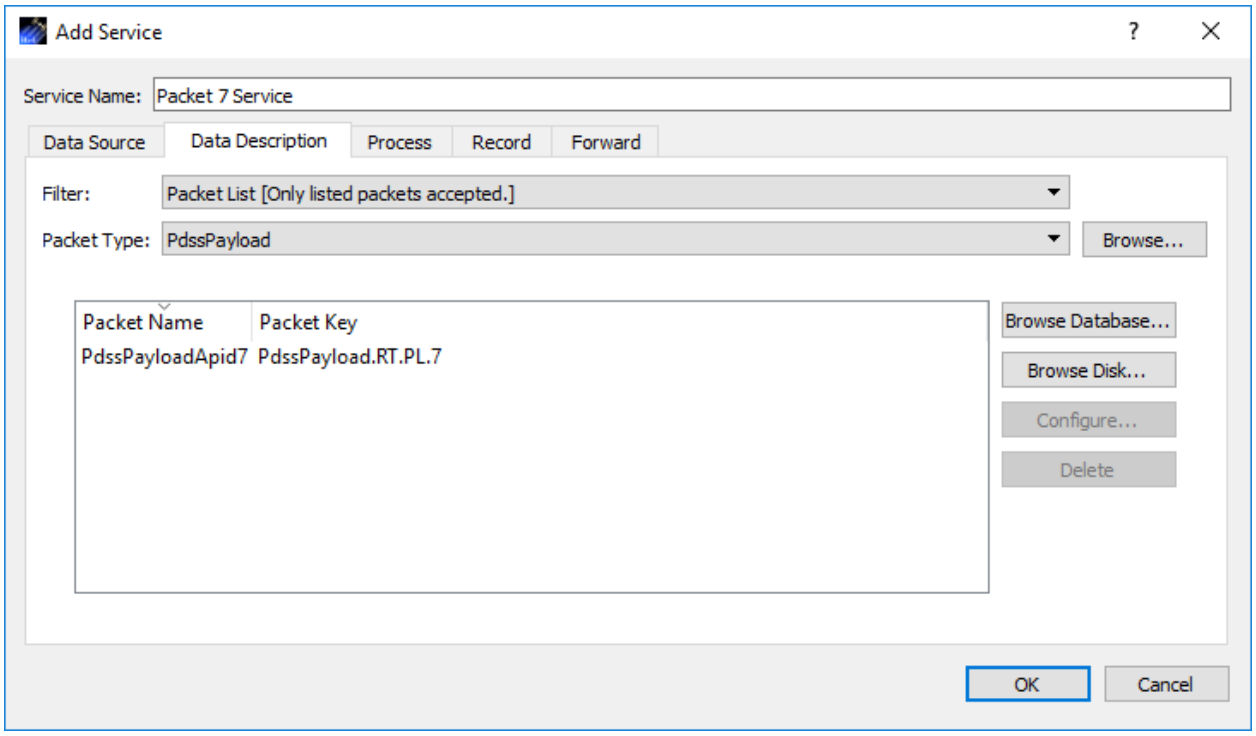


Figure 13 Service Dialog (Data Description Tab)

Filter

The Filter menu contains three choices. Each is described below.

Packet List [Only listed packets accepted]

Packet List provides a way to identify specific packets that should be accepted. Packet information is added to the list by browsing the database or by selecting a metadata definition file stored on the local file system disk. When a packet is added to the list the Packet Name and Packet Key are displayed. The Packet Key contains the values for each unique identifier defined by the packet type. Some packet types contain packet identifiers that are user selectable. When adding a packet to the list you will be prompted to select a value for any user selectable identifiers if a default value is not provided in the packet definition. The Configure button can be used to change the value of a user selectable identifier after a packet has been added to the list. The Delete button can be used to delete a packet from the list. The 'Packet List' option is required if processing is turned on.

Pattern Match Using Packet Type [Only packets that match pattern accepted. Processing Not Available.]

Pattern Match Using Packet Type provides a way to filter incoming packets using the identification fields unique to the packet type. Figure 14 shows the identifiers that can be used to filter incoming PDSS Payload packets. The Data Mode (EHSP=DataMode) value has been set to '*' (wildcard) to indicate that any data mode value should be accepted (Real-Time, Dump1, Dump2, etc.). The EHS Secondary Protocol Header Type

(EHSP=SecHdrType) is a fixed identifier so the value cannot be changed. The APID (CP=APID) is set to '7' to indicate that the APID value must be 7 or the packet should be filtered out. Therefore any PDSS Payload packets with APID 7 will be accepted using this Filter.

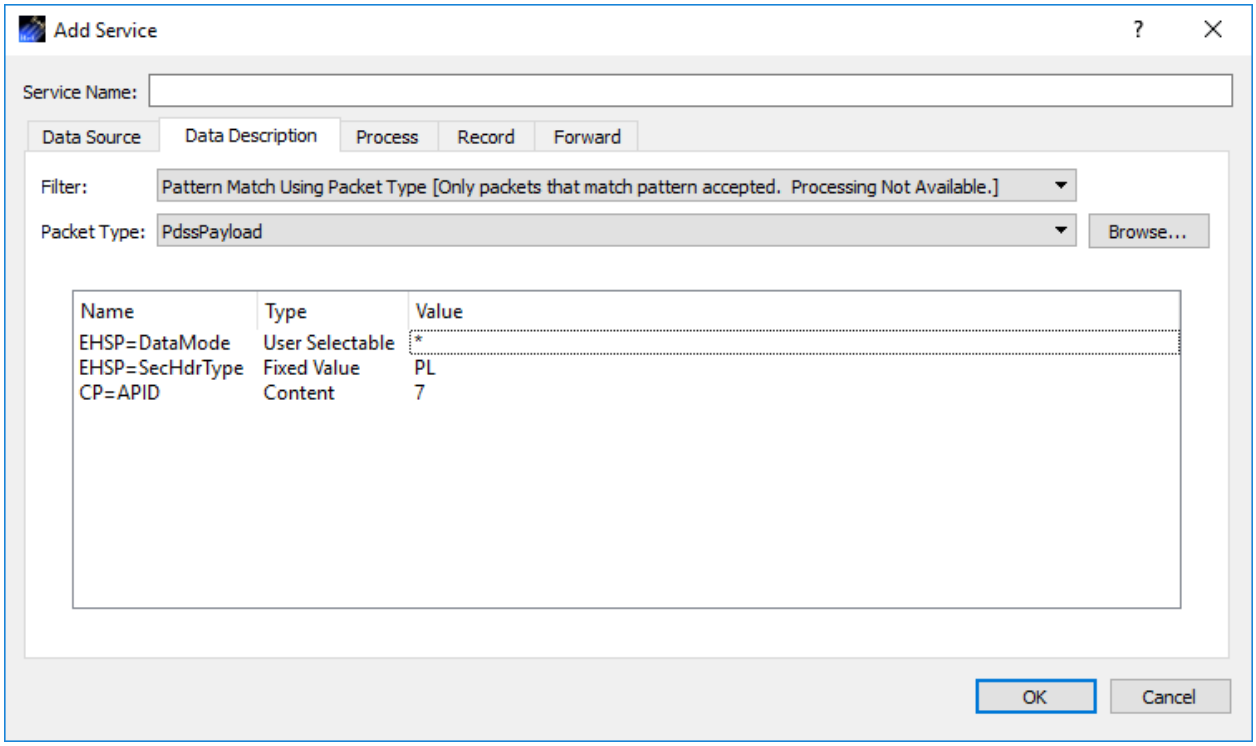


Figure 14 Pattern Match Using Packet Type

None [All arriving data accepted. Processing Not Available]
None indicates no filtering should be used. If the Filter is set to 'None' all data received will be accepted. When 'None' is selected, processing is not available.

Packet Type
The Packet Type menu is used to provide information about the incoming data. Some services like processing require a Packet Type. Other services like recording and forwarding do not require a Packet Type. However, you may decide to select a Packet Type since it can be used to filter incoming data. For example, suppose you had two streams of data arriving on the same network socket. One data stream of packets all had CCSDS headers. The other data stream of packets had no header. Suppose you only wanted to record the packets that had a CCSDS header. In this case you could set the Packet Type to CCSDS and the Data application would assume the incoming packets are CCSDS packets and would only record the packets if the bits corresponding to APID were a match. [Note: If a non-CCSDS packet arrives the Data application will assume it is a CCSDS packet and attempt to handle it as such.] For more information about Packet Types, please reference the TReK Concepts document.

Encrypted Data

When the Filter Type is set to None, the Packet Type options are None and Encrypted. If you will be receiving encrypted data, and you do not want to decrypt the data, set the Filter Type to None and the Packet Type to Encrypted. The incoming encrypted data can be recorded or forwarded. If you will be receiving encrypted data and choose to decrypt the data, select the type of Filtering you would like to apply and the packet type that describes the decrypted data. The Packet Type should not be set to Encrypted since the data will be decrypted.

6.1.3 Service Dialog (Process Tab)

The Service Dialog Process tab is shown in Figure 15. The Process tab is used to configure the service to process incoming data and identify the packets that should be processed.

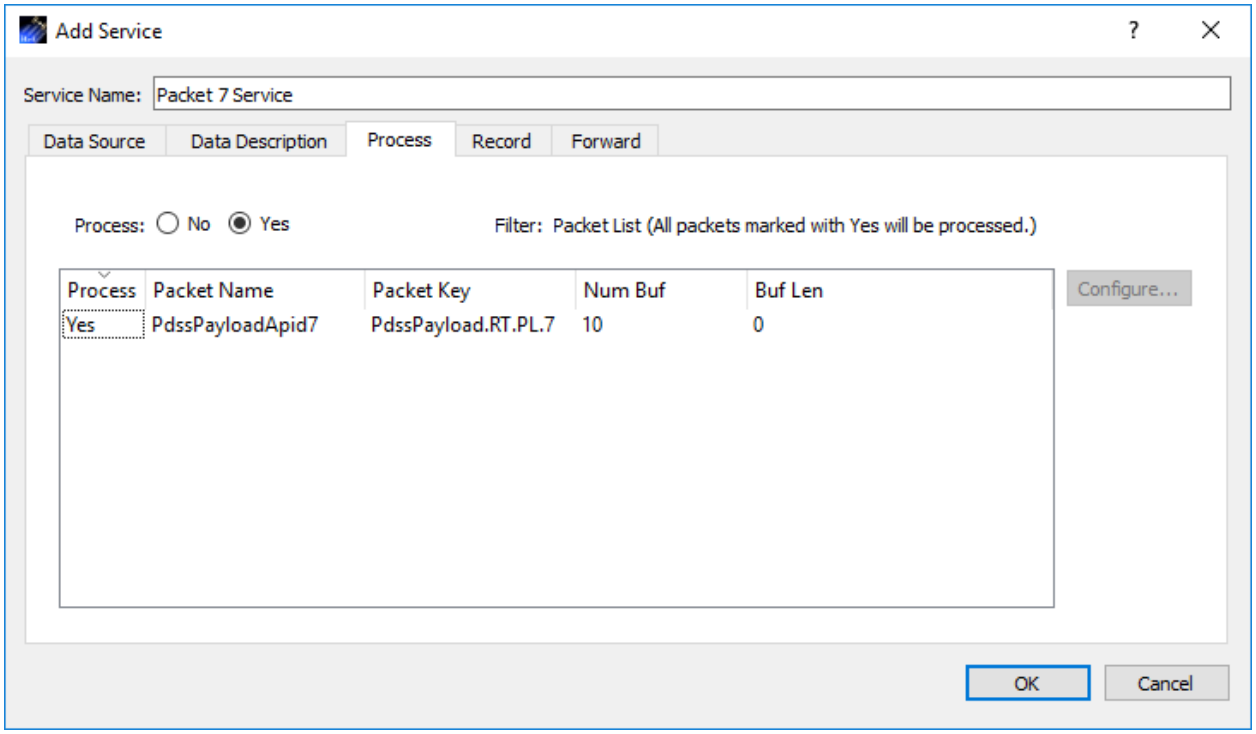


Figure 15 Service Dialog (Processing Tab)

Each field is described below.

<u>Process Radio Buttons</u>
The No and Yes radio buttons disable or enable Processing.

<u>Packet List</u>
If processing is turned on, the packet list is used to identify the list of incoming packets that should be processed. The packets displayed in the Packet List are the ones that were entered on the Data Description tab. You may configure the service to receive multiple

packets and use this list to limit the packets that are processed. The Process column Yes or No value indicates whether the packet should be processed. The Configure button is used to configure one or more properties associated with processing the packet. Multiple packets can be selected and modified at the same time. The 'Num Buf' column identifies the number of buffers to use for arriving packets and the 'Buf Len' column identifies the length of the buffers. These properties can be configured using the Configure dialog accessed by the Configure button.

Configure

The Configure button is used to modify processing properties associated with the packets selected. This includes whether the packet should be processed, the Number of Buffers, and the Buffer Length. A value of 0 for the Buffer Length indicates the length should be calculated using information in the packet definition.

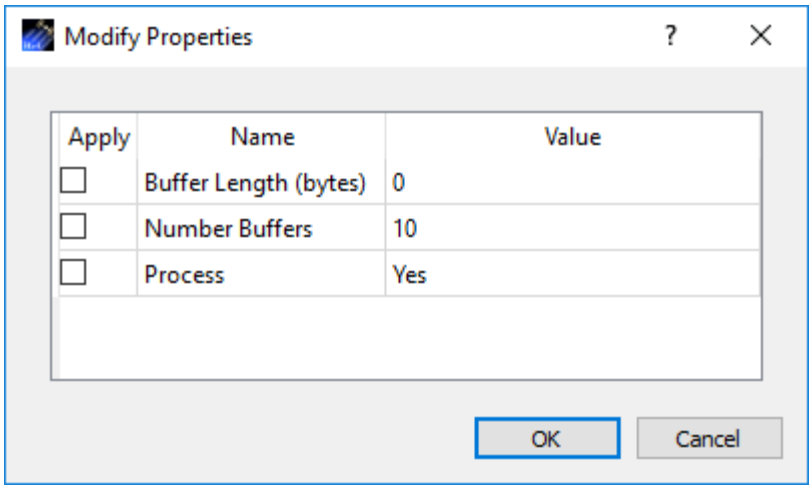


Figure 16 Service Dialog Processing Tab Modify Properties Dialog

6.1.4 Service Dialog (Record Tab)

The Service Dialog Record tab is shown in Figure 17. The Record tab is used to configure the service to record incoming data and other properties associated with recording.

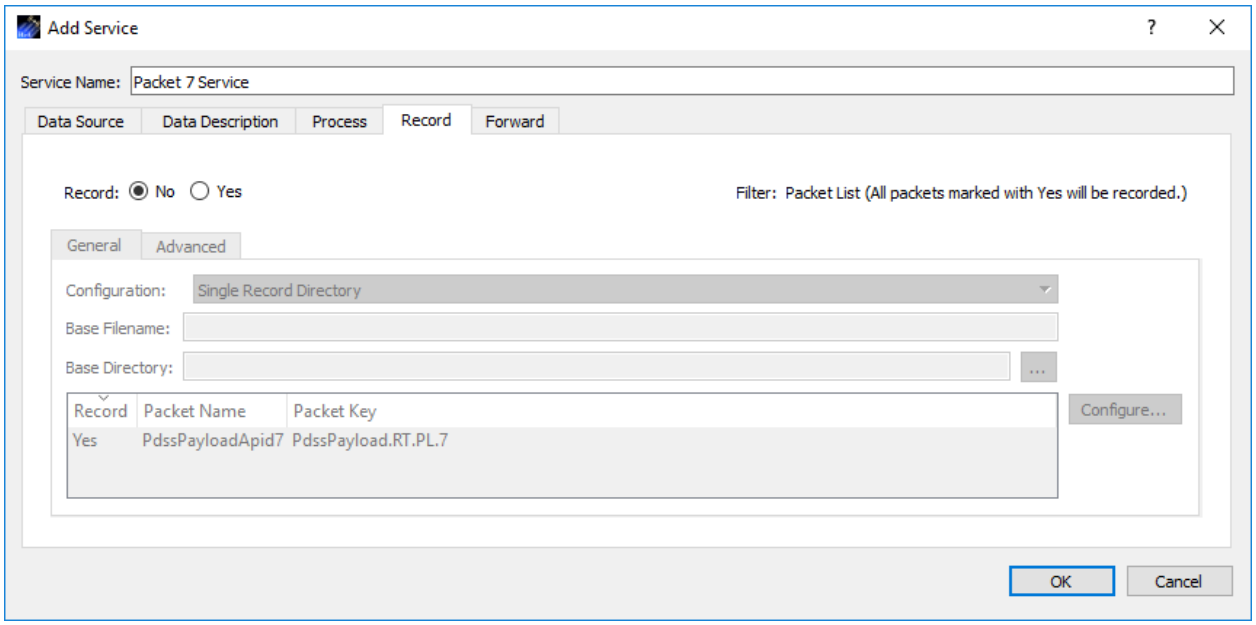


Figure 17 Service Dialog (Record Tab)

6.1.4.1 Record Tab (General Tab)

The Record Tab General Tab is shown in Figure 18. It is used to enter general recording information. The Filter selection will determine which packets are recorded. The packets displayed in the Packet List are the ones that were entered on the Data Description tab. You may configure the service to receive multiple packets and use this list to limit the packets that are recorded. The Record column Yes or No value indicates whether the packet should be recorded. The Configure button is used to configure the Yes or No property. Multiple packets can be selected and modified at the same time.

