Oracle® Communications Diameter Signaling Router

Integrated DIH User's Guide

E63644 Revision 02

September 2015

ORACLE®

Oracle® Communications Diameter Signaling Router Integrated DIH User's Guide

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This section contains an overview of the available information for the Integrated Diameter Intelligence Hub (IDIH) feature. The contents include sections on the organization, scope, and audience of the documentation, as well how to receive customer support assistance.

Overview

This documentation provides information about the functions of the Integrated Diameter Intelligence Hub (IDIH) feature.

This feature:

- Allows the user to create and manage trace filters on DSR to capture messages needed for troubleshooting service issues
- Presents traces to the user using the graphical visualization capabilities provided by IDIH
- Allows the user to filter, view, and store the results with IDIH

The IDIH feature allows the user to capture detailed information about selected Diameter transactions and transmit this information to IDIH for further analysis. The integration of troubleshooting capabilities into the DSR product provides a high value proposition for customers to be able to troubleshoot issues that might be identified with the Diameter traffic transmitted to the DSR.

These troubleshooting capabilities can supplement other network monitoring functions provided by the customer's OSS and network support centers to help quickly pinpoint the root cause of signaling issues associated with connections, peer signaling nodes, or individual subscribers.

Note: IDIH is not a replacement of the features in previous DIH releases.

Scope and Audience

This documentation is intended for personnel who maintain operation of the DSR.

Manual Organization

Information in this document is organized into the following sections:

- *Introduction* contains general information about this document, how to contact *My Oracle Support (MOS)*, and *Locate Product Documentation on the Oracle Help Center Site*.
- *IDIH Configuration and Maintenance on DSR GUI* provides configuration and maintenance information of the IDIH feature.
- *Trace Analysis* provides information about traces used by the IDIH.
- *IDIH Admin Privileges* provides basic information about admin privileges that may be associated with IDIH
- *IDIH Alarms* provides basic information about alarms associated with the IDIH feature.
- *Supported Diameter Interfaces* provides information about the Diameter interfaces supported by IDIH.
- *DSR Application Metadata-Generating Events* provides basic information about metadata-generating events associated with the DSR applications.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Help Center Site* for more information.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com*.

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.

3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Chapter 2

IDIH Configuration and Maintenance on DSR GUI

Topics:

This chapter contains information on how to configure IDIH on the DSR GUI.

Remote Servers

To use IDIH, a remote server connection must be configured. The **Communication Agent -> Configuration -> Remote Servers** screen on the NOAM is used to configure connections to remote servers.

Once a remote server with IDIH is configured on the NOAM, the IP address for the server appears in the **IDIH IP Address** field on the **Diameter -> Troubleshooting with IDIH -> Configuration -> Options** screen on the SOAM.

For detailed information about configuring remote servers in DSR, refer to the *Communication Agent User's Guide*.

For detailed information about configuring remote servers in IDIH, refer to the *IDIH Installation* document.

IDIH Options Configuration on DSR

The **Diameter > Troubleshooting with IDIH > Configuration > Options** GUI screen on an SOAM Server is used to configure Options for the IDIH on DSR. If these options are not configured, the user will not be able to access IDIH from DSR.

Options Elements

Table 2: IDIH Options Elements describes the fields on the IDIH Options screen.

The correct IDIH Host Name corresponds with the name of the configured ComAgent remote server.

The IDIH visualization address is entered by the user and is necessary for single sign-on to access IDIH directly from DSR without credentials.

Table 2: IDIH Options Elements

Field (* indicates a required field)	Description	Data Input Notes
*Max Bandwidth	The maximum amount of bandwidth specified in Mbps that is used for sending TTRs to IDIH. When the TTR bandwidth exceeds the configured maximum, DSR will discard TTRs so that the bandwidth required to send the remaining TTRs between DA-MP and IDIH does not exceed the configured maximum	Format: text box; numeric Range: 0-25 Default: 25 Mbps (26214400 bps)

Field (* indicates a required field)	Description	Data Input Notes
IDIH Host Name	The Host Name of the peer IDIH server used for sending the messages.	Format: pulldown list Default: N/A
IDIH Visualization Address	The IP address or FQDN of the remote IDIH server that visualizes the trace (when the link "Analyze with IDIH" is clicked on the "Maintenance" screen). If an IP address is used in place of a FQDN then IDIH SSO functionality will not work from the DSR SOAM.	Format: text box Default: N/A

IDIH Global Options Configuration on DSR

The **Diameter > Troubleshooting with IDIH > Configuration > Global Options** GUI screen on an SOAM Server is used to configure Global Options for the IDIH on DSR.

Global Options Elements

Table 3: IDIH Global Options Elements describes the fields on the IDIH Global Options screen.

Table 3: IDIH Global Options Elements

Field	Description	Data Input Notes
Max active network traces	The number of max active network traces indicates how many active network traces are allowed at each DSR site within the network.	Format: Text box Default: 2 Range: 2-8
Max active site traces (per site)	The number of max active site traces (per site) indicates how many active site traces are allowed at each DSR site within the network. The number is automatically updated when the number of "Max active network traces" is changed.	Format: Text box Default: 6 Range: 0-6

Trace Overview

A trace is a set of conditions (subdivided into scope and content) which, when met, cause trace data to be forwarded to IDIH.

The DSR plays the role of determining which messages should be captured, based on trace criteria that are created and activated by the user. The trace criteria identifies the "scope" as well as the "content".

- "Scope" refers to the non-protocol-related elements (such as connections or peers) that are used to select messages for trace content evaluation.
- "Content" refers to the protocol-related elements (such as command codes, AVPs, etc.) that are used to refine the trace criteria.

As request and answer messages are processed by the DSR, they are analyzed for matching any of the active trace definitions, and if so, transfer message components along with supplemental information to the IDIH called trace data. The IDIH can assemble the trace data, and present it to the user leveraging graphical visualization interfaces for additional filtering and analysis.

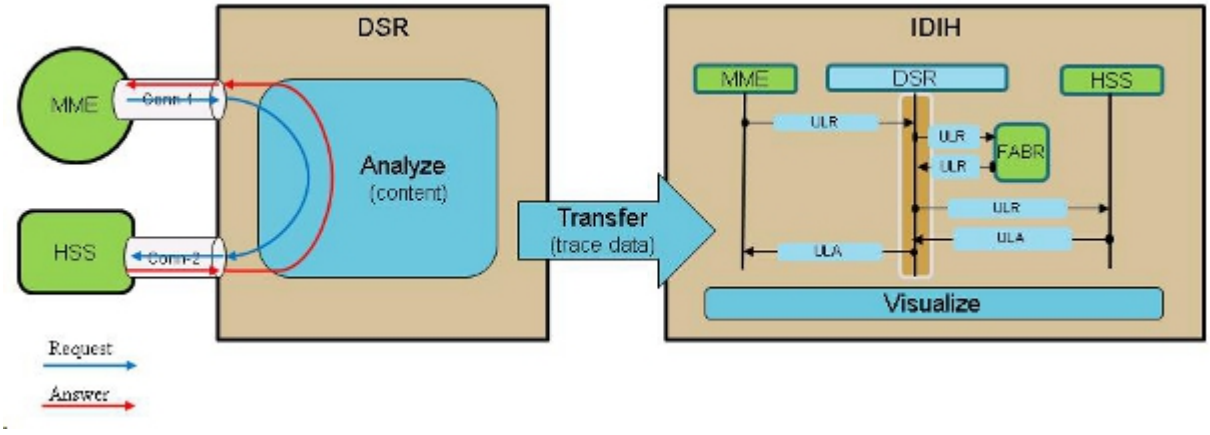

Figure 1: IDIH Trace Overview

IDIH does not guarantee a fixed number of days of data storage. Storage life is based on disk space. Some of the factors impacting storage life are trace parameters (very inclusive or very discriminatory) and record size.

During congestion, the DSR will suspend trace forwarding until the condition clears, at which time, trace forwarding will resume.

Note: Trace data lost during the time of congestion will not be recovered.

Network IDIH

Network IDIH is an extension of the IDIH feature. The IDIH feature allowed users to capture targeted transactions at a single site, and to store and visualize them at a local IDIH. Network IDIH introduces the concept of a "network trace' , which allows users to capture targeted transactions simultaneously at all DSR sites. Captured records are still stored at the local IDIH, however Network DIH allows the

user to visualize the captured records on any IDIH, regardless of where within the network they were captured. The single-site traces available in IDIH are still supported, and are referred to as "site traces" in this document.

Site Traces

Creating A Site Trace

A site trace is created from the **Diameter > Troubleshooting with IDIH > Configuration > Traces** screen. Select **Trace Location as Site Trace** when creating the trace. All trace content types, content values, scope types, and scope values are supported.

A site trace can only be created (and edited and deleted) on the site that will run the trace. When a site trace is created, IDIH will record the site at which the trace was created, and will only allow a GUI launched from that site to edit, delete, start or stop the trace.

Starting A Site Trace

A site trace is started from the **Diameter > Troubleshooting with IDIH > Maintenance > Traces** screen. A site trace can only be started from the GUI at the site that created the trace.

Running A Site Trace

Only DA-MPs at the same site that the site trace was created at will attempt to match a given site trace. DA-MPs will send all TTRs that match site traces to the local site IDIH.

Stopping A Site Trace

A site trace can be manually stopped from the from the **Diameter > Troubleshooting with IDIH > Maintenance > Traces** screen. A site trace can only be stopped from the GUI at the site that is running the trace. A site trace will be automatically stopped when either the "Time Duration" or "Number of Matches" limits are reached.

Viewing Site Trace Status

The status of site traces can be viewed from the **Diameter > Troubleshooting with IDIH > Configuration > Traces**. The status of a site trace can only be viewed from the GUI at the site that is running the trace.

Network Traces

Creating A Network Trace

A network trace is created from the **Diameter > Troubleshooting with IDIH > Configuration > Traces** screen. Select **Trace Location as Network Trace** when creating the trace. All trace content types, content values, scope types, and scope values are supported.

Network traces can be created at any site, and can be edited, deleted, started or stopped at any site. A network trace created at Site A, for example, could be edited at Site B and deleted at Site C.

Starting A Network Trace

A network trace is started from the **Diameter > Troubleshooting with IDIH > Maintenance > Traces** screen. Network traces can be started at any site.

Running A Network Trace

All sites will attempt to run every active network trace. However, it is possible for the user to specify a scope type/value that will prevent some sites from matching the trace. For example, a network trace created at Site A specifies Peer scope, and selects the peer "Peer1". Only sites that have a peer named "Peer1" will be able to match the scope. DA-MPs at all sites should verify that they can match the scope type/value of each network trace. If not, then the network trace should not be run. (This trace would still count against the site's active network trace limit

DA-MPs will send all TTRs that match network traces to the local site IDIH.

Stopping A Network Trace

A network trace can be manually stopped from the **Diameter > Troubleshooting with IDIH > Maintenance > Traces** screen. Network traces can be manually stopped at any site. Network traces are automatically stopped if they have reached their configured time duration.

Network traces are not automatically stopped if they hit their match count limit. The site that reached its match count limit will no longer attempt to match the trace once the match count limit is reached, but other sites will continue to attempt to match the trace. Even if all sites hit their match count limit, the network trace will not be automatically stopped; it continues to count as an active network trace until its time duration is exhausted, or until it is manually stopped.

Viewing Network Trace Status

The status of network traces can be viewed from the **Diameter > Troubleshooting with IDIH > Maintenance > Traces**. The status of a network trace can be viewed from the GUI at any site, however the information that is displayed is the status of the trace at the local site. Summary status of the network trace over all sites is not available.

IDIH Traces Configuration on DSR

The **Diameter > Troubleshooting with IDIH > Configuration > Traces** GUI screen on an SOAM server is used to configure traces used by the IDIH.

On the **Diameter > Troubleshooting with IDIH > Configuration > Traces** screen, the user can:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order by clicking the column heading. By default, the list is sorted in ascending alphabetical order.
- Click the **Insert** button.

  The **Diameter > Troubleshooting with IDIH > Configuration > Traces [Insert]** screen opens. The user can add new Traces.

- Select a Trace entry in the list, and click the **Edit** button.

The **Diameter > Troubleshooting with IDIH > Configuration > Traces [Edit]** screen opens. The selected Trace entry can be edited.

- Select a Trace entry in the list, and click the **Delete** button to remove the selected entry.

Traces Elements

Table 4: IDIH Traces Elements describes the fields on the Traces screen.

