Oracle® Communications
Tekelec HLR Router

HLR Router Alarms, KPIs, and Measurements Reference

910-6572-001 Revision C

February 2014

ORACLE®

Oracle® Communications HLR Router Alarms, KPIs, and Measurements Reference

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

Overview

The *HLR Alarms, KPIs, and Measurements* documentation provides information about HLR alarms and events, KPIs, and measurements, provides corrective maintenance procedures, and other information used in maintaining the system.

This documentation provides:

- Information relevant to understanding alarms and events that may occur on the application
- Recovery procedures for addressing alarms and events, as necessary
- Procedures for viewing alarms and events, generating alarms reports, and viewing and exporting alarms and events history
- Information relevant to understanding KPIs in the application
- The procedure for viewing KPIs
- Lists of KPIs
- Information relevant to understanding measurements in the application
- Measurement report elements, and the procedures for printing and exporting measurements
- Lists of measurements by function

Scope and Audience

This manual does not describe how to install or replace software or hardware.

This manual is intended for personnel who must maintain operation of the HLR. The manual provides lists of alarms, events, KPIs, and measurements along with preventive and corrective procedures that will aid personnel in maintaining the HLR.

The corrective maintenance procedures are those used in response to a system alarm or output message. These procedures are used to aid in the detection, isolation, and repair of faults.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Related Publications

The EAGLE XG HLR Router documentation set includes the following publications, which provide information for the configuration and use of EAGLE XG HLR Router and related applications.

Getting Started includes a product overview, system architecture, and functions. It also explains the EAGLE XG HLR Router GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets. Available from the application GUI and on the documentation DVD.

Feature Notice describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Customer Support Site. Available from the application GUI and on the documentation DVD.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the EAGLE XG HLR Router, both for initial setup and maintenance.

HLR Router Online Help explains how to use the HLR Router GUI pages to manage the configuration and maintenance of the EAGLE XG Database and the EAGLE XG HLR Router. Available from the application GUI and on the documentation DVD.

HLR Router Administration Guide describes HLR Router architecture, functions, system and PDBI configuration; Signaling and Transport configuration; the Query Server; and PDE CSV file formats. Available from the application GUI and on the documentation DVD.

HLR Router Alarms, KPIs, and Measurements Reference Guide provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual measurement value; and explains how to generate reports containing current

alarm, event, KPI, and measurement information. Available from the application GUI and on the documentation DVD.

SS7/Sigtran User Guide describes HLR Router's Signaling Network Interface, which provides standard SCCP functionality, traditional MTP3 routing capabilities, and a standardM3UA interface to the external network. The SS7/Sigtran section of the documentation explains how to use the SS7/Sigtran GUI pages to perform configuration and maintenance tasks related to adjacent servers, SS7 signaling points, link sets, associations, routes, and SS7 Sigtran options. Available from the application GUI and on the documentation DVD.

Transport Manager User Guide describes the configuration of "Transports" (SCTP associations and UDP connections with remote hosts over an underlying IP network). Available from the application GUI and on the documentation DVD.

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter

2

Alarms and Events, KPIs, and Measurements Overview

Topics:

This section provides general information about the application's alarms and events, KPIs, and measurements.

Purpose of this documentation

This documentation provides:

- Information relevant to understanding alarms and events that may occur on the application
- Recovery procedures for addressing alarms and events, as necessary
- Procedures for viewing alarms and events, generating alarms reports, and viewing and exporting alarms and events history
- Information relevant to understanding KPIs in the application
- The procedure for viewing KPIs
- Lists of KPIs
- Information relevant to understanding measurements in the application
- Measurement report elements, and the procedures for printing and exporting measurements
- Lists of measurements by function

Documentation organization

Information in this document is organized into the following sections :

Introduction	Contains general information about the scope of this manual, its targeted audience, and Tekelec Customer Care Center contact information
Alarms and Events, KPIs, and Measurements Overview	Documentation purpose and organization, alarms and event overview information and tasks
Alarms	Information and recovery procedures for alarms and events, organized first by alarm category, then numerically by the number that appears in the application
KPIs	Detailed KPI information, organized alphabetically by KPI name
Measurements	Detailed measurement information, organized alphabetically by measurement category

Opening a file

Use this procedure to open a file stored in the file management storage area.

1. Select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select an **NE Name**.
3. Click **List Files**.

   The **Status & Manage Files** list page for the selected network element displays all files stored in its file management storage area.

4. Click the **Filename** of the file to be opened.

   Your browser's **File Download** window appears.

5. Click **Open** to open the file.

Data Export

From the Data Export page you can set an export target to receive exported performance data. Several types of performance data can be filtered and exported using this feature. For more information about how to create data export tasks, see:

- *Exporting active alarms*
- *Exporting alarm and event history*
- *Exporting KPIs*
- *Exporting measurements reports*

From the Data Export page you can manage file compression strategy and schedule the frequency with which data files are exported.

Data Export elements

This table describes the elements on the Data Export page.

Table 1: Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server.	Must be a valid hostname, IPv4 address, or IPv6 address. Range: Maximum length is 24 characters; alphanumeric characters (a-z, A-Z, and 0-9) and minus sign. Hostname must start and end with an alphanumeric. To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None
Username	Username used to access the export server	Format: Textbox Range: Maximum length is 32 characters; alphanumeric characters (a-z, A-Z, and 0-9). To clear the current export server and remove the file transfer task,

Element	Description	Data Input Notes
		specify an empty hostname and username. Default: None
Directory on Export Server	Directory path on the export server where the exported data files are to be transferred	Format: Textbox Range: Maximum length is 255 characters; valid value is any UNIX string. Default: None
Path to rsync on Export Server	Optional path to the rsync binary on the export server	Format: Textbox Range: Maximum length is 4096 characters; alphanumeric characters (a-z, A-Z, and 0-9),dash, underscore, period, and forward slash. Default: If no path is specified, the username's home directory on the export server is used
Backup File Copy Enabled	Enables or disables the transfer of the backup files.	Format: Checkbox Default: Disabled (unchecked)
File Compression	Compression algorithm used when exported data files are initially created on the local host.	Format: Radio button Range: gzip, bzip2, or none Default: gzip
Upload Frequency	Frequency at which the export occurs	Format: Radio button Range: fifteen minutes, hourly, daily or weekly Default: weekly
Minute	If The Upload Frequency is Hourly, this is the minute of each hour when the transfer is set to begin	Format: Scrolling list Range: 0 to 59 Default: zero
Time of Day	If the Upload Frequency is Daily of Weekly, this is the time of day the export occurs	Format: Time textbox Range: HH:MM AM/PM in 15-minute increments Default: 12:00 AM

Element	Description	Data Input Notes
Day of Week	If Upload Frequency is Weekly, this is the day of the week when exported data files will be transferred to the export server	Format: Radio button Range: Sunday through Saturday Default: Sunday
SSH Key Exchange	This button launches a dialog box. The dialog requests username and password and initiates SSH key exchange.	Format: Button
Transfer Now	This button initiates an immediate attempt to transfer any data files in the export directory to the export server.	Format: Button

Configuring data export

The Data Export page enables you to configure a server to receive exported performance and configuration data. Use this procedure to configure data export.

1. Select **Administration > Remote Servers > Data Export**.
   The Data Export page appears.
2. Enter a **Hostname**.
   See the Data Export elements for details about the **Hostname** field and other fields that appear on this page.
3. Enter a **Username**.
4. Enter a **Directory Path** on the Export server.
5. Enter the **Path to Rsync** on the Export server.
6. Select whether to enable the transfer of the backup file. To leave the backup disabled, do not check the box.
7. Select the **File Compression** type.
8. Select the **Upload Frequency**.
9. If you selected hourly for the upload frequency, select the **Minute** intervals.
10. If you selected daily or weekly for the upload frequency, select the **Time of Day**.
11. If you selected weekly for the upload frequency, select the **Day of the Week**.
12. Click **Exchange SSH Key** to transfer the SSH keys to the export server.
    A password dialog box appears.
13. Enter the password.
    The server will attempt to exchange keys with the specified export server. After the SSH keys are successfully exchanged, continue with the next step.
14. Click **OK** or **Apply**.
    The export server is now configured and available to receive performance and configuration data.

Tasks

The **Tasks** pages display the active, long running tasks and scheduled tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results for long running tasks, while the **Scheduled Task**s page provides a location to view, edit, and delete tasks that are scheduled to occur.

Active Tasks

The **Active Tasks** page displays the long running tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results, all of which can be generated into a report. Additionally, you can pause, restart, or delete tasks from this page.

Active Tasks elements

The **Active Tasks** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes elements on the **Active Tasks** page.

Table 2: Active Tasks Elements

Active Tasks Element	Description
ID	Task ID
Name	Task name
Status	Current status of the task. Status values include: running, paused, completed, exception, and trapped.
Start Time	Time and date when the task was started
Update Time	Time and date the task's status was last updated
Result	Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.
Result Details	Details about the result of the task
Progress	Current progress of the task

Deleting a task

Use this procedure to delete one or more tasks.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

Note: Hovering the cursor over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Select one or more tasks.

   Note: To delete a single task or multiple tasks, the status of each task selected must be one of the following: completed, exception, or trapped.

   Note: You can select multiple rows to delete at one time. To select multiple rows, press and hold Ctrl as you click to select specific rows.

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Deleting all completed tasks

Use this procedure to delete all completed tasks.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the cursor over any tab displays the name of the server.

   All active tasks on the selected server are displayed.
3. Click **Delete all Completed**.
   A confirmation box appears.
4. Click **OK** to delete all completed tasks.
   All tasks with the status of completed are deleted.

Canceling a running or paused task

Use this procedure to cancel a task that is running or paused.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the cursor over any tab displays the name of the server.

   All active tasks on the selected server are displayed.
3. Select a task.
4. Click **Cancel**.
   A confirmation box appears.
5. Click **OK** to cancel the selected task.
   The selected task is canceled.

Pausing a task

Use this procedure to pause a task.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select a task.

   Note: A task may be paused only if the status of the task is running.

4. Click **Pause**.
   A confirmation box appears.
5. Click **OK** to pause the selected task.
   The selected task is paused. For information about restarting a paused task, see *Restarting a task*.

Restarting a task

Use this procedure to restart a task.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select a paused task.

   Note: A task may be restarted only if the status of the task is paused.

4. Click **Restart**.
   A confirmation box appears.
5. Click **OK** to restart the selected task.
   The selected task is restarted.

Active Tasks report elements

The **Active Tasks Report** page displays report data for selected tasks. This table describes elements on the **Active Tasks Report** page.

Table 3: Active Tasks Report Elements

Active Tasks Report Element	Description
Task ID	Task ID
Display Name	Task name

Active Tasks Report Element	Description
Task State	Current status of the task. Status values include: running, paused, completed, exception, and trapped.
Admin State	Confirms task status
Start Time	Time and date when the task was started
Last Update Time	Time and date the task's status was last updated
Elapsed Time	Time to complete the task
Result	Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.
Result Details	Details about the result of the task

Generating an active task report

Use this procedure to generate an active task report.

1. Select **Status & Manage > Tasks > Active Tasks**.

   The **Active Tasks** page appears.

2. Select a server.

   Note: Hovering the mouse over any tab displays the name of the server.

   All active tasks on the selected server are displayed.

3. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

4. Click **Report**.
   The **Tasks Report** page appears.
5. Click **Print** to print the report.
6. Click **Save** to save the report.

Scheduled Tasks

The periodic export of certain data can be scheduled through the GUI. The **Scheduled Tasks** page provides you with a location to view, edit, delete and generate reports of these scheduled tasks. For more information about the types of data that can be exported, see:

- *Exporting active alarms*
- *Exporting alarm and event history*
- *Exporting KPIs*
- *Exporting measurements reports*

Viewing scheduled tasks

Use this procedure to view the scheduled tasks.

Select **Status & Manage > Tasks > Scheduled Tasks**.

The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

Scheduled Tasks elements

The **Scheduled Tasks** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes elements on the **Scheduled Tasks** page.

Table 4: Scheduled Tasks Elements

Scheduled Tasks Element	Description
Task Name	Name given at the time of task creation
Description	Description of the task
Time of Day	The hour and minute the task is scheduled to run
Day-of-Week	Day of the week the task is scheduled to run
Network Elem	The Network Element associated with the task

Editing a scheduled task

Use this procedure to edit a scheduled task.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select a task.
3. Click **Edit**.
   The **Data Export** page for the selected task appears.
4. Edit the available fields as necessary.
   See *Scheduled Tasks elements* for details about the fields that appear on this page.
5. Click **OK** or **Apply** to submit the changes and return to the **Scheduled Tasks** page.

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.
3. Click **Delete**.

A confirmation box appears.

4. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

3. Click **Report**.
   The **Scheduled Tasks Report** page appears.
4. Click **Print** to print the report.
5. Click **Save** to save the report.

Chapter 3

Alarms and Events

Topics:

This section provides general alarm/event information, and lists the types of alarms and events that can occur on the system. Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the View History GUI menu option.

Note: Some of the alarms in this document are shared with other applications and may not appear in this particular product.

General alarms and events information

This section provides general information about alarms and events, including an alarms overview, types of alarms/events, and alarms-related procedures.

Alarms and events overview

Alarms provide information pertaining to a system's operational condition that a network manager may need to act upon. An alarm might represent a change in an external condition, for example, a communications link has changed from connected to disconnected state. Alarms can have these severities:

- Critical application error
- Major application error
- Minor application error
- Cleared

An alarm is considered inactive once it has been cleared and cleared alarms are logged on the **Alarms & Events** > **View History** page of the GUI.

Events note the occurrence of a transient condition. Events have a severity of Info and are logged on the **View History** page.

Note: Some events may be throttled because the frequently generated events can overload the MP or OAM server's system or event history log (e.g., generating an event for every ingress message failure). By specifying a throttle interval (in seconds), the events will appear no more frequently than once during the interval duration period (e.g., if the throttle interval is 5-seconds, the event will be logged no frequently than once every 5-seconds).

The following figure shows how Alarms and Events are organized in the application.

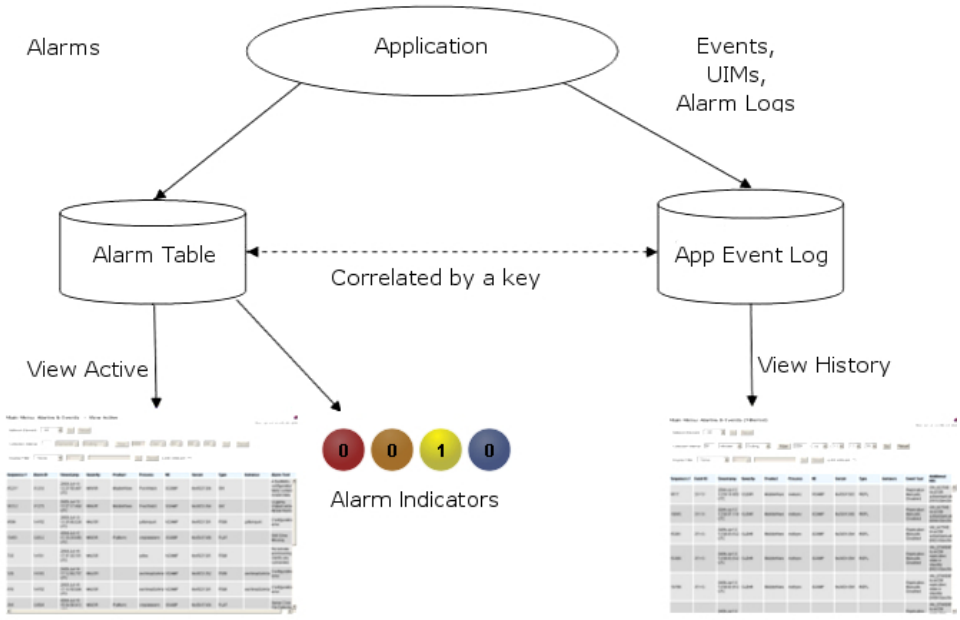


Figure 1: Flow of Alarms

Alarms and events are recorded in a database log table. Application event logging provides an efficient way to record event instance information in a manageable form, and is used to:

- Record events that represent alarmed conditions
- Record events for later browsing
- Implement an event interface for generating SNMP traps

Alarm indicators, located in the User Interface banner, indicate all critical, major, and minor active alarms. A number and an alarm indicator combined represent the number of active alarms at a specific level of severity. For example, if you see the number six in the orange-colored alarm indicator, that means there are six major active alarms.

●	Active Critical Alarm (bright red)
●	Active Major Alarm (bright orange)
●	Active Minor Alarm (bright yellow)
●	No active Critical Alarm (pale red)
●	No active Major Alarm (pale orange)
●	No active Minor Alarm (pale yellow)
○	Not Connected (white)

Figure 2: Alarm Indicators Legend

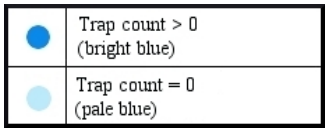


Figure 3: Trap Count Indicator Legend

Alarm and event ID ranges

The **AlarmID** listed for each alarm falls into one of the following process classifications:

Table 5: Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5099
OAM	10000-10999
SBR	12000-12999
ComAgent	19800-19909
DSR Diagnostics	19910-19999
Diameter	22000-22350, 22900-22999
RBAR	22400-22424
Generic Application	22500-22599
FABR	22600-22640
PDRA	22700-22799
CPA	22800-22849
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32700
GLA	33100-33149

Alarm and event types

This table describes the possible alarm/event types that can be displayed.

Note: Not all applications use all of the alarm types listed.

Table 6: Alarm and Event Types

Type Name	Type
APPL	Application
CAF	Communication Agent (ComAgent)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
CHG	Charging
CNG	Congestion Control
COLL	Collection
CPA	Charging Proxy Application
DAS	Diameter Application Server (Message Copy)
DB	Database
DIAM	Diameter
DISK	Disk
DNS	Domain Name Service
DPS	Data Processor Server
ERA	Event Responder Application
FABR	Full Address Based Resolution
HA	High Availability
HSS	Home Subscriber Server
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOG	Logging
MEAS	Measurements
MEM	Memory
NP	Number Portability
OAM	Operations, Administration & Maintenance
PDRA	Policy DRA
pSBR	Policy SBR
PLAT	Platform
PROC	Process

Type Name	Type
PROV	Provisioning
NAT	Network Address Translation
RBAR	Range-Based Address Resolution
REPL	Replication
SBRA	Session Binding Repository Application
SCTP	Stream Control Transmission Protocol
SDS	Subscriber Database Server
SIGC	Signaling Compression
SIP	Session Initiation Protocol Interface
SL	Selective Logging
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack
SW	Software (generic event type)
TCP	Transmission Control Protocol

Viewing active alarms

Active alarms are displayed in a scrollable, optionally filterable table. By default, the active alarms are sorted by time stamp with the most recent alarm at the top.

Use this procedure to view active alarms.

Note: The alarms and events that appear in **View Active** vary depending on whether you are logged in to an NOAMP or SOAM. Alarm collection is handled solely by NOAMP servers in systems that do not support SOAMs.

1. Select **Alarms & Events > View Active**.
   The **View Active** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The active alarms are displayed according to the specified criteria.

   The active alarms table updates automatically. When new alarms are generated, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

   If a new alarm is generated while automatic updates are suspended, a new message appears: `(Alarm updates are suspended. Available updates pending.)`

   To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

Active alarms data export elements

This table describes the elements on the **View Active Export** alarms page.

Table 7: Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting active alarms

You can schedule periodic exports of alarm data from the **Alarms and Events View Active** page. Active alarm data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **View Active** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Alarm details can be exported to a file by clicking the **Export** button on the **View Active** page. The system automatically creates and writes the exported active alarm details to a CSV file in the file management area.

If filtering has been applied in the **View Active** page, only filtered, active alarms are exported.

Use this procedure to export active alarms to a file.Use this procedure to schedule a data export task.

1. Select **Alarms & Events > View Active**.
   The **View Active** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The active alarms are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Active Alarm Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Active alarms data export elements* .
5. Select the **Export Frequency**.
6. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

7. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

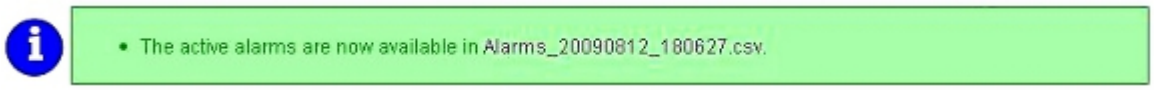
8. Click **OK** or **Apply** to initiate the active alarms export task.

   From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see .

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

   - *Viewing scheduled tasks*
   - *Editing a scheduled task*
   - *Deleting a scheduled task*
   - *Generating a scheduled task report*

9. Click **Export**.
   The file is exported.
10. Click the link in the green message box to go directly to the **Status & Manage > Files** page.



From the **Status & Manage > Files** page, you can view a list of files available for download, including the active alarms file you exported during this procedure. For more information, see *Opening a file*.

Generating a report of active alarms

Use this procedure to generate a report.

1. Select **Alarms & Events > View Active**.

   The **View Active** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The active alarms are displayed according to the specified criteria. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.
3. Click **Report**.
   The View Active Report is generated. This report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Viewing alarm and event history

All historical alarms and events are displayed in a scrollable, optionally filterable table. The historical alarms and events are sorted, by default, by time stamp with the most recent one at the top. Use this procedure to view alarm and event history.

Note: The alarms and events that appear in **View History** vary depending on whether you are logged in to an NOAMP or SOAM. Alarm collection is handled solely by NOAMP servers in systems that do not support SOAMs.

1. Select **Alarms & Events > View History** .
   The **View History** page appears.
2. If necessary, specify filter criteria and click **Go**.

   Note: Some fields, such as **Additional Info**, truncate data to a limited number of characters. When this happens, a **More** link appears. Click **More** to view a report that displays all relevant data.

   Historical alarms and events are displayed according to the specified criteria.

   The historical alarms table updates automatically. When new historial data is available, the table is automatically updated, and the view returns to the top row of the table.

3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

   If a new alarm is generated while automatic updates are suspended, a new message appears: `(Alarm updates are suspended. Available updates pending.)`

   To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

Historical events data export elements

This table describes the elements on the **View History Export** page.

Table 8: Schedule Event Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting alarm and event history

You can schedule periodic exports of historical data from the **Alarms and Events View History** page. Historical data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **View History** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

The details of historical alarms and events can be exported to a file by clicking the **Export** button on the **View History** page. The system automatically creates and writes the exported historical alarm details to a CSV file in the file management area.

If filtering has been applied in the **View History** page, only filtered historical alarms and events are exported. Use this procedure to export alarm and event history to a file. Use this procedure to schedule a data export task.

1. Select **Alarms & Events > View History**.
   The **View History** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Event Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Historical events data export elements* .
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes.**
7. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

8. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

9. Click **OK** or **Apply** to initiate the data export task.

   The data export task is scheduled. From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see .

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

   - *Viewing scheduled tasks*
   - *Editing a scheduled task*
   - *Deleting a scheduled task*
   - *Generating a scheduled task report*

10. Click **Export**.
    The file is exported.

11. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see *Opening a file*.

Generating a report of historical alarms and events

Use this procedure to generate a report.