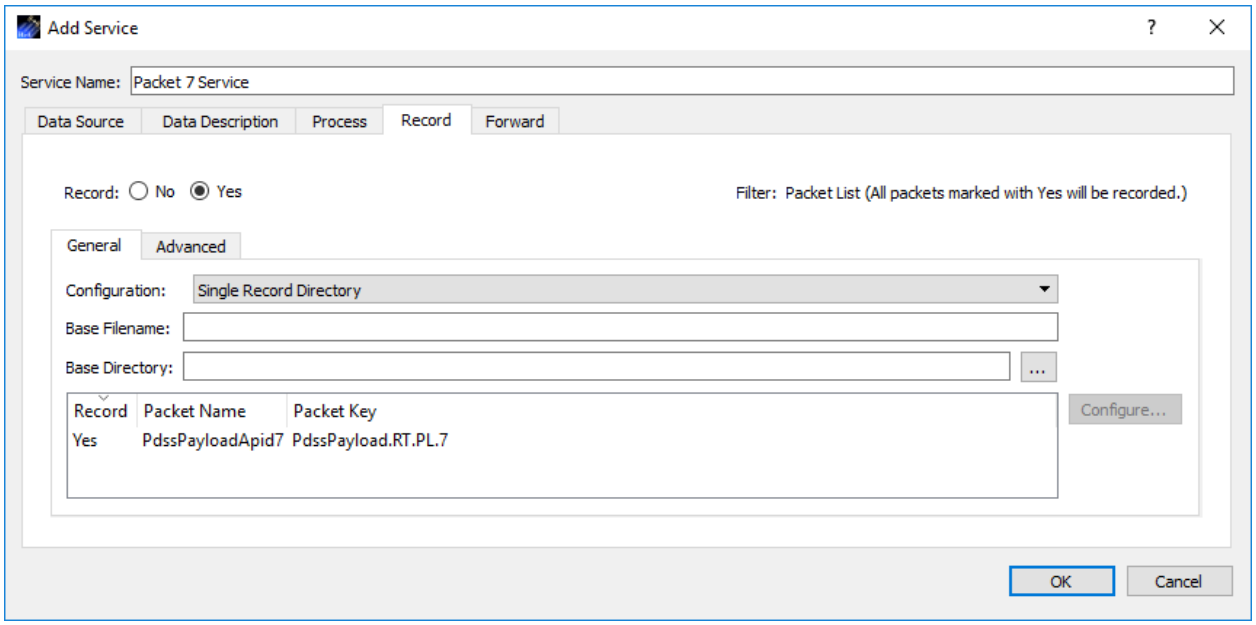


Figure 18 Service Dialog Record Tab (General Tab)

Each field is described below.

Record

The No and Yes radio buttons disable or enable data recording. The Filter setting determines which packets are recorded. If the Filter is set to Packet List, the Record column determines which packets will be recorded.

Configuration

The recording configuration identifies the configuration to use when recording the incoming data. The Configuration option menu contains three choices. Each is described below.

Single Record Directory

The Single Record Directory option will record all the data into a single directory. The configuration for this option is shown in Figure 18. This configuration requires an entry for Base Filename and Base Directory.

Base Filename

Single Record Directory requires a Base Filename. When a packet is recorded, the raw packet data is stored in one or more files in a local directory. A base filename (provided by you) is used for part of the filename and the rest of the filename is generated by the TReK software. The complete filename indicates the time the file was created or the embedded time of the first packet in the file if an embedded time field was identified in the packet definition. You may also choose to create a complete filename the includes both the open and close time of the file or the embedded time of the first and last packet in the file if an embedded time field was identified in the packet definition. When you want to play the data back, you will be asked to provide this Base Filename.

Base Directory

Single Record Directory requires a Base Directory. The Directory information is used to identify which directory should be used for the recorded data files. When you want to play the data back, you will be asked to provide this Directory information so the TReK Playback application can find the files. This field requires a complete directory path. An example of this is C:\Users\<username>\trek_workspace\recorded_data\. If you don't like to type or you need help defining the complete path, you can push the … (dot dot dot) button located to the right of the Directory field. This will bring up a Browse dialog you can use to select the local directory where you want to store the recorded data files.

Multiple Record Directories Auto-Generated Based on Incoming Data

The Multiple Record Directories Auto-Generated Based on Incoming Data option will record data into multiple sub-directories based on the packet key. Figure 19 shows the configuration of this option. A Base Directory is required.

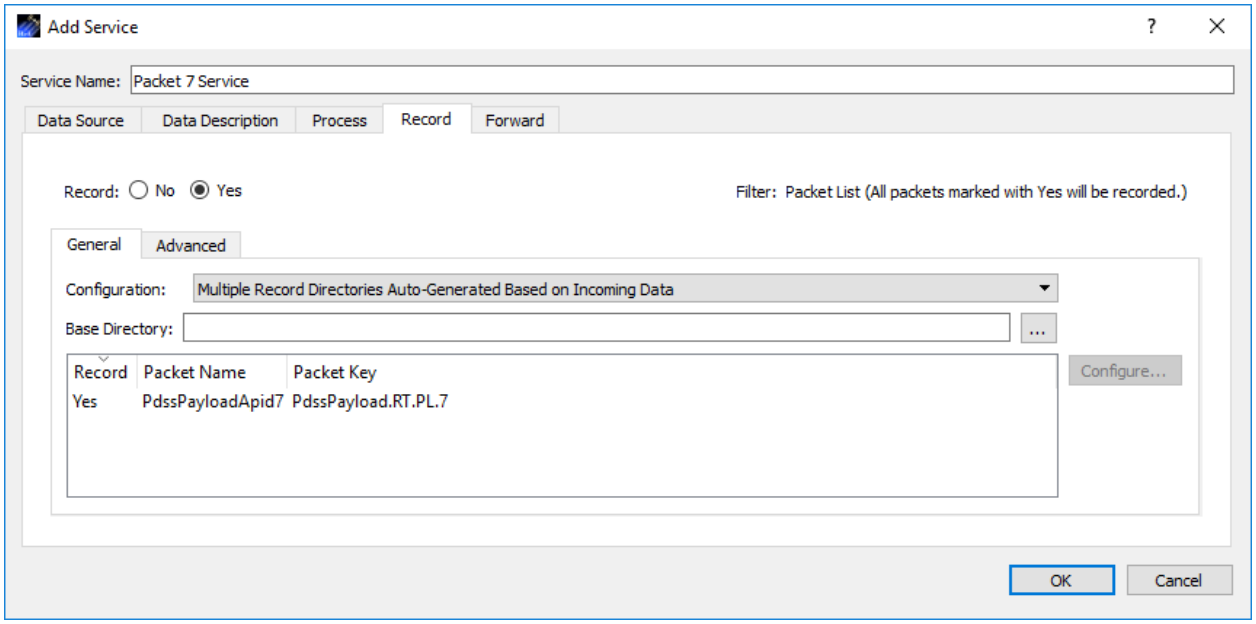


Figure 19 Multiple Record Directories Auto-Generated on Incoming Data

Base Directory

The Base Directory is used to identify the top level directory for the recorded data files that will be stored in subdirectories according to packet type. Figure 20 shows an example of Auto-Generated subfolders.

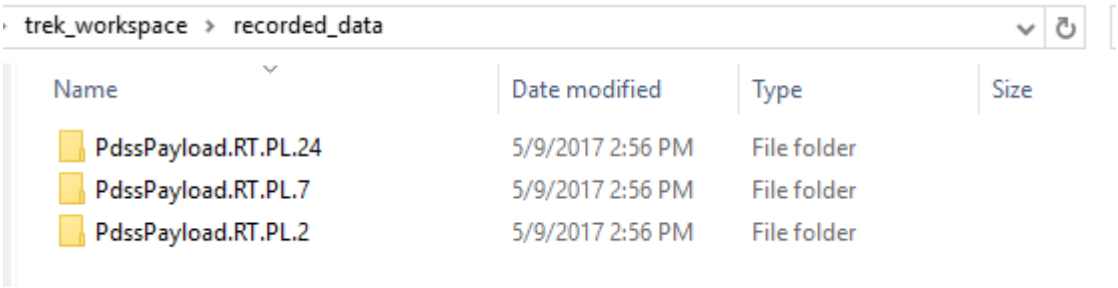


Figure 20 Auto-Generated Folders for Recorded Data Files

User Specified Record Directories and Base Filenames

The User Specified Record Directories and Base Filenames option provide a way to enter a user specified directory and base filename for each individual packet in the list. The Filter option must be set to 'Packet List' to use this option. Figure 21 shows the configuration for this option. The Configure dialog is used to enter a Base Filename and Base Directory for each packet in the list.

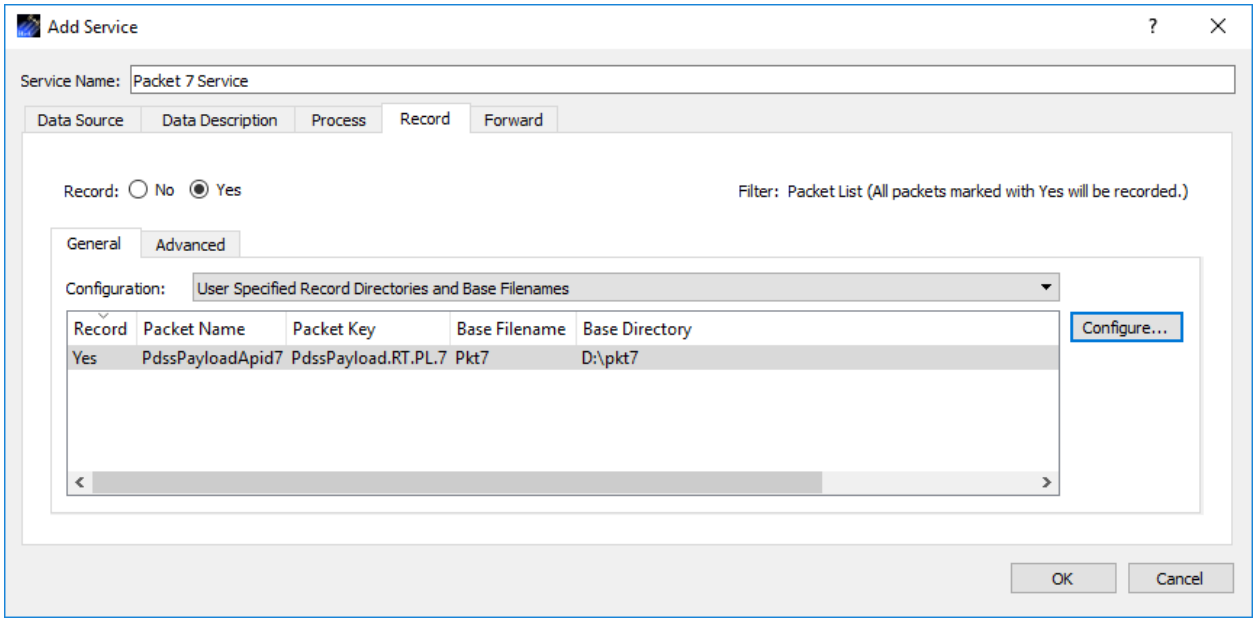


Figure 21 User Specified Record Directories and Base Filenames

6.1.4.2 Record Tab (Advanced Tab)

The Record Tab Advanced Tab is shown in Figure 22. It is used to enter advanced recording information.

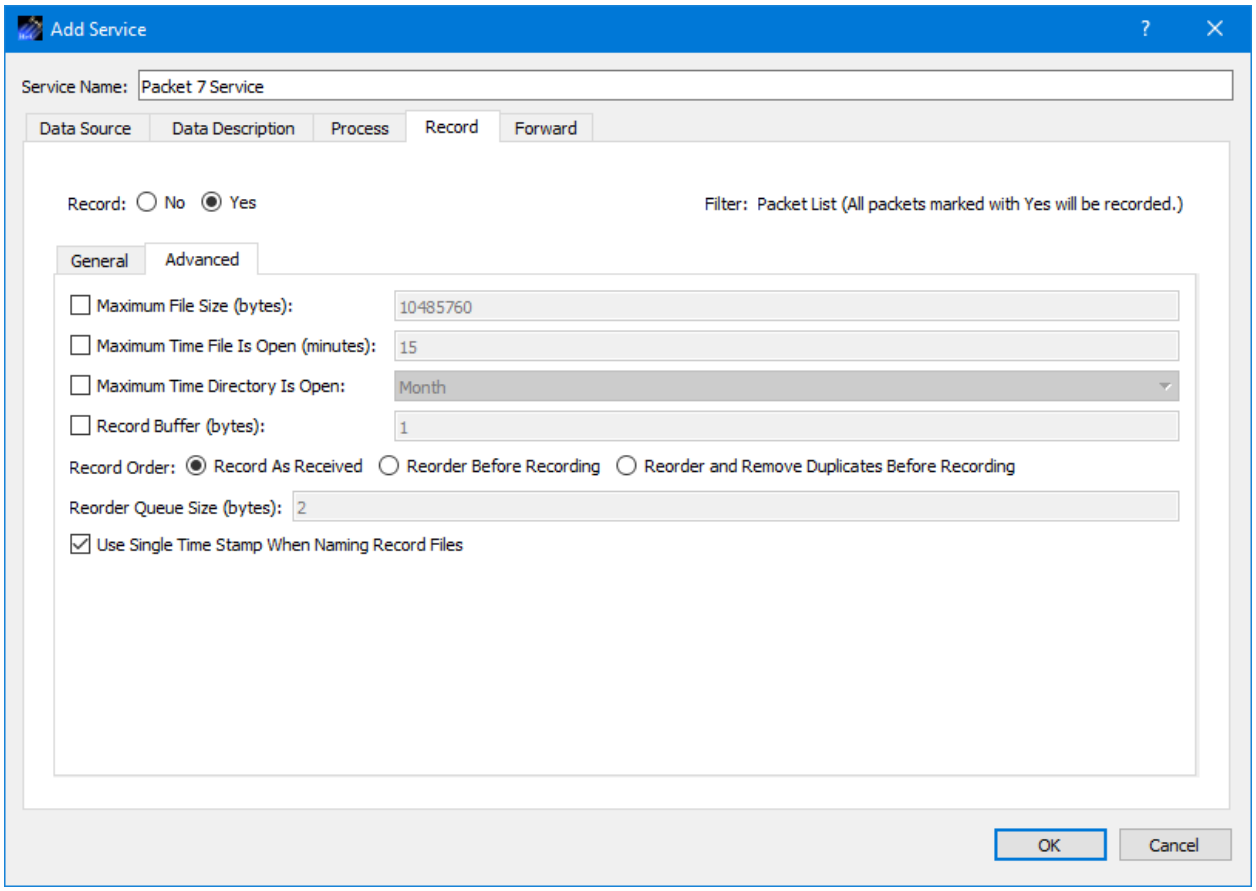


Figure 22 Service Dialog Record Tab (Advanced Tab)

Each field is described below.

<u>Maximum File Size</u>
The Maximum File Size information is used to determine when to close a recorded data file. A new record file is opened immediately after the current record file is closed.

<u>Maximum Time File Is Open</u>
The Maximum Time File Is Open Checkbox is used to indicate whether the file should be closed based on a maximum time. The Maximum Time File Is Open property is used in addition to the Maximum File Size property. If the maximum file size is reached before the maximum time, the file will be closed based on maximum file size. However, if the maximum time is reached before the maximum size is reached, the file will be closed based on the maximum time. The file open timer starts when the record file is created. A new record file is opened immediately after the current record file is closed. A record file will not be closed based on maximum time if no packets have been recorded in the file.

<u>Maximum Time Directory Is Open</u>
The Maximum Time Directory Is Open Checkbox is used to indicate whether recording files should be placed in sub-directories within the parent base directory. The directories

will be open/closed based on Day, Calendar Week, Calendar Month, or Year. A new record file is opened immediately after the current record file is closed.

Record Buffer

A Record Buffer may be used to buffer multiple packets up to the record buffer size in bytes prior to making a write call to the record file. Zero implies every packet has an associated write call to the record file. A record buffer may be used to improve the performance of the record library.

Record Order

There are three options for Record Order. Each is described below:

*Record as Receive*d

Record as Received will record packets in the order they are received.

Reorder Before Recording

Reorder Before Recording will reorder packets in time order using the embedded time stamp in the individual packets. The reorder queue must be sized to hold the maximum sequence of out of order packets or the packets will not be recorded correctly. For example, packets arriving in the order A,B,C,D,M,N,O,E,F,G,H,I,J,K,L,P,Q,R would require a reorder queue size of four to record the proper packet sequence of A,B,C,D,E,F,G,H,I,J,L,K,M,N,O,P,Q,R.

Reorder and Remove Duplicates Before Recording

Reorder and Remove Duplicates Before Recording will reorder packets in time order using the embedded time stamp in the individual packets. Duplicate packets will not be recorded. Duplicate packets are identified using the packet's embedded time and sequence count. The reorder queue must be sized to hold the maximum sequence of out of order packets or duplicate packets or the packets will not be recorded correctly. For example, packets arriving in the order A,B,C,D,M,E,F,G,H,I,J,K,L,M,N,O,P,Q,R would require a reorder queue size of two to record the proper packet sequence of A,B,C,D,E,F,G,H,I,J,L,K,M,N,O,P,Q,R.