Table 4: IDIH Traces Elements

Field (* indicates a required field)	Description	Data Input Notes
*Trace Name	A name that uniquely identifies the Trace.	Format: text box Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Default: N/A
Trace Location	Indicates whether a trace runs at the current site or at all sites in the network	Format: radio button
Trace Content		
*Content Type	The Diameter message contents to be matched for this trace. The combination of content type/content values specify the content elements and content values that a candidate message must match before the transaction that the message belongs to is sent to DIH. Content Type: • Non-success answers - answers with (Experimental) Result-Code >= 3000, or any message with the E-bit set • (Ad Hoc)Requests - any request that matches the specified content values • (Ad Hoc Answers) - any answer that matches the specified content values • User Identity - any message that contains the specified	Format: pulldown list Range: Non-success answers, Requests, Answers, Ad Hoc Requests, Ad Hoc Answers, User Identity, Equipment Identity Default: -Select-

Field (* indicates a required field)	Description	Data Input Notes
	IMSI or MSISDN. AVPs searched for the specified IMSI/MSISDN value are automatically determined by the application ID(s) selected. • Equipment Identity - any message that contains the specified IMEI. AVPs searched for the specified IMEI value are automatically determined by the application ID(s) selected.	
Content Values	After selecting the content type, the screen displays the "Content Values" for selecting content elements and entering content values.	Default: N/A
Trace Scope		
*Scope Type	The scope used for this trace. Scope Type: • Connection - messages arriving or leaving on specified connection are candidates for tracing • Peer - messages arriving or leaving on specified peer are candidates for tracing • DSR Application - messages going to or returning from specified DSR application are candidates for tracing • All - all messages are candidates for tracing	Format: pulldown list Range: Connection, Peer, DSR Application, All Default: -Select-
*Scope Value	The scope value used for this trace. Selection values will be populated based on the Scope Type selected.	Format: pulldown list Default: -Select-
Trace Duration		
*Number of Matches	Number of Matches - stop the trace after matching this many messages	Format: text box; numeric Range: 1-1000 Default: N/A

Field (* indicates a required field)	Description	Data Input Notes
*Time of Duration	Time - stop the trace after it has been active for this amount of time (HH:MM:SS)	Format: text box; numeric Range: 00:00:01 - 96:00:00 Default: N/A
Notes	Descriptive information about the trace	Format: Text box Range: A 255-character string Default: N/A

Insert

The **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces -> [Insert]** screen is used to create a new trace.

Note: A maximum of 100 traces may be inserted.

The fields are described in *Traces Elements*.

1. Select **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces**.
2. Click **Insert**.

   The **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces -> [Insert]** screen appears.

3. Enter a trace name in the **Trace Name** field.

   The name must meet these requirements:

   - Maximum length of 32 characters
   - Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit

4. Select a **Trace Location** by selecting either the **Site Trace** button or the **Network Trace** button.
5. Select a Content Type from the **Content Type** pulldown list.
   There are seven Content Types supported: Non-success answers, Requests, Answers, Ad Hoc Requests, Ad Hoc Answers, User Identity, and Equipment Identity.
6. The **Content Type** field determines what **Content Values** are available.

   If the **Content Type** is set to "Non-success answers", then no other content values are available.

   If the **Content Type** is set to "Requests", then the user may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and/or Destination-Realm. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

   If the **Content Type** is set to "Answers", then the user may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

If the **Content Type** is set to "Ad Hoc Requests", then the user may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and/or Destination-Realm. Additionally, an optional content value is available to select an AVP to be checked. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

Note: The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

Note: For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the "Exists" and "Does not exist" operators are allowed.

If the **Content Type** is set to "Ad Hoc Answers", then the user may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Additionally, an optional content value is available to select an AVP to be checked. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

Note: The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

Note: For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the "Exists" and "Does not exist" operators are allowed.

If the **Content Type** is set to "User Identity", then the user may select an Application-ID. The Application-ID pulldown list shows a pre-defined list of supported Diameter interfaces, although the user cannot add anything new to the list.

Note: After an Application-ID is selected, the user can specify a user in the associate AVP as the criteria for selecting messages, which is identified by either IMSI or MSISDN.

If the **Content Type** is set to "Equipment Identity", then the user may select an Application-ID. The Application-ID pulldown list shows a pre-defined list of supported Diameter interfaces, although the user cannot add anything new to the list.

Note: After an Application-ID is selected, the user can specify equipment in the associated AVP as the criteria for selecting messages, which is identified by IMEI.

For a list of supported Diameter interfaces, refer to *Supported Diameter Interfaces*.

7. Select a Scope Type from the **Scope Type** pulldown list.

   The scope for a trace can be for a specific **Connection**, specified **Peers**, specified **DSR Applications**, or **All** messages.

8. Select a Scope Value from the **Scope Value** pulldown list
   The scope value is determined by which Scope Type is selected.
9. Enter a number of matches for the trace to find in the **Number of Matches** field.

   Note: A maximum of 1000 matches is permitted.

10. Enter a duration time for the trace in the **Time of Duration** field.
    The duration can be up to 96 hours.
11. Enter a comment describing the trace in the **Notes** field.

    Note: Entering a value in the **Notes** field is optional.

Edit

The **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces -> [Edit]** screen is used to edit a trace.

Note: If a trace is "Active", it cannot be edited.

The fields are described in *Traces Elements*.

1. Select **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces**.
2. Click **Edit**.

   The **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces -> [Edit]** screen appears.

3. The **Content Type** field determines what **Content Values** are available.

   If the **Content Type** is set to "Non-success answers", then no other content values are available.

   If the **Content Type** is set to "Requests", then the user may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and/or Destination-Realm. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

   If the **Content Type** is set to "Answers", then the user may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

   If the **Content Type** is set to "Ad Hoc Requests", then the user may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and/or Destination-Realm. Additionally, an optional content value is available to select an AVP to be checked. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

   Note: The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

   Note: For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the "Exists" and "Does not exist" operators are allowed.

   If the **Content Type** is set to "Ad Hoc Answers", then the user may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Additionally, an optional content value is available to select an AVP to be checked. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

   Note: The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

   Note: For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the "Exists" and "Does not exist" operators are allowed.

   If the **Content Type** is set to "User Identity", then the user may select an Application-ID. The Application-ID pulldown list shows a pre-defined list of supported Diameter interfaces, although the user cannot add anything new to the list.

Note: After an Application-ID is selected, the user can specify a user in the associate AVP as the criteria for selecting messages, which is identified by either IMSI or MSISDN.

If the **Content Type** is set to "Equipment Identity", then the user may select an Application-ID. The Application-ID pulldown list shows a pre-defined list of supported Diameter interfaces, although the user cannot add anything new to the list.

Note: After an Application-ID is selected, the user can specify equipment in the associated AVP as the criteria for selecting messages, which is identified by IMEI.

For a list of supported Diameter interfaces, refer to *Supported Diameter Interfaces*.

4. Select a Scope Type from the **Scope Type** pulldown list.

   The scope for a trace can be for a specific **Connection**, specified **Peers**, specified **DSR Applications**, or **All** messages.

5. Select a Scope Value from the **Scope Value** pulldown list
   The scope value is determined by which Scope Type is selected.
6. Enter a number of matches for the trace to find in the **Number of Matches** field.

   Note: A maximum of 1000 matches is permitted.

7. Enter a duration time for the trace in the **Time of Duration** field.
   The duration can be up to 96 hours.
8. Edit the comment in the **Notes** field.

   Note: Editing the **Notes** field is optional.

Delete

The **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces** screen allows a trace to be deleted.

Note: If a trace is "Active", it cannot be deleted.

The fields are described in *Traces Elements*.

1. Select **Diameter -> Troubleshooting with IDIH -> Configuration -> Traces** .
2. Select the trace to be deleted.
3. Click on **Delete**.

   A confirmation pop up window appears.

4. Perform one of these actions:
   - Click **OK** - the trace will be deleted.
   - Click **Cancel** - to return to the previous screen without deleting the trace.

IDIH Traces Maintenance on DSR

Once a trace is created, it appears on the **Diameter > Troubleshooting with IDIH > Maintenance > Traces** GUI screen on the SOAM server.

The user can filter the list of entries to display only the desired entries, as well as sort the list entries in ascending or descending order by clicking on a column heading.

A trace begins with a Network Operational Status and a Site Operational Status of "Inactive". Over the course of a trace's existence, the Network Operational Status may display a value of Inactive, Active, Completed, or "None", depending on what action is occurring. The Site Operational Status displays a value of Inactive, Active, Impaired, or Completed

To start a trace, select a trace in the list and click the **Start** button. Once a trace is started, its Status changes to "Active." While a trace is "Active", the Number of Matches, Matches Remaining, and Time Remaining will be displayed.

Note: To start multiple traces at once, hold **CTRL**, select the desired entries, and click the **Start** button. Only up to 8 traces may be "Active" at once (a combination of Network and Site traces depending on the settings configured on the **Diameter > Troubleshooting with IDIH > Configuration > Global Options** GUI screen).

If desired, the user can select a trace in the list and click the **Stop** button to stop it from running. To stop multiple traces at once, hold **CTRL**, select the desired traces, and click the **Stop** button.

If a problem occurs while the trace is running (due to trace limiting or trace throttling, for example), the trace will stop and its Status changes to "Impaired" and the **Impaired?** column will show as "Yes."

Depending on if a trace's status is "Active" or "Impaired", the Site Operational Reason will be:

- Inactive - a trace is not active because it is impaired
- Normal - a trace is running normally
- Disabled on Some MPs - a trace has been disabled on some MPs
- Disabled on All MPs (network traces only)
- Throttled

  Note: This state can occur for 2 reasons:

  - The IDIH has exceed the max bandwidth configured in *Options Elements*
  - An abatement threshold is reached

- DSR-IDIH Connection Down on Some MPs - the connection between DSR and IDIH is down on some MPs
- Manually Stopped - a running trace was stopped by the user
- Match Limit Reached - the limit on the number of matches configured in *Traces Elements* has been reached
- Time Limit Reached - the duration time configured in *Traces Elements* has been reached.
- DA MP Restarted - used only for the case where a trace is stopped due to an MP restarting or a DSR/IDIH connection status change
- Activation Failed on Some MPs

When a trace is finished running, the Status changes to "Completed."

Note: The maximum allowed number of "Completed" traces is 1000. Once over that number, no more traces can be activated and the trace list must be cleaned up.

The **Start/Stop Time** column for Active traces shows the time that the trace was started. For Completed traces, it shows the time that the trace was stopped.

The **Notes** column displays additional user-contributed information about a trace being run.

The **Action** column allows the user to select the **Analyze with IDIH** link.

If the user clicks the **Analyze with IDIH** link associated with a particular trace, a more detailed analysis of that trace opens in the ProTrace Application. Refer to the *ProTrace User's Guide* fo further information.

Note: When using **Analyze with IDIH**, the user is able to access IDIH using single sign-on. If single sign-on is unavailable, the user may use the "idihtrace" user ID to access IDIH. See *Accessing IDIH from DSR* for further information about the "idihtrace" user.

Note: Only up to 6 active traces may be analyzed at once.

If the user clicks the **Launch IDIH** button, a historical list of all available traces on IDIH will open.

The user can delete a trace in the list by clicking the **Delete** button.

Note: If a trace is "Active", it cannot be deleted.

The user can also check the **Pause Updates** box to prevent the **Maintenance > Traces** screen from automatically refreshing.

Accessing IDIH from DSR

Users will be able to access IDIH using single sign-on which does not require the user to login again for IDIH, provided a primary DNS server is being used in conjunction with IDIH. However, using this mechanism, users will be able to access only the ProTrace application.

Note: Single sign-on must be configured prior to accessing IDIH from DSR. For information about how to configure single sign-on, refer to the *Operations, Administration, and Maintenance (OAM) User's Guide*.

To log into IDIH from DSR SOAM GUI:

1. Using a Web browser, type the **FQDN** for a DSR SOAM.
2. Log into the SOAM by entering the correct **User Name** and the corresponding **Password**.

   Note: Check with the system administrator for the user name and password.
3. Navigate to **Diameter** > **Troubleshooting with IDIH** > **Maintenance** > **Traces**.
4. Click the **Launch IDIH** button.
5. Alternatively, select a trace and click **Analyze With IDIH**.

In the absence of a DNS server, the user may authenticate directly on the IDIH server using the "idihtrace" user ID. This user ID provides the same level of functionality as using single sign-on from the SOAM.

The procedure for accessing IDIH with the "idihtrace" user ID is almost the same as for signing in using single sign-on with the exception of replacing **FQDN** with **IP Address** in the above procedure.

IDIH Access Control

Access to IDIH can be permitted or restricted based on settings found on the NOAM **Main Menu > Administration > Access Control > Groups** screen.