1. Select **Alarms & Events > View History**.

   The **View History** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Report**.
   The View History Report is generated. This report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Security Log View History elements

This table describes the elements of the **Security Log > View History** page.

Table 9: Security Log View History Elements

Security Log History Element	Element Description
Timestamp	The date and time the security record was generated (fractional seconds resolution).
User	The user initiating the action.
Sess ID	The session identifier.
Remote IP	The remote IP address for the user.
Message	Summary details about the action which generated the security record.
Status	The status of the action, either SUCCESS or ERROR.
Screen	The page on which the action occurred, the Login page, for example.
Action	The user action, login, for example.
Details	Additional details about the action which generated the security record.

Security Log History Element	Element Description
Server	The server which processed the action.

Viewing security log files

Use this procedure to view security log files.

1. Select **Security Log > View History**.

   The **View History** page appears.

2. Specify the **Collection Interval**.
3. If necessary, specify filter criteria and click **Go**.

   Note: Some fields, such as **Details**, truncate data to a limited number of characters. When this happens, a **More** link appears. Click **More** to view a report that displays all relevant data.

The security log history is displayed according to the specified criteria.

Security log data export elements

This table describes the elements on the **View History Export Security Log** page.

Table 10: Schedule Security Log Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Once, Hourly, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Export Frequency, this is the minute of each hour	Format: Textbox or Scrolling List Range: 0 to 59

Element	Description	Data Input Notes
	when the data will be written to the export directory.	Default: 0
Time of Day	Time of day the export occurs	Format: Scrolling List Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting security log files

You can schedule periodic exports of security log data from the **Security Log View History** page. Security log data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **View History** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to export security log files.Use this procedure to schedule a data export task.

1. Select **Security Log > View History**.

   The **View History** page appears.

2. If necessary, specify filter criteria and click **Go**.
   The security log files are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Security Log Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Security log data export elements* .
5. Enter a **Description** for the export task.
6. Select the **Export Frequency**.
7. If you selected Hourly as the export frequency, select the **Minute** of each hour for the data export.
8. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

9. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

10. Click **OK** or **Apply** to initiate the security log export task.

From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see .

Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

- *Viewing scheduled tasks*
- *Editing a scheduled task*
- *Deleting a scheduled task*
- *Generating a scheduled task report*

11. Click **Export**.
    The file is exported.
12. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

From the **Status & Manage > Files** page, you can view a list of files available for download, including the security log history you exported during this procedure.

If an export fails for any reason, an error message appears indicating this failure.

Note: Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export doesn't start. You must wait until the other export is complete before you can begin your export.

Generating a Security Log report

Use this procedure to generate a report.

1. Select **Security Log > View History**.

   The **View History** page appears.

2. Specify the **Collection Interval**.
3. Specify the filter criteria, if necessary, and click **Go**.
   The security log files are displayed according to the specified criteria. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.
4. Click **Report**.
   The Security Log Report is generated. This report can be printed or saved to a file.
5. Click **Print** to print the report.
6. Click **Save** to save the report to a file.

OAM (10000-10999)

This section provides information and recovery procedures for OAM alarms, ranging from 10000-10999.

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of alarm types see *Alarm and event types*.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm
- Instance: the instance of a managed object for which an alarm or event is generated.

  Note: The value in the Instance field can vary, depending on the process generating the alarm.

- HA Score: high availability score; determines if switchover is necessary
- Auto Clear Seconds: the number of seconds that have to pass before the alarm will clear itself.

  Note: Some alarms and events have an Auto Clear Seconds of 0 (zero), indicating that these alarms and events do not auto-clear

- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

10000 - Incompatible database version

Alarm Type: DB

Description: The database version is incompatible with the installed software database version.

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: 300

OID: tekelecIncompatibleDatabaseVersionNotify

Recovery: Contact the Tekelec *Customer Care Center*.

10001 - Database backup started

Event Type: DB

Description: The database backup has started.

Severity: Info

Instance: GUI

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecBackupStartNotify

Recovery: No action required.

10002 - Database backup completed

Event Type: DB

Description: Backup completed

Severity: Info

Instance: GUI

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecBackupCompleteNotify

Recovery:

No action required.

10003 - Database backup failed

Event Type: DB

Description: The database backup has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecBackupFailNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

10004 - Database restoration started

Event Type: DB

Description: The database restoration has started.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecRestoreStartNotify

Recovery:

No action required.

10005 - Database restoration completed

Event Type: DB

Description: The database restoration is completed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecRestoreCompleteNotify

Recovery:

No action required.

10006 - Database restoration failed

Event Type: DB

Description: The database restoration has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecRestoreFailNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

10008 - Database provisioning manually disabled

Alarm Type: DB

Description: Database provisioning has been manually disabled.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecProvisioningManuallyDisabled

Recovery:

No action required.

10009 - Config and Prov db not yet synchronized

Alarm Type: REPL

Description: The configuration and the provisioning databases are not yet synchronized.

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: oAGTCfgProvDbNoSync

Recovery:

1. Monitor the replication status using the Status & Manage > Replication GUI page.
2. If alarm persists for more than one hour, contact Tekelec *Customer Care Center*.

10010 - Stateful db from mate not yet synchronized

Alarm Type: HA

Description: The stateful database is not synchronized with the mate database.

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: oAGTStDbNoSync

Recovery:

If alarm persists for more than 30 seconds, contact the Tekelec *Customer Care Center*.

10011 - Cannot monitor table

Alarm Type: OAM

Description: Monitoring for table cannot be set up.

Severity: Major

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: oAGTCantMonitorTable

Recovery:

Contact the Tekelec *Customer Care Center*.

10012 - Table change responder failed

Alarm Type: OAM

Description: The responder for a monitored table failed to respond to a table change.

Severity: Major

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: oAGTResponderFailed

Recovery:

Contact the Tekelec *Customer Care Center*.

10013 - Application restart in progress

Alarm Type: HA

Description: An application restart is in progress.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: oAGTApplSWDisabled

Recovery:

If duration of alarm is greater than two seconds, contact the Tekelec *Customer Care Center*.

10020 - Backup failure

Alarm Type: DB

Description: Database backup failed.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: apwBackupFailure

Recovery:

Alarm will clear if a backup (Automated or Manual) of the same group data is successful. Contact the Tekelec *Customer Care Center* if failures persist.

10074 - Standby server degraded while mate server stabilizes

Alarm Type: HA

Description: The standby server has temporarily degraded while the new active server stabilizes following a switch of activity.

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: hASbyRecoveryInProgress

Recovery:

No action required; the alarm clears automatically when standby server is recovered. This is part of the normal recovery process for the server that transitioned to standby as a result of a failover.

10075 - Application processes have been manually stopped

Alarm Type: HA

Description: The server is no longer providing services because application processes have been manually stopped.

Severity: Minor

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: haMtceStopApplications

Recovery:

If maintenance actions are complete, restart application processes on the server from the **Status & Manage** > **Servers** page by selecting the Restart Applications action for the server that raised the alarm.

Once successfully restarted the alarm will clear.

10078 - Application not restarted on standby server due to disabled failure cleanup mode

Event Type: HA

Description: The Applications on the Standby server have not been restarted after an active-to- standby transition since h_FailureCleanupMode is set to 0.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: failureRecoveryWithoutAppRestart

Recovery:

Contact the Tekelec *Customer Care Center*.

10100 - Log export started

Event Type: LOG

Description: Log files export operation has started.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportStart

Recovery:

No action required.

10101 - Log export successful

Event Type: LOG

Description: The log files export operation completed successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportSuccess

Recovery:

No action required.

10102 - Log export failed

Event Type: LOG

Description: The log files export operation failed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportFailed

Recovery:

1. Verify the export request and try the export again.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

10103 - Log export already in progress

Event Type: LOG

Description: Log files export operation not run - export can only run on Active Network OAMP server.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportNotRun

Recovery:

Restart export operation after existing export completes.

10104 - Log export file transfer failed

Event Type: LOG

Description: The performance data export remote copy operation failed.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecExportXferFailed

Recovery:

Contact the Tekelec *Customer Care Center* for assistance.

10105 - Log export cancelled - user request

Event Type: LOG

Description: The log files export operation cancelled by user.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportCancelledUser

Recovery:

Contact the Tekelec *Customer Care Center* for assistance.

10106 - Log export cancelled - duplicate request

Event Type: LOG

Description: The log files export operation was cancelled because a scheduled export is queued already.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportCancelledDuplicate

Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. If the problem persists, contact the Tekelec *Customer Care Center* for assistance.

10107 - Log export cancelled - queue full

Event Type: LOG

Description: The log files export operation cancelled because the export queue is full.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportCancelledDuplicate

Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.
2. If the problem persists, contact the Tekelec *Customer Care Center* for assistance.

10108 - Duplicate scheduled log export task

Alarm Type: LOG

Description: A duplicate scheduled log export task has been queued.

Severity: Minor

Instance: <Target ID>

Note: <Target ID> refers to the scheduled task ID found by running a report from **Main Menu** > **Status & Manage** > **Tasks** > **Scheduled Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportDupSchedTask

Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. If the problem persists, contact the Tekelec *Customer Care Center* for assistance.

10109 - Log export queue is full

Alarm Type: LOG

Description: The log export queue is full

Severity: Minor

Instance: <Queue Name>

Note: <Queue Name> refers to the name of the queue used for the export task ID found by running a report from either **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks** or **Main Menu** > **Status & Manage** > **Tasks** > **Scheduled Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogExportQueueFull

Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure that the queue does not fill up.
2. If the problem persists, contact the Tekelec *Customer Care Center* for assistance.

10151 - Login successful

Event Type: LOG

Description: The login operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLoginSuccess

Recovery:

No action required.

10152 - Login failed

Event Type: LOG

Description: The login operation failed

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLoginFailed

Recovery:

Verify login information and case is correct, and re-enter.

10153 - Logout successful

Event Type: LOG

Description: The logout operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecLogoutSuccess

Recovery:

No action required.

10154 - User Account Disabled

Event Type: LOG

Description: User account has been disabled

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: userAccountDisabled

Recovery:

The alarm will clear if the account is automatically re-enabled. Otherwise, the administrator must enable or delete user account.

10200 - Remote database reinitialization in progress

Alarm Type: CFG

Description: The remote database reinitialization is in progress. This alarm is raised on the active NOAMP server for the server being added to the server group.

Severity: Minor

Instance: <hostname of remote server>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: apwSgDbReinit

Recovery:

1. Check to see that the remote server is configured.
2. Make sure the remote server is responding to network connections.
3. If this does not clear the alarm, delete this server from the server group.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

HLR Router Alarms (14000-14999)

This section provides information and recovery procedures for HLR Router alarms, ranging from 14000 - 14999.

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of alarm types see *Alarm and event types*.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm
- Instance: the instance of a managed object for which an alarm or event is generated.

  Note: The value in the Instance field can vary, depending on the process generating the alarm.

- HA Score: high availability score; determines if switchover is necessary
- Auto Clear Seconds: the number of seconds that have to pass before the alarm will clear itself.

  Note: Some alarms and events have an Auto Clear Seconds of 0 (zero), indicating that these alarms and events do not auto-clear

- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

14100 - PDB interface disabled

Alarm Type: PDBI

Description: The PDBI Interface has been manually disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdbiInterfaceDisabledNotify

Recovery:

Enable the PDBI interface.

14101 - No remote client connections

Alarm Type: PDBI

Description: PDBI is enabled and no remote provisioning clients are connected.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdbiNoRemoteConnectionsNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG Database > Configuration > PDBI > Connections** and make sure the appropriate PDBI connections are configured. If they are not configured, insert the PDBI connections.
3. Confirm that the remote clients are running.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14102 - PDBI Connection failed

Alarm Type: PDBI

Description: Initialization has failed.

Severity: Major

Instance: Connection ID : IP Address

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterPdbiConnectionFailedNotify

Recovery:

1. Check the connectivity between the primary NOAMP and the provisioning clients.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

14120 - PDBI Connection established

Event Type: PDBI

Description: This event is generated each time a remote provisioning client has successfully established a connection.

Instance: Connection ID : IP Address

OID: eagleXgHlrRouterPdbiConnectionEstablishedNotify

Recovery:

Informational event; no action required.

14121 - PDBI Connection terminated

Event Type: PDBI

Description: This event is generated each time a remote provisioning client connection terminates.

Instance: Connection ID : IP Address

OID: eagleXgHlrRouterPdbiConnectionTerminatedNotify

Recovery:

Informational event; no action required.

14122 - PDBI connection denied

Event Type: PDBI

Description: This event is generated each time a local or remote provisioning client initiated connection establishment is denied due to:

- interface not enabled
- connection originating from an unauthorized IP address
- maximum number of allowed remote client connections have been reached
- connection to standby PDBA not permitted

Instance: Connection ID : IP Address

OID: eagleXgHlrRouterPdbiConnectionDeniedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG Database > Configuration > PDBI > Connections**:
   - make sure the Allow Connections box is checked.
   - check to see if the Maximum Number of Connections on this page has been exceeded.
3. If step 2 does not resolve the alarm, select **Eagle XG Database > Configuration > PDBI > Connections**.
4. Check if the connection listed is an allowed connection.
   - If the connection is not allowed, insert a new connection.
   - If the connection is allowed, click the corresponding **Edit** button and make sure the connection is configured properly.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

14140 - PDB import throttled

Alarm Type: PDBI

Description: PDB import throttled to prevent from overrunning IDB service processes.

Severity: Minor

Instance: Connection ID : IP Address

HA Score: Normal

Auto Clear Seconds: 5

OID: eagleXgHlrRouterPdbiImportThrottledNotify

Recovery:

1. The alarm is automatically cleared within five seconds of when the throttling subsides.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

14150 - PDB import initialization failed

Alarm Type: PDBI

Description: Initialization error.

Severity: Major

Instance: pdbimport

HA Score: Normal

Auto Clear Seconds: 43200

OID: eagleXgHlrRouterPdbiImportInitializationFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following import options:
   - Remote Import Enabled
   - Remote Import Mode
   - Remote Import Host IP Address
   - Remote Import User
   - Remote Import Password
   - Remote Import Directory
3. Clear any incorrect import options and replace with the correct import configuration.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14151 - PDB import generation failed

Alarm Type: PDBI

Description: File import has failed.

Severity: Major

Instance: pdbimport

HA Score: Normal

Auto Clear Seconds: 43200

OID: eagleXgHlrRouterPdbiImportGenerationFailedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

14152 - PDB import transfer failed

Alarm Type: PDBI

Description: File transfer from remote host has failed.

Severity: Major

Instance: pdbimport

HA Score: Normal

Auto Clear Seconds: 43200

OID: eagleXgHlrRouterPdbiImportTransferFailedNotify

Recovery:

1. Check the remote host connectivity.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following import options:
   - Remote Import Enabled
   - Remote Import Mode
   - Remote Import Host IP Address
   - Remote Import User
   - Remote Import Password
   - Remote Import Directory
3. Clear any incorrect import options and replace with the correct import configuration.
4. This alarm can be caused by an invalid ssh-key exchange. To recover from an invalid ssh-key that has created in error
   a) Deselect/clear all the current data fields for remote import, then **Apply** the settings
   b) Reset all the data fields for remote import, then **Apply** the settings.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

14153 - PDB export initialization failed

Alarm Type: PDBI

Description: Export initialization error

Severity: Major

Instance: pdbexport

HA Score: Normal

Auto Clear Seconds: 43200

OID: eagleXgHlrRouterPdbiExportInitializationFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following export options:
   - Remote Export Transfers Enabled
   - Remote Export Host IP Address
   - Remote Export User
   - Remote Export Password

- Remote Export Directory

3. Clear any incorrect export options and replace with the correct export configuration.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14154 - PDB export generation failed

Alarm Type: PDBI

Description: The scheduled export has failed.

Severity: Major

Instance: pdbexport

HA Score: Normal

Auto Clear Seconds: 43200

OID: eagleXgHlrRouterPdbiExportGenerationFailedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

14155 - PDB export transfer failed

Alarm Type: PDBI

Description: Failure to transfer file to the remote host

Severity: Major

Instance: pdbexport

HA Score: Normal

Auto Clear Seconds: 43200

OID: eagleXgHlrRouterPdbiExportTransferFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following export options:
   - Remote Export Transfers Enabled
   - Remote Export Host IP Address
   - Remote Export User
   - Remote Export Password
   - Remote Export Directory
3. Clear any incorrect export options and replace with the correct export configuration.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14160 - PDBI Import successful

Event Type: PDBI

Description: This event is generated each time a PDBI import is successful.

Instance: pdbiimport

OID: eagleXgHlrRouterPdbiImportOperationCompletedNotify

Recovery:

Informational event; no action required.

14161 - PDBI Export successful

Event Type: PDBI

Description: This event is generated each time a PDBI export is successful.

Instance: pdbiexport

OID: eagleXgHlrRouterPdbiExportOperationCompletedNotify

Recovery:

Informational event; no action required.

14170 - EPAP Audit started and in progress

Event Type: PDBI

Description: EPAP Audit started and in progress.

Instance: PDBA

OID: pdbiEpapAuditStartedAndInProgress

Recovery:

No action required.

14171 - EPAP Audit aborted

Event Type: PDBI

Description: EPAP Audit aborted.

Instance: PDBA

OID: pdbiEpapAuditAborted

Recovery:

No action required.

14172 - EPAP Audit failed to complete

Event Type: PDBI

Description: EPAP Audit failed to complete.

Instance: PDBA

OID: pdbiEpapAuditFailedToComplete

Recovery:

This condition may indicate that a connection was down or lost and the audit status shows as "Failed." Please contact Tekelec Customer Care for assistance.

14173 - EPAP Audit completed

Event Type: PDBI

Description: EPAP Audit completed.

Instance: PDBA

OID: pdbiEpapAuditCompleted

Recovery:

No action required.

14174 - NPA Split activation failed

Event Type: PDBI

Description: NPA Split activation failed.

Instance: PDBA

OID: pdbiNpaSplitActivationFailed

Recovery:

This condition may indicate the system error, and the NPA split status now shows as "Failed." Please contact Tekelec Customer Care for assistance.

14175 - NPA Split started and is active

Event Type: PDBI

Description: NPA Split started and is active.

Instance: PDBA

OID: pdbiNpaSplitStartedAndIsActive

Recovery:

No action required.

14176 - NPA Split completion failed

Event Type: PDBI

Description: NPA Split completion failed.

Instance: PDBA

OID: pdbiNpaSplitCompletionFailed

Recovery:

This condition may indicate the system error, and the NPA split status now shows as "Failed." Please contact Tekelec Customer Care for assistance.

14177 - NPA Split completed

Event Type: PDBI

Description: NPA Split completed.

Instance: PDBA

OID: pdbiNpaSplitCompleted

Recovery:

No action required.

14200 - Failed to initialize PDE task

Alarm Type: PDE

Description: The application failed to initialize the PDE task.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeInitFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > PDE > Options.**
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14201 - PDE failed to collect performance data

Alarm Type: PDE

Description: Performance data was not collected by PDE.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeCollectionFailedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

14202 - PDE failed to generate report in CSV format

Alarm Type: PDE

Description: The PDE has failed to generate a report in format.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeGenerationFailedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

14203 - PDE failed to transfer CSV file

Alarm Type: PDE

Description: The PDE has failed to transfer the CSV file.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeTransferFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > PDE > Options.**
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14210 - Failed to initialize Key Exchange for PDE

Alarm Type: PDE

Description: The key exchange for PDE has failed to initialize.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeKeyExchInitFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > PDE > Options.**
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14211 - Failed to exchange keys for PDE

Alarm Type: PDE

Description: The key exchange for PDE has failed.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeKeyExchangeFailedNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > PDE > Options.**
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14212 - Failed to delete password from PDE Options table

Alarm Type: PDE

Description: The password was not deleted from the PDE Options table.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: eagleXgHlrRouterPdeDeletePasswordFailedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

14230 - PDE successful

Event Type: PDE

Description: This event is generated each time a PDE task is successfully completed.

Instance: N/A

OID: eagleXgHlrRouterPdeAgentSuccessNotify

Recovery:

Informational event; no action required.

14231 - PDE Key Exchange successful

Event Type: PDE

Description: This event is generated each time a PDE key exchange is successfully completed.

Instance: N/A

OID: eagleXgHlrRouterPdeKeyExchangeSuccessNotify

Recovery:

Informational event; no action required.

14301 - ERA Responder failed

Alarm Type: ERA

Description: The event responder failed.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autclear.

OID: eagleXgHlrRouterEraResponderFailedNotify

Recovery:

If the problem persists, contact the Tekelec *Customer Care Center*.

14400 - Default value not configured in ExhrOptions table

Alarm Type: HLR

Description: Asserted when the 'exhr' process attempts to use a default value that is not configured.

Severity: Major

Instance: Name of default value in ExhrOptions table

HA Score: Normal

Auto Clear Seconds: 5

OID: eagleXgHlrRouterSigDefaultValueNotConfiguredNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > Configuration > Options** and configure the following options as necessary:
   - Default Country Code
   - Default Network Destination Code
   - Default Mobile Country Code
   - Default Mobile Network Code
3. If the problem persists, contact the Tekelec *Customer Care Center*.

14401 - Service config entry not configured

Alarm Type: HLR

Description: Asserted when the 'exhr' process attempts to find a ServiceConfig entry for a TT/SSN pair that is not configured.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 5

OID: eagleXgHlrRouterSigServiceConfigEntryNotConfiguredNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > Configuration > Service Config.**
3. **Edit** an existing, or **Insert** a new, service configuration.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14402 - Number trans entry not configured

Alarm Type: HLR

Description: Asserted when the 'exhr' process attempts to find a NumberTrans entry for a CC/NDC that is not configured.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 5

OID: eagleXgHlrRouterSigNumberTransEntryNotConfiguredNotify

Recovery:

1. Log into the primary NOAMP.
2. Select **Eagle XG HLR Router > Configuration > Substitutions.**
3. **Edit** an existing, or **Insert** a new, substitution.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14403 - Exception entry not configured

Alarm Type: HLR

Description: Asserted when the 'exhr' process attempts to find an Exception entry for a TT/NP/DPC tuple that is not configured.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 5

OID: eagleXgHlrRouterSigExceptionEntryNotConfiguredNotify

Recovery:

1. Log into a SOAM.
2. Select **Eagle XG HLR Router > Configuration > Exception Routing.**
3. **Edit** an existing, or **Insert** a new, exception.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

14405 - Invalid CdPA GTI

Event Type: HLR

Description: The Called Party Global Title Indicator is invalid.

Instance: GTI

OID: eagleXgHlrRouterSigInvalidCdpaGtiNotify

Recovery:

1. Correct the Global Title Indicator.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

14406 - Cannot route to Network Entity

Event Type: HLR

Description: Data cannot be routed to the Network Entity.

Instance: Network Entity

OID: eagleXgHlrRouterSigCannotRouteToNetworkEntityNotify

Recovery:

1. Log into the active NOAMP.
2. Select **EAGLE XG Database > Configuration > Network Entity**.
3. Click the **Update** tab.
4. Look up the relevant Network Entity and fix the Network Entity's configuration.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

14407 - Mate not configured

Alarm Type: HLR

Description: The mated network entity is not configured.