Reorder Queue Size

The Reorder Queue Size is the queue size used to reorder the packets. It should be set to a value greater than or equal to the expected maximum sequence error of the received packets. If the queue size is smaller than the maximum sequence error, packets may not be reordered in the proper sequence. If the reorder queue size is set to zero, the record library will set the reorder queue size to twice or double the recorded packet's maximum sequence error assuming a sequence count field is defined in the packet's header.

Use Single Time Stamp When Naming Record Files

If this is checked, the recorded data files will use a single time stamp when adding timestamp information to the filename. If this is not checked, the recorded data files will contain start time and a stop time when timestamp information is added to the filename.

6.1.5 Service Dialog (Forward Tab)

The Service Dialog Forward tab is shown in Figure 23. The Forward tab is used to configure the service to forward incoming data. The Filter Type will determine which packets will be forwarded. If the Filter is set to Packet List, the Packet List will further determine whether a packet is forwarded.

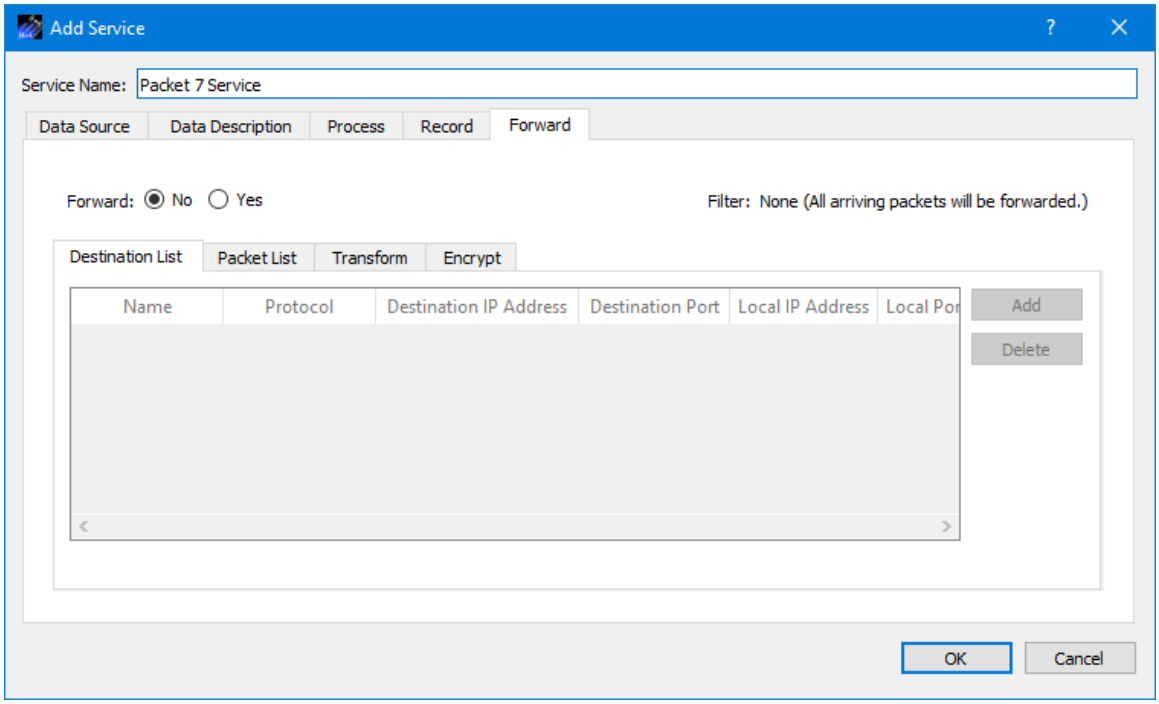


Figure 23 Service Dialog (Forward Tab)

Each field is described below.

<u>Forward</u>

The No and Yes radio buttons disable or enable data forwarding of incoming packets described in the service. The Filter Type setting determines which packets are forwarded.

<u>Destination List</u>

The destination list is used to identify the list of destinations to which the data should be forwarded. Each destination must include a user defined name that is unique in this destination list, a Protocol, and the applicable settings required for the protocol selected. The Protocols supported are UDP and TCP. The Protocol menu provides the capability to select the type of socket to use when forwarding the data: UDP, TCP Client, or TCP Listener socket. Figure 24 shows three different destinations in the Destination List. When using a TCP Listener socket it is not necessary to define a Destination IP Address or a Destination Port. When the Local Port is set to 0, the operating system will

automatically select a port to use for the socket that is created to send data to the destination. This is the default as it saves you the trouble of keeping up with ports. However, you can enter a specific port if you would like. This is advisable if you are using a TCP Listener socket since another party will be connecting to the socket. The + and - buttons are used to add a row to the list and delete a row from the list respectively.

Note: Regardless of whether the Forward selection is set to Yes or No, only valid destination information will be saved in the service. If Forward is set to No, any invalid destination information will be removed when you click OK.

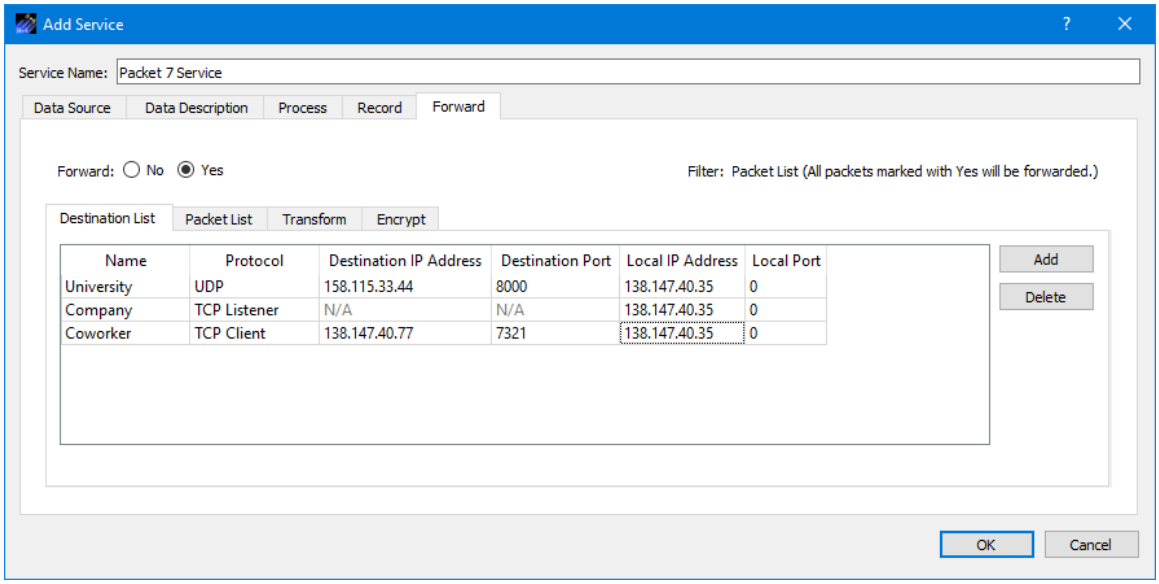


Figure 24 Forward Destinations

The Packet List tab is shown in Figure 25.

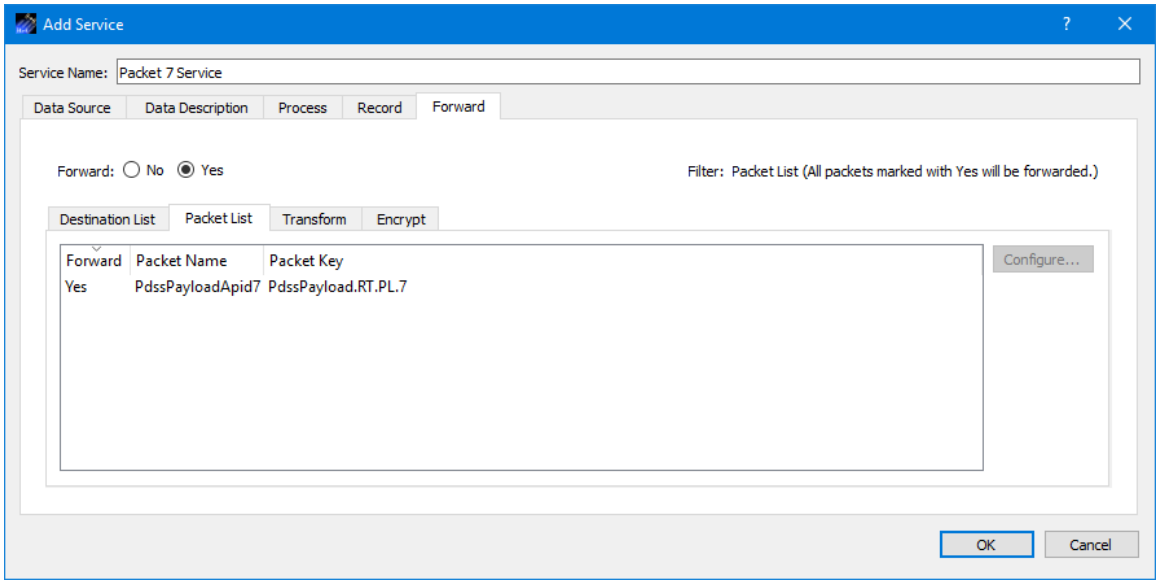


Figure 25 Service Dialog Forward Tab Packet List

The packets displayed in the Packet List are the ones that were entered on the Data Description tab. You may configure the service to receive multiple packets and use this list to limit the packets that are forwarded. The Forward column Yes or No value indicates whether the packet should be forwarded. The Configure button is used to configure the Yes or No property. Multiple packets can be selected and modified at the same time.

The Transform tab is shown in Figure 26. The Transform tab provides the capability to enable the transform feature which can be used to remove a specific number of bytes from the beginning of each packet before the packet is forwarded.

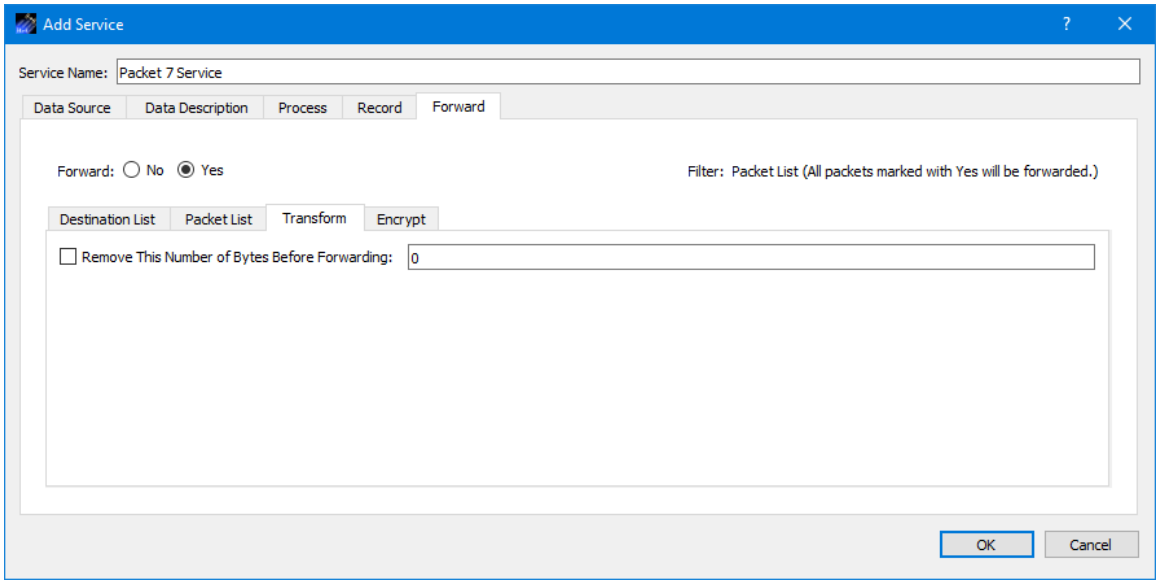


Figure 26 Service Dialog Forward Tab Transform

The Encrypt tab is shown in Figure 27. The Encrypt tab provides the capability to encrypt data sent to a destination. Encryption is controlled per destination.

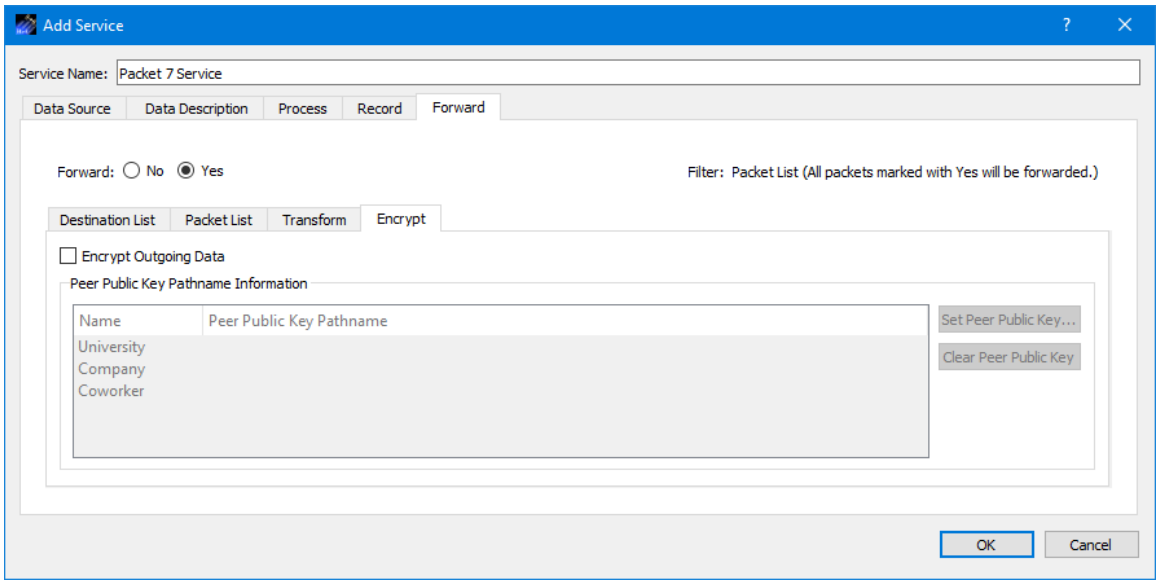


Figure 27 Service Dialog Forward Tab Encrypt

The Peer Public Key Information is populated using the Destination List. To encrypt data going to a specific destination, check the Encrypt Outgoing Data checkbox, and identify the absolute path to the Peer Public Key associated with that destination. If no Peer Public Key Pathname is identified, the data forwarded to that destination will not be encrypted (even if the Encrypt Outgoing Data checkbox is checked). The Set Peer Public Key button is used to browse the local disk for a peer public key file. The Clear Peer

Public Key button is used to clear a peer public key pathname. One or more rows must be selected to use the Set Peer Public Key and Clear Peer Public Key buttons.

6.2 Parameters

When one or more services are configured with processing turned on, the Parameters dialog will list all the parameters from all the packets that are configured to be processed. The Parameters dialog is shown in Figure 28. If a parameter is selected, the Details button can be used to access detailed information about the parameter as shown in Figure 29.