For further information about how to modify these settings, refer to the *Operations, Administration, and Maintenance (OAM) User's Guide*.

Chapter 3

Trace Analysis

Topics:

This chapter provides information about functionality that will be used within IDIH to analyze traces.

ProTrace

ProTrace is the tool that is used to view traces that have been configured on DSR.

The main screen contains two areas - Trace List Panel and Query List Panel.

Trace List Panel

With the ProTrace application, the trace list shows all traces configured by DSR; the list can also be filtered

The traces list contains 6 columns. Most of the column headings can be used to sort the displayed sessions list by clicking on the heading. Click once to sort in ascending order and again to sort in descending order for that column.

The column headings are:

- Trace Name - trace name
- Status - the completion status of the trace, which can be either "In-Progress" or "Completed".
- Type - the type of trace, which is either "Site" or "Network" based on trace records details and can be filtered
- Start Time - the start date and time for the trace
- Stop Time - the end date and time of the trace
- TTR Count - the number of messages matched in a particular trace

Alarm Status Indicator

When logged in to IDIH, either directly or from DSR launch, the portal header displays a count of current alams, as shown in *Figure 2: Alarm Status indicator*. The alarm status indicator is a count of the highest severity of all open alarms and the alarm status indicator (circle) is the color (user defined, idihadmin) of the highest severity. For example, if there are zero critical, two major, one minor, and three warnings, then the alarm status indicator contains 2+ and the color is the user-defined color for major severity. The + is used to indicate that there are additional alarms at a lesser severity. The + does not appear if, for example, there are zero critical, two major, zero minor, and zero warnings.

Initially, the alarm status is empty (non-visible). Then, after a short interval, the system queries for open alarms and updates the alarm status indicator. After the first update, the system updates the alarm status indicator every 30 seconds.

Figure 2: Alarm Status indicator

Selecting the alarm status indicator shows a brief description of the open alarms. The system displays the list of open alarms in tabular form, as shown in *Figure 3: Alarm List*. This list can be dismissed by pressing the Close button on the Open Alarm dialog window.

Note: Only open alarms may be viewed. No other actions are provided such as clear, acknowledge, etc.

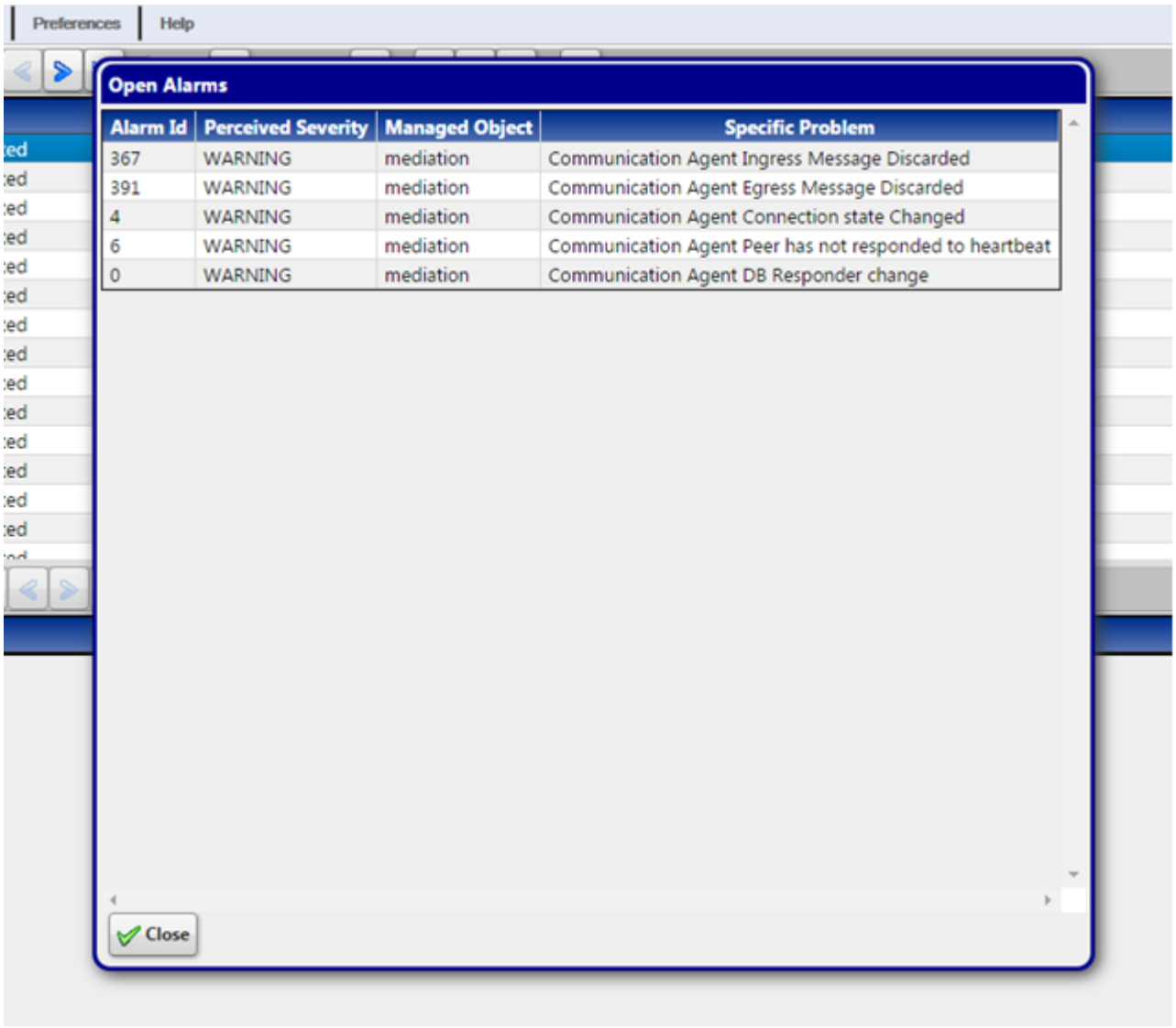

Figure 3: Alarm List

Trace List Toolbar

The toolbar provides a means of selecting and organizing traces. Below is a description of each button on the toolbar.

Figure 4: Trace List Toolbar

Filter - clicking this button opens the **System Query Dialog** popup where the user can filter the list of sessions displayed by the various columns and their values.

First page - clicking this button opens the first page of sessions.

Previous page - clicking this button opens the previous page of sessions.

Next page - clicking this button opens the next page of sessions.

Last page - clicking this button opens the last page of sessions.

Set Size - use this button to set the number of selected trace records / total trace records displayed from 10-500 per page.

Refresh - clicking this button re-loads the current screen and shows any changes that have been made.

Delete - clicking this button deletes a selected trace.

Obtain Trace Conditions - clicking this button opens a popup window that provides additional details about a selected trace.

Obtain Trace Info - clicking this button displays a popup dialog displaying trace information for the selected row from the Trace List page. The information displayed includes the summary information for the selected trace, and all the Network IDIH sites and their counts for the selected trace

Run Default Query - clicking this button runs a query on the selected trace in the list and provides a detailed analysis for those traces.

In addition to these buttons, there is also a saved filters pull-down to select a saved filter, and a page count showing what page out of the total sessions pages being viewed.

Query List Panel

The Query List panel contains list of queries the user can execute on the selected trace. These queries are user's saved queries or queries shared by other users. The list has a toolbar where the user can quickly invoke operation on a selected query. It includes:

- Creating a new query
- Modifying selected query
- Deleting selected query
- Executing selected query

When the user selects a trace in Trace List panel, the queries in Query List is reloaded. Only queries which are "compatible" with selected trace are show.

The Query List panel table contains four columns. The table queries change depending on what view is selected based on which trace is selected, but the columns are constant. The column headings can be used to sort the list by clicking on the heading. Click once to sort in ascending order and again to sort in descending order for that column.

The column headings are:

- Query Name - that shows the name of the query
- Query Description - shows a description of a given query
- Owner - shows the user name that created the query
- Created - shows the date the query was created

Query List Toolbar

The toolbar provides a means of selecting and organizing queries. Below is a description of each button on the toolbar.

Figure 5: Query List Toolbar

Filter - clicking this button opens the **System Query Dialog** page where you can filter out all non-essential queries.

First page - clicking this button opens the first page of queries.

Previous page - clicking this button opens the previous page of queries.

Next page - clicking this button opens the next page of queries.

Last page - clicking this button opens the last page of queries.

Set Size - use this button to set the queries list size from 10-500 per page

Refresh - clicking this button re-loads the current screen and shows any changes that have been made.

Create New Query - clicking this button opens the Query Dialogue screen to add a specific query.

Modify Selected Query - clicking this button opens the current query for modification.

Delete Selected Query - clicking this button deletes the current query.

Run Selected Query - clicking this button runs a query of the selected trace in the list and provides a detailed analysis for the selected trace.

Note: The user can only view/operate on a single trace at a time.

Change Begin/End Time for the Query - clicking this button opens the **Query Settings** page where the user can modify the begin and end dates and times for a given query.

In addition to these buttons there is also a queries count showing how many queries are in the list and what range you are viewing.

Creating or Modifying a Query

To create a new query or modify existing query, click the **Create New Query** or **Modify Selected Query**. The Query Dialog box opens.

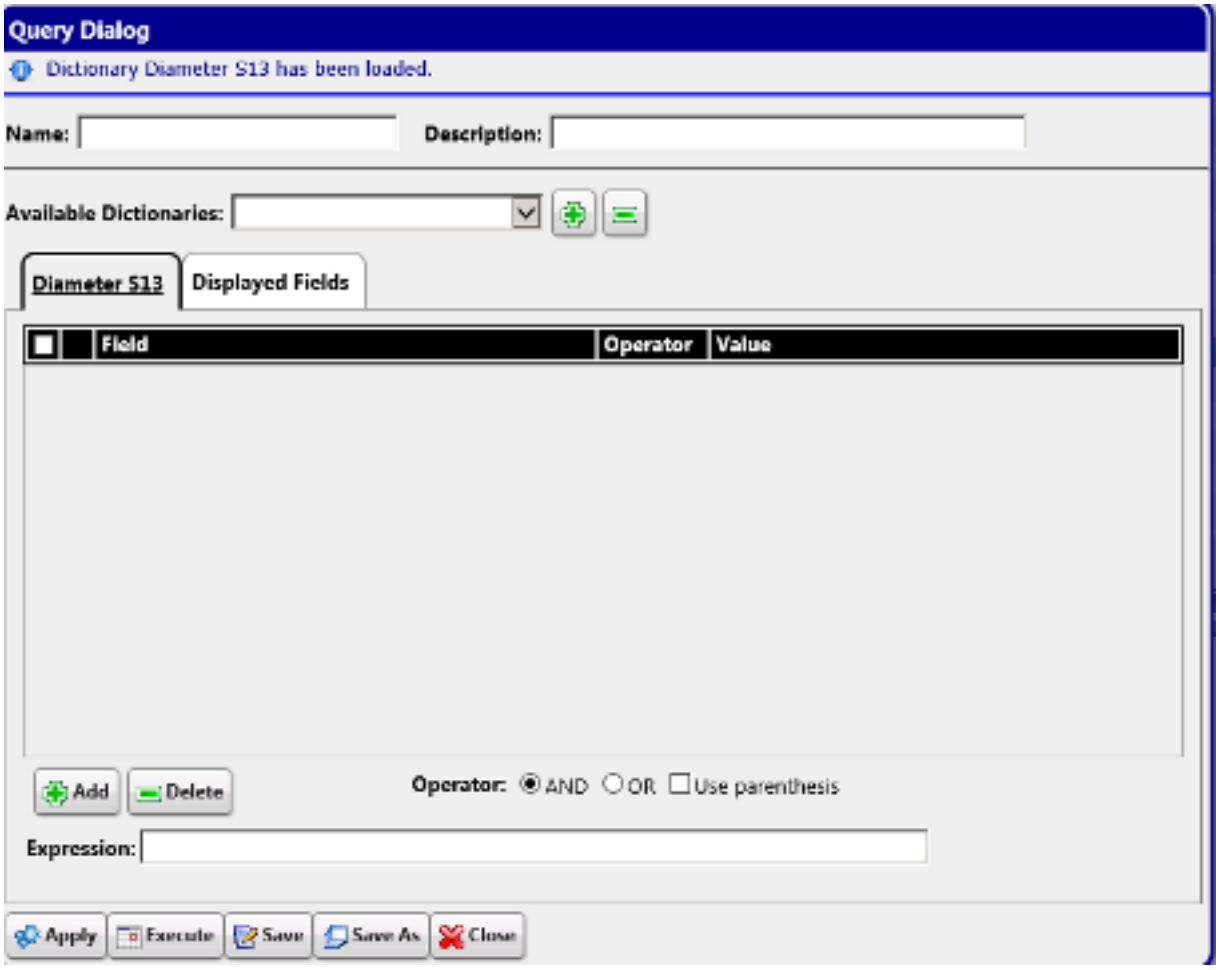

Figure 6: Query Dialog

The query must have at least one dictionary. To add a dictionary, select a dictionary from the **Available Dictionaries** pulldown list and click the **(+)** button. To remove a dictionary, click the **(-)** button.