Instance: Network Entity

OID: eagleXgHlrRouterSigMateNotConfiguredNotify

Recovery:

1. Log into the active NOAMP.
2. Select **EAGLE XG HLR Router > Configuration > Mated Entities**.
3. Insert a new Network Entity mate configuration.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

SS7/Sigtran Alarms (19000-19999)

This section provides information and recovery procedures for SS7/Sigtran alarms, ranging from 19000 - 19999.

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of alarm types see *Alarm and event types*.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm

- Instance: the instance of a managed object for which an alarm or event is generated.

  Note: The value in the Instance field can vary, depending on the process generating the alarm.

- HA Score: high availability score; determines if switchover is necessary
- Auto Clear Seconds: the number of seconds that have to pass before the alarm will clear itself.

  Note: Some alarms and events have an Auto Clear Seconds of 0 (zero), indicating that these alarms and events do not auto-clear

- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

19200 - RSP/Destination unavailable

Alarm Type: SS7

Description: Unable to access the SS7 Destination Point Code because the RSP status is Unavailable.

Severity: Critical

Instance: RSP Name

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: prodnameawpss7M3rlRspUnavailableNotify

Recovery:

1. RSP/Destination status can be monitored from **SS7/Sigtran>Maintenance >Remote Signaling Points**.
   - If the RSP/Destination becomes Unavailable due to a link set failure, the MP server will attempt to automatically recover all links not manually disabled.
   - If the RSP/Destination becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19201 - RSP/Destination route unavailable

Alarm Type: SS7

Description: Unable to access the SS7 Destination point code via this route.

Severity: Minor

Instance: <Route Name>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlRouteUnavailableNotify

Recovery:

1. Route status can be monitored from **SS7/Sigtran>Maintenance>Remote Signaling Points**.
   - If the route becomes Unavailable due to a link set failure, the MP server will attempt to automatically recover all links not manually disabled.
   - If the route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19202 - Linkset unavailable

Alarm Type: SS7

Description: The SS7 link set to an adjacent signaling point has failed.

Severity: Major

Instance: <LinkSetName>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlLinksetUnavailableNotify

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link set status can be monitored from **SS7/Sigtran>Maintenance>Linksets**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

19203 - Link unavailable

Alarm Type: SS7

Description: M3UA has reported to M3RL that a link is out of service.

Severity: Minor

Instance: <Link Name>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlLinkUnavailableNotify

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link status can be monitored from **SS7/Sigtran>Maintenance>Links**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

19204 - Preferred route unavailable

Alarm Type: SS7

Description: M3RL has started to utilize a lower priority (higher cost) route to route traffic toward a given destination address, because the higher priority (lower cost) route specified for that RSP/Destination has become Unavailable.

Severity: Major

Instance: RSP Name

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlPreferredRouteUnavailableNotify

Recovery:

1. If the preferred route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Route status can be monitored from **SS7/Sigtran>Maintenance>Remote Signaling Points**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

19205 - TFP received

Event Type: SS7

Description: The TFP message was received by M3RL layer; an adjacent point code has reported that it has no longer has any available routes to the RSP/Destination.

Instance: N/A

OID: awpss7M3rlTfpReceivedNotify

Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran>Maintenance>Remote Signaling Points**.
2. Follow local procedures to determine the reason that the PC was prohibited.

19206 - TFA received

Event Type: SS7

Description: TFA message received by M3RL layer; an adjacent point code has reported that it has an available route to the RSP/Destination.

Instance: N/A

OID: awpss7M3rlTfaReceivedNotify

Recovery:

Monitor the RSP/Destination status from **SS7/Sigtran>Maintenance>Remote Signaling Points**.

19207 - TFR received

Event Type: SS7

Description: TFR message received by M3RL layer; an adjacent point code has reported that an available route to the RSP/Destination has a restriction/limitation.

Instance: N/A

OID: awpss7M3rlTfrReceivedNotify

Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran>Maintenance>Remote Signaling Points**.
2. Follow local procedures to determine the reason that the PC was prohibited.

19208 - TFC received

Event Type: SS7

Description: TFC message received by M3RL layer; an adjacent or non-adjacent point code is reporting the congestion level of a RSP/Destination.

Instance: N/A

OID: awpss7M3rlTfcReceivedNotify

Recovery:

1. RSP/Destination status can be monitored from **SS7/Sigtran>Maintenance>Remote Signaling Points**.
2. Follow local procedures to determine the reason that the PC was prohibited.

19209 - M3RL routing error

Event Type: SS7

Description: A message was discarded due to a routing error.

Instance: N/A

OID: awpss7M3rlRoutingFailureInvalidDpcNotify

Recovery:

1. Each MP's assigned point code can be monitored from **SS7/Sigtran>Maintenance>Local Signaling Points**.
2. If the event was caused by:
   - The DPC of an egress message is not configured as a remote signaling point, then look at the routing label in the event additional information, determine the DPC, and verify that the DPC is configured as an RSP.
   - The DPC of an egress message is configured but not available for routing, then look at the routing label in the event additional information, determine the DPC, verify that a route exists for the DPC, and use the RSP status screen to verify that a route is available for the RSP.
   - The DPC of an ingress message does not match the TPC or CPC of the MP server group, then either signaling is being misdirected by the STP toward the MP, or the MP server's LSP is misconfigured. Look at the routing label in the event additional information for the OPC and DPC of the ingress message.
3. If a high number of these errors occurs, then an internal routing table problem may exist. Please contact Tekelec *Customer Care Center* for assistance.

19210 - M3RL routing error - invalid NI

Event Type: SS7

Description: The message was discarded due to a routing error. The NI (Network Indicator) value received in a message from the network is not assigned to the MP. This event is generated under the following circumstances:

- The NI in the MTP3 routing label of the ingress message is not supported for the given network signaling domain for a provisioned Local Signaling Point.
- For an ingress ANSI SCCP message, Bit-8 in the SCCP CDPA address indicator octet indicates that the CDPA is encoded as per international specifications:
  - A "0" in Bit 8 indicates that the address is international and that both the address indicator and the address are coded according to international specifications.
  - A "1" in Bit 8 indicates that the address is national and that both the address indicator and the address are coded according to national specifications.

    The NI cannot be International for ANSI messages, since the ordering of the subsystem number indicator field and the point code indicator fields are in the reverse order in the ITU specification.

Instance: N/A

OID: awpss7M3rlRoutingFailureInvalidNiNotify

Recovery:

1. The Signaling Transfer Point or Signaling Gateway routing tables may be inconsistent with the NI assigned to the MP. You can monitor each MP's assigned NI value from the GUI main menu under **SS7/Sigtran>Configuration> Local Signaling Points**.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19211 - M3RL routing error - invalid SI

Event Type: SS7

Description: The message was discarded due to a routing error. The SI value received in a message from the network is associated with a User Part that is not currently supported.

Instance: RSP Name

OID: awpss7M3rlRoutingFailureInvalidSiNotify

Recovery:

1. If the SI received is not a **0** (SNM) or **3** (SCCP), verify that the STP/SG and the point code that created the message have correct routing information.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

Alarm 19212

Alarm Type: SS7

Name: CFG-DB Validation Error

Description: An unexpected condition has occurred while performing a database update. Because the nature of the error was not critical, database updates are still enabled, but this error should be investigated as soon as possible by Tekelec.

Severity: Major

Instance: Not applicable

HA Score: Normal

Auto Clear Seconds: 0

Throttle Settings: 86,400 seconds

Resolution:

Call Tekelec Technical Services.

Alarm 19213

Alarm Type: SS7

Na me: CFG-DB Update Failure

Description: An unexpected condition has occurred while performing a database update. Because the nature of the error was critical, database updates are now disabled.

Severity: Critical

Instance: Not applicable.

HA Score: Normal

Auto Clear Seconds: 0

Throttle Settings: 86,400 seconds

Resolution:

Please contact Tekelec Technical Services immediately for assistance with this alarm.

Alarm 19214

Alarm Type: SS7

Name: CFG-DB post-update Error

Description: An unexpected condition has occurred while performing a database update. Because the nature of the error was not critical, database updates are still enabled, but this error should be investigated as soon as possible by Tekelec.

Severity: Major

Instance: Not applicable

HA Score: Normal

Auto Clear Seconds: 0

Throttle Settings: 86400 seconds

Resolution:

Please contact Tekelec Technical Services for assistance with this alarm.

Alarm 19215

Alarm Type: SS7

Name: CFG-DB post-update Failure

Description: An unexpected condition has occurred while performing a database update. Because the nature of the error was critical, database updates are now disabled.

Severity: Critical

Instance: Not applicable

HA Score: Normal

Auto Clear Seconds: 0

Throttle Settings: 86400 seconds

Resolution:

Please contact Tekelec Technical Services immediately for assistance with this alarm.

Alarm 19216

Alarm Type: SS7

Name: Measurement Initialization Failure

Description: Measurement subsystem initialization has failed for the specified measurement.

Severity: Critical

Instance: Not applicable

HA Score: Normal

Auto Clear Seconds: 0

Throttle Settings: 86400 seconds

Resolution:

PLease contact Tekelec Technical Services for assistance with this alarm.

19217 - Node isolated - all links down

Alarm Type: SS7

Description: All configured links are down; either failed or disabled. No M3UA signaling is possible. The node is isolated from the network. All M3UA connectivity to the SS7/Sigtran network has either failed or has been manually disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlNodeIsolatedAllLinkDownNotify

Recovery:

1. Select **SS7/Sigtran>Maintenance>Links** to check whether any of the links are manually disabled that should not be. If so, click **Enable** to enable the manually disabled links.
2. Select **SS7/Sigtran>Maintenance>Associations** to check whether any of the associations that host links are enabled but not in the **Normal** state:
   - If any associations are manually disabled that should not be, click **Enable** to enable the manually disabled associations.
   - If the association operational reason is **Connecting**, check the IP network to determine if IP connectivity still exists between the MP server and the IP signaling gateway.
   - If the association operational reason is **Up Pending**, check the IP signaling gateway to determine if M3UA has been disabled on the SG.
3. View the active alarms and event history logs by selecting **Alarms & Event >View Active** and **Alarms & Events>View History**. Look for significant events that may affect the IP network, associations, or links.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

19901 - CFG DB validation error

Alarm Type: STK

Description: A minor database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: dbcCfgDbValidationErrorNotify

Recovery:

Since the error is not critical, database updates are still enabled; nevertheless, this error should be investigated as soon as possible. Please contact the Tekelec *Customer Care Center* for assistance.

19902 - CFG DB update failure

Alarm Type: STK

Description: A critical database validation error was detected on the MP server during an update. The MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: dbcCfgDbUpdateFailureNotify

Recovery:

This error is critical and database updates are now disabled; contact the Tekelec *Customer Care Center* for assistance.

19903 - CFG DB post update error

Alarm Type: STK

Description: A minor database validation error was detected on the MP server after a database update. The MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are allowed.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: dbcCfgDbPostUpdateErrorNotify

Recovery:

Since this error is not critical, database updates are still enabled; nevertheless, this error should be investigated as soon as possible. Please contact the Tekelec *Customer Care Center* for assistance.

19904 - CFG DB post update failure

Alarm Type: STK

Description: A critical database validation error was detected on the MP server after a database update. The MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: dbcCfgDbPostFailureNotify

Recovery:

This error is critical and database updates are now disabled; contact the Tekelec *Customer Care Center*.

19905 - Measurement initialization failure

Alarm Type: STK

Description: The measurement subsystem initialization failed for the specified measurement.

Severity: Critical

Instance: <measTagName>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: dcbMeasurementInitializationFailureNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

19220 - Association down

Alarm Type: SS7

Description: A configured association is not in the ASP-UP protocol state. Additional information for the alarm can be found by locating the row with a sequence number that matches the active alarm sequence number in **Alarms & Events>View History** and viewing the **Additional Info** column. This column includes the local and remote IP addresses and ports, the administrative state, and the protocol state of the association.

Note: It is normal to have an association alarm if the association is in the **Blocked** or **Disabled** administrative state.

Severity: Minor

Instance: <AssocName>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7AssociationDownNotify

Recovery:

1. Verify that IP network connectivity exists between the MP server and the adjacent server.
2. If the association is manually **Blocked** or **Disabled**, then no further action is necessary.
3. Verify that the association's local IP address and port number are configured on the IP signaling gateway. This gateways accepts connections only from IP addresses and ports that it is configured to accept connections from.
4. Verify that the association's remote IP address and port correctly identify an SCTP listening port on the adjacent server.
5. Select **Alarms & Events>View History** and check the event history logs for additional SS7 events or alarms from this MP server.
6. Verify that the adjacent server on the signaling gateway is not under maintenance.
7. If the problem persists, contact the Tekelec *Customer Care Center*.

19221 - Failed to configure association

Event Type: SS7

Description: The socket options failed to set on the association. This event is generated any time an association cannot be configured to match that association's specific configuration set.

Instance: <AssocName>

OID: awpss7FailedToConfigureAssociationNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

19222 - Failed to connect association

Event Type: SS7

Description: The SCTP association failed to connect.

Instance: <AssocName>

OID: awpss7FailedToConnectAssociationNotify

Recovery:

1. Verify that the association's local IP address and port number are configured on the IP signaling gateway. This gateway accepts connections only from IP addresses and ports that it is configured to accept connections from.
2. Verify that the association's remote IP address and port correctly identify an SCTP listening port on the adjacent server.
3. Verify that IP network connectivity exists between the MP server and the adjacent server.
4. Select **Alarms & Events>View History** and check the event history logs for additional SS7 events or alarms from this MP server.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19223 - Received malformed SCTP message (invalid length)

Event Type: SS7

Description: A malformed message (i.e., one with a message length of zero or a message length greater than 512 bytes) is received on the association.

Instance: <AssocName>

OID: awpss7ReceivedMalformedSctpMessageNotify

Recovery:

1. Investigate the `from` IP address and port to determine what exceeds the expected SCTP maximum message length.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19224 - Far-end closed the association

Event Type: SS7

Description: The far-end of the SCTP association sent a SHUTDOWN or ABORT message to close the association.

Instance: <AssocName>

OID: awpss7FarEndClosedTheAssociationNotify

Recovery:

1. Investigate the adjacent server at the specified IP address and port to determine if it failed or if it is under maintenance.
2. Check the adjacent server for alarms or logs that might indicate the cause for their closing the association.
3. Follow local procedures to determine the reason that the far-end SSN is down. If it is not down, but it continues to be reported as down, contact the Tekelec *Customer Care Center*.

19225 - Association closed due to lack of response

Event Type: SS7

Description: The adjacent server at the specified IP address and port failed to respond to attempts to deliver an SCTP packet or SCTP heartbeat. The association is closed and the MP server automatically attempts to reestablish the connection.

Instance: <AssocName>

OID: awpss7AssociationClosedDueToLackOfResponseNotify

Recovery:

1. Verify that IP network connectivity still exists between the MP server and the adjacent server.
2. Select **Alarms & Events>View History** and check the event history logs for additional SS7 events or alarms from this MP server.
3. Verify that the adjacent server on the signaling gateway is not under maintenance.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

19226 - Timedout waiting for ASP-UP-ACK

Event Type: SS7

Description: When an association is in the **Enabled** administrative state, part of the association initialization involves sending an ASP-UP from the MP server and receiving an ASP-UP-ACK from the adjacent server. If ASP-UP is sent, but no ASP-UP-ACK is received within State Management ACK Timer milliseconds, this event is generated and the ASP-UP is attempted again. ASP-UP attempts will continue indefinitely until the association administrative state is set to **Blocked** or **Disabled**, or the SCTP transport fails, or the ASP-UP-ACK is received.

Instance: <AssocName>

OID: awpss7TimedOutWaitingForAspUpAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. Verify that the timer value for State Management ACK Timer is not set too short to allow the adjacent server to respond with an ASP-UP-ACK. This should be rare if the network is not congested.
3. If the problem persists, contact the Tekelec *Customer Care Center*.

19227 - Received unsolicited ASP-DOWN-ACK

Event Type: SS7

Description: The adjacent server at the specified IP address and port has sent an ASP-DOWN-ACK, but not in response to an ASP-DOWN message from the MP server. Normally this indicates that the far-end of the association is being taken down for maintenance. If the association administrative state is **Enabled**, the MP server will automatically attempt to bring the association back to ASP-UP. This is done by sending an ASP-UP. The MP server will continue to send ASP-UP until an ASP-UP-ACK is received, the SCTP association comes down, or the association administrative state is changed to **Blocked** or **Disabled**.

Instance: <AssocName>

OID: awpss7ReceivedUnsolicitedAspDownAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19228 - Local association maintenance state change

Event Type: SS7

Description: This event is generated if the association administrative state is manually changed.

Instance: <AssocName>

OID: awpss7LocalAssociationMaintenanceStateChangeNotify

Recovery:

No action required.

19229 - Timed out waiting for ASP-ACTIVE-ACK

Event Type: SS7

Description: No ASP-ACTIVE-ACK is received in response to an ASP-ACTIVE message on the link within State Management ACK Timer milliseconds.

Instance: <LinkName>

OID: awpss7TimedOutWaitingForAspActiveAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. Verify that the timer value for State Management ACK Timer is not set too short to allow the adjacent server to respond with an ASP-ACTIVE-ACK. This should be rare if the network is not congested.
3. If the problem persists, contact the Tekelec *Customer Care Center*.

19230 - Received unsolicited ASP-INACTIVE-ACK

Event Type: SS7

Description: An unsolicited ASP-INACTIVE-ACK is received on the link.

Instance: <LinkName>

OID: awpss7ReceivedUnsolicitedAspInactiveAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19231 - Received invalid M3UA message

Event Type: SS7

Description: The far-end has sent an invalid M3UA message to which the MP server has responded with an M3UA ERROR message.

Instance: <LinkName> or <AssocName> Information about the type of error and the accompanying diagnostic data is included in the event additional information.

OID: awpss7ReceivedInvalidM3uaMessageNotify

Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the malformed message.
   - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
   - Error code 0x03 indicates an unsupported M3UA message class.
   - Error code 0x04 indicates an unsupported M3UA message type.
   - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
   - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
   - Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
   - Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
   - Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
   - Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19232 - Failed to send DATA message

Event Type: SS7

Description: An attempt to send an M3UA DATA message has failed. The message has been discarded. Possible reasons for the failure include:

- The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing the MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
- The socket has closed just as the send was being processed.

Instance: <LinkName>

OID: awpss7FailedToSendDataMessageNotify

Recovery:

1. Select **Alarms & Events>View History** and check the event history logs for additional SS7 events or alarms from this MP server.
2. Verify that the adjacent server on the signaling gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.
3. If the problem persists, contact the Tekelec *Customer Care Center*.

19233 - Failed to send non-DATA message

Event Type: SS7

Description: An attempt to send an M3UA non-DATA message has failed. Non-DATA messages include SSNM, ASPSM, ASPTM, and MGMT messages. The message has been discarded. Possible reasons for the failure include:

- The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing the MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
- The socket has closed just as the send was being processed.

Instance: <LinkName> or <AssocName>

Note: Information about the type of error and the accompanying diagnostic data is included in the event additional information.

OID: awpss7FailedToSendNonDataMessageNotify

Recovery:

1. Select **Alarms & Events>View History** and check the event history logs for additional SS7 events or alarms from this MP server.
2. Verify that the adjacent server on the signaling gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.
3. If the problem persists, contact the Tekelec *Customer Care Center*.

19234 - Local link maintenance state change

Event Type: SS7

Description: The link administrative state is manually changed from one administrative state to another.

Instance: <LinkName>

OID: awpss7LocalLinkMaintenanceStateChangeNotify

Recovery:

1. No action required if this was an expected change due to some maintenance activity. Otherwise, security logs can be examined on the SOAM server to determine which user changed the administrative state.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19235 - Received M3UA error

Event Type: SS7

Description: An M3UA ERROR message is received from the adjacent server.

Instance: <LinkName> or <AssocName>

Note: Information about the type of error and the accompanying diagnostic data is included in the event additional information.

OID: awpss7ReceivedM3uaErrorNotify

Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the ERROR message.
   - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
   - Error code 0x03 indicates an unsupported M3UA message class.
   - Error code 0x04 indicates an unsupported M3UA message type.
   - Error code 0x05 indicates an unsupported M3UA traffic mode.
   - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
   - Error code 0x09 indicates an invalid SCTP stream identifier. A DATA message was sent on stream 0.
   - Error code 0x0D indicates that the message was refused due to management blocking. An ASP Up or ASP Active message was received, but refused for management reasons.
   - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
   - Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
   - Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
   - Error code 0x14 indicates that the destination status is unknown. This message can be sent in response to a DAUD from the MP server if the SG cannot or does not wish to provide the destination status or congestion information.
   - Error Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
   - Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19240 - Remote SCCP subsystem prohibited

Alarm Type: SS7

Description: The status of remote SCCP subsystem has changed to **Prohibited**.

Severity: Minor

Instance: <RMU>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7RemoteSccpSubsystemProhibitedNotify

Recovery:

1. You can monitor destination status from **SS7/Sigtran>Maintenance>Remote Signaling Points** and RMU/subsystem status from **SS7/Sigtran>Maintenance>Remote MTP3 Users**.

- If the subsystem's status changed to **Prohibited** because SCMG received a SSP message, an audit of the status of the RMU via the SCCP subsystem status test (SST) procedure is performed.
- If the subsystem's status changed to **Prohibited** because SCCP received a MTP-PAUSE indication from M3RL, then recovery actions of restoring the RSP/Destination status to **Available** will be invoked by M3RL.
- If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS `cause=unequipped user` indication from M3RL, then no automatic recovery will be initiated. Only manual action at the remote node can correct a remote point code that has not been configured with SCCP.
- If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS `cause=unknown` or `inaccessible` indication from M3RL, then SCCP will automatically invoke subsystem status testing depending upon the network type:
  - ANSI: subsystem status testing of all RMUs associated with the point code.
  - ITU: subsystem status testing SCMG (`SSN=1`) associated with the point code.

2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Select **Alarms & Events>View History** and check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. Follow local procedures to determine the reason that the far-end SSN is down. If it is not down, but it continues to be reported as down, contact the Tekelec *Customer Care Center*.

19241 - SCCP malformed or unsupported message

Event Type: SS7

Description: SCCP discarded a message because the message was malformed or unsupported. The following connectionless message types are supported: UDT, XUDT,UDTS, and XUDTS. The following SCMG message types are supported: SSA, SSP, and SST.

Instance: N/A

OID: awpss7SccpMsgTypeUnrecognizedNotify

Recovery:

1. Investigate:
   - If the originator of the message is misconfigured.
   - If the network is misconfigured, causing messages to be routed to the wrong RSP/Destination.
   - If the message type is currently unsupported.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19242 - SCCP Hop counter violation

Event Type: SS7

Description: SCCP discarded an ingress message because a Hop Counter violation was detected.

Instance: N/A

OID: awpss7SccpHopCounterViolationNotify

Recovery:

1. One of the following conditions causes this error:
   - The originator of the message is setting the initial value too low.
   - The message is being rerouted too many times by the STPs, possibly because of an STP routing misconfiguration that has caused message looping.
2. Contact the Tekelec *Customer Care Center*.

19243 - SCCP routing failure

Event Type: SS7

Description: SCCP was unable to route or process a message during SCCP processing for reasons (other than a global title translation failure, detected SCCP loop) possibly requiring operator intervention.