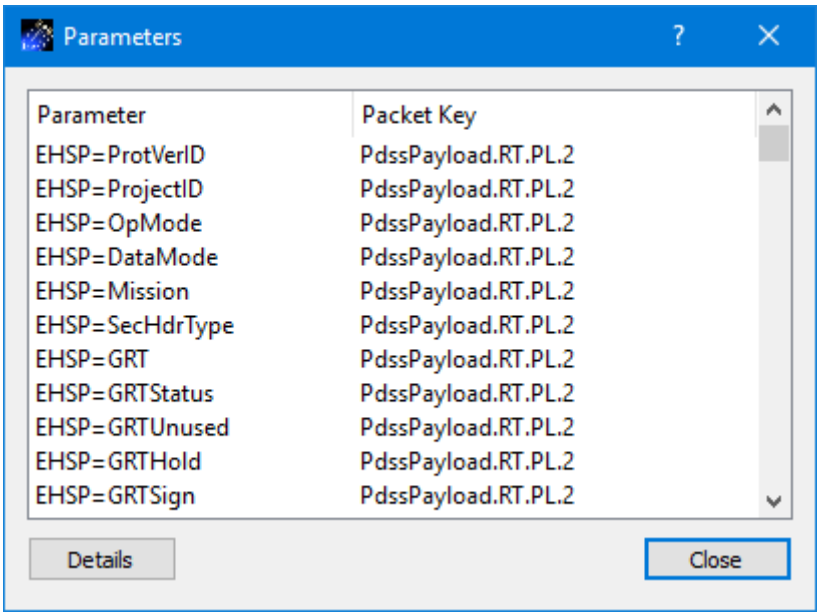


Figure 28 Parameters Dialog

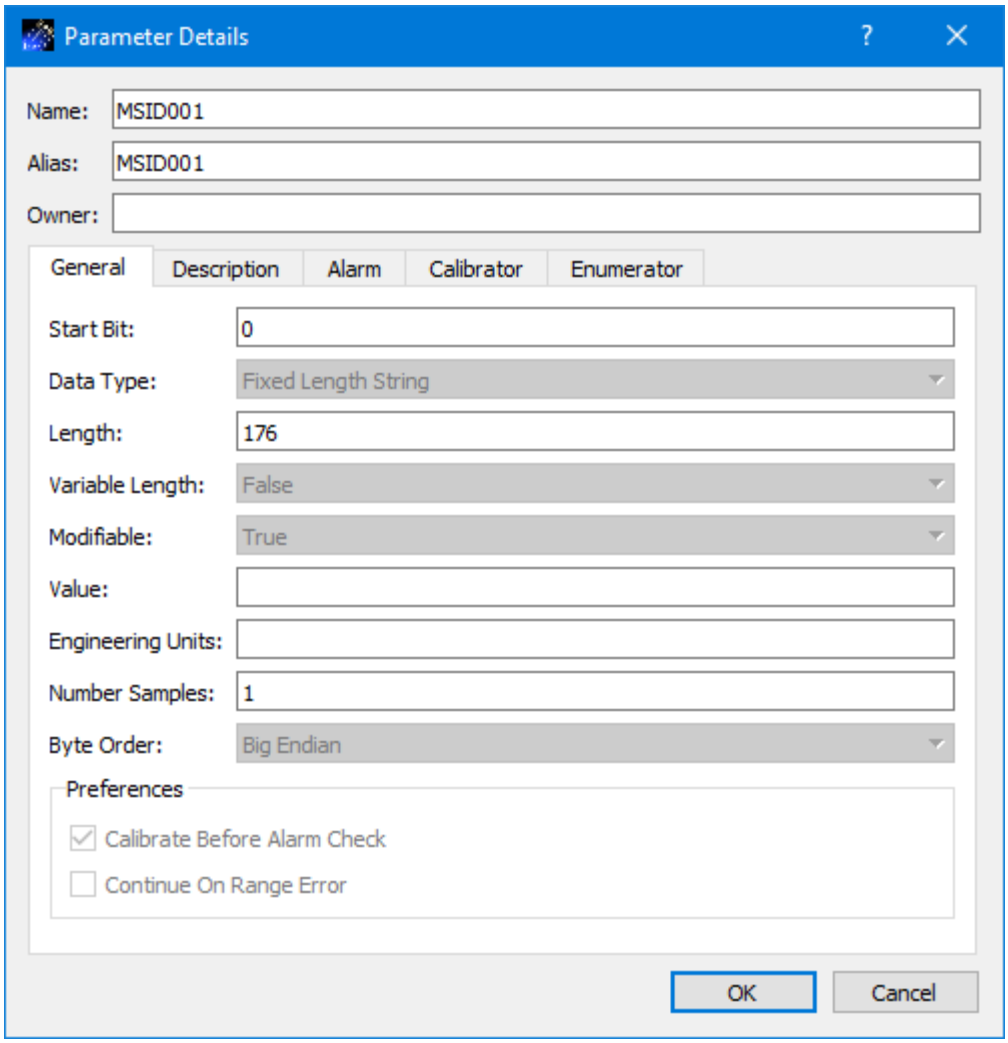


Figure 29 Parameter Details Dialog

6.3 Displays

When a service is configured with processing turned on, the Data application will auto-generate pre-defined displays to view the processed data. A predefined display is configured to show all the parameters in a packet and there is one display per unique packet. The predefined displays can be accessed using the Show Displays menu item on the Parameter menu. The Displays dialog is shown in Figure 30. Predefined Displays are only available when a service is active and configured with processing on for one or more packets. To open and start a display, select the display in the list and push the Start button or double click on the display in the list. The Displays dialog can be closed after the display is started. Custom Displays can also be defined. If any custom displays exist they will be listed in the Displays dialog. Please reference section 6.4 for information about custom displays.

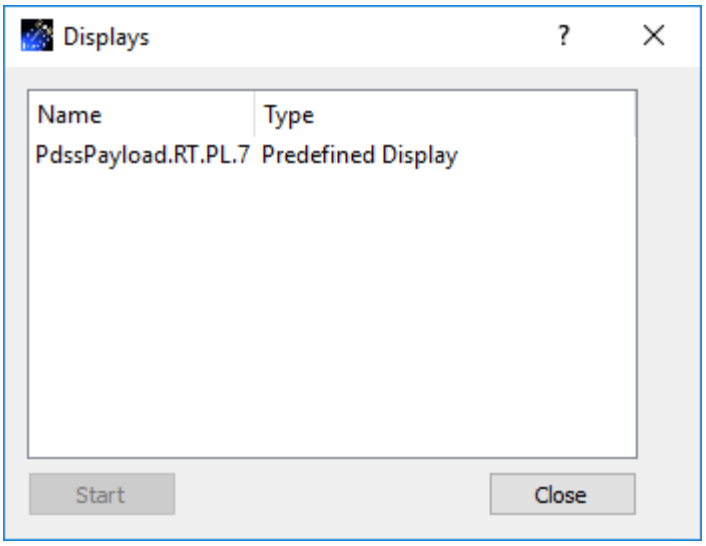
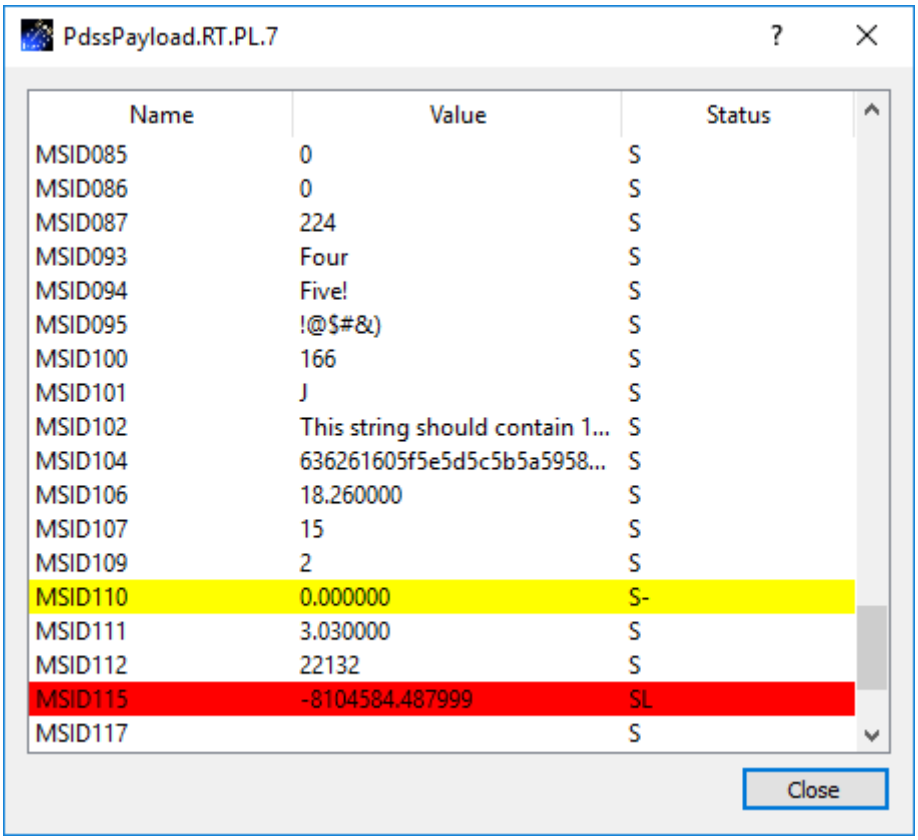


Figure 30 Displays Dialog

Figure 31 shows a predefined display running. The Name column displays the name of the parameter. The Value column displays the value of the parameter. The Status column displays a status character indicating the status of the parameter value. If you double click anywhere in the display the Status Characters Dialog shown in Figure 32 will be displayed. This dialog provides information about the status character shown in the Status column. The lines in the display with the yellow and red highlights indicate that limits associated with those parameters were exceeded.



Name	Value	Status
MSID085	0	S
MSID086	0	S
MSID087	224	S
MSID093	Four	S
MSID094	Five!	S
MSID095	!@$#&)	S
MSID100	166	S
MSID101	J	S
MSID102	This string should contain 1...	S
MSID104	636261605f5e5d5c5b5a5958...	S
MSID106	18.260000	S
MSID107	15	S
MSID109	2	S
MSID110	0.000000	S-
MSID111	3.030000	S
MSID112	22132	S
MSID115	-8104584.487999	SL
MSID117		S

Figure 31 Predefined Display

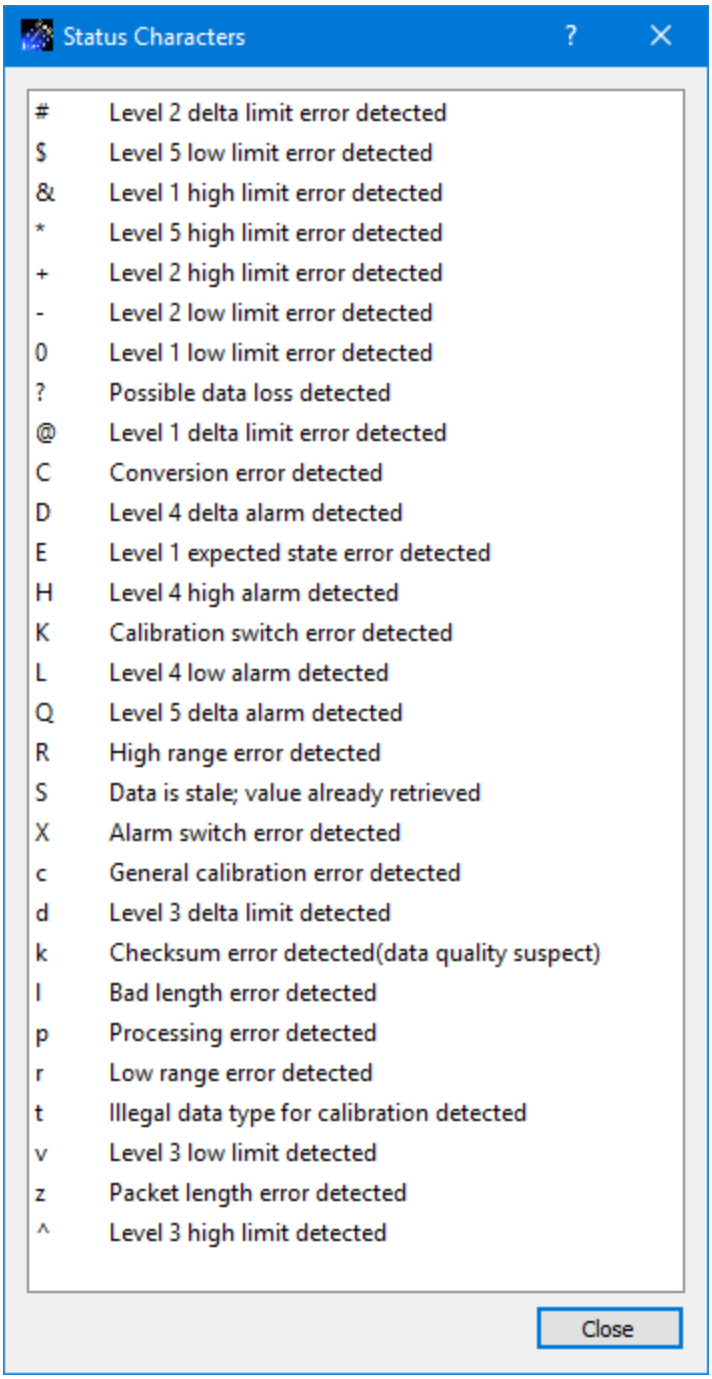


Figure 32 Status Characters Dialog

6.4 Manage Custom Displays

The Manage Custom Displays dialog provides the capability to create, modify, delete, export, and import custom displays. It is shown in Figure 33. Custom Displays only exist in the current application configuration. If you save the configuration, the displays

will be saved in the configuration file. If you would like to use a display in a different configuration, you can export it and then import it into the other configuration. The default location for custom displays is the trek_workspace/display directory. However, you can export and import a custom display from outside the trek_workspace.

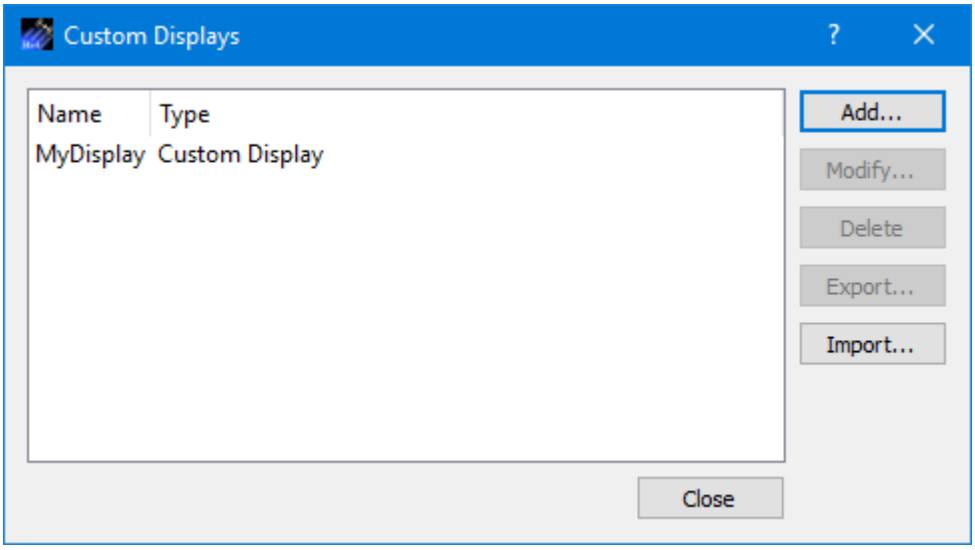


Figure 33 Manage Custom Displays Dialog

Each field is described below.

Add
The Add button provides access to the Add Custom Display dialog. This dialog is used to create a new custom display.

Modify
The Modify button provides access to the Modify Custom Display dialog. This dialog is used to modify an existing custom display.

Delete
The Delete button provides the capability to delete a custom display.

Export
The Export button provides access to the Export Display dialog.

Import
The Import button provides the capability to import a display.

Close
The Close button closes the dialog.

6.4.1 Add Custom Display Dialog

The Add Custom Display dialog is used to create a new custom display. It is shown in Figure 34.

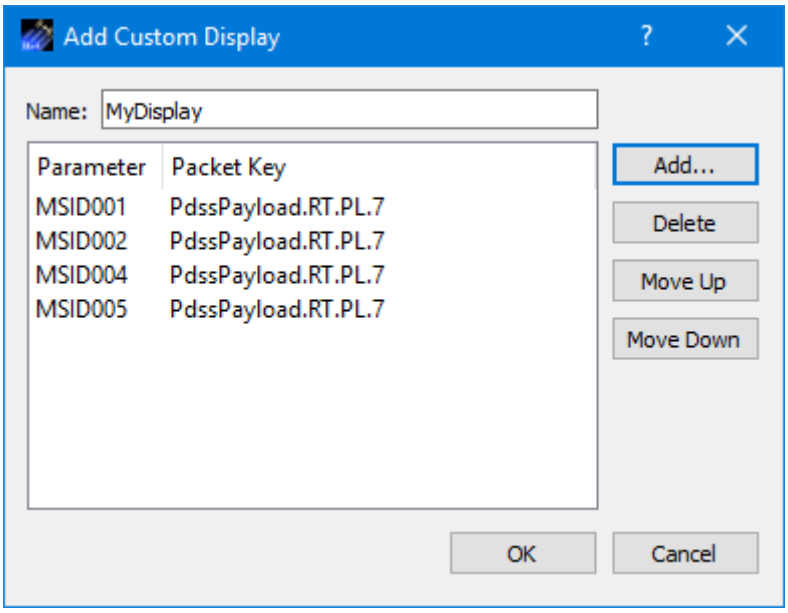


Figure 34 Add Custom Display Dialog

Each item is described below.

<u>Name</u>
The Name field is used to provide a unique name for the custom display.

<u>Parameter List</u>
The Parameter List identifies the parameters that will be on the display. They will be displayed in the order shown in the Parameter List.

<u>Add</u>
The Add button provides access to the Parameters dialog where you can select one or more parameters to add to the display.

<u>Delete</u>
The Delete button can be used to delete a parameter from the Parameter List.

<u>Move Up</u>
When a parameter in the Parameter List is selected, the Move Up button can be used to move the parameter up one row in the list.

<u>Move Down</u>
When a parameter in the Parameter List is selected, the Move Down button can be used to move the parameter down one row in the list.

6.4.2 Modify Custom Display Dialog

The Modify Custom Display dialog is used to modify an existing custom display. It provides the same capabilities that are available in the Add Custom Display dialog.

6.4.3 Export Display Dialog

The Export Display dialog is used to save a custom display outside the current Data application configuration. The default location is the trek_workspace/display directory. However, it can be exported to another location. The Export Display dialog is shown in Figure 35.