Once the dictionary has been added to the query, the conditions can be added using the **Add** button. The query can have no conditions, otherwise the query will match all Transaction Detail Records (TDRs) for a given dictionary. Each dictionary has its own conditions, making it possible to search for TDRs from different dictionaries with different conditions.

When adding a condition, the corresponding label is added into the **Expression** field. It is added to the end of the expression with the selected **Operator** (AND or OR). Similarly, when the condition is removed from the query, the corresponding label is automatically removed from the expression and the expression is adjusted. When **Use Bracket** is selected, then the whole expression is closed in brackets before adding the new condition.

Note: The user can edit the expression to be more complex such as "(A AND B) or C"

The query is validated before it is saved or executed. The following things are verified:

- Name is filled (verified for Save operation only, for Query Execution operation the name can be empty)

- All conditions have correct operator and correct value (an empty value is not allowed and it must correspond to field type)

  Note: The user can also use wild cards in the value field. To see descriptions of these wild cards, hover on the most right-hand "?" in the query dialog after selecting a field.

- Expression is well formed Boolean expression

Whenever any error occurs, the user is notified either in the Message Panel at the top of the Dialog box or next to the GUI element which caused the error (a condition or expression box).

Note: For filtering on source and destination node fields, provide either the IP address or select the node name from the list. Selecting the node name means filtering on the list of IP addresses assigned to the selected node. If the same IP Address is being reused across the nodes, filtered data would display other nodes as well.

By default, when a dictionary is added into the query, all displayable fields from that dictionary are selected as Displayed Fields. If desired, change the Display Fields in the **Displayed Fields** tab. There are 3 modes to choose from:

1. All fields (all fields are added into Displayed Fields)
2. Common (all common fields from all dictionaries are selected; if there is just one dictionary then all fields are selected)
3. Custom fields (the user can select fields of his/her choice)

The Displayed Fields are selected separately per dictionary. If there is more than one dictionary, then fields in the query result are merged together based on the field name. All fields with the same name are displayed in the same column.

Click **Save** to save a query for later use. The query appears in the Query List panel.

Click **Save As** to open a prompt asking for a new name. Confirms the name. A new query is created and saved for later use. The query appears in the Query List panel.

Now the query is ready for execution. Execute the query by clicking the **Apply** button.

Executing a Query

When a query is executed, it is always executed on the currently selected trace from the Trace List panel and Trace Viewer is displayed. A query can be executed in multiple ways:

1. By clicking the **Apply** button from the **Query Dialog** window (when creating or modifying a query)
2. By clicking the **Run Default Query** icon on the Trace List toolbar
3. By selecting the query in Query List panel and clicking the **Run Selected Query** icon in the Query List toolbar

Enter the time in which the search is about to be performed. The Begin and End time are pre-populated with the real begin and end date of the selected trace. Click on the icons next to the date and time text boxes and select the date in calendar and time in time selection widgets for better convenience.

By selecting the **Execute in New** button, the Trace Viewer is shown in a new browser window and the query is executed.

Trace Viewer

The Trace Viewer is displayed when the user executes a trace and contains the TDRs for the trace for the user to analyze.

The Trace Viewer is divided into three panels:

- TDRs List Panel
- Event List Panel (Event List or Event Diagram)
- Diameter Full Decoding Panel

ProTrace allows the user to organize the panels in 6 different layouts (positions of each panel). Some layouts contain only some panels. Each layout is depicted by an icon which shows how the panels are organized. For information about how to change the layour, refer to *Changing the Page Layout*.

TDR Panel

The TDR panel contains list of transactions (TDRs) that matched a given query. If the query does not have any conditions, then the panel will include all TDRs captured for the selected trace and for interfaces selected by the query. The TDRs belonging to the same TTR are displayed next to each other with the same background color. The fields displayed in the result are defined in Query display fields. The result is divided into pages (the user can define the page size) and the user can navigate through the pages (first page, previous and next page).

The user is also able to perform the following actions:

- Use navigation buttons to go to first, previous or next page
- Reverse sorting (Ascending, descending)
- Set the page size (number of records per page) for TDR table
- Get the number of records which match the current query
- Display statistics of the current trace
- Modify the query and re-execute it to refine the transactions
- Export a file that contains a summary of TDR records, an event diagram, a list of TTR events, and a full decoding panel for every Diameter payload message. There are multiple formats in which the file may be exported:
  - Export TTR as HTML - exports the file from the currently selected TTR in an HTML format
  - Export TTR as PCAP - exports the file from the currently selected TTR in a PCAP format that is directly downloaded to the user's ▶server◀ without a progress bar or a way to cancel the export
  - Export trace as PCAP - exports the contents of a trace into a PCAP format that is directly downloaded to the user's ▶server◀, indicated by a progress bar that also allows the user to cancel the export. If the export is cancelled, ProTrace exports all information that was downloaded prior to the cancellation.

    Note: ProTrace exports payload data in IPv4 or IPv6 based on the original transport type. TCP or SCTP transport is used in the export based on the original transport type. Source IP, source port, destination IP and destination port from the payload are used. When the payload size exceeds the maximum of TCP/SCTP packet size, the payload is segmented into multiple IP packets so that 3rd party tools can assemble and present it as a single diameter payload.

Note: Payloads sent from DSR to IDIH contain Diameter layer only (no IP or TCP/SCTP layers). Therefore, IDIH makes a best effort to simulate those layers when constructing the PCAP file for export. Trace export will export up to 20-25 MB of payload data. The rest of the payloads will be ignored. The user can refine the query to accommodate all the payloads the user wants to export and re-export it again. When TLS or DTLS is used as the transport the export will display TCP for TLS and SCTP for DTLS as the Transport value.

- Change the layout of the panels

The TDR list for a network trace highlights all TDRs that are related in the same fashion as highlighting is for site TDRs. All related TDRs are grouped and highlighted (white or blue), regardless if the TDRs are from a network trace or site trace. When TLS or DTLS is used as the transport, ProTrace will display these two protocols in the Transport column.

TDR Panel Toolbar

The function buttons on the TDRs list toolbar are as follows:

Figure 7: TDRs List Toolbar

First page - clicking this button opens the first page of queries

Previous page - clicking this button opens the previous page of queries.

Next page - clicking this button opens the next page of queries.

Reverse Sorting - clicking this button reverses the sort order of the xDR list.

Set Size - this shows how many TDRs are displayed per page, the user can modify the number of TDRs on the page by typing in another number and clicking the **check** to the right. The user can set the page size from 10 to 5000 TDRs per page. A larger page size will take longer to display.

Pause refresh - stops automatic refresh so that you can work on filters or records without data changing.

Go Back to Trace List - returns to the Trace List

Show Statistics - opens the **Trace Statistics** window and shows statistics associated with the selected trace. See *IDIH Trace Statistics* for further information.

Modify Query - opens the **Query dialog** screen of an existing query.

Note: A user can also add conditions to a query by right clicking an individual cell in the TDRs List and clicking **Add to Conditions**. These new conditions are added to the current query and are not applied until the icon is used to apply the changed query.

Change Begin/End time for the Query - allows the user to change the time a query begins or ends

TTR Export - exports the TTR results. These results are exported in HTML format.

Search - searches for specific TDR records.

Search next - continues search of TDR records.

Change layout - enables you to change the page layout using a variety of combinations. See *Changing the Page Layout* for further information.

Selected Trace - Shows the name of the Trace currently being analyzed

Query selected - placing the cursor over on this icon opens a small information pop-up showing the name, description, and network information of the query being run. This information is useful because it confirms the user is looking at the correct trace

TDR List Retrieval

Network traces require TDR data to be retrieved from multiple sites and may take longer to process based on the number of sites, network latency, etc. When retrieving network trace results from the **Analyze with IDIH** function on the DSR GUI or from the main ProTrace page and the trace is a network trace, then ProTrace displays a progress dialog, which displays the following information as shown in *Figure 8: TDR List Retrieval*:

- Time Period
- Progress bar
- Network result status - x out of y processed, where x is the current number of processes and y is the total
- Network Table with individual IDIH site information (Name, address, and status)
- **Cancel** Button

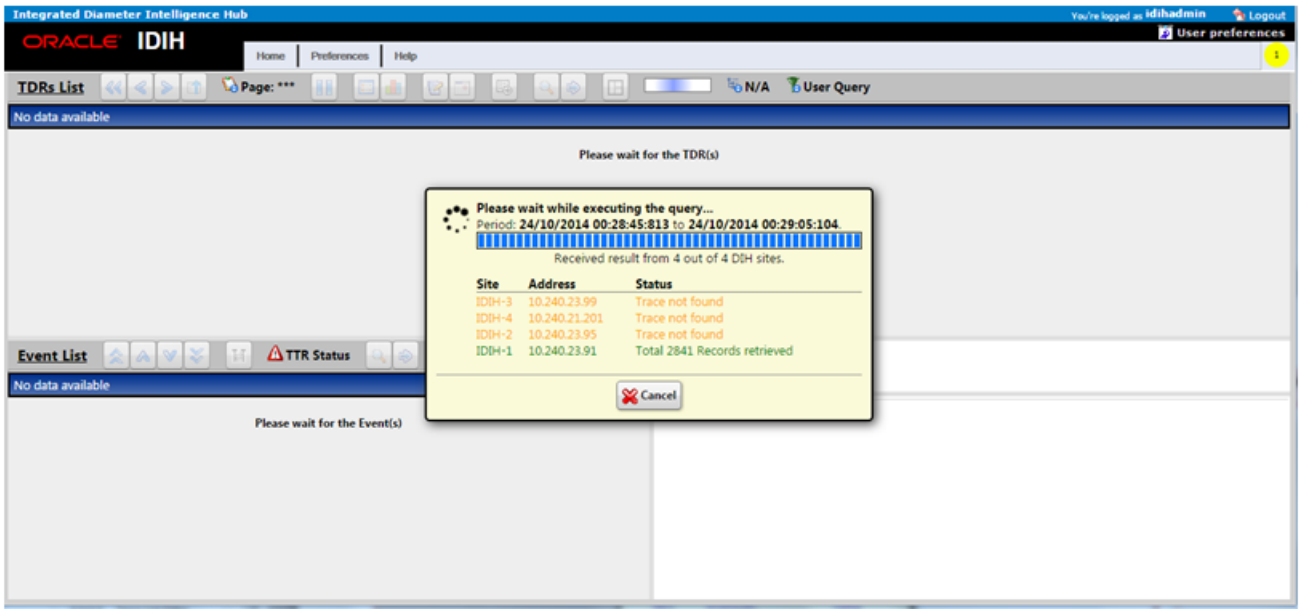

Figure 8: TDR List Retrieval

Message Copy

When the TTR was copied during the Message Copy feature to DAS, it is indicated in the TDR. The TDR contains two fields which have references to either the copied TTR or to the original TTR. The fields are called **LinkedTTR** and **CorrelationID**. If these references exist in the TDR (these fields are not empty), then the TDR is highlighted with a different text color.

When the user right clicks on a TDR, a popup menu is displayed and the user can select **Search Message Copy**.

When the user selects **Search Message Copy**, a new query is created and executed. The query populates the Trace Viewer with TDRs that have the same **LinkedTTR** or **CorrelationID** values as the original TDR that was used to start the search.

When the original Answer message appears in the copied message, it is included in the group AVP with code 2156 and vendor ID 323. This AVP appears in the Full Decoding Panel as "MSG-Copy-Answer".

In the original TTR, apart from standard events, two new events will appear if a message is copied - "Message Copy Triggered" and "Message Copied". Depending on where the trigger point is set, there may be up to 4 "Message Copy Triggered" events. These events will have the scope set as "IR Data". "Message Copied" events will have the scope set as "IA Data". Each "Message Copy Triggered" event will have Message Copy Configuration Set name (MCCS) as its instance data, as well as where the Message Copy was triggered.

A copied TTR will start with a new Event "Copied Message". The "Copied Message" event's scope will be "IG" (Internally Generated). MCCS will be used as the instance data. MCCS will result in selecting the route list and subsequently the route group. These standard events will be seen, but their scope will be "IG Data".