Instance: N/A

OID: awpss7SccpRoutingFailureNotify

Recovery:

1. These failures are typically associated with invalid information received in the SCCP messages. Check for the following:
   - A misconfiguration of the SCCP at the originating or terminating node
   - Network routing misconfiguration at the STPs
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19244 - SCCP routing failure network status

Event Type: SS7

Description: SCCP was unable to route or process a message during SCCP processing due to transient conditions such as RSP/destination failures and remote or local subsystem failures.

Instance: N/A

OID: awpss7SccpRoutingFailureNetworkStatusNotify

Recovery:

1. Monitor status on the GUI main menu as follows:
   - Destination status from **SS7/Sigtran>Maintenance>Remote Signaling Points**.
   - RMU/subsystem status from **SS7/Sigtran>Maintenance>Remote MTP3 Users**.
   - Local subsystem status from **SS7/Sigtran>Maintenance>Local SCCP Users**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.

5. If the problem persists, contact the Tekelec *Customer Care Center*.

19245 - SCCP GTT failure

Event Type: SS7

Description: SCCP Global Title Translation has failed to determine a destination for a PDU. SCCP is invoking the message return procedure. Note that this event is throttled once per 10-second interval.

Instance: N/A

OID: awpss7SccpGttFailureNotify

Recovery:

1. Global title translation has failed. For the cause of the failure, look at the SCCP return cause and the called party address information in the event additional information field. Look for the following items:
   - Missing global title translation data.
   - Incorrect called party address information in the ingress message.
   - Point code paused or congested.
   - Subsystem prohibited or congested.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

19246 - Local SCCP subsystem prohibited

Alarm Type: SS7

Description: The status of the local SCCP subsystem has changed to **Prohibited**. This alarm is raised for one of the following conditions:

- When a new local SSN is configured and is in the disabled state.
- When a GUI maintenance operation is performed to disable the state of the local SSN.·
- On a system restart where the local SSN was is disabled state prior to the system restart.

Severity: Major

Instance: <LSP>, <SSN>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: SCCPLocalSubsystemProhibited

Recovery:

To clear the alarm:

a) On the GUI main menu, select **SS7/Sigtran>Maintenance>Local SCCP User**.
b) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
c) Click **Enable** to put the appropriate local SSN in the enabled state.
   A confirmation message appears.

d) Click **OK**.

The **Enable** link will be grayed out once the SSN transitions to the enabled state.

19250 - SS7 process CPU utilization

Alarm Type: SS7

Description: The SS7 process, which is responsible for handling all SS7 traffic, is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, or Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7Ss7ProcessCpuUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage>Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The SS7 process may be experiencing problems. You monitor the alarm log from **Alarms & Events>View Active**.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19251 - Ingress message rate

Alarm Type: SS7

Description: The ingress message rate (messages per second) for the MP is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7IngressMsgRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage>Server.**
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second. Contact the Tekelec *Customer Care Center* for assistance if needed.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity. Contact the Tekelec *Customer Care Center* for assistance if needed.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

19252 - PDU buffer pool utilization

Alarm Type: SS7

Description: The percent utilization of the MP's PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: <PoolName> Values: ANSI, ITUI, ITUN

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7PduBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage>Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load.You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being de-allocated to the pool when a PDU is successfully transmitted into the network. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log from **Alarms & Events>View Active**.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19253 - SCCP stack event queue utilization

Alarm Type: SS7

Description: The percent utilization of the MP's SCCP stack event queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7SccpStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage>Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the SCCP Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log under **Alarms & Events>View Active**.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19254 - M3RL stack event queue utilization

Alarm Type: SS7

Description: The percent utilization of the MP's M3RL Stack Event Queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage>Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage >KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3RL Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events>View Active**.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19255 - M3RL network management event queue utilization

Alarm Type: SS7

Description: The percent utilization of the MP's M3RL Network Management Event Queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlNetMgmtEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage>Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP under **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP under **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3RL Network Management Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events>View Active**.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19256 - M3UA stack event queue utilization

Alarm Type: SS7

Description: The percent utilization of the MP's M3UA Stack Event Queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3uaStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage>Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3UA Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events>View Active**.
5. If the problem persists, contact the Tekelec *Customer Care Center*.

19258 - SCTP Aggregate Egress queue utilization

Alarm Type: SS7

Description: The percent utilization of events queued to all SCTP associations on the MP server is approaching maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events>View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7SctpAggregateAssocWriteQueueUtilNotify

Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events>View Active**.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage>Server**.
4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

6. If the problem persists, contact the Tekelec *Customer Care Center*.

Transport Manager Alarms and Events (19400-19499)

This section provides information and recovery procedures for alarms and events, ranging from 19400-19499.

Table 11: Transport Manager Alarms Summary

Alarm-ID	Alarm Condition	Severity	HA Score	Instance	MIB Required (Y/N)
19400	Transport Down	Major	Normal	Transport	Yes

Table 12: Transport Manger Events Summary

Event-ID	Event Condition	Scope / Instance	MIB Required (Y/N)
19401	Failed to configure Transport	Transport Name	No
19402	Failed to connect Transport	Transport Name	No
19403	Received malformed SCTP message (invalid length)	Transport Name	No
19404	Far-end closed the Transport	Transport Name	No
19405	Transport closed due to lack of response	Transport Name	No
19406	Local Transport maintenance state change	Transport Name	No
19407	Failed to send Transport DATA message	Transport Name	No
19408	Single Transport Egress-Queue Utilization	Transport Name	Yes
19409	*(Informational) Message Rejected By ACL Filtering*	*Transport Name*	*No*
19410	Adjacent Node IP Address state change	Transport Name	No

19411	SCTP Transport closed due to failure of multihoming validation.	Transport Name	No
19412	SCTP Transport Configuration mismatched for Adjacent Node IP Addresses	Transport Name	No
19413	SCTP Transport closed due to unsupported peer address event received	Transport Name	No

19400 - Transport Down

Alarm Type: TMF

Description: Transport Down

Severity: Major

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrTransportDownNotify

Recovery:

1. The Active alarm instance data, which can be viewed from **Main Menu** > **Alarms & Events** > **View Active**, contains the Transport Name as configured in **Main Menu** > **Transport Manager** > **Configuration** > **Transport**

   Additional Information for the alarm can be found in **Main Menu** > **Alarms & Events** > **View Active or View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column. This column will include the local and remote IP addresses and ports, the administrative state, and the protocol state of the association.

   This alarm is raised when:

   - The association is configured and the admin state is enabled, but the SCTP transport is not in the ASP-UP protocol state for the M3UA plugin, or
   - The association is configured, but the SCTP transport is not in the APP-UP state for other plugins

   Note: It is normal to have an association alarm if the association is in the Blocked or Disabled administrative state.

   This alarm is cleared when:

   - The association recieved an ASP-UP-ACK from the far-end and the SCTP transport in the ASP-UP state for the M3UA plugin, or
   - The SCTP transport is an APP-UP state for other plugins, or
   - The association is disabled/deleted

If an association's protocol state does not match the association's administrative state, the system will automatically attempt to recover the association if configured as Initiator and enabled. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed association (default: 10 seconds).

Association administrative states are set from **Main Menu** > **Transport Manager** > **Maintenance** > **'Transport'** by clicking on the desired action for the row containing the association. This screen is also used to monitor association status.

To troubleshoot:

- If the association is manually Blocked or Disabled, then no further action is necessary.
- Verify that the association's local IP address and port number are configured on the IP signaling gateway (Some signaling gateways will only accept connections from IP addresses and ports that they are configured to accept from).
- Verify that the association's remote IP address and port correctly identify an SCTP listening port on the adjacent server.
- Verify that IP network connectivity exists between the MP server and the adjacent server.
- Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
- Verify that the adjacent server on the signaling gateway is not under maintenance.
- Contact Tekelec for assistance if needed.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19401 - Failed to configure Transport

Alarm Type: TMF

Description: Failed to configure Transport

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrFailedToConfigureTransportNotify

Recovery:

OID: awptransmgrTransportDownNotify

1. A Transport is configured each time the Transport attempts to connect or reconnect. If transport configuration failes, please contact Tekelec for assistance.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

19402 - Failed to connect Transport

Alarm Type: TMF

Description: Failed to connect Transport

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrFailedToConnectTransportNotify

Recovery:

1. The Transport named in the Instance field has failed in a connection attempt. If configured as an SCTP Initiator, the system will automatically attempt to recover the association/connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If configured as an SCTP or UDP Listener, no further action is taken.

   To troubleshoot

   - Verify that the transport's local IP address and port number are configured on the ADjacent NOde (Some Nodes will only accept connections from IP addresses and ports they are configured to accept connections from).
   - Verify that the transport's remote IP address and port correctly identify an SCTP listening port on the adjacent node.
   - Verify that IP network connectivity exists between the MP and the adjacent node.
   - Verify that the timers in the transport's configuration set are not set too short to allow the connection to proceed. This should be rare if the IP network is functioning correctly.
   - Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
   - Verify that the adjacent server on the signaling gateway is not under maintenance.
   - Contact Tekelec for assistance if needed.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19403 - Received malformed SCTP message (invalid length)

Alarm Type: TMF

Description: 19403 - Received malformed SCTP message (invalid length)

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds: 0

OID: awptransmgrReceivedMalformedTransSctpMessageNotify

Recovery:

1. An SCTP message was recieved containing a message not valid in length.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

19404 - Far-end closed the Transport

Alarm Type: TMF

Description: Far-end closed the Transport

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrFarEndClosedTheTransportNotify

Recovery:

1. The far-end of the SCTP association sent a SHUTDOWN or ABORT message to close the association. If an Initiator, the MP server automatically attempts to reestablish the connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed association (default: 10 seconds). If a Listener, the MP server will only open the socket and await further messages from the far-end.

   To Troubleshoot:

   - Investigate the adjacent node at the specified IP address and port to determine if it failed or if it is under maintenance.
   - Check the adjacent node for alarms or logs that might indicate the cause for their closing the association.
   - Contact Tekelec for assistance if needed.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19405 - Transport closed due to lack of response

Alarm Type: TMF

Description: Transport closed due to lack of response

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrTransportClosedDueToLackOfResponseNotify

Recovery:

1. The adjacent node at the specified IP address and port failed to respond to attempts to deliver an SCTP DATA packet or SCTP heartbeat. If an SCTP Initiator, the transport is closed and the MP server automatically attempts to reestablish the connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If a Listener, the MP server will only open the socket and await further messages from the far-end.

To troubleshoot:

- Verify that IP network connectivity still exists between the MP server and the adjacent server.
- Verify that the timers in the transport's configuration set are not set too short to allow the signaling to succeed. This should be rare if the IP network is fuctioning correctly.
- Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
- Verify that the adjacent server on the signaling gateway is not under maintenance.
- Contact Tekelec for assistance if needed.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19406 - Local Transport maintenance state change

Alarm Type: TMF

Description: Local Transport maintenance state change

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrLocalTransportMaintenanceStateChangeNotify

Recovery:

1. No customer action is necessary if this was an expected change due to some maintenance activity. Otherwise, security logs can be examined on the NO/SO server to determine which user changed the administrative state.

   Transport status can be viewed using **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19407 - Failed to send Transport DATA Message

Alarm Type: TMF

Description: Failed to send Transport DATA Message

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrFailedToSendTransDataMessageNotify

Recovery:

1. An attempt to send an SS7 M3UA/ENUM DATA message has failed. The message has been discarded.

For SCTP, Possible reasons for the failure include:

- The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing hte MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
- The socket has closed just as the send was being processed.

To Troubleshoot:

- Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
- Verify that the adjacent server on the signaling gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.
- Contact Tekelec for assistance if needed.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19408 - Single Transport Egress-Queue Utilization

Alarm Type: TMF

Description: The percent utilization of the MP's single Transport Egress-Queue is approaching its maximum capacity

Severity: Based on defined Thresholds. Minor, Major, Critical Engineered Max Value = 1000

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrTransSingleWriteQueueUtilNotify

Recovery:

1. The percent utilization of the MP's Transport Writer Queue is approachign its maximum capacity. If this problem persists and the queue reaches 100% utilization, all new egress messages from the Transport will be discarded.

   This alarm should not normally occur when no other congestion alarms are asserted. This may occur for a variety of reasons:

   1. An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being recieved form the network.
   2. The SCTP Association Writer process may be experiencing a problem preventing it from processing events from its event queue. The alarm log should be examined form **Main Menu** > **Alarms & Events**. Contact Tekelec for assistance if needed.
   3. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining Mps in the server site. MP server status can be monitored form **Main Menu** > **Status & Control** > **Server Status**.
   4. The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be recieving approximately the same ingress transaction per second. Contact Tekelec for assistance if needed.
   5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Main Menu** > **Status & Control** > **KPI**

Display. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity. Contact TEkelec for assistance if needed.

2. If alarm persists, contact the Tekelec *Customer Care Center* .

19409 - Message Rejected by ACL Filtering

Alarm Type: TMF

Description: The message is rejected based on configured Access Control List for Transport

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrMessageRejectedByAclFilteringNotify

Recovery:

1. To troubleshoot:
   - Verify that the ENUM Server's IP address is the ACL, or that the ACL is empty.

   Contact Tekelec for assistance if needed.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

19410 - Adjacent Node IP Address state change

Alarm Type: TMF

Description: State change of an IP Address of a multihomed Adjacent Node in SCTP Transport

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrAdjIpAddrStateChangeNotify

Recovery:

1. To troubleshoot:
   - Verify that IP network connectivity still exists between the MP server and the adjacent server.

   Contact Tekelec for assistance if needed.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

19411 - SCTP Transport closed due to failure of multihoming validation

Alarm Type: TMF

Description: SCTP Transport closed due to failure of multihoming validation

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrSctpTransportRefusedNotify

Recovery:

1. If one of the IP Address Validation for Adjacent Nodes Failed.
   - If an IP address is configured for the Transport: the actual far-end IP address of the SCTP connection did not match the configured IP address for the Transport's validation mode.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

19412 - SCTP Transport Transport Configuration Mismatch

Alarm Type: TMF

Description: IP address advertised by an Adjacent Node in INIT/INIT-ACK chunk are different from configured IP Addresses

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrSctpTransportCfgMismatchNotify

Recovery:

1. Recheck the Configured IP Address and Transport configuration and validation mode.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

19413 - SCTP Transport closed due to unsupported peer type evenet recieved.

Alarm Type: TMF

Description: SCCTP Transport closed due to unsupported add/delete peer IP Address event recieved in Peer Address Notification

Severity: Info

Instance:

HA Score: Normal

Auto Clear Seconds:

OID: awptransmgrTransportClosedDueToUnsupportedEventNotify

Recovery:

1. Disable SCTP Dynamic Address Reconfiguration at the Adjacent Node.
2. If alarm persists, contact the Tekelec *Customer Care Center* .

Platform (31000-32700)

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32700.

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of Event types see *Alarm and event types*.
- Description: describes the reason for the alarm
- Default Severity: the severity of the alarm. This severity may vary, depending on user-defined and specific application settings.
- OID: alarm identifier that appears in SNMP traps
- Alarm ID: alarm identifier used internally to Tekelec
- Recovery: provides any necessary steps for correcting or preventing the alarm

31000 - S/W fault

Alarm Type: SW

Description: Program impaired by s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterSwFaultNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact Tekelec *Customer Care Center*.

31001 - S/W status

Alarm Type: SW

Description: Program status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterSWStatusNotify

Recovery:

No action required.

31002 - Process watchdog failure

Alarm Type: SW

Description: Process watchdog timed out

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterProcWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact Tekelec *Customer Care Center*.

31003 - Tab thread watchdog failure

Alarm Type: SW

Description: Tab thread watchdog timed out

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterTabThreadWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact Tekelec *Customer Care Center*.

31100 - Database replication fault

Alarm Type: SW

Description: The Database replication process is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact Tekelec *Customer Care Center*.

31101 - Database replication to slave failure

Alarm Type: REPL

Description: Database replication to a slave Database has failed

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbRepToSlaveFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31102 - Database replication from master failure

Alarm Type: REPL

Description: Database replication from a master Database has failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbRepFromMasterFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31103- DB Replication update fault

Alarm Type: REPL

Description: Database replication process cannot apply update to DB

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbRepUpdateFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact Tekelec *Customer Care Center*.

31104 - DB Replication latency over threshold

Alarm Type: REPL

Description: Database replication latency has exceeded thresholds

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbRepLatencyNotify

Recovery:

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, contact Tekelec *Customer Care Center*.

31105 - Database merge fault

Alarm Type: SW

Description: The database merge process (inetmerge) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbMergeFaultNotify

Recovery:

1. Export event history for the given server and inetmerge task.
2. Contact Tekelec *Customer Care Center*.

31106 - Database merge to parent failure

Alarm Type: COLL

Description: Database merging to the parent Merge Node has failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterDbMergeToParentFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31107 - Database merge from child failure

Alarm Type: COLL

Description: Database merging from a child Source Node has failed

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbMergeFromChildFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31108 - Database merge latency over threshold

Alarm Type: COLL

Description: Database Merge latency has exceeded thresholds

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbMergeLatencyNotify

Recovery:

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, contact Tekelec *Customer Care Center*

31109 - Topology config error

Alarm Type: DB

Description: Topology is configured incorrectly

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterTopErrorNotify

Recovery:

1. This alarm may occur during initial installation and configuration of a server. No action is necessary at that time.
2. If this alarm occurs after successful initial installation and configuration of a server, contact the Tekelec *Customer Care Center*.

31110 - Database audit fault

Alarm Type: SW

Description: The Database service process (idbsvc) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbAuditFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact Tekelec *Customer Care Center*.

31111 - Database merge audit in progress

Alarm Type: COLL

Description: Database Merge Audit between mate nodes in progress

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbMergeAuditNotify

Recovery:

No action required.

31112 - Stateful db synchronization from mate server

Alarm Type: REPL

Description: Stateful database is not yet synchronized with mate database.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 30

OID: eagleXgHlrRouterDbRepUpLogTransTimeoutNotify

Recovery:

No action required. Contact Tekelec *Customer Care Center* if this occurs frequently.

31113 - DB replication manually disabled

Alarm Type: REPL

Description: DB Replication Manually Disabled

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterDbReplicationManuallyDisabledNotify

Recovery:

No action required.

31114 - DB replication over SOAP has failed

Alarm Type: REPL

Description: Database replication of configuration data via SOAP has failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 3600

OID: eagleXgHlrRouterDbReplicationSoapFaultNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31115 - Database service fault

Alarm Type: SW

Description: The Database service process (idbsvc) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbServiceFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact Tekelec *Customer Care Center*.

31116 - Excessive shared memory

Alarm Type: MEM

Description: The amount of shared memory consumed exceeds configured thresholds

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterExcessiveSharedMemoryConsumptionNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31117 - Low disk free

Alarm Type: DISK

Description: The amount of free disk is below configured thresholds

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterLowDiskFreeNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact Tekelec *Customer Care Center*.

31118 - Database disk store fault

Alarm Type: DISK

Description: Writing the database to disk failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbDiskStoreFaultNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact Tekelec *Customer Care Center*.

31119 - Database updatelog overrun

Alarm Type: DB

Description: The Database update log was overrun increasing risk of data loss

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbUpdateLogOverrunNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31120 - Database updatelog write fault

Alarm Type: DB

Description: A Database change cannot be stored in the updatelog

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbUpdateLogWriteFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31121 - Low disk free early warning

Alarm Type: DISK

Description: The amount of free disk is below configured early warning thresholds

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterLowDiskFreeEarlyWarningNotify

Recovery:

1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
2. If there are no files known to be unneeded, contact Tekelec *Customer Care Center*.

31122 - Excessive shared memory early warning

Alarm Type: MEM

Description: The amount of shared memory consumed exceeds configured early warning thresholds

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31123 - Database replication audit command complete

Alarm Type: REPL

Description: ADIC found one or more errors that are not automatically fixable.

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbADICWarnNotify

Recovery:

No action required.

31124 - ADIC error

Alarm Type: REPL

Description: An ADIC detected errors

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbRepAuditCmdErrorNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31125 - Database durability degraded

Alarm Type: REPL

Description: Database durability has dropped below configured durability level

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbDurabilityDegradedNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server IMI addresses.
2. If the problem persists, contact Tekelec *Customer Care Center*.

31126- Audit blocked

Alarm Type: REPL

Description: Site Audit Controls blocked an inter-site replication audit due to the number in progress per configuration.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterAuditBlockedNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31127 - DB Replication Audit Complete

Alarm Type: REPL

Description: DB replication audit completed

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbRepAuditComplete

Recovery:

No action required.

31128 - ADIC Found Error

Alarm Type: REPL

Description: ADIC found one or more errors that are not automatically fixable.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbADICError

Recovery:

Contact the *Customer Care Center*.

31129 - ADIC Found Minor Issue

Alarm Type: REPL

Description: ADIC found one or more minor issues that can most likely be ignored

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 14400

OID: eagleXgHlrRouterDbADICWarn

Recovery:

No action required.

31130 - Network health warning

Alarm Type: NET

Description: Network health issue detected

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterNetworkHealthWarningNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server IMI addresses.
2. If the problem persists, contact Tekelec *Customer Care Center*.

31140 - Database perl fault

Alarm Type: SW

Description: Perl interface to Database is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbPerlFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31145 - Database SQL fault

Alarm Type: SW

Description: SQL interface to Database is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbSQLFaultNotify

Recovery:

1. Export event history for the given server, and Imysqld task.
2. Contact Tekelec *Customer Care Center*.

31146- DB mastership fault

Alarm Type: SW

Description: DB replication is impaired due to no mastering process (inetrep/inetrep).

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. Contact Tekelec *Customer Care Center*.

31147- DB upsynclog overrun

Alarm Type: SW

Description: UpSyncLog is not big enough for (WAN) replication.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbUpSyncLogOverrunNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31148- DB lock error detected

Alarm Type: DB

Description: The DB service process (idbsvc) has detected an IDB lock-related error caused by another process. The alarm likely indicates a DB lock-related programming error, or it could be a side effect of a process crash.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbLockErrorNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31200 - Process management fault

Alarm Type: SW

Description: The process manager (procmgr) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterProcMgmtFaultNotify

Recovery:

1. Export event history for the given server, all processes.
2. Contact Tekelec *Customer Care Center*.

31201 - Process not running

Alarm Type: PROC

Description: A managed process cannot be started or has unexpectedly terminated

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterProcNotRunningNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31202 - Unkillable zombie process

Alarm Type: PROC

Description: A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterProcZombieProcess

Recovery:

1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. Contact Tekelec *Customer Care Center*.

31206 - Process mgmt monitoring fault

Alarm Type: SW

Description: The process manager monitor (pm.watchdog) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterProcMgmtMonFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31207 - Process resource monitoring fault

Alarm Type: SW

Description: The process resource monitor (ProcWatch) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterProcResourceMonFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31208 - IP port server fault

Alarm Type: SW

Description: The run environment port mapper (re.portmap) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterPortServerFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31209 - Hostname lookup failed

Alarm Type: SW

Description: Unable to resolve a hostname specified in the NodeInfo table

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHostLookupFailedNotify

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, contact Tekelec *Customer Care Center*.