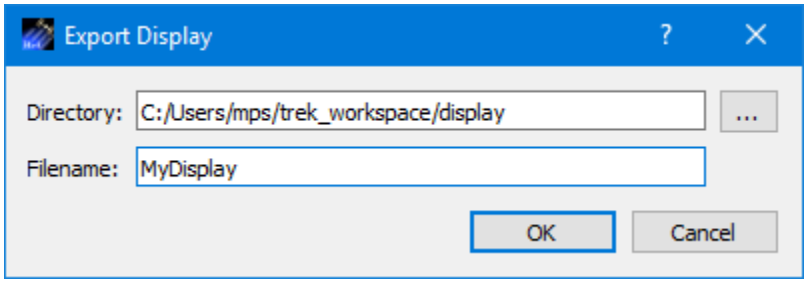


Figure 35 Export Display Dialog

6.5 Manage Monitor Sets Dialog

The Manage Monitor Sets dialog is used to create, modify, or delete a monitor set. A monitor set identifies one or more parameters to monitor for alarm conditions (limit or expected state alarms). A parameter can only be monitored if it has an alarm assigned. The Manage Monitor Sets dialog is shown in Figure 36. Monitor Sets only exist in the current application configuration. If you save the configuration, the monitor sets will be saved in the configuration file. If you would like to use a monitor set in a different configuration, you can export it and then import it into the other configuration. The default location for monitor sets is the trek_workspace/monitor_set directory. However, you can export and import a monitor set from outside the trek_workspace.

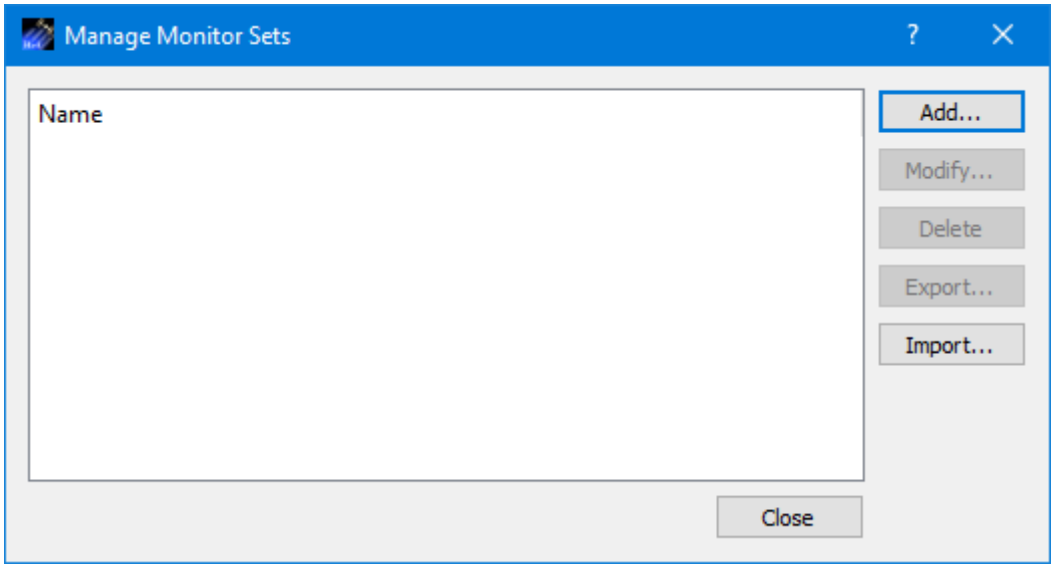


Figure 36 Manage Monitor Sets Dialog

Each field is described below.

Add
The Add button provides access to the Add Monitor Set dialog. This dialog is used to create a new monitor set.

Modify
The Modify button provides access to the Modify Monitor Set dialog. This dialog is used to modify an existing monitor set.

Delete
The Delete button provides the capability to delete a monitor set.

Export
The Export button provides access to the Export Monitor Set dialog.

Import
The Import button provides the capability to import a monitor set.

Close
The Close button closes the dialog.

6.5.1 Add Monitor Set Dialog

The Add Monitor Set dialog is used to create a new monitor set. It is shown in Figure 37.

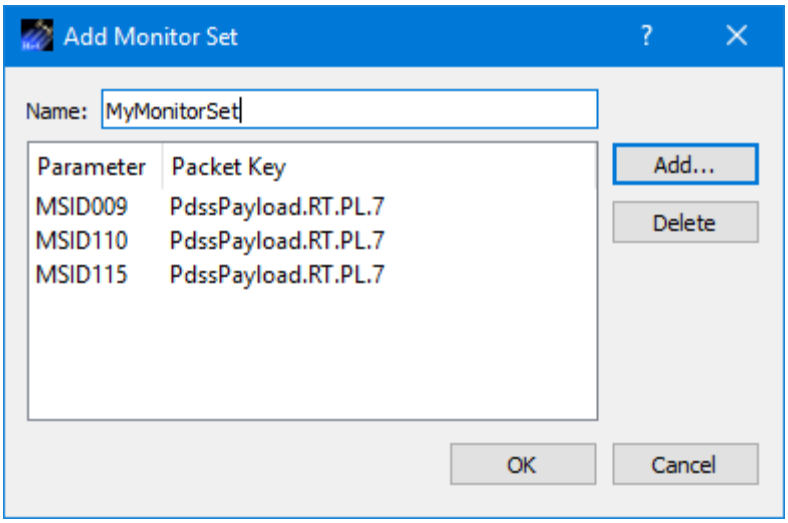


Figure 37 Add Monitor Set Dialog

Each item is described below.

<u>Name</u>
The Name field is used to provide a unique name for the monitor set.

<u>Parameter List</u>
The Parameter List identifies the parameters to be monitored.

<u>Add</u>
The Add button provides access to the Parameters dialog where you can select one or more parameters to add to the parameter list. The Parameters dialog will only list parameters that have Alarms assigned.

<u>Delete</u>
The Delete button can be used to delete a parameter from the Parameter List.

6.5.2 Modify Monitor Set Dialog

The Modify Monitor Set dialog is used to modify an existing monitor set. It provides the same capabilities that are available in the Add Monitor Set dialog.

6.5.3 Export Monitor Set Dialog

The Export Monitor Set dialog is used to save a monitor set outside the current Data application configuration. The default location is the trek_workspace/monitor_set directory. However, it can be exported to another location. The Export Monitor Set dialog is shown in Figure 38.

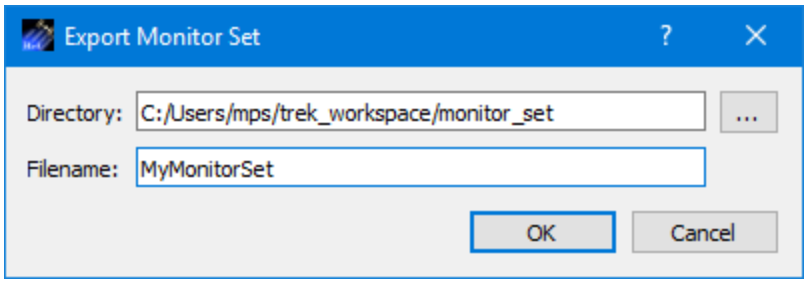


Figure 38 Export Monitor Set Dialog

6.6 Manage Monitoring Dialog

The Manage Monitoring dialog is used to start and stop monitoring for a monitor set. The Manage Monitoring dialog will only display monitor sets that exist in the current application configuration. The State (Inactive or Active) will be displayed for each monitor set in the list. The Manage Monitoring dialog is shown in Figure 39.

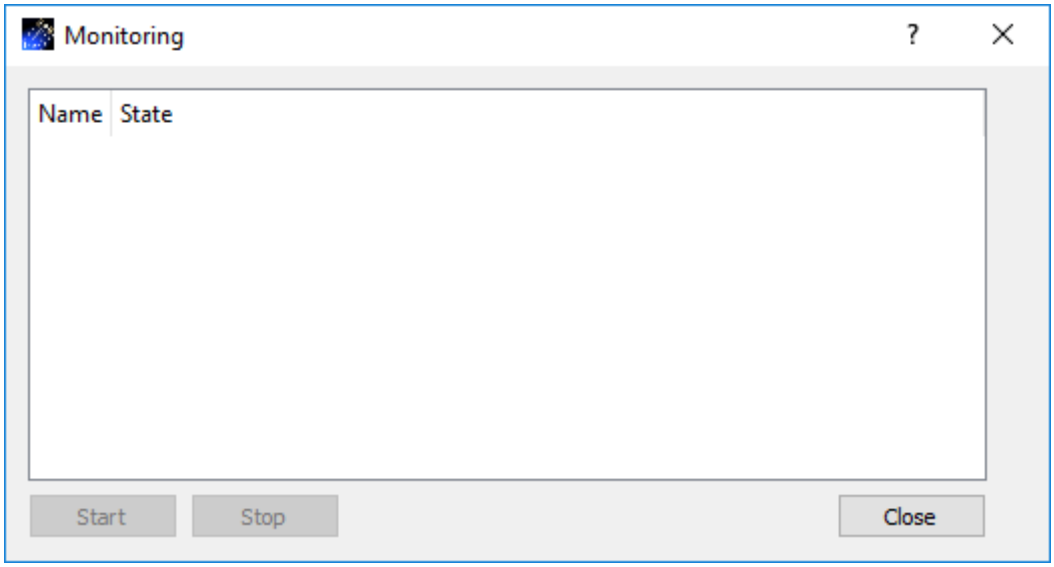


Figure 39 Manage Monitoring Dialog

Each item is described below.

<u>Start</u>
The Start button provides the capability to start monitoring for a selected monitor set.

<u>Stop</u>
The Stop button provides the capability to stop monitoring for a selected monitor set.

Close
The Close button closes the dialog.

6.7 Monitor Messages Dialog

The Monitor Messages dialog displays monitor messages for all monitor sets being monitored. The Monitor Messages dialog is shown in Figure 40.

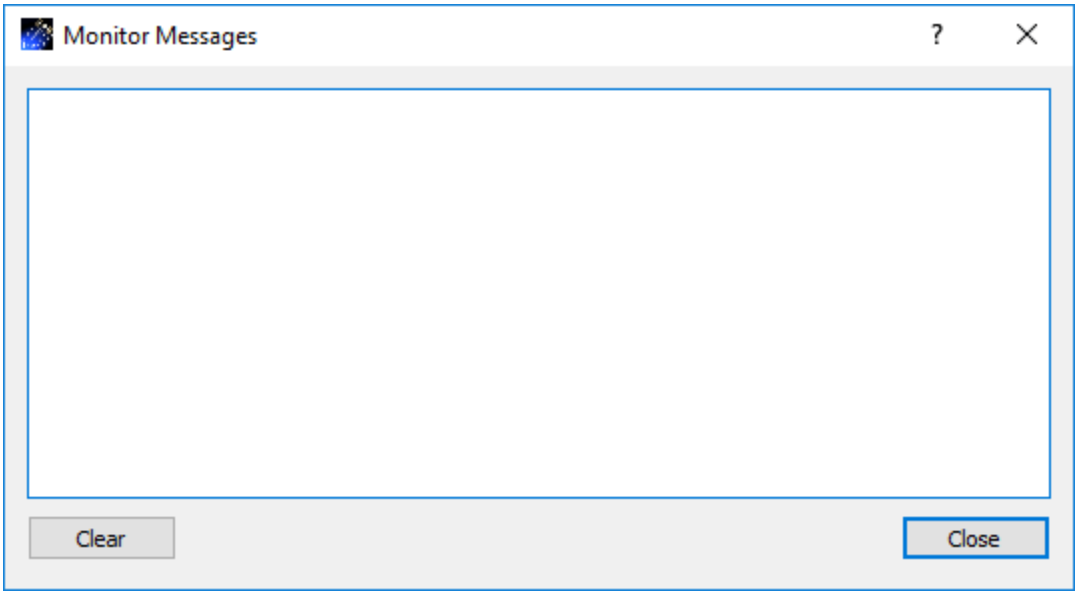


Figure 40 Monitor Messages Dialog

Each item is described below.

Clear
The Clear button provides the capability to clear all the messages in the dialog. This action cannot be reversed.

Close
The Close button closes the dialog.

6.8 Configure Monitor Message Logging Dialog

The Configure Monitor Message Logging dialog provides the capability to configure monitor message logging. If you turn on monitor message logging, monitor messages generated after logging is turned on will be written to the specified log file. The Configure Monitor Message Logging dialog is shown in Figure 41.

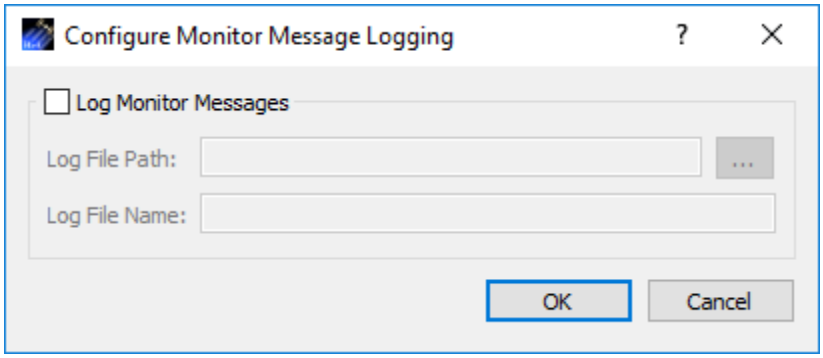


Figure 41 Configure Monitor Message Logging Dialog

Each item is described below.

Log Monitor Messages
The Log Monitor Messages checkbox provides the capability to turn logging on or off. If the Log Monitor Messages checkbox is not checked, logging will be off. If the Log Monitor Messages checkbox is checked, logging will be on.

Log File Path
The Log File Path should contain the absolute path to the directory where the log file should be written. If you don't like to type or you need help defining the complete path, you can push the … (dot dot dot) button located to the right of the Log File Path field. This will bring up a Browse dialog you can use to select the local directory where you want to store the log files.

Log File Name
The Log File Name field should contain the name to use for the log file.

The log file generated will use the log file name you enter followed by a timestamp. It will look similar to the following:

Example Log File: monitor_2017-06-06-12-06-41.log

6.9 Statistics

Statistics displays information about incoming data and services such as processing, recording, and forwarding. Statistics information is displayed in a dock window in the Main Window and in the Statistics dialog available from the Options menu. Figure 42 shows the Statistics dock window in the Main Window. Figure 43 shows the Statistics dialog.

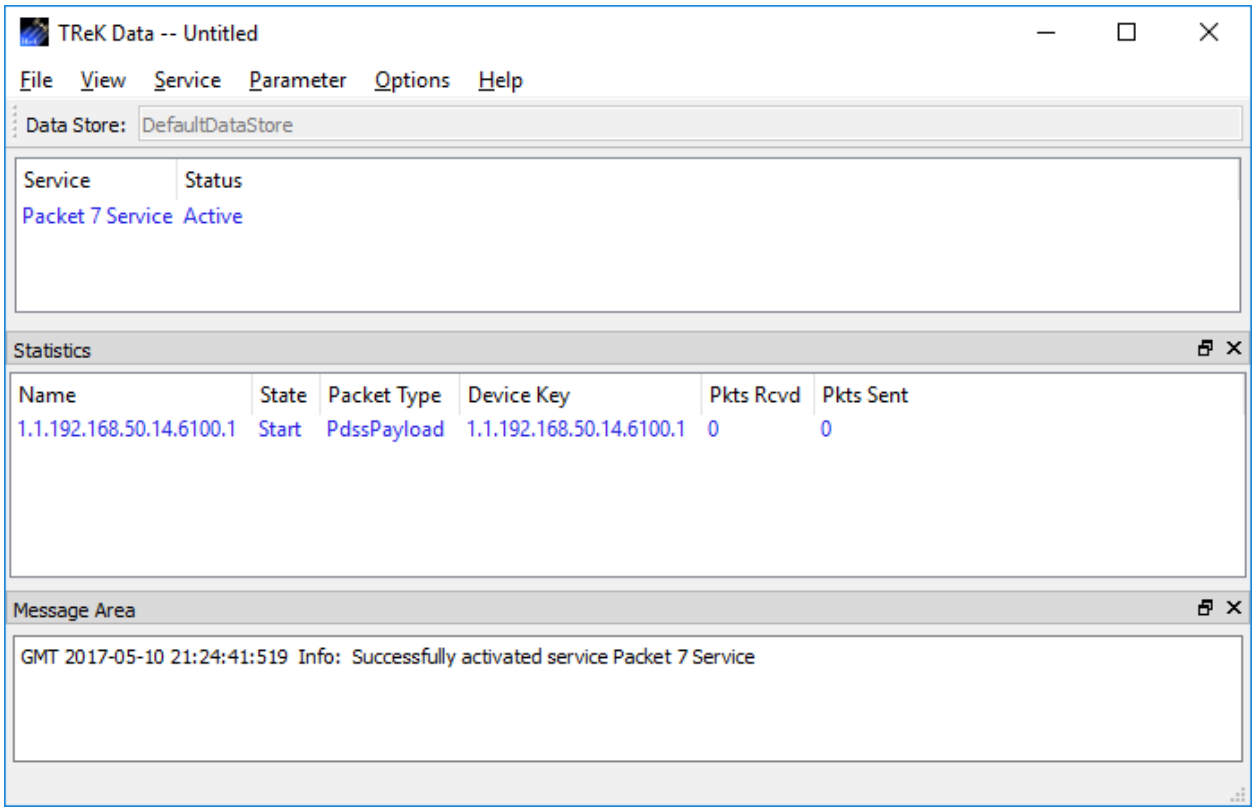


Figure 42 Statistics in the Main Window

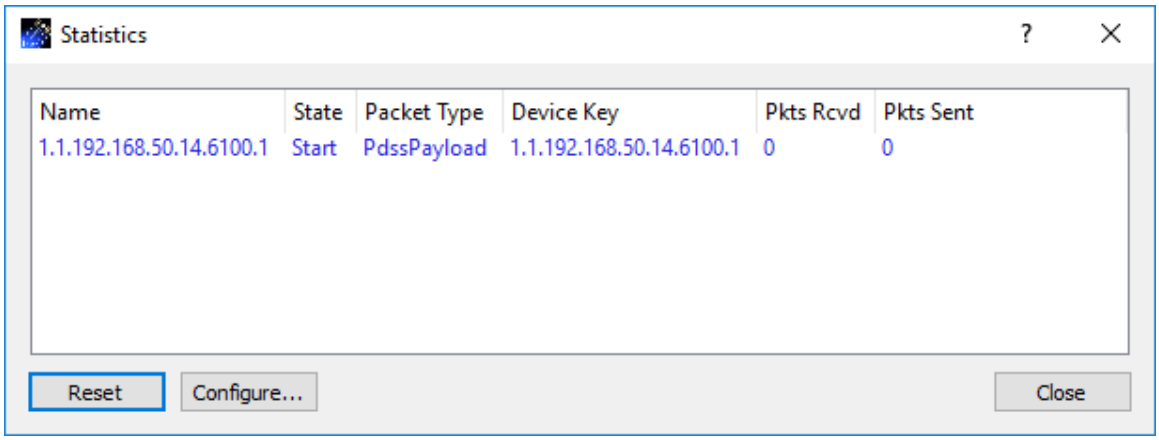


Figure 43 Statistics Dialog

Statistics can be configured to display different views of the statistics information. The view options can be accessed using the Statistics area pop-up menu. The pop-up menu is shown in Figure 44 and can be accessed by clicking the right mouse button in the statistics area.