TTR Events Panel

The TTR Event Panel displays a list of all TTR events associated with the selected transaction (TDR). Whenever the user selects a TDR in the TDR Panel, the TTR Event Panel is refreshed with the corresponding TTR events. The Event table has the following columns:

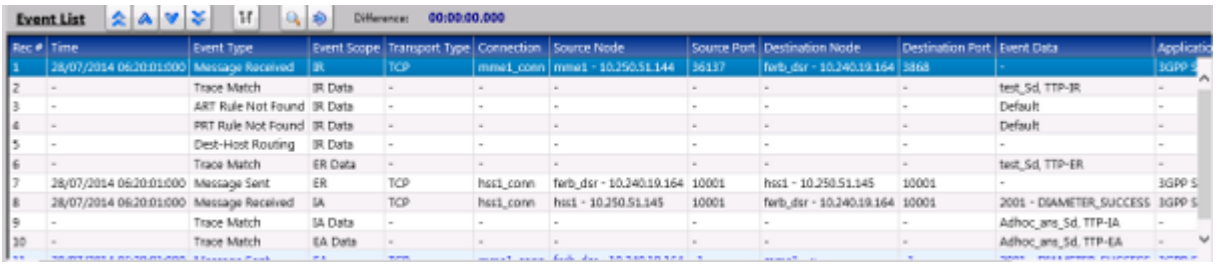

Figure 9: Event List Panel

the user can also click **Toggle Ladder Diagram** to view events in an Event Diagram.

- **Time** (the column is populated for payload events only. It contains the time when the message was received or sent)
- **Event Type** and **Event Scope**

Event Type	Event Scope
Message Received	IR (Ingress Request), IA (Ingress Answer)
Message Sent	ER (Egress Request), EA (Egress Answer)
Message Created	App Data (Application Data)
App Invoked	App (Application)
App Result	App Data
App Invocation Failed	IR Data, IA Data

Event Type	Event Scope
Trace Match	IR Data, ER Data, IA Data, EA Data
Linked TTR	
ART Rule Match	IR Data
PRT Rule Match	IR Data
Unavailability Action	IR Data, IA Data
Route List Selected	IR Data
Dest-Host Routing	IR Data
Alternate Implicit Routing	IR Data
Route Group Selected	IR Data
Mediation Rule Match	IR Data, IA Data, ER Data, EA Data
Request Rerouted	IR Data
Answer Timeout	IA
Answer Matching Failed	IA Data
Address Resolution Match	App Data
Routing Exception	App Data
DP Query Sent	App Data
DP Response Received	App Data
DP Query Failure	App Data
DP Response Timeout	App Data
SBR Query Sent	App Data
SBR Response Received	App Data
SBR Query Failure	App Data
SBR Response Timeout	App Data

- **Transport Type** ("TCP" or "SCTP" for payload events only)
- **Connection Id** (The name of the connection defined in DSR)
- **Source Node** ("<Node name> - <IP address>" for payload events; IP is translated and node name is displayed if there is a record in Local Node or Peer Node reference data at DSR for the given IP address)
- **Source Port** (TCP/STCP IP port number for payload events)
- **Destination Node** ("<Node name> - <IP address>" for payload events; IP is translated and node name is displayed if there is a record in Local Node or Peer Node reference data at DSR for the given IP address)
- **Destination Port** (TCP/STCP IP port number for payload events)

- **Event Data** (Event data from TTR event; Event Data for Answer payload events contains the result code from ResultCode AVP (code 268) or ExperimentalResultCode AVP (code 298) in the form of "<Error Code> - <Error description>")
- **Application** (Diameter Application for payload events, empty for the rest)
- **Command Code** (Diameter message command code in form of "<Short name> - <Long name>" for payload events)
- **DSR-DSR** (If the Diameter message transpired between two DSR nodes, then the column shows a "YES" value. If the message transpired between one DSR node and either a client (e.g. MME) or server (e.g. HSS), then the column shows a "NO" value. This value is required for N-IDIH to create a correct ladder diagram from the event list)

Ladder Diagram

The Ladder Diagram shows the TTR events in graphical form. It is just another form of information shown in TTR Event panel. Additionally, ProTrace will process and display “Client Redirect” events when received.

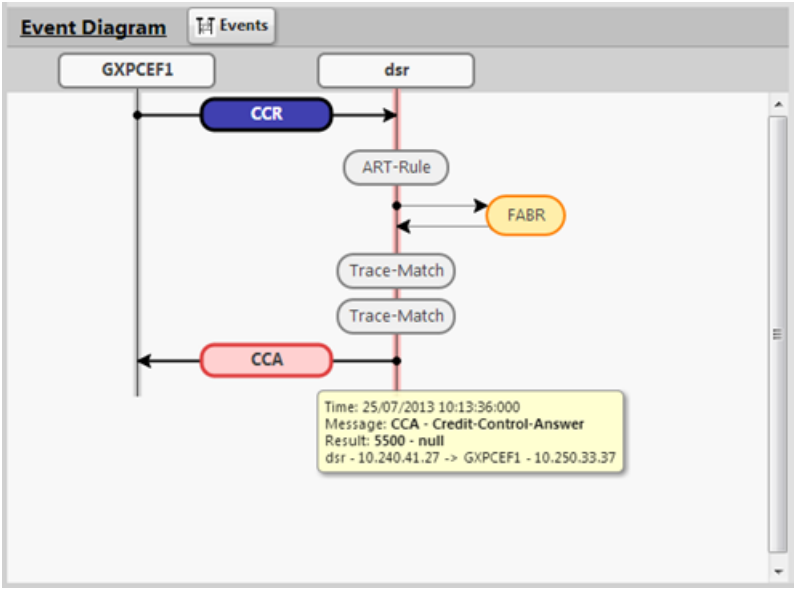

Figure 10: Ladder Diagram

The user can hover or click on a bubble of the ladder diagram which may show information about that particular bubble in the Diameter Full Decoding Panel.

The user can also click **Toggle Event Table** to view events in tabular form, which also allows for a selected row to appear in the Diameter Full Decoding Panel.

Table 5: Ladder Diagram Visualization defines how the TTR events are visualized in the ladder diagram:

Table 5: Ladder Diagram Visualization

Event Type	Event Scope	Event Diagram Visualization	Title	Tooltip
Request Message Sent/Received	IR, ER	Blue bubble with arrow from source node to destination node	Command Code short name (for example ULR for Update Location Request)	Time, Command Code
Answer Message Sent or Received with Success Result Code (RC< 3000)	IA, EA	Green bubble with arrow from source node to destination node	Command Code short name (for example ULA for Update Location Answer).	Time, Command Code, Result
Answer Message Sent or Received with Success Result Code (RC >= 3000)	IA, EA	Red bubble with arrow from source node to destination node	Command Code short name (for example ULA for Update Location Answer)	Time, Command Code, Result
Message Created	App Data	Gray bubble on DSR node	"Message-Created"	
App Invoked	App	Orange bubble next to DSR node with arrows from DSR to and from Application bubble	"<Name>" from Event Data	"Application: <Name>" (Event Data)
App Result	App Data	App Result appends a text to the corresponding Application's tooltip		"Result: <Event Data>" appended in previous Application's (App Invoked) tooltip
App Invocation Failed	IR Data, IA Data	App Invocation Failed makes the corresponding Application bubble red and appends text to its tooltip.		Appends "Invocation Failed: <Event Data>" red text in previous Application's tooltip
Trace Match	IR Data, ER Data, IA Data, EA Data	Gray bubble on DSR node	"Trace-Match"	"Matched Trace: <Event Data>"
Linked TTR		No visualization		
ART Rule Match	IR Data	Gray bubble on DSR node	"ART-Rule"	"ART Rule: <Event Data>"

Event Type	Event Scope	Event Diagram Visualization	Title	Tooltip
PRT Rule Match	IR Data	Gray bubble on DSR node	"PRT-Rule"	"PRT Rule: <Event Data>"
Unavailability Action	IR Data, IA Data	Unavailability Action makes the previous event bubble red.		Appends "Unavailability Action" red text in the previous bubble's tooltip
Route List Selected	IR Data	Gray bubble on DSR node	"Route-List"	"Selected List: <Event Data>"
Dest-Host Routing	IR Data	Gray bubble on DSR node	"Dest-Host-Routing"	
Alternate Implicit Routing		Alternate Implicit Routing makes previous metadata bubble red and appends a text in its tooltip.		Appends "Alternate Implicit Routing" red text in the previous metadata bubble's tooltip
Route Group Selected	IR Data	Gray bubble on DSR node	"Route-Group"	"Route Group: <Event Data>">" (Event Data contains group name)
Mediation Rule Match	IR Data, ER Data, IA Data, EA Data	Gray bubble on DSR node	"Mediation-Rule"	"Matched Rule: <Event Data>" (Event Data contains rule name)
Request Rerouted	IR Data	Gray bubble on DSR node	"REQ-Rerouted"	"Attempts: #<Event Data>" (Event Data contains attempt #)
Answer Timeout	IA	Arrow from source node to destination node	"Answer Timeout"	No tooltip
Answer Matching Failed	IA Data	Red bubble on DSR node	"ANS-Match-Failed"	
Address Resolution Match	App Data	Address Resolution Match appends a text to the corresponding Application bubble.		"Address Resolution: <Event Data>" (Event Data formatted as a list)
Routing Exception	App Data	Routing Exception appends a text to the corresponding Application bubble.		"Routing Exception: <Event Data>"

Event Type	Event Scope	Event Diagram Visualization	Title	Tooltip
DP Query Sent	App Data	DP Query Sent appends a text to the corresponding Application bubble.		"DP Query Sent: <Event Data>" (Event Data formatted as a list)
DP Response Received	App Data	DP Response Received appends a text to the corresponding Application bubble.		"DP Response Received: <Event Data>" (Event Data formatted as a list)
DP Query Failure	App Data	DP Query Failure appends a text to the corresponding Application bubble.		Appends red text "DP Query Failure: <Event Data>"(Event Data formatted as a list)
DP Response Timeout	App Data	DP Response Timeout appends a text to the corresponding Application bubble.		Appends red text "DP Response Timeout: <Event Data>"(Event Data formatted as a list)
SBR Query Sent	App Data	SBR Query Sent appends a text to the corresponding Application bubble.		"SBR Query Sent: <Event Data>" (Event Data formatted as a list)
SBR Response Received	App Data	SBR Response Received appends a text to the corresponding Application bubble.		"SBR Response Received: <Event Data>" (Event Data formatted as a list)
SBR Query Failure	App Data	SBR Query Failure appends a text to the corresponding Application bubble.		Appends red text "SBR Query Failure: <Event Data>" (Event Data formatted as a list)
SBR Response Timeout	App Data	SBR Response Timeout appends a text to the corresponding Application bubble.		Appends red text "SBR Response Timeout: <Event Data>" (Event Data formatted as a list)
Message Copied	IA	MSG-Copied bubble appears on DSR node	"MSG-Copied"	No tooltip
Copied Message	IG (Internally Generated)	Copied-MSG bubble appears on DSR node	"Copied-MSG"	Copied Message ID appears in the tooltip

Event Type	Event Scope	Event Diagram Visualization	Title	Tooltip
Message Copy Triggered	IR, ER	MC-Triggered bubble appears on DSR node	"MC-Triggered"	No tooltip
Request Redirected	IR Data	Gray bubble on DSR node	"REQ-Redirected"	"Attempts: #<Event Data>" (Event Data contains attempt #)

Diameter Full Decoding Panel

When the user selects a payload event in the Events Panel or a balloon from the Event Diagram, the corresponding message is displayed fully decoded in the Full Decoding Panel. This view explains every byte of the selected diameter message.

The Diameter Full Decoding Panel is further divided into two panels. The first panel shows the payload bytes of the messages. The second panel displays the Diameter Message Header and all AVPs decoded into a readable format. It shows every field of the header and AVP as defined by the Diameter RFC. Each field of the message header and AVP is displayed on separate lines.