31213 - Process scheduler fault

Alarm Type: SW

Description: The process scheduler (ProcSched/runat) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterProcSchedulerFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31214 - Scheduled process fault

Alarm Type: PROC

Description: A scheduled process cannot be executed or abnormally terminated

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterScheduleProcessFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31215 - Process resources exceeded

Alarm Type: SW

Description: A process is consuming excessive system resources

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 14400

OID: eagleXgHlrRouterProcResourcesExceededFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31216 - SysMetric configuration error

Alarm Type: SW

Description: A SysMetric Configuration table contains invalid data

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterSysMetricConfigErrorNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31220 - HA configuration monitor fault

Alarm Type: SW

Description: The HA configuration monitor is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaCfgMonitorFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31221 - HA alarm monitor fault

Alarm Type: SW

Description: The high availability alarm monitor is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaAlarmMonitorFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31222 - HA not configured

Alarm Type: HA

Description: High availability is disabled due to system configuration

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaNotConfiguredNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31223 - HA Heartbeat transmit failure

Alarm Type: HA

Description: The high availability monitor failed to send heartbeat

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaHbTransmitFailureNotify

Recovery:

1. This alarm clears automatically when the server successfully registers for HA heartbeating.
2. If this alarm does not clear after a couple minutes, contact Tekelec *Customer Care Center*.

31224 - HA configuration error

Alarm Type: HA

Description: High availability configuration error

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaCfgErrorNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

31225 - HA service start failure

Alarm Type: HA

Description: The high availability service failed to start

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaSvcStartFailureNotify

Recovery:

1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, contact Tekelec *Customer Care Center*.

31226 - HA availability status degraded

Alarm Type: HA

Description: The high availability status is degraded due to raised alarms

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact Tekelec *Customer Care Center*.

31227 - HA availability status failed

Alarm Type: HA

Description: The high availability status is failed due to raised alarms

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaAvailFailedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact Tekelec *Customer Care Center*.

31228 - HA standby offline

Alarm Type: HA

Description: High availability standby server is offline

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterHaStandbyOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues and/or contact Tekelec *Customer Care Center*.

31229 - HA score changed

Alarm Type: HA

Description: High availability health score changed

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaScoreChangeNotify

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

Alarm Type: SW

Description: The recent alarm event manager (raclerk) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterRecAlarmEvProcFaultNotify

Recovery:

1. Export event history for the given server and raclerk task.
2. Contact Tekelec *Customer Care Center*.

31231 - Platform alarm agent fault

Alarm Type: SW

Description: The platform alarm agent impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterPlatAlarmAgentNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31232- Late heartbeat warning

Alarm Type: HA

Description: High availability server has not received a heartbeat within the configured interval. High availability server has not received a message on specified path within the configured interval.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaLateHeartbeatWarningNotify

Recovery:

No action required; this is a warning and can be due to transient conditions. If there continues to be no heartbeat from the server, alarm 31228 occurs.

31233 - HA Secondary Path DownHA Path Down

Alarm Type: HA

Description: High availability secondary path loss of connectivityHigh availability path loss of connectivity

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaSecPathDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the secondary path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues on the secondary network.
3. Contact the Tekelec *Customer Care Center*.

31234 - Untrusted Time Upon Initialization

Alarm Type: REPL

Description: Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server.

Severity: Critical

Instance:

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterUtrustedTimeOnInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, contact the *Customer Care Center*.

31235 - Untrusted Time After Initialization

Alarm Type: REPL

Description: After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, etc. There are often accompanying Platform alarms to guide correction. Generally, applications remaining be running, but time-stamped data is likely incorrect, reports may be negatively affected, some behavior may be improper, etc.

Severity: Critical

Instance:

HA Score: Normal

Auto Clear Seconds: 0

OID: eagleXgHlrRouterUntrustedTimePostOnInit

Recovery:

1. Correct NTP configuration.
2. If the problem persists, contact the *Customer Care Center*.

31240 - Measurements collection fault

Alarm Type: SW

Description: The measurments collector (statclerk) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterMeasCollectorFaultNotify

Recovery:

1. Export event history for the given server and statclerk task.
2. Contact Tekelec *Customer Care Center*.

31250 - RE port mapping fault

Alarm Type: SW

Description: The IP service port mapper (re.portmap) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterRePortMappingFaultNotify

Recovery:

This typically indicate a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.

31260 - Database SNMP Agent

Alarm Type: SW

Description: The Database SNMP agent (snmpIdbAgentcmsnmpa) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterDbcomcolSnmpAgentNotify

Recovery:

1. Export event history for the given server and all processes.
2. Contact Tekelec *Customer Care Center*.

31270 - Logging output

Alarm Type: SW

Description: Logging output set to Above Normal

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterLoggingOutputNotify

Recovery:

Extra diagnostic logs are being collected, potentially degrading system performance. Contact Tekelec *Customer Care Center*.

31280 - HA Active to Standby transition

Alarm Type: HA

Description: HA active to standby activity transition

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31281 - HA Standby to Active transition

Alarm Type: HA

Description: HA standby to active activity transition

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterStandbyToActiveTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31282- HA Management Fault

Alarm Type: HA

Description: The HA manager (cmha) is impaired by a software fault.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaMgmtFaultNotify

Recovery:

Export event history for the given server and cmha task, then contact Tekelec *Customer Care Center*.

31283- HA Server Offline

Alarm Type: HA

Description: High availability server is offline

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0

OID: eagleXgHlrRouterHAServerOfflineNotify

Recovery

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues and/or contact Tekelec *Customer Care Center*.

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Type: HA

Description: High availability remote subscriber has not received a heartbeat within the configured interval.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaRemoteHeartbeatWarningNotify

Recovery:

1. No action required. This is a warning and can be due to transient conditions. The remote subscriber will move to another server in the cluster.
2. If there continues to be no heartbeat from the server, contact the Tekelec *Customer Care Center*.

31290- HA Process Status

Alarm Type: HA

Description: HA manager (cmha) status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaProcessStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31291- HA Election Status

Alarm Type: HA

Description: HA DC Election status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHAElectionStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31292- HA Policy Status

Alarm Type: HA

Description: HA Policy plan status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaPolicyStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31293- HA Resource Link Status

Alarm Type: HA

Description: HA ResourceAgent Link status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaRaLinkStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31294- HA Resource Status

Alarm Type: HA

Description: HA Resource registration status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaResourceStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31295- HA Action Status

Alarm Type: HA

Description: HA Resource action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaActionStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31296- HA Monitor Status

Alarm Type: HA

Description: HA Monitor action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaMonitorStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31297- HA Resource Agent Info

Alarm Type: HA

Description: HA Resource Agent Info

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaRaInfoNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31298- HA Resource Agent Detail

Alarm Type: HA

Description: Resource Agent application detailed information

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaRaDetailNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31299 - HA Notification Status

Alarm Type: HA

Description: HA Notification status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaNotification

Recovery:

No action required.

31300 - HA Control Status

Alarm Type: HA

Description: HA Control action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgHlrRouterHaControl

Recovery:

No action required.

32113 - Uncorrectable ECC memory error

Alarm Type: TPD

Description: This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdEccUncorrectableErrorNotify

Recovery

Contact the Tekelec *Customer Care Center* to request hardware replacement.

32114 - SNMP get failure

Alarm Type: TPD

Description: The server failed to receive SNMP information from the switch.

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdSNMPGetFailure

Recovery

1. Use the following command to verify the switch is active: `ping switch1A/B` (this requires command line access).
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Type: TPD

This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good.

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPDaemonNotSynchronizedFailure

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32116 - TPD Server's Time Has Gone Backwards

Alarm Type: TPD

This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good.

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPTimeGoneBackwards

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32117 - TPD NTP Offset Check Failure

Alarm Type: TPD

This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ntpOffsetCheckFailure

Recovery:

1. Run syscheck in verbose mode.
2. Contact the Tekelec *Customer Care Center*.

32300 – Server fan failure

Alarm Type: TPD

Description: This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdFanErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32301 - Server internal disk error

Alarm Type: TPD

Description: This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdIntDiskErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32302 – Server RAID disk error

Alarm Type: TPD

Description: This alarm indicates that the offboard storage server had a problem with its hardware disks.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdRaidDiskErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32303 - Server Platform error

Alarm Type: TPD

Description: This alarm indicates an error such as a corrupt system configuration or missing files.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 9zero)

OID: eagleXgHlrRouterTpdPlatformErrorNotify

Recovery

Contact the *Customer Care Center* and provide the system health check output.

32304 - Server file system error

Alarm Type: TPD

Description: This alarm indicates unsuccessful writing to at least one of the server's file systems.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdFileSystemErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32305 - Server Platform process error

Alarm Type: TPD

Description: This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdPlatProcessErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32307 - Server swap space shortage failure

Alarm Type: TPD

Description: This alarm indicates that the server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdSwapSpaceShortageErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32308 - Server provisioning network error

Alarm Type: TPD

Description: This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdProvNetworkErrorNotify

Recovery

1. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.
2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.
4. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, contact the Tekelec *Customer Care Center*.

32312 - Server disk space shortage error

Alarm Type: TPD

Description: This alarm indicates that one of the following conditions has occurred:

- A filesystem has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the filesystem.
- More than 90% of the total number of available files have been allocated on the filesystem.
- A filesystem has a different number of blocks than it had when installed.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDiskSpaceShortageErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32313 - Server default route network error

Alarm Type: TPD

Description: This alarm indicates that the default network route of the server is experiencing a problem.

Caution: When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDefaultRouteNetworkErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32314 - Server temperature error

Alarm Type: TPD

Description: The internal temperature within the server is unacceptably high.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdTemperatureErrorNotify

Recovery

1. Ensure that nothing is blocking the fan's intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32315 – Server mainboard voltage error

Alarm Type: TPD

Description: This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdMainboardVoltageErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32316 – Server power feed error

Alarm Type: TPD

Description: This alarm indicates that one of the power feeds to the server has failed. If this alarm occurs in conjunction with any Breaker Panel alarm, there might be a problem with the breaker panel.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdPowerFeedErrorNotify

Recovery

1. Verify that all the server power feed cables to the server that is reporting the error are securely connected.
2. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
3. Follow the power feed to its connection on the power source. Ensure that the power source is ON and that the power feed is properly secured.
4. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
5. If the power source is functioning properly and the wires are all secure, have an electrician check the voltage on the power feed.
6. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
7. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32317 - Server disk health test error

Alarm Type: TPD

Description: Either the hard drive has failed or failure is imminent.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDiskHealthErrorNotify

Recovery

1. Perform the recovery procedures for the other alarms that accompany this alarm.
2. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32318 - Server disk unavailable error

Alarm Type: TPD

Description: The `smartd` service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDiskUnavailableErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32319 – Device error

Alarm Type: TPD

This alarm indicates that the offboard storage server had a problem with its disk volume filling up.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDeviceErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32320 – Device interface error

Alarm Type: TPD

Description: This alarm indicates that the IP bond is either not configured or down.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDeviceIfErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32321 – Correctable ECC memory error

Alarm Type: TPD

Description: This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdEccCorrectableErrorNotify

Recovery

No recovery necessary. If the condition persists, contact the Tekelec *Customer Care Center* to request hardware replacement.

32322 – Power Supply A error

Alarm Type: TPD

Description: This alarm indicates that power supply 1 (feed A) has failed.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdPowerSupply1ErrorNotify

Recovery

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32323 – Power Supply B error

Alarm Type: TPD

Description: This alarm indicates that power supply 2 (feed B) has failed.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdPowerSupply2ErrorNotify

Recovery

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32324 – Breaker panel feed error

Alarm Type: TPD

Description: This alarm indicates that the server is not receiving information from the breaker panel relays.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdBrkPnlFeedErrorNotify

Recovery

1. Verify that the same alarm is displayed by multiple servers:
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.
3. If the problem has not been resolved, call the Tekelec *Customer Care Center* to request that the breaker panel be replaced.

32325 – Breaker panel breaker error

Alarm Type: TPD

Description: This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see *Figure 4: Breaker Panel LEDs*) identify whether the fault occurred on the input power or the output power, as follows:

- A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit.

  Note: LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.

- A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.

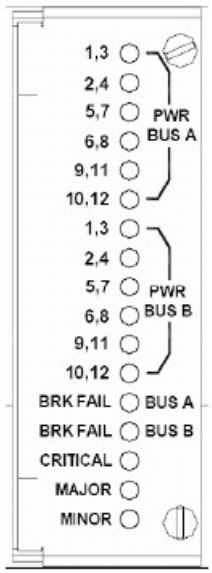


Figure 4: Breaker Panel LEDs

Description: This alarm indicates that a power fault has been identified by the breaker panel.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: TPDBrkPnlBreakerErrorNotify

Recovery

1. Verify that the same alarm is displayed by multiple serversboth servers (the single breaker panel normally sends alarm information to both servers):
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by both serversmultiple servers, go to the next step.
2. Look at the breaker panel assignments in *Figure 5: Breaker Panel Setting*. For each breaker assignment, and verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

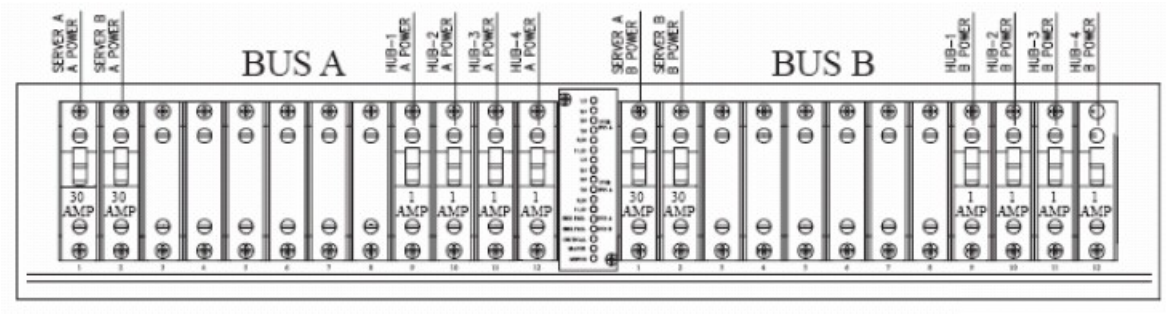


Figure 5: Breaker Panel Setting

If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Contact the Tekelec *Customer Care Center*

a) Verify that the customer provided source for the affected power feed is operational. If the power source is properly functioning, have an electrician remove the plastic cover from the rear of the breaker panel and verify the power source is indeed connected to the input power feed connector on the rear of the breaker panel. Correct any issues found.
b) Check the LEDs in the PWR BUS A group and the PWR BUS B group again.

- If the LEDs are now illuminated Green, the issue has been resolved.
- Proceed to *Substep c* to verify that the alarm has been cleared.
- If the LEDs are still illuminated Red, continue to the next sub-step.

c) Have the electrician verify the integrity of the input power feed. The input voltage should measure nominally -48VDC (that is, between -41VDC and -60VDC). If the supplied voltage is not within the acceptable range, the input power source must be repaired or replaced.

Note: Be sure the voltmeter is connected properly. The locations of the BAT and RTN connections are in mirror image on either side of the breaker panel.

If the measured voltage is within the acceptable range, the breaker panel may be malfunctioning. The breaker panel must be replaced.

d) Check the LEDs in the PWR BUS A group and the PWR BUS B group again after the necessary actions have been taken to correct any issues found.

- If the LEDs are now illuminated Green, the issue has been resolved. Proceed to *Step 3* to verify that the alarm has been cleared.
- If the LEDs are still illuminated Red, skip to *Step 4*

3. Check the BRK FAIL LEDs for BUS A and for BUS B.

- If one of the BRK FAIL LEDs is illuminated Red, then one or more of the respective Input Breakers has tripped. (A tripped breaker is indicated by the toggle located in the center position.) Perform the following steps to repair this issue:

a) For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.
b) After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, contact the Tekelec *Customer Care Center*

- If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, continue with the next step.
- If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise contact the Tekelec *Customer Care Center*

4. Check to see if the alarm has cleared.
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
5. If the problem has not been resolved, contact the Tekelec *Customer Care Center*

32326 – Breaker panel monitoring error

Alarm Type: TPD

Description: This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself.

Note: When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm

- 32324-Breaker Panel Feed Error or
- 32325-Breaker Panel Breaker Error

until the Breaker Panel Monitoring Error has been corrected.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdBrkPnlMntErrorNotify

Recovery

1. Verify that the same alarm is displayed by multiple servers:
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).
3. If the alarm has not been cleared, contact the Tekelec *Customer Care Center*.

32327 – Server HA Keepalive error

Alarm Type: TPD

Description: This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHaKeepaliveErrorNotify

Recovery

1. Determine if the mate server is currently down and bring it up if possible.
2. Determine if the keepalive interface is down.
3. Determine if heartbeart is running (service TKLCha status).

   Note: This step may require command line ability.

4. Contact the Tekelec *Customer Care Center*.

32331 – HP disk problem

Alarm Type: TPD

Description: This major alarm indicates that there is an issue with either a physical or logical disk in the HP disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHpDiskProblemNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32332 – HP Smart Array controller problem

Alarm Type: TPD

Description: This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHpDiskCtrlrProblemNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32333 – HP hpacucliStatus utility problem

Alarm Type: TPD

Description: This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus daemon is either not running, or hung.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHPACUCLIProblemNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32334 - Multipath device access link problem

Alarm Type: TPD

Description: One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdMpathDeviceProblemNotify

Recovery

32335 - Switch link down error

Alarm Type: TPD

Description: The link is down.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdSwitchLinkDownErrorNotify

Recovery

1. Verify the cabling between the port and the remote side.

2. Verify networking on the remote end.
3. If the problem persists, contact the Tekelec *Customer Care Center* who should verify port settings on both the server and the switch.

32336– Half Open Socket Limit

Alarm Type: TPD

Description: This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHalfOpenSockLimitNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32337 - E5-APP-B Firmware Flash

Alarm Type: TPD

Description: This alarm indicates there was an error while trying to update the firmware flash on the E5-APP-B cards.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.38

Recovery:

Contact the Tekelec *Customer Care Center*.

32338 - E5-APP-B Serial mezzanine seating

Alarm Type: TPD

Description: This alarm indicates the serial mezzanine board was not properly seated.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.39

Recovery:

Contact the Tekelec *Customer Care Center*.

32339 - Max pid limit

Alarm Type: TPD

Description: This alarm indicates that the maximum number of running processes has reached the major threshold.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMaxPidLimit

Recovery:

1. Run syscheck in verbose mode.
2. Contact the Tekelec *Customer Care Center*.

32340 - Server NTP Daemon Lost Synchronization

Alarm Type: TPD

Description: This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMaxPidLimit

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. Contact the Tekelec *Customer Care Center*.

32341 - Server NTP Daemon Never Synchronized Error

Alarm Type: TPD

Description: This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPDaemonNeverSynchronized

Recovery:

1. Verify NTP settings and that NTP sources can be reached.

2. Contact the Tekelec *Customer Care Center*.

32342 - NTP Offset Check Error

Alarm Type: TPD

Description: This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ntpOffsetCheckError

Recovery:

1. Verify NTP settings and that NTP are providing accurate time.
2. Contact the Tekelec *Customer Care Center*.

32343 - RAID disk problem

Alarm Type: TPD

Description: This alarms indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskProblem

Recovery:

1. Run syscheck in verbose mode.
2. Contact the Tekelec *Customer Care Center*.

32344 - RAID controller problem

Alarm Type: TPD

Description: This alarms indicates that RAID controller needs intervention. State reported by syscheck is not "Normal" and/or BBU (backup battery unit) state is not "Operational".

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskCtrlrProblem

Recovery:

1. Run syscheck in verbose mode.
2. Contact the Tekelec *Customer Care Center*.

32403 – PM&C backup failed

Alarm Type: PM&C

The PM&C application has a failure that needs to be investigated.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterpmacBackupErrorNotify

1. Attempt a manual backup using the PM&C GUI.
2. If the problems persists, contact the Tekelec *Customer Care Center*.

32500 – Server disk space shortage warning

Alarm Type: TPD

Description: This alarm indicates that one of the following conditions has occurred:

- A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system.
- More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDiskSpaceShortageWarningNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32501 – Server application process error

Alarm Type: TPD

Description: This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdApplicationProcessErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32502 – Server hardware configuration error

Alarm Type: TPD

Description: This alarm indicates that one or more of the server's hardware components are not in compliance with Tekelec specifications (refer to the appropriate hardware manual).

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHardwareConfigErrorNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32503 – Server RAM shortage warning

Alarm Type: TPD

Description: This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.4

Recovery

Contact the Tekelec *Customer Care Center*.

32505 – Server swap space shortage warning

Alarm Type: TPD

Description: This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

Note: For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdSwapSpaceShortageWarningNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32506 – Server default router not defined

Alarm Type: TPD

Description: This alarm indicates that the default network route is either not configured or the current configuration contains an invalid IP address or hostname.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDefaultRouteNotDefinedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32507 – Server temperature warning

Alarm Type: TPD

Description: This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdTemperatureWarningNotify

Recovery

1. Ensure that nothing is blocking the fan's intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Replace the filter (refer to the appropriate hardware manual).

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the filter is replaced before the alarm cleared.

4. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32508 – Server core file detected

Alarm Type: TPD

Description: This alarm indicates that an application process has failed and debug information is available.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdCoreFileDetectedNotify

Recovery

32509 – Server NTP Daemon not synchronized

Alarm Type: TPD

Description: This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdNTPDeamonNotSynchronizedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32510 – CMOS battery voltage low

Alarm Type: TPD

Description: The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdCMOSBatteryVoltageLowNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32511 – Server disk self test warning

Alarm Type: TPD

Description: A non-fatal disk issue (such as a sector cannot be read) exists.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdSmartTestWarnNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32512 – Device warning

Alarm Type: TPD

Description: This alarm indicates that either we are unable to perform an snmpget command on the configured SNMP OID or the value returned failed the specified comparison operation.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDeviceWarnNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32513 – Device interface warning

Alarm Type: TPD

Description: This alarm can be generated by either an SNMP trap or an IP bond error.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdDeviceIfWarnNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32514 – Server reboot watchdog initiated

Alarm Type: TPD

Description: This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdWatchdogRebootNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32515 – Server HA failover inhibited

Alarm Type: TPD

Description: This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHaInhibitedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32516 – Server HA Active to Standby transition

Alarm Type: TPD

Description: This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHaActiveToStandbyTransNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32517 – Server HA Standby to Active transition

Alarm Type: TPD

Description: This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHaStandbyToActiveTransNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32518 – Platform Health Check failure

Alarm Type: TPD

Description: This alarm is used to indicate a configuration error.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdPlatformHealthCheckFailedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32519 – NTP Offset Check failure

Alarm Type: TPD

Description: This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the NTP server and the offset limit that the application has set for the system.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterNtpOffsetCheckFailedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32520 – NTP Stratum Check failure

Alarm Type: TPD

Description: This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterNtpStratumCheckFailedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32521 – SAS Presence Sensor Missing

Alarm Type: TPD

Description: This alarm indicates that the T1200 server drive sensor is not working.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterSasPresenceSensorMissingNotify

Recovery

Contact the Tekelec *Customer Care Center* to get a replacement server.

32522 – SAS Drive Missing

Alarm Type: TPD

Description: This alarm indicates that the number of drives configured for this server is not being detected.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterSasDriveMissingNotify

Recovery

Contact the Tekelec *Customer Care Center* to determine whether the issue is with a failed drive or failed configuration.