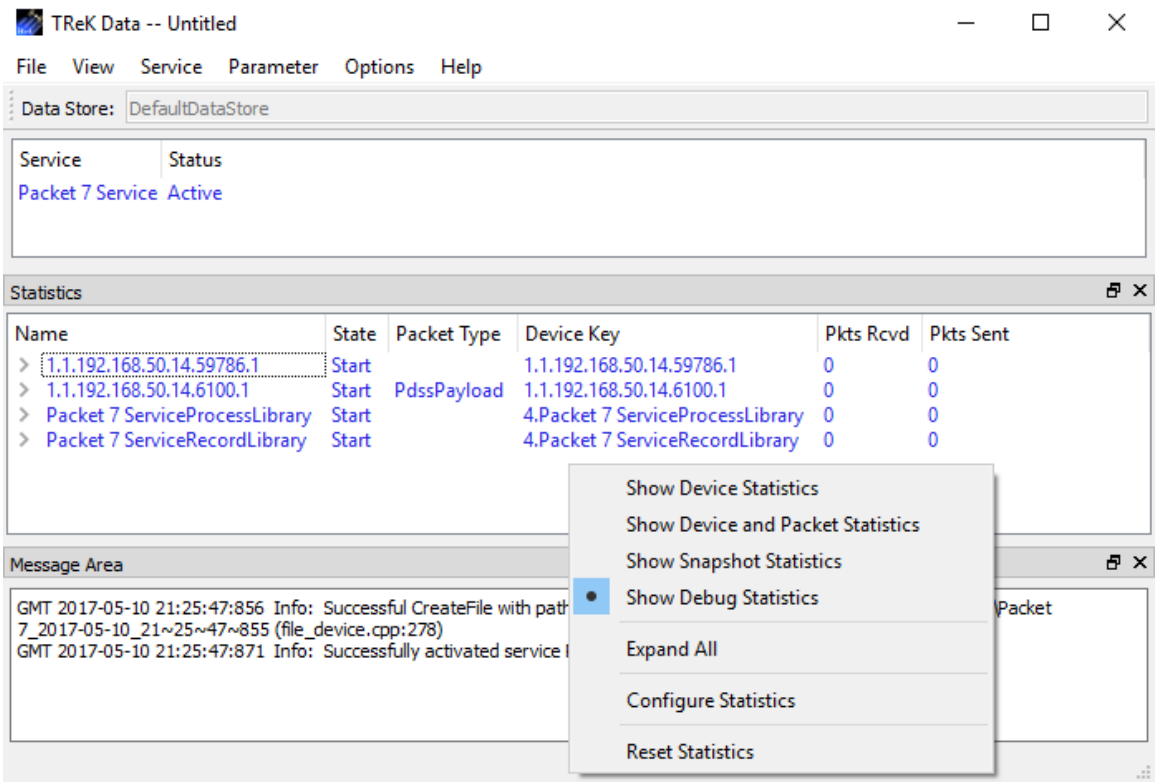


Figure 44 Statistics Pop-Up Menu

The Statistics pop-up menu has several options. Each is described below:

<u>Show Device Statistics</u>

Device Statistics is the default view. Device Statistics displays all the network sockets or devices in use by all active services being used to receive or forward data. When the device is a network socket it will include the IP address and Port. When the device is a library device that performs a specific function such as handling bundle protocol data, the name will reflect the device's function. Figure 45 shows the device statistics view. In this example, there is one network socket displayed. When data is received on this socket the Pkts Rcvd column will update reflecting the number of packets received. If a socket is being used to forward data, the Pkts Sent column will reflect the number of packets sent.

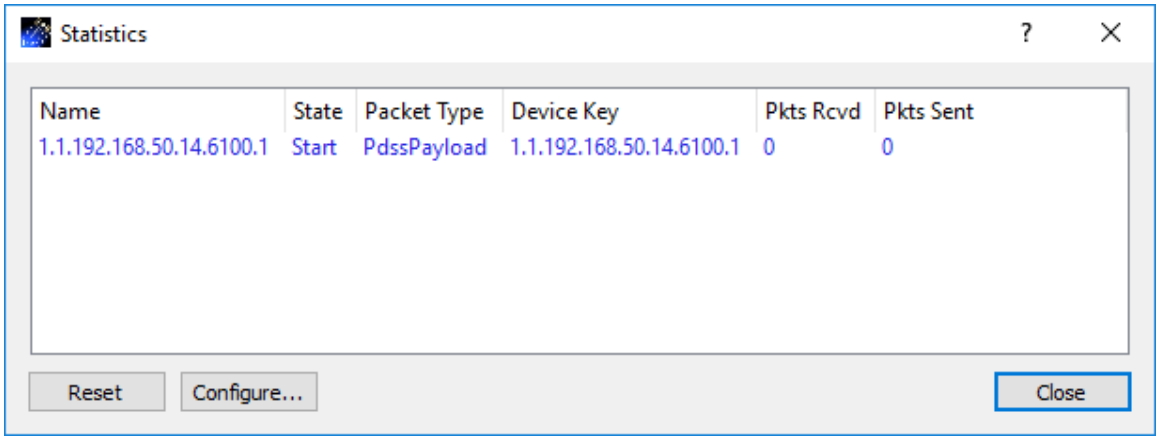


Figure 45 Device Statistics View

<u>Show Device and Packet Statistics</u>

The Device and Packet Statistics option will display both device statistics and packet statistics. Figure 46 shows the device and packet statistics view. In this example, there is one network socket displayed and this device can be expanded to display additional packet statistics. In this view you can see that this device was configured to accept packets with the packet key "PdssPayload.RT.PL.7". When any data is received on this socket the Pkts Rcvd column will update reflecting the number of packets received. The line showing packet statistics will reflect the number of packets received that match the packet key "PdssPayload.RT.PL.7".

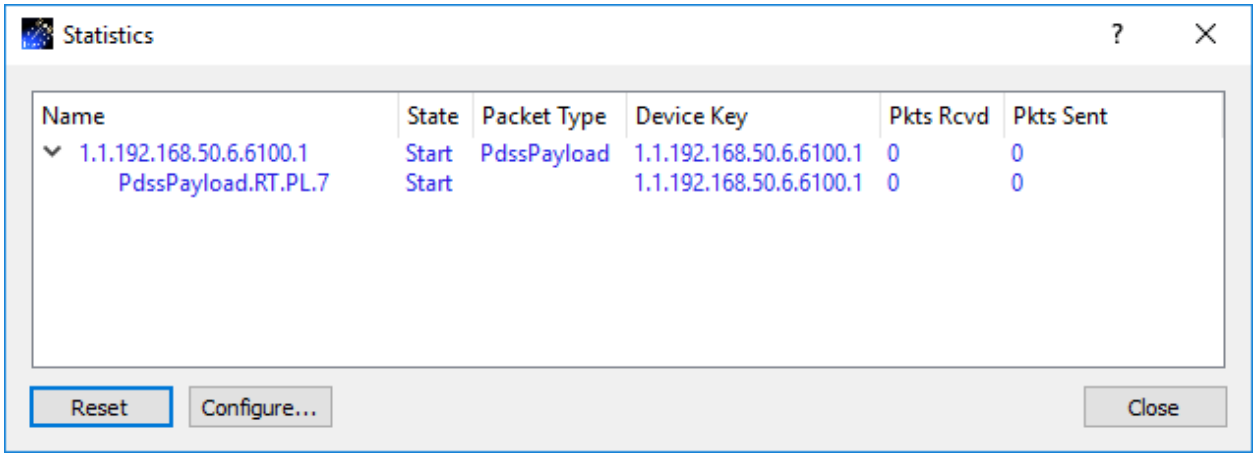


Figure 46 Device and Packet Statistics

Figure 47 shows a network socket that has received 87 packets and packet statistics for "PdssPayload.RT.PL.7" that has received 76 packets. This indicates that some packets were received on the network socket that did not match the "PdssPayload.RT.PL.7" packet key. This can be helpful in understanding what incoming data you are receiving.

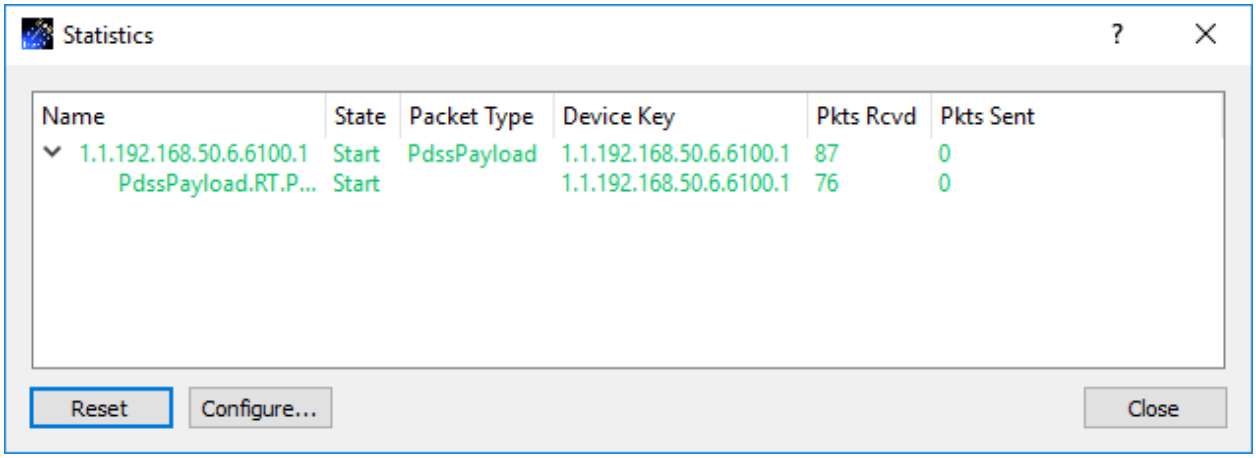


Figure 47 Device Receiving Unexpected Packets

Show Snapshot Statistics

Figure 48 shows the Snapshot view. This view provides a snapshot of the current state of incoming packets. In Figure 48 you can see that two packets are blue and one is green. Blue indicates the software is configured to receive the packets but no packets have been received. Green indicates packets are arriving.

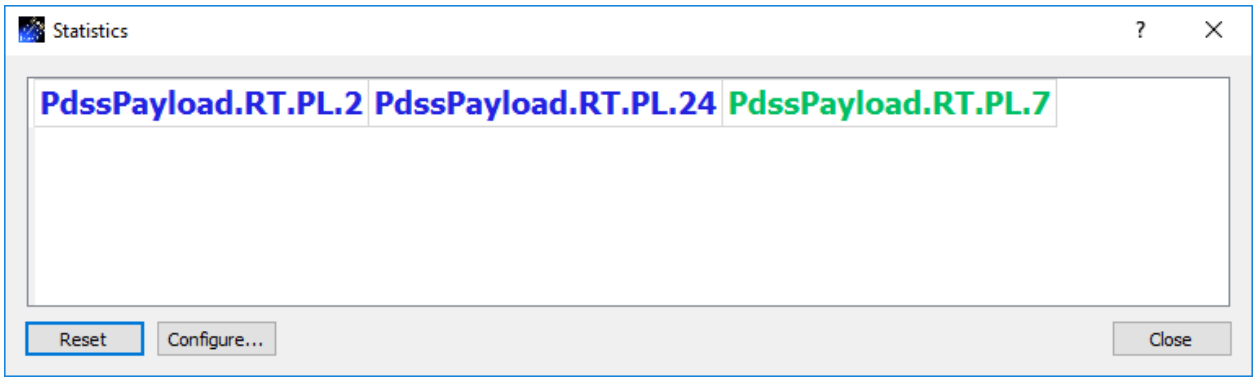


Figure 48 Snapshot Statistics

Show Debug Statistics

The Debug Statistics view shows the most detailed information of all the various views. It shows device statistics and packet statistics associated with each type of function requested (processing, recording, and forwarding) for each active service. In Figure 49 there is one service in the service list. It is named "Packet 7 Service". The statistics dock window has been configured to show the Debug Statistics View. The Packet 7 Service is configured to receive data on IP Address 192.168.50.14 port 6100. The Data Description tab Filter Type was set to 'Packet List' and one packet was listed with packet key "PdssPayload.RT.PL.7" . The Packet 7 Service is configured to process the data received, record the data received, and forward the data received using the UDP protocol. In the statistics area, the line with the name "1.1.192.168.50.14.6100.1" is a network socket that the Packet 7 Service created to receive data using IP Address 192.168.50.14

and port 6100. The line with the name "1.1.192.168.50.14.55551.1" is a network socket that the Packet 7 Service created to forward data using IP Address 192.168.50.14 and port 55551. The line with the name "Packet 7 ServiceProcessLibrary" identifies the processing statistics for the Packet 7 Service. The line with the name "Packet 7 ServiceRecordLibrary" identifies the recording statistics for the Packet 7 Service. The Pkts Rcvd and Pkts Sent columns reflect the associated statistics for each line item. 101 packets were received. 100 packets were sent (forwarded). 100 packets were processed. 100 packets were recorded. You may be wondering why 101 packets were received but only 100 packets were processed, recorded, and forwarded. The answer to this question can be found by expanding the view. The view can be expanded by selecting "Expand All" on the Statistics pop-up menu.

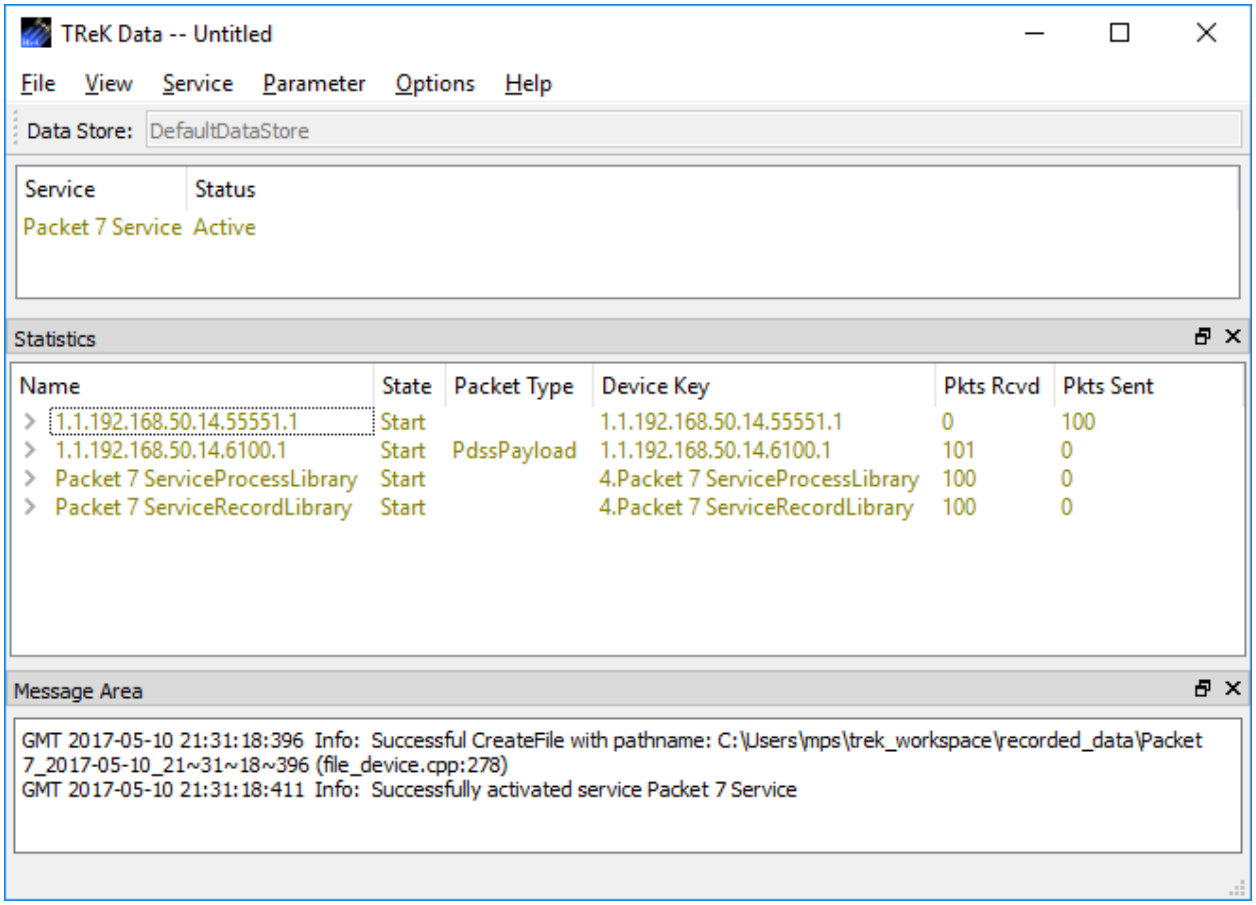


Figure 49 Debug Statistics View for Packet 7 Service

Figure 50 shows the Debug Statistics Expanded View for the Packet 7 Service. Now you can see the packet keys for the packets that were received on the network socket at 192.168.50.14 port 6100. You can see that 100 packets with the packet key "PdssPayload.RT.PL.7" were received and 1 packet with the packet key "PdssPayload.RT.UDSM.7" was received. This solves the mystery of the extra packet. Since the Packet 7 Service was configured to receive packets that matched the packet key

"PdssPayload.RT.PL.7" the "PdssPayload.RT.UDSM.7" packet was identified but it was not processed, recorded, or forwarded per the service's configuration.