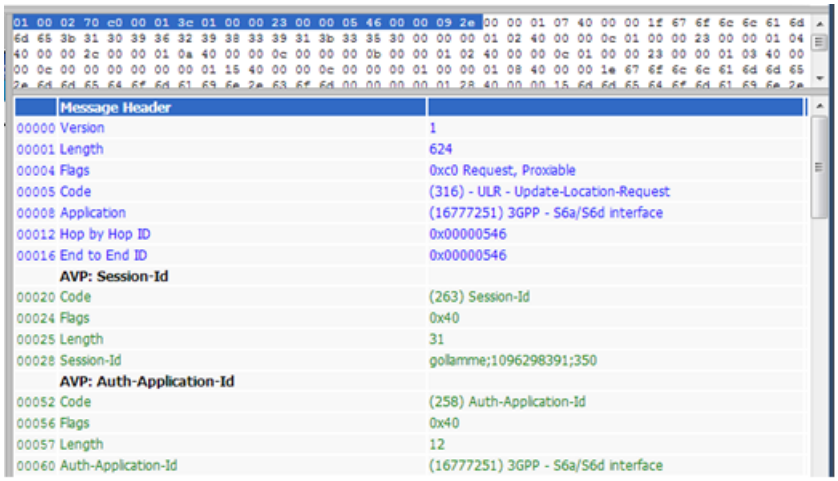

Figure 11: Diameter Full Decoding Panel

The detailed decoding list has the following columns:

- **Offset** (An offset address of the field from the beginning of the diameter payload. Version field of Diameter Message Header has offset 0)
- **AVP / Field Name**
- **Value and description** (Value and possible description)

Table 6: Diameter Full Decoding Panel

AVP Type	Display
Integer32/Unsigned32	Numeric value

AVP Type	Display
Integer64/Unsigned64	
Enumerated	Numeric value + description of the value if known
Grouped	Names of all child AVPs
UTF8String	UTF string from the bytes
OctetString	If all bytes are displayable (codes are from 32 to 128 ASCII) then it is displayed as UTF string, otherwise the hex decode is displayed
IPAddress	D.D.D.D or XXXX:XXXX:…:XXXX:XXXX depending on IP version (IPv4 or IPv6) (where D is decimal digit and X hexadecimal digit)
AppId	Application Id and Name if known
VendorId	Vendor Id and Name if known

Custom AVPs, Commands, and Vendors

The user can add custom AVPs, commands and vendors through an XML configuration file called diameter dictionary file. The Diameter decoder component, which is responsible for diameter message/AVP decoding, will look at its start-up at the specific location (at the Application server itself) and if it finds the dictionary file there, it will use it to decode diameter messages.

If a change is made to this dictionary file, the application server must be restarted to pick-up the changes.

The custom diameter dictionary file must be valid XML file, which contains one single root element called "dictionary." All other tags defining custom commands, vendors and AVP must be included inside of this tag.

Adding Custom AVPs

Simple AVP Tag Format

The following format must be used to define new custom AVP:

```
 <avp name="<avpName>"
display="<displayText>"
[vendor-id="<vendorId>"]
code="<code>"
type="<type>"/>
```

where

- **avpName** must be unique AVP identifier in the dictionary file, if the vendorId is present then the name should be preceded by vendor-id (see the example below)
- **vendorId** is optional and if present then must be either defined in the custom dictionary file, or must be one of the predefined ones
- **type** must be one of the following predefined types:

- OctetString
- Integer32, Unsigned32, Integer64, Unsigned64
- UTFString
- IPAddress
- TBCD

Example:

```
<avp name = "3GPP:3GPP-IMSI"
display="3GPP-IMSI"
code="1"
vendor-id="3GPP"
type="UTF8String"/>
```

Enumerated AVP Tag Format

The following XML tag format must be used to define new enumerated AVP

```
:<avp name="<avpName>"
display="<displayText>"
[vendor-id="<vendorId>"]
code="<code>"
type="type">
<enumcode="<value>"
name="<enumDisplayText>">
. . .
</avp>
```

where

- **avpName** , **displayText**, **vendorId**, **code** and **type** are the same as in case of simple AVP format
- **value** is the numeric value and **enumDisplayText** is a text which is displayed in the full decoding window. If a named value is not defined, the decoder displays just simple numeric value

Example:

```
<avp name="Framed-Routing" display="Framed-Routing" code="10" type="Enumerated"
 >
        <enum code="0" name="None"/>
        <enum code="1" name="Broadcast"/>
        <enum code="2" name="Listen"/>
        <enum code="3" name="Broadcast-Listen"/>
    </avp>
```

Grouped AVP Tag Format

The following XML tag format must be used to define new custom grouped AVP:

```
<avp name="<avpName>"
display="<displayText>"
[vendor-id="<vendorId>"]
code="<code>"
type="type">
<avpref="<refAvpName>">
. . .
</avp>
```

where

- **avpName** , **displayText**, **vendorId**, **code** and **type** are the same as in case of simple AVP format
- **refAVPName** must be name of an existing AVP define in the custom dictionary

Example:

```
<avp name="3GPP:User-Identity" display="User-Identity" code="700" vendor-id="3GPP"
 type="Grouped">
        <avp ref="Public-Identity"/>
        <avp ref="3GPP:MSISDN"/>
        <avp ref="3GPP:Public-Identity"/>
    </avp>
```

Adding Custom Commands

Command Tag Format

The following XML tag format must be used to define new custom command code:

```
<command code="<code>"
short-name="<shortName>"
name="<commandName>"/>
```

where

- **code** is the command code,
- **shortName** appears in the ladder diagram events,
- **commandName** appears in the full decoding of a message

Example:

```
<command code="316"
short-name="UL"
name="Update-Location"/>
```

Adding Vendors

The following vendors are already defined and can be used without defining them again:

Vendor-Id	Vendor Code	Vendor
ER	193	Ericsson
3GPP	10415	3GPP Project
3GPP2	5535	3GPP Project
ETSI	13019	ETSI

If the new vendor needs to be added then the following tag must appear in the dictionary file:

```
<vendor vendor-id="<id>"
code="<code>"
name="<description>"/>
```

Example:

```
<vendor vendor-id="VF"
code="12645"
name="Vodafone"/>
```

Changing the Page Layout

The user can change the page layout of the TDR viewer (or Trace viewer) to re-arrange or hide the TDR, PDU, and Full Decode views. To change the layout, follow these steps.

Note: Changing the layout is persisted, so the next time TDR viewer is activated with a trace execution, the last layout used will be provided.

1. Click **Change Layout**.

   The layout pop-up opens.

2. Select a **Layout**.

   The page layout changes to match the user's choice. This will now be the default layout for this session type.

IDIH Trace Statistics

IDIH gathers statistics about Diameter transactions for active traces. The statistics have the following dimensions:

- TimeTag - end of the interval for which the record contains statistics
- TraceInstance - identifies trace to which this record belongs
- Node - IP address of the node
- DbLevel - MCL (Managed Object ChangeLevel)
- ResultCode - value of ResultCode AVP (code 268)
- ExperimentalResultCode - value of ExperimentalResultCode AVP (code 298)

and the following measures for the given matching dimension values:

- Count - total number of transactions
- Timeouts - number of time-out transactions

The statistics count the number of transactions for every combination of dimension values seen in received transactions. It counts transactions with result code only. If the TTR is missing an Answer message or the Answer message is missing a result code AVP, then the transaction is not counted.

The statistics are continuously generated and stored in an Oracle database. The complete statistics will be available up to five minutes after the trace has finished or has been stopped.

ProTrace reads the statistics and displays them to the user in the form of bar and pie charts.

- If the user double clicks on a bar, it executes a new query and displays TDRs for the clicked node and category (all, errors, success, timeouts)
- If the user double clicks a section in the pie chart, then it displays TDRs with the clicked result code for the selected node

The user can refresh the statistics presented by clicking the **Refresh Statistics** button.

The user also can return to the *TDR Panel Toolbar* by clicking the **Return to Traces** button.

Setting User Preferences on IDIH Dashboard

Once inside IDIH, a user can set User Preferences. These include:

- Time specifications (date format, time zone, etc.)
- Enumeration values (numerals vs. text)

Setting Time Format

Follow these steps to set the time format:

1. Click **User Preferences** on the Application board.
   The User Preferences screen is displayed.
2. Click the **Date/Time** tab.
   The Date/Time screen is displayed. The red asterisk denotes a required field.

   Note: Use the tips on the screen to help configure the time format.
3. Enter the format for these time-related displays.
   - **Date format**
   - **Time format**
   - **Date and time fields**
4. Select the formats for these time-related displays by using the drop-down arrow.
   - **Duration fields** - how the hours, minutes, seconds, and milliseconds of the Time format is displayed
   - **Time zone**

     Note: The local time zone must be chosen to get local time.
5. To reset the time-related displays to default settings, click **Reset**.
6. Click **Apply** to save settings.

Setting Mapping Preferences

The user can set the Mapping settings using the User Preferences feature.

Follow these steps to set Mapping preferences.

1. Click **User Preferences** in the Application board.
   The User Preferences screen is displayed.
2. Click the **Mapping** tab.
   The Mapping screen is displayed.
3. Check **Translate ENUM values** to display text instead of numerals.

Enumeration is used by TDRs to display text values instead of numeric. Rather than showing the numeral for Alarm Severity, the user interface will show the actual word, such as "Major" or "Critical."

4. Check **IP Address to Node Name** to translate an IP Address to a textual Node Name.
5. To reset the Mapping values to the default, click **Reset**.
6. Click **Apply** to save the changes.

Appendix A

IDIH Admin Privileges

Topics:

This chapter provides basic information about admin privileges that may be associated with IDIH

Idihadmin Privileges

During IDIH installation, a user called "idihadmin" will be set up that allows for additional privileges to access and configure the system beyond what is ordinarily required when using DSR.

Note: This user should only be used by administrators or support personnel.

To access the IDIH maintenance portal will be as "idihadmin:

1. Navigate to https://<ipaddress of IDIH appserver>/idih
2. Login with the "idihadmin" username and corresponding password.

Once logged in, the "idihadmin" user has additional privileges beyond what a user can do when using IDIH from the DSR SOAM GUI.

The "idihadmin" user can change the login password.

1. Open the **Change password** dialog box by clicking on the "idihadmin" user name at the top of the IDIH maintenance portal.
2. Enter the new password in the **Old Password** box and the new password twice in the **New Password** and **Confirm Password** boxes.
3. Click **Apply** to confirm the password change.

The "idihadmin" can access all of the IDIH applications including ProTrace on the IDIH Dashboard. The other IDIH applications are:

- Alarm Forwarding
- Audit Viewer
- Log Viewer
- OAM
- System Alarms

For detailed information about how to use these applications, as well as ProTrace, refer to the individual Help modules in each application.

Appendix B

IDIH Alarms

Topics:

This section provides information about alarms associated with the IDIH

IDIH Alarms, KPIs, and Measurements on DSR

This section describes how to access alarm, KPI, and measurements information that is available for IDIH in the DSR GUI. For more detailed information, refer to the *Alarms, KPIs, and Measurements Reference*.

Active alarms and events, as well as alarm and event history can be displayed on the **Alarms & Events > View Active** and **Alarms & Events > View History** GUI screens.

Key Performance Indicators, or KPIs, provide a means to convey performance information to the user in near real-time. KPIs can be displayed on the **Status & Manage > KPIs** GUI screen.

Measurements for IDIH are collected and reported in various measurement groups. A measurement report and measurement group can be associated with a one-to-one relationship. Measurement reports may be generated from the **Measurements > Report GUI** screen.