32523 – DRBD failover busy

Alarm Type: TPD

Description: This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.24

Recovery

A DRBD sync should not take more than 15 minutes to complete. Please wait for approximately 20 minutes, and then check if the DRBD sync has completed. If the alarm persists longer than this time period, contact the Tekelec *Customer Care Center*.

32524 – HP disk resync

Alarm Type: TPD

Description: This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependant on the size of the disk and the amount of activity on the system.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdHpDiskResyncNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32525 – Telco Fan Warning

Alarm Type: TPD

Description: This alarm indicates that the Telco switch has detected an issue with an internal fan.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdTelcoFanWarning

Recovery

1. Contact the Tekelec *Customer Care Center* to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.
2. Tekelec *Customer Care Center* personnel can perform an snmpget command or log into the switch to get detailed fan status information.

32526 – Telco Temperature Warning

Alarm Type: TPD

Description: This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdTelcoTemperatureWarning

Recovery

1. Lower the ambient air temperature around the switch as low as possible.
2. If problem persists, contact the Tekelec *Customer Care Center*.

32527 – Telco Power Supply Warning

Alarm Type: TPD

Description: This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdTelcoPowerSupplyWarning

Recovery

1. Verify breaker wasn't tripped.
2. If breaker is still good and problem persists, contact the Tekelec *Customer Care Center* who can perform a **snmpget** command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 – Invalid BIOS value

Alarm Type: TPD

Description: This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdInvalidBiosValueNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32529– Server Kernel Dump File Detected

Alarm Type: TPD

Description: This alarm indicates that the kernel has crashed and debug information is available.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdServerKernelDumpFileDetectedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32530– Server Upgrade Fail Detected

Alarm Type: TPD

Description: This alarm indicates that a TPD upgrade has failed.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgHlrRouterTpdServerUpgradeFailDetectedNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32531– Half Open Socket Warning

Alarm Type: TPD

This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHalfOpenSocketWarningNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32532– Server Upgrade Pending Accept/Reject

Alarm Type: TPD

Description: This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMaxPidWarning

Recovery

Follow the steps in the application's upgrade procedure for accepting or rejecting the upgrade.

32533 - Max pid warning

Alarm Type: TPD

Description: This alarm indicates that the maximum number of running processes has reached the minor threshold.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMaxPidWarning

Recovery:

1. Run syscheck in verbose mode.
2. Contact the Tekelec *Customer Care Center*.

32534 - NTP Source Server Is Not Able To Provide Correct Time

Alarm Type: TPD

Description: This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPSourceIsBad

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. Contact the Tekelec *Customer Care Center*.

32535 - RAID disk resync

Alarm Type: TPD

Description: This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependant on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskResync

Recovery:

1. Run syscheck in verbose mode
2. If this alarm persists for several hours (depending on a load of a server rebuild of array can take multiple hours to finish), contact the Tekelec *Customer Care Center*.

32603 – PM&C backup to remote server failed

Alarm Type: PM&C

The PMAC application has a failure that needs to be investigated.

Severity: Minor

OID: eagleXgHlrRouterpmacRemoteBackupErrorNotify

1. Verify that the remote server is operational.
2. Verify that the primary PMAC can ping the remote server.
3. Attempt a manual backup to remote server using the PMAC GUI.
4. If the problems persists, contact the Tekelec *Customer Care Center*.

Chapter 4

Key Performance Indicators (KPIs)

Topics:

This section provides general information about KPIs, and lists the KPIs that can appear on the Status & Manage KPIs GUI page.

General KPIs information

This section provides general information about KPIs, the Status and Manage KPI page, and how to view KPIs.

KPIs overview

Key Performance Indicators (KPIs) allow the user to monitor system performance data, including CPU, memory, swap space, and uptime per server. This performance data is collected from all servers within the defined topology.

The KPI display function resides on all OAM servers. Servers that provide a GUI connection rely on KPI information merged to that server. The Network OAMP servers maintain status information for all servers in the topology. System OAM servers have reliable information only for servers within the same network element.

The Status and Manage KPIs page displays performance data for the entire system. KPI data for the entire system is updated every 60 seconds. If data is not currently being collected for a particular server, the KPI for that server will be shown as Unk for "Unknown".

KPIs

The **Status & Manage > KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server.

Viewing KPIs

Use this procedure to view KPI data.

1. Select **Status & Manage > KPIs**.

   The **Status & Manage KPIs** page appears with the **Server** tab displayed. For details about the KPIs displayed on this page, see the application documentation.

2. Click to select an application tab to see KPI data relevant to the application.

   Note: The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server. Collection of KPI data is handled solely by NOAMP servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the **KPIs Export** page.

Table 13: Schedule KPI Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting KPIs

You can schedule periodic exports of security log data from the **KPIs** page. KPI data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **KPIs** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an

alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to schedule a data export task.

1. Select **Status & Manage > KPIs**.

   The **KPIs** page appears.

2. If necessary, specify filter criteria and click **Go**.
   The KPIs are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule KPI Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *KPIs data export elements* .
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes.**
7. Select the **Time of Day**.

   Note: Time of Day is not an option if **Export Frequency** equals **Once**.

8. Select the **Day of Week**.

   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

9. Click **OK** or **Apply** to initiate the KPI export task.

   From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see .

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage > Tasks**. For more information see:

   - *Viewing scheduled tasks*
   - *Editing a scheduled task*
   - *Deleting a scheduled task*
   - *Generating a scheduled task report*

EXHR KPIs

Table 14: EXHR KPIs

Measurement Tag	Description
ExhrGttExceptionRoutingtg	The total number of messages that were Exception Routed
ExhrGttPerformed	The total number of global title translations performed
ExhrMlrPerformed	Total number of messages that were MLR Performed. IMSI/DN found in MAP Layer and

Measurement Tag	Description
	in Database plus the message was successfully routed

PDBI KPIs

Table 15: PDBI KPIs

Measurement Tag	Description
PdbiConnections	The number of PDBI client connections currently established. A single connection includes a client having successfully established a TCP/IP connection, sent a PDBI connect message, and having received a successful response.
PdbiMsgsDiscarded	The number of PDBI messages discarded per second. PDBI messages being discarded is due to the connection being shutdown, server being shutdown, server's role switching from active to standby, or transaction not becoming durable within the allowed amount of time.
PdbiMsgsFailed	The number of PDBI messages that have failed to be processed due to errors per second.
PdbiMsgsImported	The number of PDBI messages imported per second.
PdbiMsgsReceived	The number of PDBI messages that have been received per second.
PdbiMsgsSent	The number of PDBI messages sent per second.
PdbiMsgsSuccessful	The number of PDBI messages that have been successfully processed per second.
PdbiTxnAborted	The number of PDBI transactions aborted per second.
pdbiTxnActive	The number of PDBI transactions that are currently active (Normal transaction mode only).
PdbiTxnCommitted	The number of PDBI transactions that have been successfully committed per second to the database (memory and on disk) on the active server of the primary NOAMP cluster.
PdbiTxnFailed	The number of PDBI transactions that have failed to be started, committed, or aborted due to errors per second.

Measurement Tag	Description
PdbiTxnNonDurable	The number of transactions that have been committed, but are not yet durable. Responses for the associated requests are not sent until the transaction has become durable.

SS7/Sigtran KPIs configuration elements

Table 16: SS7/Sigtran KPIs

Variable	Description
SCCP Xmit Msgs/Sec	SCCP messages transmitted per second
SCCP Recv Msgs/Sec	SCCP messages received per second
SS7 Process CPU Utilization	The average percent of SS7 Process CPU utilization on an MP server.
Ingress Message Rate	The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue.
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent.
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received.

Throttling KPIs

Table 17: Throttling KPIs

KPI Column Name	KPI Description
ThrottleAllow	The number of times a message was allowed, per second
ThrottleDiscard	The number of messages that were discarded as a result of matching a rule, per second
ThrottleDiscardTCAP	The number of times a TCAP error was returned in conjunction with a discard, per second
ThrottleDiscardUDTS	The number of times a UDTS was returned in conjunction with a discard, per second
ThrottleMatch	The number of messages that matched a rule, per second

KPI Column Name	KPI Description
ThrottleSimulation	The number of times a message matched a rule in the 'Simulation' mode but was not acted upon, per second
ThrottleWhitelistHit	The number of times a message matched a rule with Whitelist enabled, and the subscriber was in the Dn/Imsi Whitelist, per second
ThrottleWhitelistMiss	The number of times a message matched a rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist, per second

Chapter 5

Measurements

Topics:

This section provides general information about measurements (including measurement procedures), and lists the measurements that display on measurement reports.

General measurements information

This section provides general information about measurements, measurement-related GUI elements, and measurement report procedures.

Measurements

The measurements framework allows applications to define, update, and produce reports for various measurements.

- Measurements are ordinary counters that count occurrences of different events within the system, for example, the number of messages received. Measurement counters are also called pegs. Additional measurement types provided by the Platform framework are not used in this release.
- Applications simply peg (increment) measurements upon the occurrence of the event that needs to be measured.
- Measurements are collected and merged at the SOAM and NOAM servers as appropriate.
- The GUI allows reports to be generated from measurements.

Measurements that are being pegged locally are collected from shared memory and stored in a disk-backed database table every 5 minutes on all servers in the network. Measurements are collected every 5 minutes on a 5 minute boundary, i.e. at HH:00, HH:05, HH:10, HH:15, and so on. The collection frequency is set to 5 minutes to minimize the loss of measurement data in case of a server failure, and also to minimize the impact of measurements collection on system performance.

All servers in the network (NOAMP, SOAM, and MP servers) store a minimum of 8 hours of local measurements data. More than 5 minutes of local measurements data is retained on each server to minimize loss of measurements data in case of a network connection failure to the server merging measurements.

Measurements data older than the required retention period are deleted by the measurements framework.

Measurements are reported in groups. A measurements report group is a collection of measurement IDs. Each measurement report contains one measurement group. A measurement can be assigned to one or more existing or new measurement groups so that it is included in a measurement report. Assigning a measurement ID to a report group ensures that when you select a report group the same set of measurements is always included in the measurements report.

Note: Measurements from a server may be missing in a report if the server is down; the server is in overload; something in the Platform merging framework is not working; or the report is generated before data is available from the last collection period (there is a 25 to 30 second lag time in availability).

Measurement elements

This table describes the elements on the **Measurements Report** page.

Table 18: Measurements Elements

Element	Description	Data Input Notes
Scope	Network Elements, Server Groups, Resource Domains, Places and Place Associations for which the measurements report can be run. **Note:** Measurements for SOAM network elements are not available in systems that do not support SOAMs.	Format: Pulldown list Range: Network Elements in the topology; Server Groups in the topology; Resource Domains in the topology; Places in the topology; Place Associations in the topology **Note:** If no selection is made, the default scope is Entire Network. Default: Entire Network
Report	A selection of reports	Format: Pulldown list Range: Varies depending on application Default: Group
Column Filter	The characteristics for filtering the column display	Format: Pulldown list Range: Sub-measurement Sub-measurement Ranges: • Like: A pattern-matching distinction for sub-measurement name, for example, 123* matches any sub-measurement that begins with 123. • In: A list-matching distinction for sub-measurement ID, for example, 3,4,6-10 matches only sub-measurements 3, 4, and 6 through 10. Default: None
Time Range	The interval of time for which the data is being reported, beginning or ending on a specified date.	Format: Pulldown list Range: Days, Hours, Minutes, Seconds Interval Reference Point: Ending, Beginning Default: Days

Generating a measurements report

Use this procedure to generate and view a measurements report.

1. Select **Measurements > Report**.

   The **Measurements Report** page appears.

2. Select the **Scope**.

   For details about this field, or any field on the **Measurements Report** page, see *Measurement elements* .

3. Select the **Report**.
4. Select the **Interval**.
5. Select the **Time Range**.
6. Select **Beginning** or **Ending** as the **Time Range** interval reference point.
7. Select the **Beginning** or **Ending** date.
8. Click **Go**.

   The report is generated.

   Note: Data for the selected scope is displayed in the primary report page. Data for any available sub-scopes are displayed in tabs. For example, if the selected scope is Entire Network, report data for the entire network appears in the primary report page. The individual network entities within the entire network are considered sub-scopes.

9. To view report data for a specific sub-scope, click on the tab for that sub-scope.

   The report data appears.

Measurements data export elements

This table describes the elements on the **Measurements Report Export** page.

Table 19: Schedule Measurement Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting measurements reports

You can schedule periodic exports of data from the **Measurements Report** page. Measurements data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied on the **Measurements Report** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to save a measurements report to the file management storage area.Use this procedure to schedule a data export task.

1. Select **Measurements > Report**.

   The **Measurements Report** page appears. For a description of each field, see *Measurement elements* .

2. Generate a measurements report.

   For information about how to generate a measurements report, see *Generating a measurements report*.

3. Click to select the scope or sub-scope measurement report that you want to export.
4. Click **Export**.

   The measurement report is exported to a CSV file. Click the link at the top of the page to go directly to the **Status & Manage** > **Files** page. From the **Status & Manage** page, you can view a list of files

available for download, including the measurements report you exported during this procedure. For more information, see *Opening a file*.The **Schedule Measurement Log Data Export** page appears.

5. Check the **Report Groups** boxes corresponding to any additional measurement reports to be exported.

   Note: This step is optional, but is available to allow the export of multiple measurement group reports simultaneously.

6. Select the **Export Frequency**.

   Note: If the selected **Export Frequency** is **Fifteen Minutes** or **Hourly**, specify the **Minutes.**

7. Enter the **Task Name**.
   For more information about Task Name, or any field on this page, see *Measurements data export elements* .

   Note: **Task Name** is not an option if **Export Frequency** equals **Once**.

8. Select the **Time of Day**.

   Note: **Time of Day** is only an option if **Export Frequency** equals **Daily** or **Weekly**.

9. Select the **Day of Week**.

   Note: **Day of Week** is only an option if **Export Frequency** equals **Weekly**.

10. Click **OK** or **Apply** to initiate the data export task.

    The data export task is scheduled. From the **Status & Manage** > **Tasks** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see .

    Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage** > **Tasks**. For more information see:

    - *Viewing scheduled tasks*
    - *Editing a scheduled task*
    - *Deleting a scheduled task*
    - *Generating a scheduled task report*

OAM measurements

This section describes the OAM measurement reports. These measurements provide information about OAM system and alarm measurements. The measurements in this section are available in all Tekelec XG products.

OAM Alarm measurements

Table 20: OAM Alarm measurements

Measurement Tag	Description	Collection Interval
Alarm Crit	The number of critical alarms.	5 minutes
Alarm Major	The number of major alarms.	5 minutes
Alarm Minor	The number of minor alarms	5 minutes
Alarm State	The alarm state.	5 minutes

OAM System measurements

Table 21: OAM System measurements

Measurement Tag	Description	Collection Interval
System CPU UtilPct Average	The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System CPU UtilPct Peak	The peak CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System Disk UtilPct Average	The average disk usage for the partition on which the COMCOL database resides.	5 minutes
System Disk UtilPct Peak	The peak disk usage for the partition on which the COMCOL database resides.	5 minutes
System RAM UtilPct Average	The average committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.	5 minutes
System RAM UtilPct Peak	The peak committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement	5 minutes

Measurement Tag	Description	Collection Interval
	from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.	
System ShMem UtilPct Average	The average shared memory usage as a percentage of the limit configured by shl.set.	5 minutes
System ShMem UtilPct Peak	The peak shared memory usage as a percentage of the limit configured by shl.set.	5 minutes
System SwapIn Rate Average	The average number of memory pages swapped in to memory from disk per second.	5 minutes
System SwapIn Rate Peak	The peak number of memory pages swapped in to memory from disk per second.	5 minutes
System SwapOut Rate Average	The average number of memory pages swapped out of memory from disk per second.	5 minutes
System SwapOut Rate Peak	The peak number of memory pages swapped out of memory from disk per second.	5 minutes
System Swap UtilPct Average	The average usage of swap space as a percentage of the total configured swap space.	5 minutes
System Swap UtilPct Peak	The peak usage of swap space as a percentage of the total configured swap space.	5 minutes
System CPU CoreUtilPct Average	The average CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.	5 minutes
System CPU CoreUtilPct Peak	The peak CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.	5 minutes

SS7/Sigtran Measurements

This section provides information about SS7/Sigtran measurement reports and detailed information about each measurement.

SS7/Sigtran measurements overview

SS7/Sigtran signaling measurements provide information about SCCP functionality, MTP3 routing capabilities, and the M3UA interface to the external network and can alert you to SS7/Sigtran issues before an alarm or event is triggered. This section of the documentation provides overview information about SS7/Sigtran measurement reports and detailed information about each measurement on the report, including potential customer actions.

Association Exception measurements

Table 22: Association Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxTrFarEndClose	Number of times the far end closed the SCTP connection.	30 min
EvTrManClose	The number of times the Transport was manually closed. This includes manual changes of the transport administrative state that caused the transport to transition from APP-UP to Disabled.	30 min
EvTrNoRespClose	The number of times the Transport was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the transport.	30 min
EvTrCnxFail	The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections. The number of times an open attempt on UDP socket in Listen Mode failed on the Transport.	30 min
TxTrSendFail	The number of times the SCTP/UDP sends failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.	30 min
RxTrRcvFail	The number of times an SCTP receive attempt failed on the transport. Failure to receive message	30 min

Measurement Tag	Description	Collection Interval
	via SCTP might result in a message being discarded.	
EvTrSockInitFail	Number of times the socket initialization failed.	30 min
RxM3uaERROR	The number of times an M3UA ERROR message is received by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.	30 min
TmSingleTransQueueFull	The number of egress messages that were discarded because the single Transport Writer Queue was full.	30 min
EvAsnUpAckTO	Number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during association start-up (when the association is in the **Enabled** administrative state).	30 min
RxAsnUnsolDownAck	Number of unsolicited M3UA ASP-DOWN-ACK messages received on the association. Unsolicited ASP-DOWN-ACK messages can be sent by the SG to indicate that the SG cannot process traffic on the association.	30 min
RxAsnInvalidM3ua	Number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.	30 min
EvSctpAdjIPToDwn	Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.	30 min
EvSctpTransRej	Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.	30 min

RxTrFarEndClose

Measurement Group: Association Exception

Measurement Type: Simple

Description: Number of times the far end closed the SCTP connection

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time the far-end of the association closes the association by sending either SHUTDOWN or ABORT.

Measurement Scope: NE, Server

Recovery:

1. If the closing of the association was expected, no further action is necessary, the association will be recovered as soon as the far-end is ready to connect again. If the closing of the association was not expected. You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Look in the event history from the GUI main menu under **Alarms & Events>View History** for **Event ID 19224** to determine exactly when the far-end closed the association.
3. Look for other events for the association or MP server in the event history.
4. Verify that IP connectivity still exists between the MP server and the SG.
5. Verify whether the far-end of the association is undergoing maintenance.
6. Contact the Tekelec *Customer Care Center* for assistance if needed.

EvTrManClose

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the association was manually closed. This includes manual changes of the association administrative state that cause the association to transition from ASP-UP to either ASP-DOWN or **Disabled**.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time a manual change is made to the association administrative state from **Enabled** to **Blocked** or from **Enabled** to **Disabled**, causing the association to transition out of ASP-UP protocol state.

Measurement Scope: NE, Server

Recovery:

1. If the association is known to be under maintenance no further action is necessary. If the association was not known to be under maintenance, you can view the Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. View the event history from the GUI main menu under **Alarms & Events>View History** and look for **Event ID 19228**. **Event ID 19228** shows the manual association state transitions and contains a time-stamp of when the change occurred.
3. View the security logs from the GUI main menu under **Security Logs**. You can search the logs using the time-stamp from the event history log to determine which login performed the manual state change on the association.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

EvTrNoRespClose

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the association was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the association or to SCTP heartbeating if enabled.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an established SCTP association is closed by the MP server due to lack of response at the SCTP level from the far-end of the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. If it has a non-zero value, the association has been closed due to the lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the signaling gateway. You can view the Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Look in the event history from the GUI main menu under **Alarms & Events>View History** for **Event ID 19225.**
3. Verify IP connectivity between the MP server and the signaling gateway.
4. Determine if the far-end of the association is congested, possibly causing slow response times on the association.
5. Check the IP network between the MP server and the signaling gateway for excessive retransmissions.
6. Contact the Tekelec *Customer Care Center* for assistance if needed.

EvTrCnxFail

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the SCTP connection attempt failed on the association. This includes only unsuccessful attempts to connect to the signaling gateway . It does not include failure of established connections.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an SCTP connect attempt fails.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the signaling gateway at least once and failed to establish the SCTP connection.You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Check the event history log from the GUI main menu under **Alarms & Events>View History**, looking for **Event ID 19222**. **Event ID 19222** provides details about the cause of the failure.
3. Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address. You can view the Adjacent Servers from the GUI main menu under **SS7/Sigtran>Configuration>Adjacent Servers**.

4. Verify that the remote port configured for the association correctly identifies the port that the signaling gateway is listening on for SCTP connections. You can view the configured port from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.
5. Verify the IP network connectivity between the MP server and the signaling gateway.
6. If the signaling gateway must be configured to connect to the MP server's IP address and port, verify that the signaling gateway configuration matches the association configuration. You can view association data from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.
7. Contact the Tekelec *Customer Care Center* for assistance if needed.

TxTrSendFail

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the SCTP Send failed for non-DATA M3UA signaling on the association. The number includes the sending of any non-DATA messages on an established association.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an attempt to send M3UA signaling fails for any reason and the information being sent cannot be mapped to a specific link

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this association using SCTP has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association. You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Look in the GUI main menu under **Alarms & Events>View History** in the event history log for **Event ID 19233**. **Event ID 19233** provides information on the cause of the failure to send.
3. Verify that the IP network between the MP server and the SG is functioning as expected.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxTrRcvFail

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed. You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Look in the event history log from the GUI main menu under **Alarms & Events>View History** for **Event ID 19223**. **Event ID 19223** gives more information about what caused the failure.
3. Try to bring the sockets back into alignment by manually **Disabling** and **Enabling** the association.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

EvTrSockInitFail

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the socket initialization failed. Socket initialization includes configuring the association according to the settings in the GUI under **SS7/Sigtran >Configuration>Associations>Configuration Sets**.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time one or more socket options cannot be set according to the settings in the association's configuration set.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value indicates a problem with the association setup prior to attempting to connect the association. If this occurs, look for **Event ID 19221** in the GUI under **Alarms & Events>View History**. **Event 19221** provides details about the configuration failure.
2. Contact the Tekelec *Customer Care Center* for further assistance.

RxM3uaERROR

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of M3UA ERROR messages received on the association. An M3UA ERROR message is sent by the far-end to complain about an invalid M3UA message that it received.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA ERROR message is received that cannot be mapped to a specific link.

Measurement Scope: NE, Server

Recovery:

1. This measurement will have a value of zero. A non-zero value indicates a problem with M3UA signaling sent by the MP server.
2. Look for **Event ID 19235** from the GUI main menu under **Alarms & Events>View History**. **Event ID19235** provides more information about the receipt of the ERROR message.

3. If the ERROR reason in **Event ID 19235** indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

EvAsnUpAckTO

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during the association start-up (when the association is in the **Enabled** administrative state).