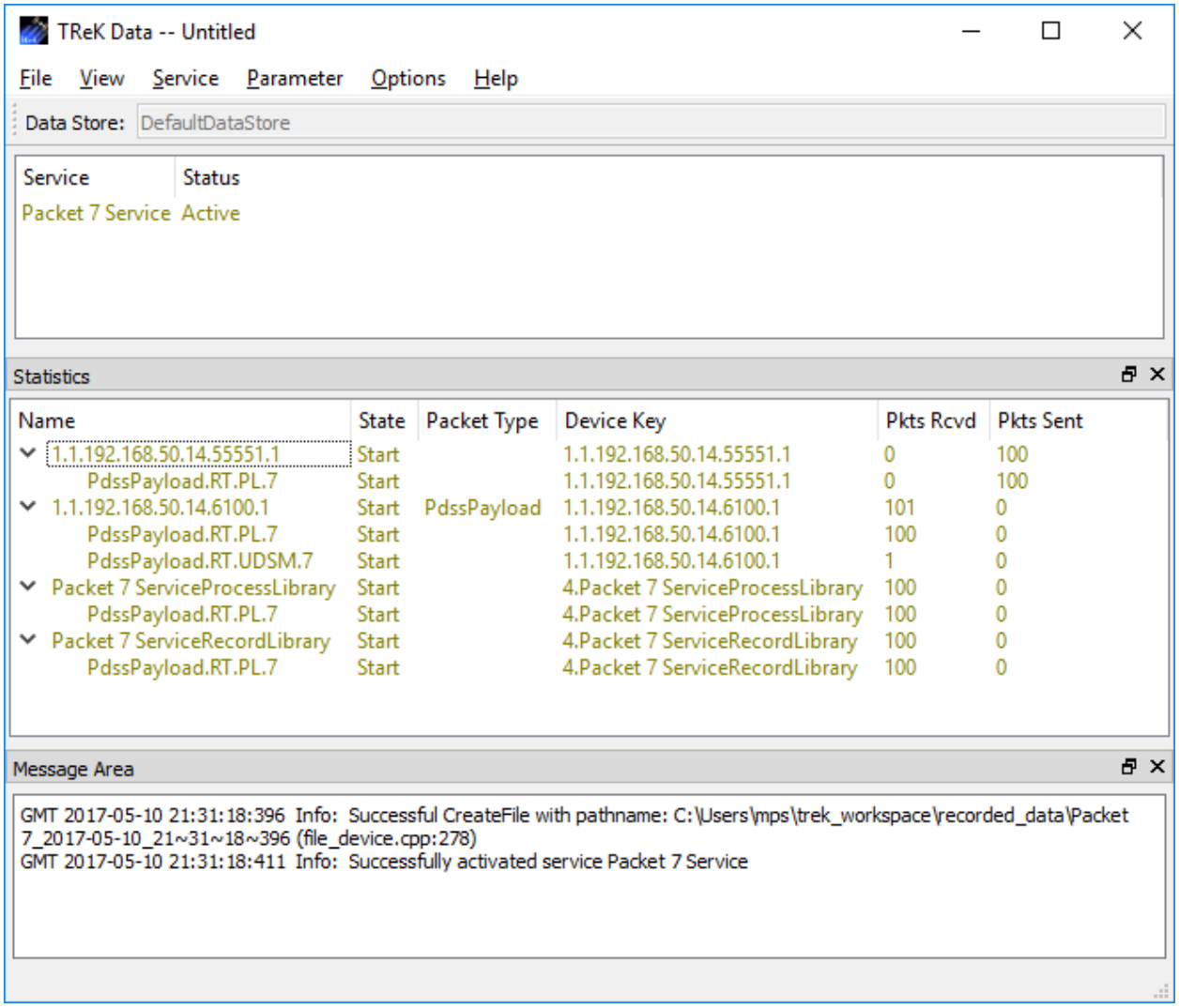


Figure 50 Debug Statistics Expanded View for Packet 7 Service

Expand All

The Expand All option will expand the Statistics tree to show all items. The Statistics tree will only appear for views that show packet statistics such as the 'Device and Packet Statistics' view and the "Debug Statistics' view.

Configure Statistics

The statistics information displayed can be configured using the Configure Statistics dialog. This dialog can be accessed using the statistics pop-up menu or the Configure button in the Statistics dialog. Detailed information is covered in section 6.9.1.

Reset Statistics
Reset Statistics will reset all statistics in all views to zero.

6.9.1 Configure Statistics Dialog

The Configure Statistics Dialog is shown in Figure 51.

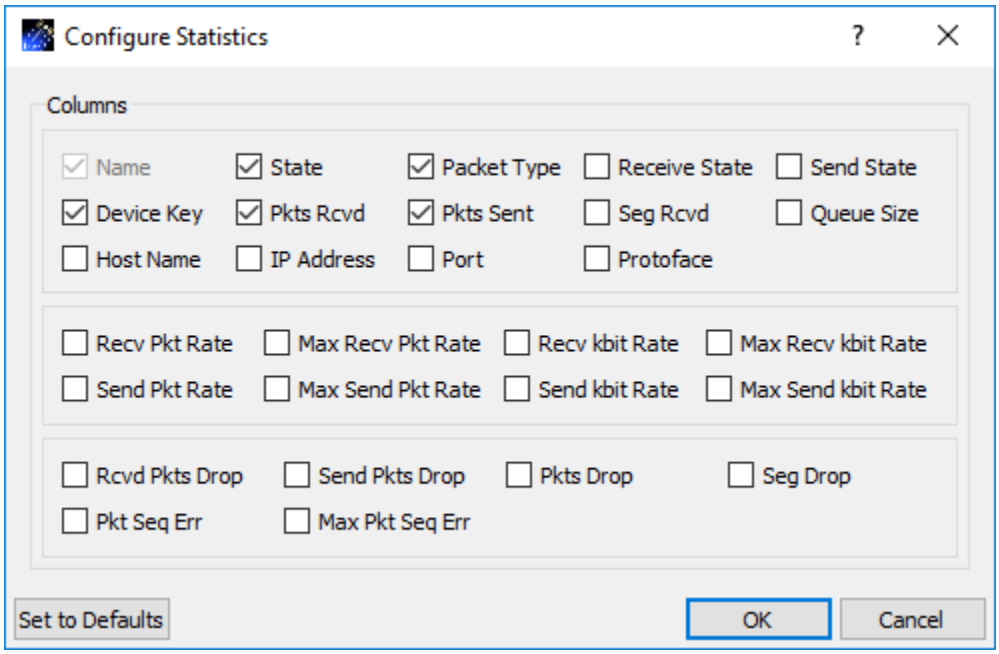


Figure 51 Configure Statistics Dialog

Each field is described below.

Name
Name is a character string that uniquely identifies each device and packet type. The device name is the device key if no device name is provided when the device is created. The packet name is the packet key associated with the packet.

State
State is the current state or condition of a device. Valid states include Start, Stop, Pause, Pulse, Ready and Undefined. If you check the State checkbox, the State column will be displayed.

Packet Type
Packet Type is a character string identifying the configuration of a device's packet header processor. If a device does not have to have an associated packet header processor, the Packet Type column is blank. Packet header processors process individual fields in the

packet header producing packet keys. If you check the Packet Type checkbox, the Packet Type column will be displayed.

Receive State
Receive State is the current receive state of an object. Valid receive states include Ready To Receive, Receiving and Not Receiving. If you check the Receive State checkbox, the Receive State column will be displayed.

Send State
Send State is the current receive state of an object. Valid receive states include Ready To Send, Sending and Not Sending. If you check the Send State checkbox, the Send State column will be displayed.

Device Key
Device Key is a character string that uniquely identifies each device. If you check the Device Key checkbox, the Device Key column will be displayed.

Pkts Rcvd
Packets received represents the number of packets received. If you check the Pkts Rcvd checkbox, the Pkts Rcvd column will be displayed.

Pkts Sent
The number of packets sent to a destination. If you check the Pkts Sent checkbox, the Pkts Sent column will be displayed. Pkts Sent is not the same as packets forwarded. Pkts Sent is used to represent the number of packets sent across a socket that is configured to receive and send packets. Pkts Sent never indicates packets forwarded. To see the number of packets forwarded, look at the Pkts Fwd column.

Seg Rcvd
Segments Received represents the number of segments received. This column is only applicable for TCP. If you check the Seg Rcvd checkbox, the Seg Rcvd column will be displayed.

Queue Size
Queue Size is the size of the queue that temporarily buffers packets that are being processed by a device. A device does not have to be associated with a queue. The device's queue size is defined when the device is created. If you check the Queue Size checkbox, the Queue Size column will be displayed.

Host Name
Host Name is a unique identifier that serves as the name of the computer. If you check the Host Name checkbox, the Host Name column will be displayed.

IP Address
IP Address is the IP address of a device if the device is a socket. If you check the IP Address checkbox, the IP Address column will be displayed.

Port
Port is the port number of the device if it is a socket. The port number is a string identifying the type of socket (e.g., client, listener or server) formatted as “c/l/s”. If the socket is a client socket then the port number will be followed by two "/" (e.g., 6100//). If the client socket is connected to a listener socket, the listener's port number is also listed (e.g., 6100/5432/). If the socket is a server socket then the client port number that is connected to the server is listed first, followed by two "/" and the server's listener port number (e.g., 6100//7890). If the socket is a listener socket the listener's port number is listed between two "/" (e.g., /5555/). If you check the Port checkbox, the Port column will be displayed.

Protoface
Protoface is the IP transportation protocol, either TCP or UDP, of a socket device. If you check the Protoface checkbox, the Protoface column will be displayed.

Recv Pkt Rate
Receive Packet Rate represents the number of packets received in the last second. If you check the Recv Pkt Rate checkbox, the Recv Pkt Rate column will be displayed.

Max Recv Pkt Rate
Maximum Receive Packet Rate represents the maximum packet rate seen thus far. If you check the Max Recv Pkt Rate checkbox, the Max Recv Pkt Rate column will be displayed.

Recv kbit Rate
Receive kilobit Rate represents the current number of kilobits per second that are being received. If you check the Recv kbit Rate checkbox, the Recv kbit Rate column will be displayed.

Max Recv kbit Rate
Maximum Receive kilobit Rate represents the maximum kilobit rate seen thus far. If you check the Max Recv kbit Rate checkbox, the Max Recv kbit Rate column will be displayed.

Send Pkt Rate
Send Packet Rate represents the number of packets sent in the last second. If you check the Send Pkt Rate checkbox, the Send Pkt Rate column will be displayed.

Max Send Pkt Rate
Maximum Send Packet Rate represents the maximum packet rate sent thus far. If you check the Max Send Pkt Rate checkbox, the Max Send Pkt Rate column will be displayed.

Send kbit Rate
Send kilobit Rate represents the current number of kilobits per second that are being sent. If you check the Send kbit Rate checkbox, the Send kbit Rate column will be displayed.

Max Send kbit Rate
Maximum Send kilobit Rate represents the maximum kilobit rate sent thus far. If you check the Max Send kbit Rate checkbox, the Max Send kbit Rate column will be displayed.

Rcvd Pkts Drop
Received Packets Dropped represents the number of packets that TReK received and then dropped. If you check the Rcvd Pkts Drop checkbox, the Rcvd Pkts Drop column will be displayed.

Send Pkts Drop
Send Packets Dropped represents the number of packets that TReK attempted to send but dropped. If you check the Send Pkts Drop checkbox, the Send Pkts Drop column will be displayed.

Pkts Drop
Packets Dropped represents the number of packets that were dropped because they could not be processed by another device. If you check the Pkts Drop checkbox, the Pkts Drop column will be displayed.

Seg Drop
Segments Dropped represents the number of segments that TReK received and then dropped. This column is only applicable for TCP. If you check the Seg Drop checkbox, the Seg Drop column will be displayed

Pkt Seq Err
Packet Sequence Error represents the number of packet sequence errors that occurred for a packet that is being received. A packet sequence error occurs when a packet arrives out of order (i.e. a packet with a sequence count of six was expected but instead a packet with a sequence count of seven was received). This calculation assumes a zero sequence count implies a sequence count reset and is not considered a packet sequence error. If you check the Pkt Seq Err checkbox, the Pkt Seq Err column will be displayed.

Max Pkt Seq Err
Maximum Packet Sequence Error represents the maximum packet sequence error that occurred for a packet that is being received. TReK determines the maximum packet sequence error by calculating the delta or difference between the expected packet sequence count and the actual packet sequence count. This calculation assumes a zero sequence count implies a sequence count reset and is not considered a packet sequence error. If you check the Max Pkt Seq Err checkbox, the Max Pkt Seq Err column will be displayed.

Set To Defaults
Set To Defaults will set all the fields to their default values.

6.10 Configure Statistics Snapshot Recording Dialog

The Configure Statistics Snapshot Recording dialog is shown in Figure 52. Statistics are generated and captured in memory as you use the application. A snapshot of the statistics can also be recorded to a file by turning on Statistics Snapshot Recording. When Statistics Snapshot Recording is on, the snapshot is updated once a second with the latest statistics and written to a file. Previous statistics snapshot information is overwritten each time the latest statistics information is written to the file. Statistics are only available when there are services that are active. If you deactivate all services before turning off Statistics Snapshot Recording, the statistics snapshot file will be empty.

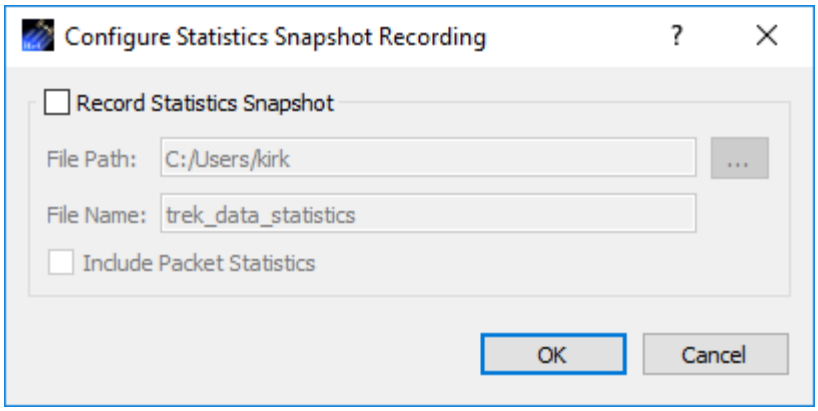


Figure 52 Configure Statistics Snapshot Recording Dialog

Each field is described below:

Record Statistics Snapshot
The Data application provides the capability to write a snapshot of application statistics to a file. If you check Record Statistics Snapshot, a snapshot of the application statistics will be written to the file specified.

File Path
The File Path should contain the absolute path to the directory where the statistics snapshot file should be written.

File Name
The File Name field should contain the name to use for the statistics snapshot file.

Include Packet Statistics

The Include Packet Statistics checkbox specifies whether packet statistics should be written to the file.

6.11 View Packet Dialog

The View Packet Dialog is shown in Figure 53. It is used to view the packet content of any active packet or active device. The packet content will be displayed in a text/hexadecimal format if packet header information is available. It will be displayed in hexadecimal format if no packet header information is available.