Alarms Associated with IDIH

Table 7: IDIH Alarms

2002	Mediation Server Communication Alarm	Communication with mediation subsystem failure	Communications subsystem failure
2003	DSR OAM Communication Alarm	Communication with DSR OAM failure	Communications subsystem failure
4000	ImpParser - Application data queue utilization	The percent utilization of the thread data queue is approaching defined threshold capacity	Threshold Crossed
4001	ImpParser - Incoming TTR count over threshold	ImpParser Incoming TTR count over threshold	Threshold Crossed
4002	ImpParser - Incoming bandwidth over threshold	ImpParser Incoming bandwidth over threshold	Threshold Crossed
4003	ImpParser - Oracle DB connection error	Connection to the database has been lost or cant be established	Communications subsystem failure
4005	ImpParser - Start event missing for stop event	Expected Start Event Missing for Stop Event	Software program error
4006	ImpParser - Overload protection	Overload protection started and all TTRs will	Threshold Crossed

		be discarded due to system overload	
4007	ImpParser - Process CPU Utilization	The Process which is responsible for handling all traffic is approaching or exceeding its engineered traffic handling capacity	CPU cycles limit exceeded
4008	ImpParser - Unable to store to Oracle DB	Unable to write or store records to Oracle DB perhaps lock or no space	Software program error
4099	Unknown Mediation Issue	An unknown error has occurred in mediation	Software program error
4101	Communication Agent Connection Down	Communication Agent Connection Down	Communications subsystem failure
4102	Communication Agent Connection Locally Blocked	Communication Agent Connection Locally Blocked	Communications subsystem failure
4103	Communication Agent Connection Remotely Blocked	Communication Agent Connection Remotely Blocked	Communications subsystem failure
4104	Communication Agent stack event queue utilization	The percent utilization of the Communication Agent Task stack queue is approaching defined threshold capacity	Threshold crossed
4105	Communication Agent configured connection waiting on remote	configured connection waiting for remote client to establish connection	Communications subsystem failure
4106	Communication Agent Failed to Align Connection	Communication Agent Failed to Align Connection	Communications subsystem failure
4107	Communication Agent CommMessage Mempool utilization	The percent utilization of the Communication Agent CommMessage mempool is approaching defined threshold capacity	Threshold crossed
4108	Communication Agent User Data FIFO Queue utilization	The percent utilization of the Communication Agent User Data FIFO Queue is approaching	Threshold crossed

		defined threshold capacity	
4109	Communication Agent Mx FIFO Queue utilization	The percent utilization of the Communication Agent Mx FIFO Queue is approaching defined threshold capacity	Threshold crossed
4110	Communication Agent Egress Message Discarded	Communication Agent Egress Message Discarded	Communications subsystem failure
4111	Communication Agent Ingress Message Discarded	Communication Agent Ingress Message Discarded	Communications subsystem failure
4112	Communication Agent Peer has not responded to heartbeat	Communication Agent Peer has not responded to heartbeat	Communications subsystem failure
4113	Communication Agent Connection state Changed	Communication Agent Connection state Changed	Communications subsystem failure
4114	Communication Agent DB Responder change	Communication Agent DB Responder detected a change in configurable control option parameter	Communications subsystem failure
4115	Communication Agent DataEvent Mempool utilization	The percent utilization of the Communication Agent DataEvent mempool is approaching defined threshold capacity	Threshold crossed
4121	Communication Agent Transaction Failure Rate	The number of failed transactions during the sampling period has exceeded configured thresholds	Communications subsystem failure
4122	Communication Agent Connection Congested	Communication Agent Connection Congested	Communications subsystem failure
4123	Communication Agent Service Registration State Change	Communication Agent Service Registration State Change	Communications subsystem failure
4124	Communication Agent Service Operational State Changed	Communication Agent Service Operational State Changed	Communications subsystem failure

4126	Communication Agent Service Egress Message Discarded	Communication Agent Service Egress Message Discarded	Communications subsystem failure
4142	Process CPU Utilization	The Process which is responsible for handling all traffic is approaching or exceeding its engineered traffic handling capacity	CPU cycles limit exceeded
4147	Measurement Initialization Failure	A measurement object failed to initialize	Software program error
4200	ImpStore - Oracle DB connection error	Connection to the database has been lost or cant be established	Communications subsystem failure
4201	ImpStore - DTS connection error	Unable to connect to the DTS input or the DTS input connection has been lost	Communications subsystem failure
4202	ImpStore - DTS read error	Unable to read from DTS input or the DTS input connection has been lost	Communications subsystem failure
4203	ImpStore - Configuration error	The configuration for impstore is not valid or contains errors	Configuration or customization error
4204	ImpStore - Unable to store to Oracle DB	Unable to write or store records to Oracle DB perhaps lock or no space	Software program error
4205	ImpStore - Congestion	Congestion, data lost	Threshold crossed
4400	ImpAggregator - Could not open DTS stream	Could not open DTS stream	Software program error
4401	ImpAggregator - Could not read from DTS stream	Could not read from DTS stream	Software program error
4402	ImpAggregator - Could not write to DTS stream	Could not write to DTS stream	Software program error
4403	ImpAggregator - Overload protection	Total number of all KPIs exceeded the limit	Threshold crossed

Appendix C

Supported Diameter Interfaces

Topics:

This section provides information about the Diameter interfaces supported by IDIH.

Supported Diameter Interfaces

The IDIH supports following Diameter Interfaces:

- S6 Diameter Interface
- Gx Diameter Interface
- Rx Diameter Interface
- Ro-Gy Diameter Interface
- Sh Diameter Interface
- Rf Diameter Interface
- Cx Diameter Interface
- Gq Prime Diameter Interface
- Base Diameter Interface
- Default/not supported Diameter Interface
- SLh Diameter Interface
- SLg Diameter Interface
- SWx Diameter Interface
- STa Diameter Interface
- Gxx Diameter Interface
- S9 Diameter Interface
- SWm Diameter Interface
- S6b Diameter Interface
- Sd Diameter Interface
- Sy Diameter Interface
- S13 Diameter Interface
- Zh Diameter Interface

Appendix D

DSR Application Metadata-Generating Events

Topics:

This appendix provides information on metadata events related to the various DSR applications.

Recording Transaction Metadata

For the IDIH feature, data will be will recorded about each Diameter transaction (including Message Copy transaction) - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the TTR in the order that the metadata-generating events actually occurred.

Together, all of the metadata records combine to document the processing performed by DSR on the entire transaction. These records can be used later to provide diagnostic information when performing troubleshooting. Metadata is recorded to a Trace Transaction Record (TTR) for each transaction so that, even if the transaction is selected to be sent to IDIH at an answer TTP (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

DSR applications will also record metadata. Application-recorded metadata will appear in the same TTR as the DPI metadata, interleaved with the DPI metadata, in the order that the metadata-generating events actually occurred.

If a Diameter transaction triggers a Message Copy transaction, the corresponding Message Copy's transaction will be recorded in a separate TTR. The regular TTR that records the normal transaction and the Message Copy TTR will correlate to each other.

Table 8: Metadata-Generating Events lists all of the metadata events that will be recorded.

Table 8: Metadata-Generating Events

Event	Instance Data	When Recorded
Ingress request received	Payload	As soon as the message has been verified by DRL to be a well-formed Diameter message
Egress request sent	Payload	Immediately before the egress request is sent to DCL.
Ingress answer received	Payload	As soon as the message has been verified by DRL to be a well-formed Diameter message
Egress answer sent	Payload	Immediately before the egress answer is sent to DCL.
Routing to Application	Application name	Immediately before routing to application
Routing to Application failed	Reason	Immediately after the routing to application failure is detected.
Application to Routing	Request routing method Override origin requested (this message) Override error reporting host requested (this message)	Immediately after the application to routing is complete.

Event	Instance Data	When Recorded
	Route list name PRT table name ART table name Invoke application unavailability action	
Trace match at: • TTP-IR • TTP-ER • TTP-IA • TTP-EA • TTP-RA • TTP-AR	Trace name, TTP name	Immediately upon detecting a trace match.
ART rule matched	ART rule name	Immediately after ART rule matching is performed (if a match was found).
ART rule not found	ART Table name	Immediately after ART rule matching is performed and no rule is found
Unavailability action selected by ART	Unavailability action	Immediately after the application invocation failure is detected. This event only applies to ingress request messages
Unavailability action selected by application	Unavailability action	Immediately after any application returns with "invoke unavailability action" specified. This event only applies to ingress answer messages
Route list selected as unavailability action	Route list name	After matching an ART rule for an application that is unavailable.
Route list selected by application	Route list name	After all applications have been invoked (if the last application selects a route list).
Route list selected for message copy	Route list name	Final route list picked for the DAS server for message copy
PRT rule matched	PRT rule name	Immediately after PRT rule matching is performed (if a match was found).
PRT rule not found	PRT table name	Immediately after PRT rule matching is performed and no rule is found

Event	Instance Data	When Recorded
Dest-Host routing selected	None	Immediately after PRT rule matching is performed (if a match is not found).
Dest-Host routing fails to select an egress connection	None	After Dest-Host routing fails to select an egress connection
Route group selected for egress transmission	Route group name	Immediately after the route group is chosen for regular transaction
Route group selected for egress transmission	Route group name	Immediately after the route group is chosen for message copy transaction to DAS .
Mediation rule match at: • RTP-1 • RTP-10 • ATP-1 • ATP-10 • RTP-4 • RTP-6 • ATP-4 • ATP-6 • RTP-11	Mediation template name, MEP name	After performing mediation template matching and executing actions for all matched rules.
A request was rerouted	Reroute attempt number	Immediately before the rerouted message is forwarded to DCL
A pending transaction timed out	None	Upon detection of the timeout
A received answer did not match a pending transaction	None	Immediately after the PTR search fails
Message Copied	TtrLinkId	Immediately after Message Copy transaction is started upon the reception of an Answer message. This event will be in the regular/originating TTR.
Copied Message	Correlation	Immediately before the message copy is routed to DAS. This event will be in the Message Copy TTR.
Message Copy Triggered	Trigger point name Message copy config set name Route list selected for DAS	Immediately after Message Copy operation intention is detected at the various points along an transaction processing path

P-DRA Metadata-Generating Events

The metadata captured by IDIH for the Policy DRA application includes the results of each query that Policy DRA makes to the session and binding database and the associated result. Whenever the result of a database query is captured in Policy DRA metadata, it will include the identity of the specific server that generated the response.

Table 9: P-DRA Metadata-Generating Events

Event	Instance Data	When Recorded
PCRF Pool Selected	• PCRF Pool Name • PCRF Sub-Pool name • Sub-Pool selection rule name	When P-DRA receives a binding-capable session initiation request
Binding Query Request Sent to pSBR	• Anchor key • APN name • PCRF Pool name • Session reference	When P-DRA sends a "Find or Create Binding" stack event to a pSBR
Binding Query Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Binding state • Binding master • Master session reference • PCRF FQDN • Suspect duration • Result code	When P-DRA receives a "Find or Create Binding Result" stack event from a pSBR
Topology Hiding Applied		• When P-DRA receives a binding-capable session initiation answer destined for a peer for which topology hiding is configured • When P-DRA receives a binding-dependent session initiation answer destined for a peer for which topology hiding is configured • When P-DRA receives an in-session answer destined for a peer for which topology hiding is configured
Create Session Request Sent to pSBR	• Session reference • Anchor key	When P-DRA sends a "Create Session" stack event to a pSBR

Event	Instance Data	When Recorded
	• MSISDN • ·IPv4/IPv6 address key • PCRF FQDN	
Create Session Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives a "Create Session Result" stack event from a pSBR
Update Binding Request Sent to pSBR	• Operation • Anchor key • Final PCRF name • Session reference	When P-DRA sends an "Update Binding" stack event to a pSBR
Update Binding Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives an "Update Binding Result" stack event from a pSBR
Find Binding Request Sent to pSBR	• Key type • Key value • APN name	When P-DRA sends a "Find Binding" stack event to a pSBR
Find Binding Result Received by pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Result code • PCRF FQDN • IMSI	When P-DRA receives a "Find Binding Result" stack event from a pSBR
Refresh Session Request Sent to pSBR	• Session ID	When P-DRA sends a "Refresh Session" stack event to a pSBR
Refresh Session Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives a "Refresh Session Result" stack event from a pSBR
Delete Session Request Sent to pSBR	• Session ID	When P-DRA sends a "Remove Session" stack event to a pSBR
Delete Session Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25)	When P-DRA receives a "Remove Session Result" stack event from a pSBR

Event	Instance Data	When Recorded
	• Result code • Session reference • Anchor key • MSISDN • IPv4/IPv6 key • PCRF FQDN	
Find Session Request Sent to pSBR	• Session ID	When P-DRA sends a "Find Session" stack event to a pSBR
Find Session Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Result code • PCRF FQDN • Session reference	When P-DRA receives a "Find Session Result" stack event from a pSBR
Remove Suspect Binding Request Sent to pSBR	• Anchor key • PCRF FQDN	When P-DRA sends a "remove Suspect Binding" stack event to a pSBR
Remove Suspect Binding Result Received from pSBR	• pSBR IP Address Type (such as IPv4) • pSBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives a "Remove Suspect Binding Result" stack event from a pSBR
Session Release Initiated		• When an "Update Binding" request fails • When a "Create Session" request fails • When a "Create Alternate Key" request fails
Session Query Initiated		• When a stale session is detected by a pSBR
Routing Exception	• Routing Exception Type (such as "pSBR Congestion") • Routing Exception Action (such as "Abandon Request")	• After any routing exception is encountered
pSBR Request Failure	• Resource name • Sub-resource ID	• After any pSBR request failure other than a response timeout is encountered
pSBR Response Timed out	• Resource name • Sub-resource ID	• When P-DRA times out waiting to receive a response

Event	Instance Data	When Recorded
		from a pSBR for a previous request

FABR Metadata-Generating Events

The Diameter Routing Function and invoked DSR Applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to IDIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

FABR will record the Application-specific metadata events described in *Table 10: FABR Metadata-Generating Events*.