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an ASP-UP has been sent and the M3UA State Management ACK Timer expires, but no ASP-UP-ACK has been received for the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. If the value is not zero, the association cannot be brought into the state necessary for M3UA ASPTM traffic because the far-end of the association is not responding by sending an ASP-UP-ACK prior to the timeout defined in the GUI under **SS7/Sigtran>Configuration>Options>M3UA**. The field that defines the timeout is the **State Management ACK Timer**.
2. You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
3. Check the event history from the GUI main menu under **Alarms & Events>View History**, looking for **Event ID 19226**. **Event ID 19226** will show when the timeout occurred.
4. Verify that the far-end of the association on the SG is not undergoing maintenance.
5. Verify that the **State Management ACK Timer** value is not set too short. This should not occur if the IP network is functioning correctly.
6. Verify that the IP network between the MP server and the SG is performing up to expectations.
7. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxAsnUnsolDownAck

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of unsolicited M3UA ASP-DOWN-ACK messages received on the association. Unsolicited ASP-DOWN-ACK messages can be sent by the SG to indicate that the SG cannot process traffic on the association.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an unsolicited ASP-DOWN-ACK is received on the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value means that the far-end of the association has stopped processing M3UA signaling. You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Check the event history from the GUI main menu under **Alarms & Events>View History**, looking for **Event ID 19227**. **Event ID 19227** will show exactly when the unsolicited ASP-DOWN-ACK was received.
3. Verify whether the far-end of the association is undergoing maintenance.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxAsnInvalidM3ua

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA message is received on the association that is invalid due to any syntactic or semantic reason.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. In case of a non-zero value in this measurement, review the event history from the GUI main menu under **Alarms & Events>View History**, looking for **Event 19231**.
2. **Event 19231** provides details about the reason for rejecting the M3UA message. If the error reason indicates a problem with routing context, verify that the routing context used for the association specified in **Event 19231** is configured to match between the ASP and the SG.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

TmSingleTransQueueFull

Measurement Group: Transport Exception

Measurement Type: Simple

Description: The number of egress messages that were discarded because the single Transport Writer Queue was full.

Collection Interval: 30 min

Peg Condition: Check whether the single peers transmit data queue limit has reached its max limit (1000). If maximum limit is reached or exceeded, then peg the measurement and discard the low priority events.

Measurement Scope: NE, Server

Recovery:

This measurement indicates that the Transport is backed up and messages might be discarded. If the value is above the defined critical threshold, an alarm (19408) is generated.

If the problem persists, contact the Tekelec *Customer Care Center*.

EvSctpAdjPToDwn

Measurement Group: Transport Exception

Measurement Type: Simple

Description: Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.

Collection Interval: 30 min

Peg Condition: This measurement shall be incremented by one each time:

- Reachibility to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected.

Measurement Scope: NE, Server

Recovery:

If all is well, the measurement will have a zero value. A non-zero value indicates that a path fault to that address was detected.

1. Check the event history log at **Main Menu>Alarms & Events> View History**; look for event ID 19410. Event ID 19410 provides more details about the actual cause of the failure.
2. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu>Transport Manager>Configuration>Adjacent Node**.
3. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

EvSctpTransRej

Measurement Group: Transport Exception

Measurement Type: Simple

Description: Number of times SCTP Transport has been rejected due to remote IP addesses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.

Collection Interval: 30 min

Peg Condition: This measurement shall be incremented by one each time:

- The association has been rejected due to IP address validation in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.

Measurement Scope: NE, Server

Recovery:

If all is well, the measurement has a zero value. A non-zero value indicates that an Adjacent Node has attempted to connect to the Peer IP Address at least once, but the connection attempt was rejected because the IP address advertised by the Adjacent Node failed validation.

1. Check the Transport history at **Main Menu>Transport Manager>Maintenance**.
2. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
3. Verify that the SCTP validation mode is the one that is needed.
4. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu>Transport Manager>Configuration>Adjacent Node**.
5. Verify that the remote port configured at **Main Menu>Transport Manager>Configuration>Transport** for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

Association Performance measurements

Table 23: Association Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxTrOctets	The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min
RxTrOctets	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min
TmSingleTransQueuePeak	The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval.	30 min
TmSingleTransQueueAvg	The average single Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 seconds).	30 min

TxTrOctets

Measurement Group: Transport Performance

Measurement Type: Simple

Description: The number of octets sent on the association. This includes octets for both DATA and non-DATA M3UA signaling. It does not include SCTP, IP, or Ethernet headers.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the message each time:

- A DATA/non-DATA message is successfully sent on the transport.

Measurement Scope: NE, Server

Recovery:

No action required.

RxTrOctets

Measurement Group: Transport Performance

Measurement Type: Simple

Description: The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.

Collection Interval: 30 min

Peg Condition: This measurement shall be incremented by the number of octets in the message each time:

- A DATA/non-DATA message is successfully received on the transport.

Measurement Scope: NE, Server

Recovery:

No action required.

TmSingleTransQueuePeak

Measurement Group: Transport Performance

Measurement Type: Max

Description: The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 seconds).

Collection Interval: 30 min

Peg Condition: Transport's queue is registered as a Stack Resource. Thee StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.

Measurement Scope: NE, Server

Recovery:

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist. Contact Tekelec for assistance if needed.

Also see Alarm19408.

TmSingleTransQueueAvg

Measurement Group: Transport Performance

Measurement Type: Average

Description: The average single Transport (SCTP/UDP) Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 seconds).

Collection Interval: 30 min

Peg Condition: The average of all SCTP Single Association Writer Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

This is a measure of how fast the Transport queue is processed and indicates the Average depth of queue over the monitored interval.

It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.

If the problem persists, contact the Tekelec *Customer Care Center*.

Association Usage measurements

Table 24: Association Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvTrCnxSuccess	The number of times the SCTP connection was successfully established on the transport. The number of times UDP socket in Listen Mode was opened successfully on the Transport.	30 min
TmAsnBlkNotDown	Number of seconds during the reporting interval during which the association was in the **Blocked** administrative state but was not in ASP-DOWN state. When the association is **Blocked**, the desired protocol state is ASP-DOWN. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.	30 min

Measurement Tag	Description	Collection Interval
RxTrOctets	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min

EvTrCnxSuccess

Measurement Group: Transport Usage

Measurement Type: Simple

Description: The number of times the SCTP connection was successfully established on the transport.

The number of times the UDP socket in Listen Mode was opened successfully on the Transport.

Collection Interval: 30 min

Peg Condition: This measurement shall be incremented by one each time:

- The SCTP association reaches the APP-UP protocol state (for example, the connection is successfully established).

  The UDP socket in Listen Mode was opened successfully.

Measurement Scope: NE, Server

Recovery:

If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise, preform the following steps:

1. You can view the transport status can be viewed from the GUI main menu under **Transport Manager>Maintenance>Transport**.
2. Look in the event history from the GUI main menu under **Alarms & Events>View History**. Look for events related to the association or the MP server to determine what might have caused the association to fail.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

TmAsnBlkNotDown

Measurement Group: Association Usage

Measurement Type: Duration

Description: The number of seconds during the reporting interval during which the association was in the **Blocked** administrative state but was not in ASP-DOWN state. When the association is **Blocked**, the desired protocol state is ASP-DOWN. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.

Collection Interval: 30 min

Peg Condition: Time is accumulated for this measurement during the collection interval when all of the following are true:

- The association is in the **Blocked** administrative state.

- The association is not in the ASP-DOWN protocol state.

Measurement Scope: NE, Server

Recovery:

1. The value of this measurement should be zero. A non-zero value indicates that the association was set to the **Blocked** administrative state, but was not able to reach the desired protocol state due to some problem. You can view the Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address. You can check the configuration from the GUI main menu under **SS7/Sigtran>Configuration>Adjacent Servers**.
3. Verify that the remote port configured for the association correctly identifies the port that the SG is listening on for SCTP connections. You can check the configuration from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.
4. Verify the IP network connectivity between the MP server and the SG.
5. If the SG must be configured to connect to the MP server's IP address and port, verify that the SG configuration matches the association configuration. You can check the configuration from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.
6. Contact the Tekelec *Customer Care Center* for assistance if needed.

TmAsnEnaNotUp

Measurement Group: Association Usage

Measurement Type: Duration

Description: The time that the association was enabled, but not in the ASP-UP state

Collection Interval: 30 min

Peg Condition: Time shall be accumulated for this measurement during the collection interval when all of the following are true:

- the association is in the Enabled administrative state
- the association is not in the ASP-UP protocol state for any reason

Measurement Scope: NE, Server

Recovery:

No action is required.

Link Exception measurements

Table 25: Link Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvLnkActAckTO	Number of times the link timed out waiting for ASP-ACTIVE-ACK. ASP-ACTIVE-ACK is sent by the	30 min

Measurement Tag	Description	Collection Interval
	SG in response to an ASP-ACTIVE message on the link. The link is not available for M3UA data signaling until ASP-ACTIVE-ACK is received.	
RxLnkUnsolInactAck	Number of times an unsolicited ASP-INACTIVE-ACK was received on the link. ASP-INACTIVE-ACK may be sent unsolicited by the SG to indicate that the specified link is no longer able to process M3UA data signaling. The MP server will begin attempts to bring the link back into the signaling state matching its administrative state. For example, if the link is **Enabled**, the MP server will attempt to restore M3UA data signaling on the link by sending an ASP-ACTIVE and waiting for an ASP-ACTIVE-ACK.	30 min
RxLnkM3uaERROR	Number of times an M3UA ERROR message was received for the link. M3UA ERROR message are sent to indicate invalid M3UA signaling.	30 min
RxLnkInvalidM3ua	Number of invalid M3UA messages received on the link. Invalid M3UA messages are messages that violate the M3UA protocol, but which can be attributed to a specific link (i.e., a valid routing context exists, or no routing context is necessary).	30 min

EvLnkActAckTO

Measurement Group: Link Exception

Measurement Type: Simple

Description: The number of times the link timed out waiting for ASP-ACTIVE-ACK. An ASP-ACTIVE-ACK is sent by the SG in response to an ASP-ACTIVE message on the link. The link is not available for M3UA data signaling until the ASP-ACTIVE-ACK is received.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time:

- An ASP-ACTIVE has been sent for the link and the M3UA State Management ACK timer has expired, but no ASP-ACTIVE-ACK was received for the link.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. You can view Link status from the GUI main menu under **SS7/Sigtran>Maintenance>Links**.
2. Check the event history log from the GUI main menu under **Alarms & Events>View History**. Look for **Event ID 19229**, which shows when the ASP-ACTIVE-ACK timeout occurs.
3. Verify that the far-end of the link on the SG is not undergoing maintenance.
4. Verify that the **State Management ACK Timer** period is not set too short.
5. Verify that the IP network between the MP server and the SG is performing up to expectations.
6. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxLnkUnsolInactAck

Measurement Group: Link Exception

Measurement Type: Simple

Description: The number of times an unsolicited ASP-INACTIVE-ACK was received on the link. ASP-INACTIVE-ACK may be sent unsolicited by the SG to indicate that the specified link is no longer able to process M3UA data signaling. The MP server will begin attempts to bring the link back into the signaling state matching its administrative state. For example, if the link is **Enabled**, the MP server will attempt to restore M3UA data signaling on the link by sending an ASP-ACTIVE and waiting for an ASP-ACTIVE-ACK.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an unsolicited ASP-INACTIVE-ACK is received on the link.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value means that the far-end of the link has stopped processing M3UA data. You can view Link status from the GUI main menu under **SS7/Sigtran>Maintenance>Links**.
2. Check the event history log from the GUI main menu under **Alarms & Events>View History**, looking for **Event ID 19230**. **Event ID 19230** will show when the unsolicited ASP-INACTIVE-ACK was received.
3. Verify whether the far-end of the link is undergoing maintenance.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxLnkM3uaERROR

Measurement Group: Link Exception

Measurement Type: Simple

Description: The number of times an M3UA ERROR message was received for the link. M3UA ERROR message are sent to indicate invalid M3UA signaling.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time:

- An M3UA ERROR message is received and that ERROR message can be attributed to a specific link (i.e., the ERROR message contains a valid routing context, or no routing context is needed).

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a value of zero. A non-zero value indicates a problem with the M3UA signaling sent by the MP server.
2. Look for **Event ID 19235** from the GUI main menu under **Alarms & Events>View History**. **Event ID 19235** provides information on the reason for the receipt of the ERROR message.
3. If the ERROR reason in **Event ID 19235** indicates a problem with routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxLnkInvalidM3ua

Measurement Group: Link Exception

Measurement Type: Simple

Description: The number of invalid M3UA messages received on the link. Invalid M3UA messages are messages that violate the M3UA protocol, but which can be attributed to a specific link (i.e., a valid routing context exists or no routing context is necessary).

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an invalid M3UA message is received for the link.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a value of zero. A non-zero value indicates a problem with the M3UA signaling received by the MP server.
2. Look for **Event ID 19231** from the GUI main menu under **Alarms & Events>View History**. **Event ID 19231** provides information on the reason the M3UA message was rejected.
3. If the ERROR reason in **Event ID 19231** indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

Link Performance measurements

Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are not counted in these measurement.

Table 26: Link Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxLnkMSU	Number of MSUs sent on the link. MSUs includes all M3UA messages, both DATA and non-DATA.	30 min
RxLnkMSU	Number of MSUs received on the link. MSUs includes all M3UA messages, both DATA and non-DATA.	30 min
TxLnkMSUOctets	Number of MSU octets sent on the link. MSU octets includes all M3UA messages, both DATA and non-DATA.	30 min
RxLnkMSUOctets	Number of MSU octets received on the link. MSU octets includes all M3UA messages, both DATA and non-DATA.	30 min

TxLnkMSU

Measurement Group: Link Performance

Measurement Type: Simple

Description: The number of MSUs sent on the link, including all M3UA messages, both DATA and non-DATA.

Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA message is sent on the link.

Measurement Scope: NE, Server

Recovery:

No action required.

RxLnkMSU

Measurement Group: Link Performance

Measurement Type: Simple

Description: The number of MSUs received on the link. MSUs includes all M3UA messages, both DATA and non-DATA. Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA message is received on the link.

Measurement Scope: NE, Server

Recovery:

No action required.

TxLnkMSUOctets

Measurement Group: Link Performance

Measurement Type: Simple

Description: The number of MSU octets sent on the link, including all M3UA messages, both DATA and non-DATA.

Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the MSU (not including SCTP, IP, or Ethernet headers) each time an M3UA message is sent on the link.

Measurement Scope: NE, Server

Recovery:

No action required.

RxLnkMSUOctets

Measurement Group: Link Performance

Measurement Type: Simple

Description: The number of MSU octets received on the link – MSU octets includes all M3UA messages, both DATA and non-DATA. Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the MSU (not including SCTP, IP, or Ethernet headers) each time an M3UA message is received on the link.

Measurement Scope: NE, Server

Recovery:

No action required.

Link Set Performance measurements

Table 27: Link Set Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxLnkSetMSU	Number of MSUs sent on the link set. MSUs includes all M3UA DATA messages sent on all links in the link set.	30 min
RxLnkSetMSU	Number of MSUs received on the link set. MSUs includes all M3UA DATA messages received on all links in the link set.	30 min
TxLnkSetMSUOctets	Number of MSU octets sent on the link set. MSU octets includes all M3UA DATA octets sent on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.	30 min
RxLnkSetMSUOctets	Number of MSU octets received on the link set. MSU octets includes all M3UA DATA octets received on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.	30 min

TxLnkSetMSU

Measurement Group: Link Set Performance

Measurement Type: Simple

Description: The number of MSUs sent on the link set , including all M3UA DATA messages sent on all links in the link set.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA DATA message is sent on a link in the link set.

Measurement Scope: NE, Server

Recovery:

No action required.

RxLnkSetMSU

Measurement Group: Link Set Performance

Measurement Type: Simple

Description: The number of MSUs received on the link set . MSUs includes all M3UA DATA messages received on all links in the link set.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA DATA message is received on a link in the link set.

Measurement Scope: NE, Server

Recovery:

No action required.

TxLnkSetMSUOctets

Measurement Group: Link Set Performance

Measurement Type: Simple

Description: The number of MSU octets sent on the link set, including all M3UA DATA octets sent on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the M3UA DATA message each time an M3UA DATA message is sent on a link in the link set.

Measurement Scope: NE, Server

Recovery:

No action required.

RxLnkSetMSUOctets

Measurement Group: Link Set Performance

Measurement Type: Simple

Description: The number of MSU octets received on the link set. MSU octets include all M3UA DATA octets received on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the M3UA DATA message each time an M3UA DATA message is received on a link in the link set.

Measurement Scope: NE, Server

Recovery:

No action required.

Link Set Usage measurements

Table 28: Link Set Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
TmM3RLLinksetUnavail	Total time (in seconds) that all links in the link set were unavailable to M3RL during the measurement interval, regardless of whether the links were automatically or manually made unavailable.	30 min

TmM3RLLinksetUnavail

Measurement Group: Link Set Usage

Measurement Type: Duration

Description: Total time (in seconds) that all links in the link set were unavailable to M3RL during the measurement interval, regardless of whether the links were automatically or manually made unavailable.

Collection Interval: 30 min

Peg Condition: M3RL must maintain an accurate time and measurement of the number of seconds during the collection period that the Link Set's state is **Unavailable**. This measurement is associated with the duration (in seconds) that **Alarm 19202 Link Set Unavailable** is asserted during the collection period.

Start of duration measurement for Link Set "X" criteria:

1. **Alarm 19202** is asserted for Link Set "X."
2. Start of new collection period AND **Alarm 19202** for Linkset "X" is already asserted (during a previous collection interval).

Stop of duration measurement for Link Set "X" criteria:

1. **Alarm 19202** for Linkset "X" is cleared (i.e, Link Set becomes **Available**).
2. End of collection interval.

Measurement Scope: NE, Server

Recovery:

This value provides a measure of the availability of a Link Set. No action required.

Link Usage measurements

Table 29: Link Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
TmLnkMOOS	Number of seconds the link is manual out of service during the reporting period. A link is manual out of service when the link is in the **Disabled** administrative state.	30 min
TmLnkOOS	Number of seconds the link is out of service for any reason during the reporting period. A link may be out of service due to: • Maintenance activity: link is **Disabled** or the link's association is **Disabled** or **Blocked**. • Failure of the link to receive ASP-ACTIVE-ACK. • Receipt of unsolicited ASP-INACTIVE-ACK from the SG. • A link's association is not in the **Normal** status: failed to establish SCTP connection, failed to receive ASP-UP-ACK, received unsolicited ASP-DOWN-ACK.	30 min
TmLnkAvailable	Number of seconds the link is in service during the reporting period. The link is considered to be in service if the link's status reason is **Normal**. An in-service link is available for M3UA DATA signaling.	30 min
EvLnkManClose	Number of times a link was closed due to manual action. This count indicates the number of times that a link transitioned from ASP-ACTIVE to ASP-INACTIVE as a direct result of someone changing the link	30 min

Measurement Tag	Description	Collection Interval
	administrative state from **Enabled** to **Disabled**.	

TmLnkMOOS

Measurement Group: Link Usage

Measurement Type: Duration

Description: The number of seconds the link is manual out of service during the reporting period. A link is manual out of service when the link is in the **Disabled** administrative state.

Collection Interval: 30 min

Peg Condition: Time is accumulated for this measurement when the link administrative state is set to **Disabled**.

Note: The link is not considered to be manually out of service if the link is in the **Enabled** administrative state even if the association that hosts the link is manually out of service.

Measurement Scope: NE, Server

Recovery:

1. If a non-zero value in this field is unexpected (i.e., no link maintenance is known to have occurred), the link status can be viewed from the GUI under **SS7/Sigtran>Maintenance>Links**.
2. Also, look in the GUI main menu under **Alarms & Events>View History** in the event history for **Event ID 19234**. **Event 19234** records each change in the link's administrative state. If the link was known to be under maintenance, this value represents the number of seconds during the reporting period that the link was in the **Disabled** administrative state.

TmLnkOOS

Measurement Group: Link Usage

Measurement Type: Duration

Description: The number of seconds the link is out of service for any reason during the reporting period. A link may be out of service due to the following conditions:

- Maintenance activity – link is **Disabled** or link's association is **Disabled** or **Blocked**.
- Failure of the link to receive ASP-ACTIVE-ACK.
- Receipt of unsolicited ASP-INACTIVE-ACK from the SG.
- The link's association is not in the **Normal** status – failed to establish SCTP connection, failed to receive ASP-UP-ACK, received unsolicited ASP-DOWN-ACK

Collection Interval: 30 min

Peg Condition: Time is accumulated for this measurement when the link status reason is not **Normal**.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a value of zero. If the link or the link's association is known to be under maintenance, then a non-zero value in this measurement is expected.

2. Otherwise, the link status can be viewed from the GUI main menu under **SS7/Sigtran>Maintenance>Links**.
3. Also look in the event history from the GUI main menu under **Alarms & Events>View History** for events related to this link or the link's association.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

TmLnkAvailable

Measurement Group: Link Usage

Measurement Type: Duration

Description: The number of seconds the link is in service during the reporting period. The link is considered to be in service if the link's status reason is **Normal**. An in-service link is available for M3UA DATA signaling.

Collection Interval: 30 min

Peg Condition: Time is accumulated for this measurement when the link status reason is **Normal**.

Measurement Scope: NE, Server

Recovery:

1. If all is well, this value should equal the length of the reporting period, meaning that the link was active for the entire reporting period. If the link-available time is not equal to the reporting period, it could be due to one of the following conditions:
   - Link maintenance. The measurements **TmLnkMOOS** and **TmLnkOOS** should have a non-zero values. See the actions for *TmLnkMOOS*.
   - Link failure. The measurement **TmLnkOOS** should have a non-zero value. See the actions for*TmLnkOOS*.
   - The link was added during the reporting period. The report indicates that the data is incomplete for the reporting period.
2. Contact the Tekelec *Customer Care Center* for assistance if needed.

EvLnkManClose

Measurement Group: Link Usage

Measurement Type: Simple

Description: The number of times a link was closed due to manual action. This count indicates the number of times that a link transitioned from ASP-ACTIVE to ASP-INACTIVE as a direct result of someone changing the link administrative state from **Enabled** to **Disabled**.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time:

- The link administrative state is changed from **Enabled** to **Disabled**, causing a protocol state transition from ASP-ACTIVE to ASP-INACTIVE.

Measurement Scope: NE, Server

Recovery:

1. If the link is known to be under maintenance, then no further action is necessary. If the link was not known to be under maintenance, then link status can be viewed from the GUI main menu under **SS7/Sigtran>Maintenance>Links**.
2. View the event history from the GUI main menu under **Alarms & Events>View History** looking for **Event ID 19234**. **Event ID 19234** shows the manual link state transitions and contains a time-stamp of when the change occurred.
3. The security logs from the GUI main menu under **Security Logs** can be searched using the time-stamp from the event history log to determine which login performed the manual state change on the link.
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

Server M3UA Exception measurements

Table 30: Server M3UA Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxM3uaERROR	Number of M3UA ERROR messages sent by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.	30 min
RxM3uaERROR	Number of times an M3UA ERROR messages received by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.	30 min
M3UAStackQueueFull	Number of messages that were discarded because the M3UA Stack Event Queue was full	30 min
SCTPAggrQueueFull	Number of egress messages that were discarded because the maximum number of SCTP messages queued in all SCTP Single Association Writer Queues exceeded a maximum capacity.	30 min
ANSIDiscardsNoPDUBuffer	ANSI ingress message discarded: no PDU buffer.	30 min

Measurement Tag	Description	Collection Interval
ITUDiscardsNoPDUBuffer	The number of ingress messages that were discarded because no ITU/ITUN PUD Buffers were available.	30 min
ItuiRxNoPDUBuffer	ITUI Ingress Message Discarded - No PDU Buffer	30 min
ItunRxNoPDUBuffer	ITUN Ingress Message Discarded - No PDU Buffer	30 min

TxM3uaERROR

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of M3UA ERROR messages sent by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an ERROR message is sent.