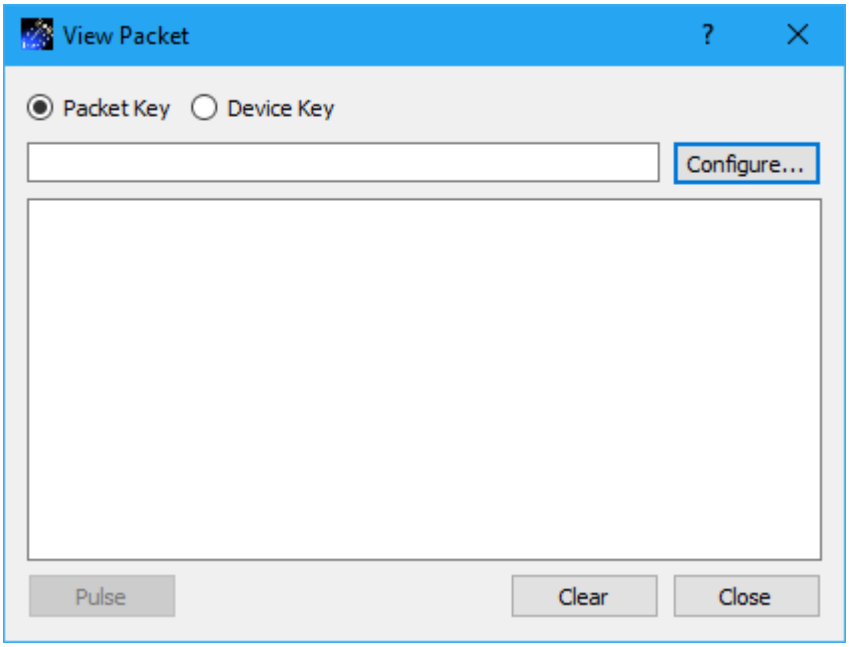


Figure 53 View Packet Dialog

Each field is described below.

<u>Packet Key</u>
The Packet Key radio button indicates you want to identify a packet key to select the packet content you want to view. When the Configure button is pushed the dialog displayed will list available packet keys.

<u>Device Key</u>
The Device Key radio button indicates you want to identify a device key to select the packet content you want to view. When the Configure button is pushed the dialog displayed will list available device keys.

Configure

The Configure button displays the Configure dialog shown in Figure 54. It is used to select a packet key or device key.

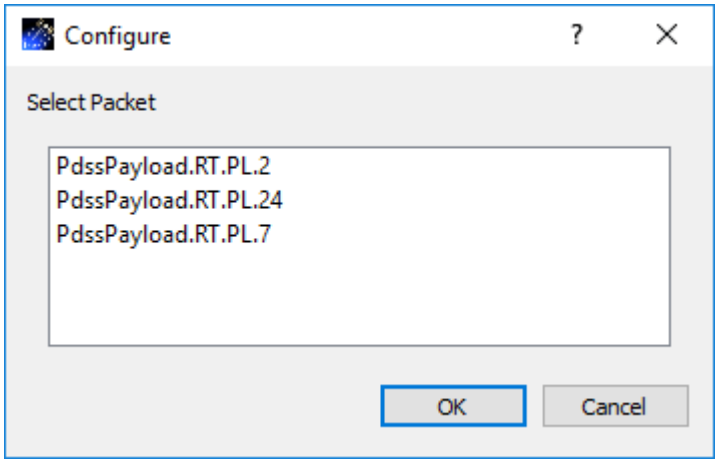


Figure 54 View Configure Dialog

Pulse

The Pulse button is used to request to the content of the latest packet that has arrived. If you push the Pulse button and no data has arrived, nothing will be displayed since there is no data to display. When you push the Pulse button after data has arrived, the packet content will be displayed as shown in Figure 55.

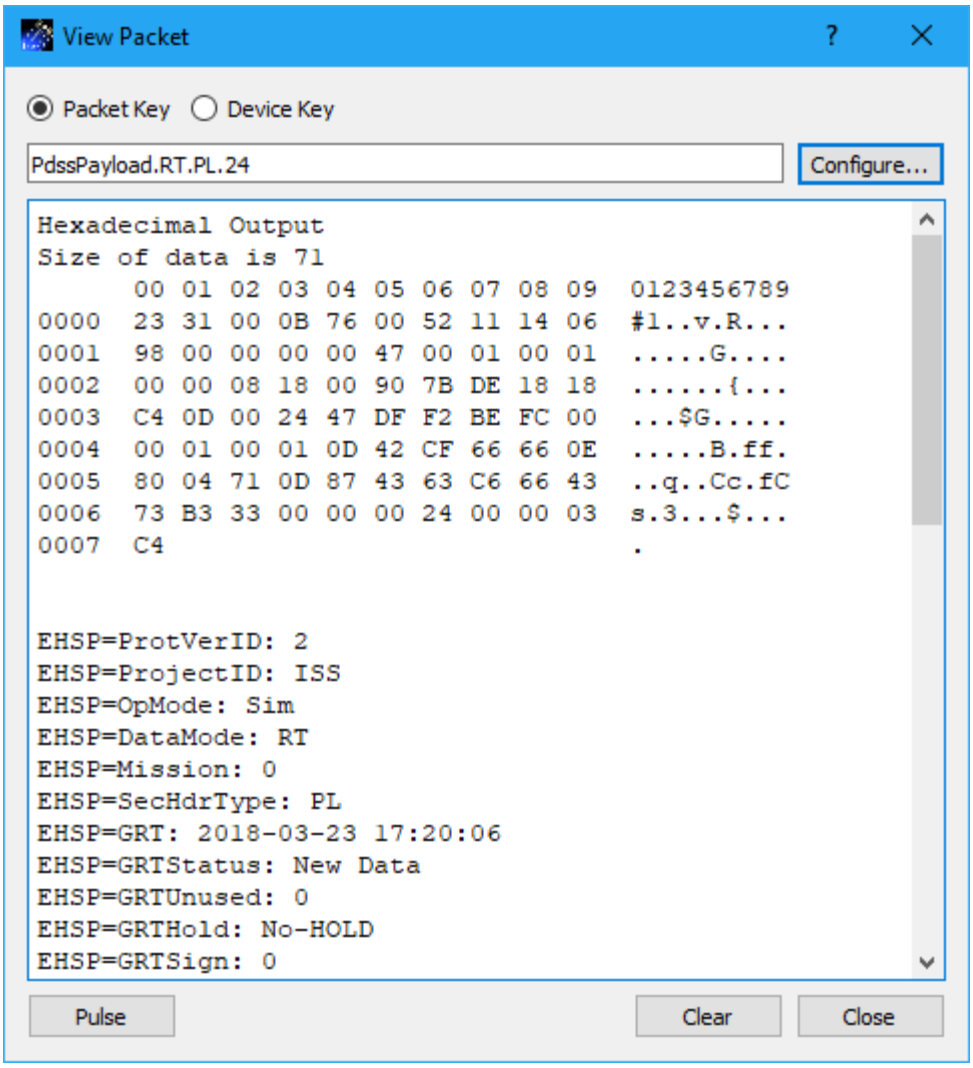


Figure 55 View Packet Example

Clear
The Clear button will clear the packet content area.

Close
The Close button will close the dialog.

6.12 Change Data Store Dialog

The Change Data Store dialog is shown in Figure 56. It is used to change the data store name. None of the services can be active when changing the data store name.

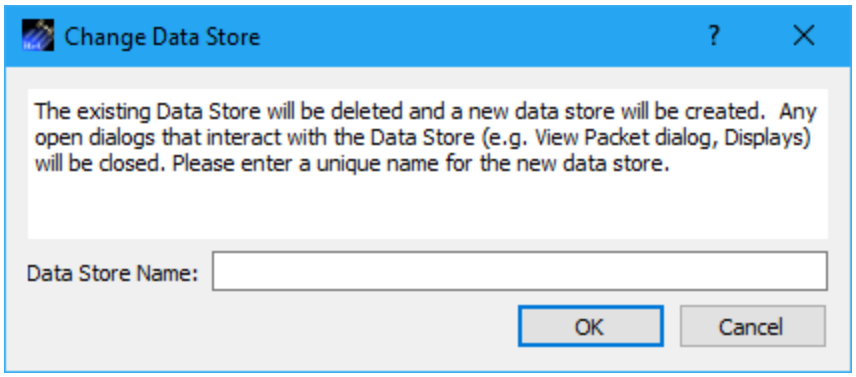


Figure 56 Change Data Store Dialog

Each field is described below.

Data Store Name

This field should contain the name of the data store. This name is important since it is one of the arguments you will pass to TReK API calls when accessing this data store to retrieve data.

6.13 Manage Cryptography Settings Dialog

The Manage Cryptography Settings dialog is shown in Figure 57. It is used to enter cryptography settings. Cryptography settings must be entered in order to successfully activate a service that uses cryptography capabilities.

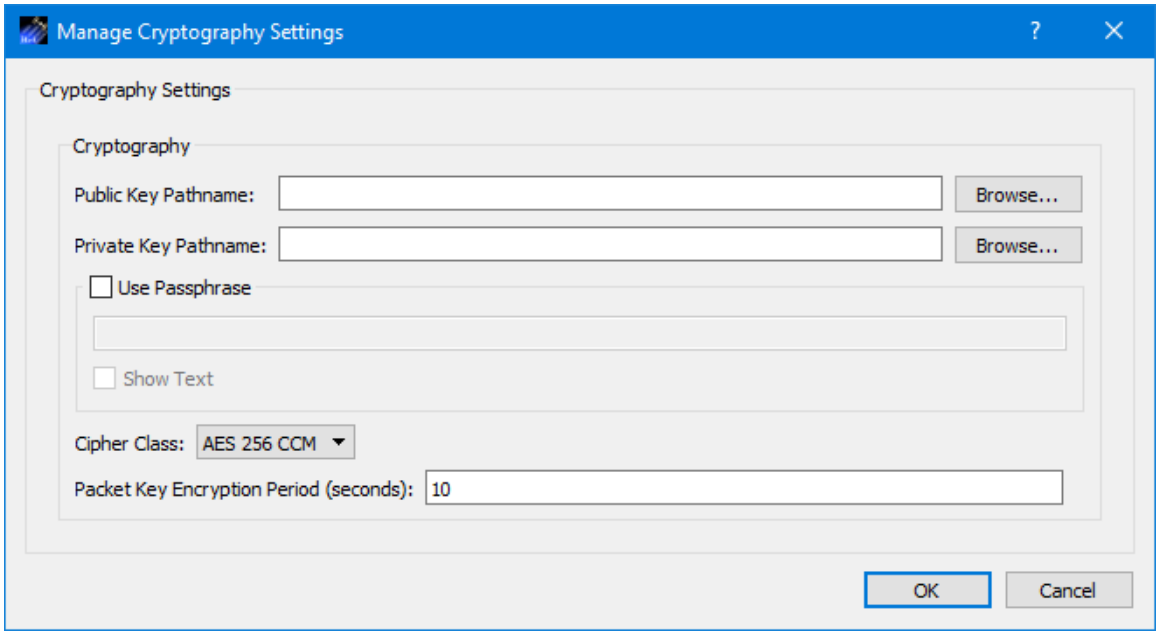


Figure 57 Manage Cryptography Settings Dialog

Each field is described below.

Public Key Pathname
This is the absolute path for the public key file.

Private Key Pathname
This is the absolute path for the private key file.

Use Passphrase
The Use Passphrase checkbox is used to specify that the private key requires a passphrase. If this box is checked, the passphrase must be entered into the text field. The passphrase text will not be displayed in the clear. If you want to see the text entered in the clear, check the Show Text checkbox. This information is not stored when you save a configuration. You will have to enter it each time you restart the application when using cryptography services.

Show Text
The Show Text checkbox is used to display the passphrase text in the clear.

Cipher Class
This option menu is used to select the cipher class.

Packet Key Encryption Period
The Packet Key Encryption period defines how often to generate a new Cipher Encryption Key (CEK) when streaming encrypted data. It can be configured to generate a new CEK for a packet stream once every "x" seconds to support encryption of high rate packet stream.

6.14 Application Messages

Various types of application messages are generated including information, progress, warning, error, and debug messages. Information, warning, and error messages will be displayed in the main window message area. All application messages are sent to the Messages dialog shown in Figure 58. The Messages dialog can be configured to display specific types of messages. By default, the Messages dialog will display information, progress, warning, and error messages. Columns in the Messages dialog can be sorted by clicking on the column header. The Messages dialog is available from the Options menu.

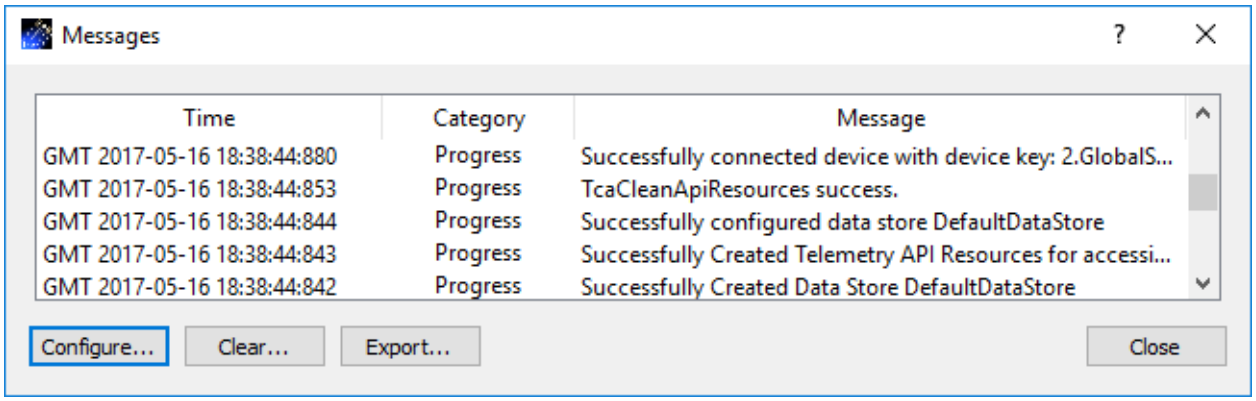


Figure 58 Messages Dialog

Configure

The Configure button provides access to the Configure Messages dialog shown in Figure 59. This dialog provides access to preferences associated with messages. Display preferences can be set to filter the types of messages (category) displayed in the Messages dialog. Export Preferences control how the time tag is added to the filename that is created when messages are exported. See the Export section for details.

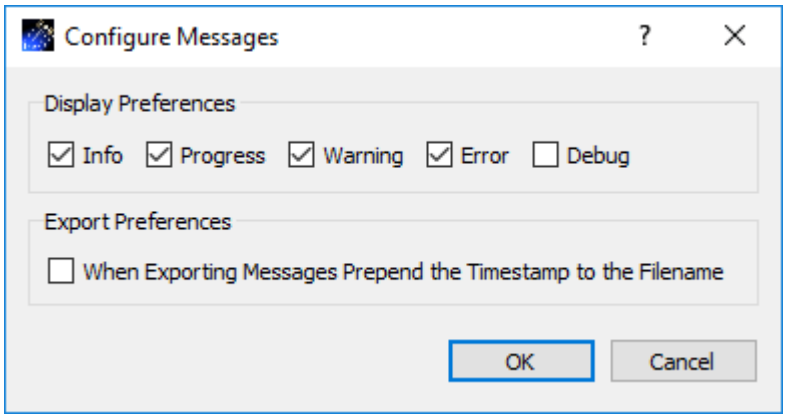


Figure 59 Configure Messages Dialog

Clear

The Clear button provides access to the Clear Messages dialog shown in Figure 60. This dialog provides two ways to clear messages in the Messages dialog. You can clear all the messages or clear selected messages. Once you clear messages, the messages are permanently deleted.

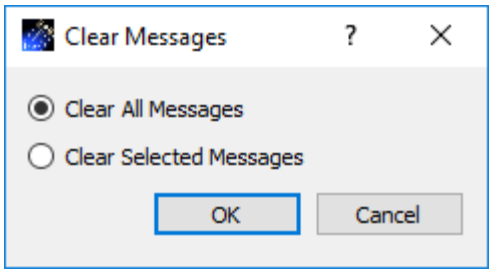


Figure 60 Clear Messages Dialog

Export

The Export button provides the capability to save all the application messages to a file. When you push the Export button you will be prompted for a directory and filename. Export will save all messages, not just the messages currently displayed in the Messages dialog (i.e. the Display Preferences are not applied). The name you provide for the file will be modified with a time tag that is added to the filename. The time tag indicates the time the file was closed. The default is to append the time tag to the filename. For example:

Filename Input: messages.txt
Filename Output: messages_2017-05-07_13~03~28.txt

If you would like to prepend the time tag to the filename you can set this preference in the Configure Messages dialog. This would result in the following:

Filename Input: messages.txt
Filename Output: 2017-05-07_13~03~28_messages.txt

6.15 Application Configuration File

The Data application saves the following information when you save a configuration:

- Contents of the Service List.

6.16 Application Settings

The Data application saves application settings each time you exit the application. The next time you run the application, the application will initialize with the previous settings. The following settings are saved:

- Application Window Size
- Configure Messages Selections

7 FAQ and Troubleshooting

This section addresses Frequently Asked Questions and provides tips for troubleshooting common gotchas.

No FAQs Yet.