Table 10: FABR Metadata-Generating Events

Event	Instance Data	When Recorded
Address Resolution Match found	• Routing Entity Type (such as "IMSI") • Routing Entity AVP (such as "Public-Identity") • Routing Entity Address (such as "311480123456789")	After FABR searches and finds a valid Routing Entity address in an ingress Request message using a prioritized set of AVPs associated with the highest priority Routing Entity Type assigned to the Address Resolution order pair (Diameter Application ID, Command Code).
DP Query Event Sent to DP for processing	• Routing Entity Data Format (such as "IMSI") • Routing Entity Address (such as "123456789012345") • Destination Type (such as "IMS-HSS")	When FABR sends a DP query event to the DP for Destination address resolution.
DP Response Event Received from DP	• DP IP Address Type (such as IPv4) • DP IP Address (such as 10.240.55.25) • Result Code String (such as "Blacklisted") • Destination Realm (such as "xyz.com")	When FABR receives a response to a previous DP query.

Event	Instance Data	When Recorded
	• Destination FQDN (such as "hss1.hss.xyz.com")	
Routing Exception	• Routing Exception Type (such as "DP Congestion") • Routing Exception Action (such as "Abandon Request")	After any Routing Exception is encountered.
DP Query Failure	• DP IP Address Type (such as IPv4) • DP IP Address (such as 10.240.55.25)	After any DP Query failure other than a response timeout is encountered.
DP Response Timed out	• DP IP Address Type (such as IPv4) • DP IP Address (such as 10.240.55.25)	When FABR times out waiting to receive a response from the DP to a previous Destination address resolution query.

RBAR Metadata-Generating Events

The Diameter Routing Function and invoked DSR Applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to IDIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

RBAR will record the Application-specific metadata events described in *Table 11: RBAR Metadata-Generating Events*.

Table 11: RBAR Metadata-Generating Events

Event	Instance Data	When Recorded
Address Resolution Match found	• Routing Entity Type (such as "IMSI") • Routing Entity AVP (such as "User Name") • Routing Entity Address (such as "123456789012345")	After RBAR searches and finds a valid Routing Entity address in an ingress Request message using a prioritized set of AVPs associated with the highest priority Routing Entity Type assigned to the Address Resolution order pair (Diameter Application ID, Command Code).

Event	Instance Data	When Recorded
Routing Entity address resolved to a Destination address for request message routing	• Destination Routing Table Format (such as "AET") • Destination Realm (such as "xyz.com") • Destination FQDN (such as "hss1.hss.xyz.com")	When a valid Routing Entity address extracted from an Ingress Request message matches an AET or DRT entry for request message routing.
Routing Exception	• Routing Exception Type (such as "Unknown Command Code") • Routing Exception Action (such as "Abandon Request")	After any Routing Exception is encountered.

MAP-Diameter IWF Metadata-Generating Events

The Diameter Routing Function and invoked DSR Applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to IDIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

The MD-IWF application of the MAP-Diameter Interworking Function doesn't support Integrated DIH.

The DM-IWF application of the MAP-Diameter Interworking Function will record the Application-specific metadata events described in *Table 12: DM-IWF Metadata-Generating Events*.

Table 12: DM-IWF Metadata-Generating Events

DM-IWF Event	Instance Data	When Recorded
Diameter-to-MAP Transactions		
Sent Egress Request to SS7-MP	Transaction ID (such as "45631") Payload	Immediately before the egress Request is sent to ComAgent.
D-to-M Request discarded	Discard Reason (such as "DM-IWF PTR pool exhausted")	DM-IWF discards a Request message received from DRL.
Ingress Answer received from SS7-MP	Transaction Id (such as "45631") SS7-MP IP address (such as "47.240.10.3") Payload	DM-IWF received an ingress Answer message from SS7-MP

DM-IWF Event	Instance Data	When Recorded
A received Answer did not match a pending transaction	None	Immediately after PTR search fails
DM-IWF Routing Exception	Routing Exception Type (such as "Internal Processing Error") Routing Exception Action (such as "Abandon Request")	When a routing exception is applied by DM-IWF
MD-IWF Routing Exception	None	When DM-IWF applies "Apply Unavailability Action" routing exception on behalf of MD-IWF.
MAP-to-Diameter Transactions		
Ingress Request received from SS7-MP	Transaction ID (such as "45631") SS7-MP address (such as "47.240.10.3") Payload	Immediately after a Request is received from SS7-MP.
Egress Answer sent to SS7-MP	Transaction ID (such as "45631") SS7-MP address (such as "47.240.10.3") Payload	Immediately after DM-IWF sends a Diameter Answer to ComAgent successfully.
D-to-M Answer discarded	Discard Reason (such as "Failed to create IWF Answer")	DM-IWF discards an Answer message received from DRL.

CPA Metadata-Generating Events

The Diameter Routing Function and invoked DSR Applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to IDIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

CPA will record the Application-specific metadata events described in *Table 13: CPA Metadata-Generating Events*.

Table 13: CPA Metadata-Generating Events

Event	Instance Data	When Recorded
SBR Query Sent	• Operation • Session ID • CDF Host • CDF Realm	When CPA retrieves an existing session binding record on the SBR.
SBR Response Received	• SBR IP Address Type • SBR IP Address • Operation • Result Code String	When CPA receives a response from SBR to a previous session binding query.
SBR Query Failure	• SBR IP Address Type • SBR IP Address	After any SBR Query failure other than a response timeout is encountered.
SBR Response Timed out	• SBR IP Address Type • SBR IP Address	When CPA times out waiting to receive a response from the SBR to a previous session binding query.

PCA Metadata-Generating Events

The Diameter Routing Function and invoked DSR Applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (TTR) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to IDIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction will be present.

PCA will record the Application-specific metadata events described in *Table 14: PCA Metadata-Generating Events*.

Table 14: PCA Metadata-Generating Events

Event	Instance Data	When Recorded
PCA Function Invoked	PCA Function Name	When an application with multiple functionality receives an ingress Diameter message (including both requests and answers) and routes it to one of its functions for processing

Event	Instance Data	When Recorded
		Note: This metadata is only recorded if the application function is enabled and available processing messages.
PCRF Pool Selected	• PCRF Pool Name • PCRF Sub-Pool name • Sub-Pool selection rule name	When P-DRA receives a binding-capable session initiation request
Binding Query Request Sent	• Anchor key • APN name • PCRF Pool name • Session reference	When P-DRA sends a "Find or Create Binding" stack event to a SBR
Binding Query Result Received	• SBR IP Address (such as 10.240.55.25) • Result code • Binding state • Binding master • Master session reference • PCRF FQDN • Suspect duration	When P-DRA receives a "Find or Create Binding Result" stack event from a SBR
Topology Hiding Applied	N/A	When P-DRA receives a bind-capable or binding-dependent session initiation/in-session answer destined for a peer for which topology hiding is configured
Create Session Request Sent	• Session ID • Session reference • Anchor key • MSISDN • IPv4/IPv6 address key • PCRF FQDN	When P-DRA sends a "Create Session" stack event to a SBR
Create Session Result Received	• SBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives a "Create Session Result" stack event from a SBR
Update Binding Request Sent	• Operation • Anchor key • Final PCRF FQDN • Session reference	When P-DRA sends an "Update Binding" stack event to a SBR
Update Binding Result Received	• SBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives an "Update Binding Result" stack event from a SBR

Event	Instance Data	When Recorded
Find Binding Request Sent	• Key type • Key value • APN name	When P-DRA sends a "Find Binding" stack event to a SBR
Find Binding Result Received	• SBR IP Address (such as 10.240.55.25) • Result code • IMSI • PCRF FQDN	When P-DRA receives a "Find Binding Result" stack event from a SBR
Refresh Session Request Sent	Session ID	When P-DRA sends a "Refresh Session" stack event to a SBR
Refresh Session Result Received	• SBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives a "Refresh Session Result" stack event from a SBR
Delete Session Request Sent	Session ID	When P-DRA sends a "Remove Session" stack event to a SBR
Delete Session Result Received	• SBR IP Address (such as 10.240.55.25) • Result code • Session reference • PCRF FQDN • Anchor key • MSISDN key • IPv4/IPv6 key	When P-DRA receives a "Remove Session Result" stack event from a SBR
Find Session Request Sent	Session ID	When P-DRA sends a "Find Session" stack event to a SBR
Find Session Result Received	• SBR IP Address (such as 10.240.55.25) • Result code • Session reference • PCRF FQDN	When P-DRA receives a "Find Session Result" stack event from a SBR
Remove Suspect Binding Request Sent	• Anchor key • PCRF FQDN	When P-DRA sends a "remove Suspect Binding" stack event to a SBR
Remove Suspect Binding Result Received	• SBR IP Address (such as 10.240.55.25) • Result code	When P-DRA receives a "Remove Suspect Binding Result" stack event from a SBR
Session Release Initiated	Application Name	When an "Update Binding" request, a "Create Session" request or, a "Create Alternate Key" request fails

Event	Instance Data	When Recorded
Session Query Initiated	Application Name	When a stale Gx session is detected by a SBR
Routing Exception	• Routing Exception Type (such as "SBR Congestion") • Routing Exception Action (such as "Abandon Request")	After any routing exception is encountered
SBR Request Failure	• After any routing exception is encountered • Resource name • Sub-resource ID • Failed Request Name	When a PCA Function fails to send a request to the SBR
SBR Response Timed out	• Resource name • Sub-resource ID	When a PCA Function times out waiting to receive a response from a SBR for a previous request
Routing Error Indication Received	Routing Error	When a PCA Function initiates a Diameter request (Session Release RAR) that is rejected by DRL due to a routing error. **Note:** The Routing Error recorded is the Error-Message AVP value of the Answer message initiated by DRL.
Create OC Session Request Sent	• Session ID • CTF Realm • CTF FQDN • OCS Realm • OCS FQDN • Subscriber ID • APN Name	When OC-DRA sends a "Create OC Session" stack event to the Session SBR
Create OC Session Result Received	• SBR IP Address • Result Code	When OC-DRA receives a "Create OC Session Result" stack event from the Session SBR
Find and Refresh OC Session Request Sent	Session ID	When OC-DRA sends a "Find and Refresh OC Session" stack event to the Session SBR
Find and Refresh OC Session Result Received	• Session ID • Result Code • CTF Realm • CTF FQDN • OCS Realm	When OC-DRA receives the "Find and Refresh OC Session Result" stack event from the Session SBR

Event	Instance Data	When Recorded
	• OCS FQDN • Subscriber ID • APN Name	
Find and Remove OC Session Request Sent	Session ID	When OC-DRA sends a "Find and Remove OC Session" stack event to the Session SBR
Find and Remove OC Session Request Received	• SBR IP Address • Result Code • CTF Realm • CTF FQDN • OCS Realm • OCS FQDN • Subscriber ID • APN Name	When OC-DRA receives the "Find and Removed OC Session Result" stack event from the Session SBR

Glossary

A

APN	Access Point Name The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.

D

DAS	Diameter Application Server
DCL	Diameter Connection Layer The software layer of the stack which implements Diameter transport connections.
DPI	Diameter Plug-In is a reusable Diameter stack consisting of DCL, DRL, and an application interface.

E

ENUM	T**E**lephone **NU**mber **M**apping - A technology for unifying various communications and telephone addresses for private and business numbers, facsimile and mobile phone numbers, SMS services, Instant Messaging and email. ENUM integrates legacy phone numbers with the Domain Name System (DNS). Users can access and maintain a directory that supports all forms of wired communication, mobile communications networks, and the Internet. ENUM allows for an end user to be reached on multiple devices via one phone number and

E

	allows the end user to determine which device to contact first or multiple devices simultaneously.
	E.164 Number Mapping

F

FQDN	Fully Qualified Domain Name
	The complete domain name for a specific computer on the Internet (i.e., www.oracle.com).
	A domain name that specifies its exact location in the tree hierarchy of the DNS.

I

IDIH	Integrated Diameter Intelligence Hub
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
	International Mobile Station Identity

M

MCL	Managed Object Change Level
MEP	Mediation Evaluation Point
MSISDN	Mobile Station International Subscriber Directory Number
	The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.

M

	Mobile Subscriber Integrated Services Digital Network [Number]
	Mobile Station International Subscriber Directory Number. The unique, network-specific subscriber number of a mobile communications subscriber. MSISDN follows the E.164 numbering plan; that is, normally the MSISDN is the phone number that is used to reach the subscriber.

P

PCRF	Policy and Charging Rules Function The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.
P-DRA	Policy DRA
pSBR	Policy SBR

T

TTP	Troubleshooting Trigger Point - A point within DRL at which the flexroute library is invoked to determine whether a Diameter message matches any of the active traces that are configured to be evaluated there.

T

TTR	Trace Transaction Record - A record describing a Diameter transaction, including all of the Diameter messages that were part of the transaction, plus the operations performed by DSR while processing those messages.