Measurement Scope: NE, Server

Recovery:

1. If all is well this measurement will have a zero value. If this measurement has a non-zero value, review the event history in the GUI under **Alarms & Events>View History**. Look for **Event ID 19231**.

   Event ID 19231 provides details about the reason for sending the M3UA ERROR message
2. If the error reason in **Event ID 19231** indicates a problem with the routing context, verify that the routing context used for the specified link is configured to match between the ASP and the SG.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxM3uaERROR

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of times M3UA ERROR messages are received by the MP server. M3UA ERROR messages are sent to inform the originator of an M3UA message that the message cannot be processed because of a problem with the message syntax or semantics.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an ERROR message is received.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. If the value is non-zero, view the event history from the GUI main menu under **Alarms & Events>View History** and look for **Event ID 19235**.
2. **Event ID 19235** provides details about the reason for receiving the M3UA ERROR message. If the reason indicates a problem with the routing context, verify that the routing context used for the link specified in **Event ID 19235** is configured to match between the ASP and the SG.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

M3UAStackQueueFull

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of messages that were discarded because the M3UA Stack Event Queue was full. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

SCTPAggrQueueFull

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of egress messages that were discarded because the number of SCTP messages queued in all SCTP Single Association Writer Queues exceeded a maximum capacity.

Collection Interval: 30 min

Peg Condition: For each SCTP Aggregate Association Writer Queue message discarded .

Measurement Scope: NE, Server

Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from GUI main menu under **Alarms & Events>View Active**.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from **Status & Manage>Server**.

4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transactions per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

ANSIRxNoPDUBuffer

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of ingress ANSI messages that were discarded because no ANSI PDU Buffers were available.

Collection Interval: 30 min

Peg Condition: For each ANSI message discarded

Measurement Scope: NE, Server

Recovery:

1. If this measurement is greater than zero, a network (IP or SS7) problem might exist or an MP-specific software problem may exist (for example, a buffer pool leak).
2. If the problem persists, contact the Tekelec *Customer Care Center*.

ItuiRxNoPDUBuffer

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of ingress ITUI messages that were discarded because no ITUI PDU Buffers were available.

Collection Interval: 30 min

Peg Condition: For each ITUI message discarded

Measurement Scope: NE, Server

Recovery:

1. If this measurement is greater than zero, a network (IP or SS7) problem might exist or an MP-specific software problem might exist (for example, a buffer pool leak).
2. If the problem persists, contact the Tekelec *Customer Care Center*.

ItunRxNoPDUBuffer

Measurement Group: Server M3UA Exception

Measurement Type: Simple

Description: The number of ingress ITUN messages that were discarded because no ITUN PDU Buffers were available.

Collection Interval: 30 min

Peg Condition: For each ITUN message discarded

Measurement Scope: NE, Server

Recovery:

1. ITUN PDU is allocated to each ITUN message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues. Under normal circumstances, the PDU Buffer Pool should never be 100% utilized.
2. If this measurement is greater than zero, then a network (IP or SS7) problem may exist or an MP-specific software problem may exist (e.g., a buffer pool leak).
3. If the problem persists, contact the Tekelec *Customer Care Center*.

Server M3UA Performance measurements

Table 31: Server M3UA Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxNonDataMsg	Non-DATA messages sent by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release.	30 min
RxNonDataMsg	Non-DATA messages received by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release.	30 min
TxNonDataOctets	Non-DATA octets sent by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.	30 min
RxNonDataOctets	Non-DATA octets received by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT,	30 min

Measurement Tag	Description	Collection Interval
	SSNM). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.	
M3UAStackQueuePeak	Peak M3UA Network Management Event Queue utilization (0-100%) measured during the collection interval.	30 min
M3UAStackQueueAvg	Average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval.	30 min
SCTPAggrQueuePeak	Peak SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.	30 min
SCTPAggrQueueAvg	Average of all SCTP Aggregate Association Writer Queue utilization samples taken during the collection interval.	30 min

TxNonDataMsg

Measurement Group: Server M3UA Performance

Measurement Type: Simple

Description: This measurement gives the level of non-DATA M3UA signaling that occurred on the MP server during the reporting period. The count includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release.

Collection Interval: 30 min, Daily

Peg Condition: This measurement is incremented by one each time any of the following occur:

- An ASP-UP message is sent.
- An ASP-DOWN message is sent.
- An ASP-ACTIVE message is sent.
- An ASP-INACTIVE message is sent.
- An ERROR message is sent.
- A DAUD message is sent.
- A BEAT message is sent.
- A BEAT-ACK message is sent.

Measurement Scope: NE, Server

Recovery:

No action required.

RxNonDataMsg

Measurement Group: Server M3UA Performance

Measurement Type: Simple

Description: This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time any of the following occur:

- An ASP-UP-ACK message is received
- An ASP-DOWN-ACK message is received
- An ASP-ACTIVE-ACK message is received
- An ASP-INACTIVE-ACK message is received
- An ERROR message is received
- A DUNA message is received
- A DAVA message is received
- A DRST message is received
- A SCON message is received
- A DUPU message is received
- A BEAT message is received
- A BEAT-ACK message is received
- A NOTIFY message is received

Measurement Scope: NE, Server

Recovery:

No action required.

TxNonDataOctets

Measurement Group: Server M3UA Performance

Measurement Type: Simple

Description: This measurement gives the number of octets of non-DATA M3UA signaling that occurred on the MP server during the reporting period. The count includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the message (not including SCTP, IP, or Ethernet headers) each time any of the following occur:

- An ASP-UP message is sent.
- An ASP-DOWN message is sent.
- An ASP-ACTIVE message is sent.
- An ASP-INACTIVE message is sent.
- An ERROR message is sent.
- A DAUD message is sent.

- A BEAT message is sent.
- A BEAT-ACK message is sent.

Measurement Scope: NE, Server

Recovery:

No action required.

RxNonDataOctets

Measurement Group: Server M3UA Performance

Measurement Type: Simple

Description: This measurement gives the number of octets of non-DATA M3UA signaling occurring on the MP server during the reporting period. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the message (not including SCTP, IP, or Ethernet headers) each time any of the following occur:

- An ASP-UP-ACK message is received
- An ASP-DOWN-ACK message is received
- An ASP-ACTIVE-ACK message is received
- An ASP-INACTIVE-ACK message is received
- An ERROR message is received
- A DUNA message is received
- A DAVA message is received
- A DRST message is received
- A SCON message is received
- A DUPU message is received
- A BEAT message is received
- A BEAT-ACK message is received
- A NOTIFY message is received

Measurement Scope: NE, Server

Recovery:

No action required.

M3UAStackQueuePeak

Measurement Group: Server M3UA Performance

Measurement Type: Max

Description: The peak M3UA Network Management Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The maximum M3UA Stack Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

M3UAStackQueueAvg

Measurement Group: Server M3UA Performance

Measurement Type: Average

Description: The average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The average of all M3UA Stack Event Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

SCTPAggrQueuePeak

Measurement Group: Server M3UA Performance

Measurement Type: Max

Description: The peak SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 30 min

Peg Condition: The maximum SCTP Aggregate Association Writer Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from the GUI main menu under **Alarms & Events>View Active**.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from **Status & Manage>Server**.
4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

SCTPAggrQueueAvg

Measurement Group: Server M3UA Performance

Measurement Type: Average

Description: The average SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 30 min

Peg Condition: The average of all SCTP Aggregate Association Writer Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from the GUI main menu under **Alarms & Events>View Active**.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from **Status & Manage>Server**.
4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage>KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the Tekelec *Customer Care Center*.

Server M3UA Usage measurements

Table 32: Server M3UA Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxASPSM	Number of ASPSM messages sent by the MP server.	30 min
RxASPSM	Number of ASPSM messages received by the server.	30 min
TxASPTM	Number of ASPTM messages sent by the MP server.	30 min
RxASPTM	Number of ASPTM messages received by the MP server.	30 min
TxDAUD	Number of DAUD messages sent by the MP server. DAUD message are sent periodically as an audit when the SG reports that a point code is unavailable or congested.	30 min
RxSSNM	Number of SSNM messages received by the MP server. SSNM messages are sent from the SG as information about point code and user part status in the network.	30 min
RxM3uaNOTIFY	Number of M3UA NOTIFY messages received by the MP server. M3UA NOTIFY messages are sent by the SG to indicate its view of the M3UA AS state. These messages do not cause any signaling behavior on the MP server.	30 min

TxASPSM

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: This measurement gives the level of ASPSM M3UA signaling that occurs on the MP server during the reporting period.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time any of the following occur:

- An ASP-UP message is sent.

- An ASP-DOWN message is sent.
- A BEAT message is sent.
- A BEAT-ACK message is sent.s

Measurement Scope: NE, Server

Recovery:

No action required.

RxASPSM

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: This measurement gives the level of ASPSM M3UA signaling occurring on the MP server during the reporting period.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time any of the following occur:

- An ASP-UP-ACK message is received
- An ASP-DOWN-ACK message is received
- A BEAT message is received
- A BEAT-ACK message is received

Measurement Scope: NE, Server

Recovery:

No action required.

TxASPTM

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: This measurement gives the level of ASPTM M3UA signaling that occurs on the MP server during the reporting period.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time any of the following occur:

- An ASP-ACTIVE message is sent.
- An ASP-INACTIVE message is sent.

Measurement Scope: NE, Server

Recovery:

No action required.

RxASPTM

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: This measurement gives the level of ASPTM M3UA signaling occurring on the MP server during the reporting period.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time any of the following occur:

- An ASP-ACTIVE-ACK message is received
- An ASP-INACTIVE-ACK message is received

Measurement Scope: NE, Server

Recovery:

No action required.

TxDAUD

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: This measurement indicates the level of auditing that occurs on the MP server during the reporting period. AUD message are sent periodically as an audit when the SG reports that a point code is unavailable or congested.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time a DAUD message is sent.

Measurement Scope: NE, Server

Recovery:

No action required.

RxSSNM

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: The number of SSNM messages received by the MP server. SSNM messages are sent from the SG as information about point code and user part status in the network. This measurement indicates the level of SSNM signaling occurring on the MP server during the reporting period.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by the number of octets in the message (not including SCTP, IP, or Ethernet headers) each time any of the following occur:

- A DUNA message is received
- A DAVA message is received
- A DRST message is received
- A SCON message is received
- A DUPU message is received

Measurement Scope: NE, Server

Recovery:

No action required.

RxM3uaNOTIFY

Measurement Group: Server M3UA Usage

Measurement Type: Simple

Description: The number of M3UA NOTIFY messages received by the MP server. M3UA NOTIFY messages are sent by the SG to indicate its view of the M3UA AS state. These messages do not cause any signaling behavior on the MP server.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time a NOTIFY message is received.

Measurement Scope: NE, Server

Recovery:

No action required.

Server MTP3 Exception measurements

Table 33: Server MTP3 Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxM3RLDestUnknown	Number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.	5 min
TxM3RLDestUnavail	Number of egress messages M3RL discarded because the RSP/Destination was Unavailable.	5 min
TxM3RLDestCong	Number of egress messages M3RL discarded because the RSP/Destination's congestion level was higher than the message's priority.	5 min
TxM3RLBufOverflow	Number of egress messages M3RL discarded because of an internal buffer overflow.	5 min
RxM3RLInvalidDPC	Number of ingress messages M3RL discarded because the DPC was not the True Point Code (TPC) or Capability Point Code (CPC) configured for the MP.	5 min

Measurement Tag	Description	Collection Interval
RxM3RLInvalidSI	Number of ingress messages M3RL discarded because the Service Indicator received was not "0" (SNM) or "3" (SCCP).	5 min
RxM3RLInvalidNI	Number of ingress messages M3RL discarded because the Network Indicator received was not the same value configured for the MP.	5 min
RxM3RLBufOverflow	Number of ingress messages M3RL discarded because of an internal buffer overflow.	5 min
M3RLStackQueueFull	Number of messages that were discarded because the M3RL Stack Event Queue was full.	5 min
M3RLNetMgtQueueFull	Number of M3RL network management messages (SI=0) that were discarded because the M3RL Network Management Event Queue was full.	5 min

TxM3RLDestUnknown

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, then an internal routing table problem exists. Contact the Tekelec *Customer Care Center* for assistance.

TxM3RLDestUnavail

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of egress messages M3RL discarded because the RSP/Destination was Unavailable.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

The RSP/Destination can be unavailable when the request is received from the User Part or while M3RL is buffering messages for a rerouting or changeover/changeback procedure.

TxM3RLDestCong

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of egress messages M3RL discarded because the RSP/Destination's congestion level was higher than the message's priority.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress messages M3RL discarded because the RSP/Destination's congestion level was higher than the message's priority. Network Management messages have the highest message priority. User Part message priorities are determined by the SCCP layer.

TxM3RLBufOverflow

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of egress messages M3RL discarded because of an internal buffer overflow.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

1. This condition should not occur but may be caused by an unusually high setting of the T1, T3, or T6 timers. The default value is 60ms but the user has the ability to set them as high as 2000ms. You can view and modify the current M3RL timer values via the GUI under **SS7/Sigtran>Configuration>MTP3 Options**.
2. An internal overflow condition may occur if the IP network is unstable causing M3RL to invoke multiple Changeover/Changeback procedures as links fail and recover. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxM3RLInvalidDPC

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: This value provides a measure of how many ingress messages are discarded because the DPC was not a True Point Code (TPC) or Capability Point Code (CPC) configured for the MP.

Collection Interval:

Peg Condition:

Measurement Scope:

Recovery:

1. From the GUI main menu under **SS7/Sigtran>Configuration>Link Sets** verify that the LSP Point Code field is set to **All** if signaling can arrive for either CPC or TPC on this link set.
2. If this measurement is large, it may indicate a routing inconsistency between STP/SG and the MP. You can view the point codes of the MP from **SS7/Sigtran>Configuration>Local Signaling Points**.

RxM3RLInvalidSI

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: This value provides a measure of how many ingress messages M3RL discarded because the Service Indicator received was not **0** (SNM) or **3** (SCCP).

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

This type of failure should never occur and usually indicates that the routing in the STP/SG or originator of the message is incorrect.

RxM3RLInvalidNI

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: This value provides a measure of how many ingress messages M3RL discarded because the Network Indicator received was the same value configured for the MP.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

If this measurement is large, it may indicate a routing inconsistency between the STP/SG and the MP. The NI values for the MP can be viewed via the GUI main menu under **SS7/Sigtran>Configuration>Local Signaling Points**. See the **SS7 Domain** column.

RxM3RLBufOverflow

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: This value provides a measure of how many ingress messages M3RL discarded because of an internal buffer overflow.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

This should never occur unless the MP is experiencing severe overload conditions and SCCP is unable to service its event queue.

M3RLStackQueueFull

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of messages that were discarded because the M3RL Stack Event Queue was full. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

M3RLNetMgtQueueFull

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of M3RL network management messages (SI=0) that were discarded because the M3RL Network Management Event Queue was full. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

Server MTP3 Performance measurements

Table 34: Server MTP3 Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxM3RLDataMsgs	Egress M3RL DATA Messages (at M3RL->M3UA interface). This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.	5 min
RxM3RLDataMsgs	Ingress M3RL DATA Messages (at M3RL->M3UA interface). This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SSNM messages.	5 min
M3RLStackQueuePeak	Peak M3RL Stack Event Queue utilization (0-100%) measured during the collection interval	5 min
M3RLStackQueueAvg	Average M3RL Stack Event Queue utilization (0-100%) measured during the collection interval.	5 min
M3RLNetMgtQueuePeak	Peak M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval	5 min
M3RLNetMgtQueueAvg	Average M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval	5 min

TxM3RLDataMsgs

Measurement Group: Server MTP3 Performance

Measurement Type: Simple

Description: This value provides a measure of how many egress DATA messages are sent from M3RL to M3UA. This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.

Collection Interval: 5 min

Peg Condition: This counter is pegged each time a M3RL DATA message is sent to M3UA. This counter includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.

Measurement Scope: NE, Server

Recovery:

No action required.

RxM3RLDataMsgs

Measurement Group: Server MTP3 Performance

Measurement Type: Simple

Description: This value provides a measure of how many ingress DATA messages M3RL is processing from the network. This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SSNM messages.

Collection Interval: 5 min

Peg Condition: This counter is pegged each time a M3RL DATA message is receive at M3RL from M3UA. This counter includes SCMG messages (which are DATA to the M3RL layer), but does not include SSNM messages.

Measurement Scope: NE, Server

Recovery:

No action required.

M3RLStackQueuePeak

Measurement Group: Server MTP3 Performance

Measurement Type: Max

Description: The peak M3RL Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Peg Condition: The maximum M3RL Stack Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

M3UAStackQueueAvg

Measurement Group: Server M3UA Performance

Measurement Type: Average

Description: The average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The average of all M3UA Stack Event Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

M3RLNetMgtQueuePeak

Measurement Group: Server MTP3 Performance

Measurement Type: Max

Description: The peak M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Peg Condition: The maximum M3RL Network Management Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

M3RLNetMgtQueueAvg

Measurement Group: Server MTP3 Performance

Measurement Type: Average

Description: The average M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Peg Condition: The average of all M3RL Network Management Event Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

Server Resource Usage measurements

Table 35: Server Resource Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
SS7ProcessPeak	Peak SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.	5 min
SS7ProcessAvg	Average SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.	5 min
RxMsgRatePeak	Peak Ingress Message Rate (in messages per second) measured during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.	5 min
RxMsgRateAvg	Average Ingress Message Rate (messages per second) during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.	5 min
AnsiPDUUtilPeak	ANSI PDU Buffer Pool Peak Utilization.	5 min

Measurement Tag	Description	Collection Interval
AnsiPDUUtilAvg	ANSI PDU Buffer Pool Average Utilization.	5 min
ItuiPDUUtilPeak	ITUI PDU Buffer Pool Peak Utilization.	5 min
ItuiPDUUtilAvg	ITUI PDU Buffer Pool Average Utilization.	5 min
ItunPDUUtilPeak	ITUN PDU Buffer Pool Peak Utilization.	5 min
ItunPDUUtilAvg	ITUN PDU Buffer Pool Average Utilization.	5 min

SS7ProcessPeak

Measurement Group: Server Resource Usage

Measurement Type: Max

Description: The peak SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 Process is responsible for all SS7-related processing.

Collection Interval: 5 min

Peg Condition: The maximum SS7 Process CPU utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

SS7ProcessAvg

Measurement Group: Server Resource Usage

Measurement Type: Average

Description: The average SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.

Collection Interval: 5 min

Peg Condition: The average of all SS7 Process CPU utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxMsgRatePeak

Measurement Group: Server Resource Usage

Measurement Type: Max

Description: The peak Ingress Message Rate (in messages per second) measured during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.

Collection Interval: 5 min

Peg Condition: The maximum Ingress Message Rate (messages per second) sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxMsgRateAvg

Measurement Group: Server Resource Usage

Measurement Type: Average

Description: The average Ingress Message Rate (messages per second) during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.

Collection Interval: 5 min

Peg Condition: The average of all Ingress Message Rate samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

AnsiPDUUtilPeak

Measurement Group: Server Resource Usage

Measurement Type: Max

Description: The peak SS7 PDU Buffer Pool utilization (0-100%) measured during the collection interval. A PDU is allocated to each message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist.

Collection Interval: 5 min

Peg Condition: The maximum SS7 PDU buffer pool utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. ANSI PDU is allocated to each ANSI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

AnsiPDUUtilAvg

Measurement Group: Server Resource Usage

Measurement Type: Average

Description: The average SS7 PDU Buffer Pool utilization (0-100%) measured during the collection interval. A PDU is allocated to each message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist.

Collection Interval: 5 min

Peg Condition: The average of all SS7 PDU buffer pool utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. ANSI PDU is allocated to each ANSI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
4. Contact the Tekelec *Customer Care Center* for assistance if needed.

ItuiPDUUtilPeak

Measurement Type: Max

Measurement Group: Server Resource Usage

Description: The peak SS7 ITUI PDU Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum SS7 ITUI PDU Buffer Pool utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. ITUI PDU is allocated to each ITUI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

4. Contact the Tekelec Customer Care Center for assistance if needed.

ItuiPDUUtilAvg

Measurement Type: Average

Measurement Group: Server Resource Usage

Description: The average SS7 ITUI PDU Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all SS7 ITUI PDU Buffer Pool utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. ITUI PDU is allocated to each ITUI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
4. Contact the Tekelec Customer Care Center for assistance if needed.

ItunPDUUtilPeak

Measurement Type: Max

Measurement Group: Server Resource Usage

Description: The peak SS7 ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum SS7 ITUN PDU Buffer Pool utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. ITUN PDU is allocated to each ITUN message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the

processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.

2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
4. Contact the Tekelec Customer Care Center for assistance if needed.

ItunPDUUtilAvg

Measurement Type: Max

Measurement Group: Server Resource Usage

Description: The average SS7 ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all SS7 ITUN PDU Buffer Pool utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. ITUN PDU is allocated to each ITUN message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
4. Contact the Tekelec Customer Care Center for assistance if needed.

Server SCCP Exception measurements

Table 36: Server SCCP Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvError	Number of error log events.	30 min

Measurement Tag	Description	Collection Interval
EvVital	Number of vital log events.	30 min
RxSCCPInvalidDPC	Number of ingress messages SCCP discarded because the DPC is not the TPC or CPC of an MP for an ingress SCCP message.	30 min
RxSCCPInvalidSSN	Number of ingress messages SCCP discarded because the CdPA SSN or affected SSN is missing/invalid for an ingress SCCP message.	30 min
RxSCCPInvalidMsg	Number of ingress messages SCCP discarded because the Message Type is not currently supported. **Note:** Only the following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. Valid SCMG Message Types: SSA, SSP, SST.	30 min
RxSCCPInvalidHop	Number of ingress messages SCCP discarded because of a Hop Counter violation associated with CdPA `RI=route on GT`.	30 min
RxSCCPInvalidClass	Number of ingress messages SCCP discarded because of an invalid protocol class. Note: Only classes 0 and 1 are supported.	30 min
RxSCCPInvalidGTI	Number of ingress messages SCCP discarded because an invalid Global Title Indicator (GTI) value was received. This only applies to messages received with `RI=route on GT`. **Note:** GTI=0 is invalid. (Applications using AWPSS7 may impose further limitations on GTI values. For example, EXHR supports: only `GTI=2` for ANSI, only `GTI=2` and `GTI=4` for ITU).	30 min

Measurement Tag	Description	Collection Interval
RxMPCongestion	Number of ingress SCCP messages that were discarded because of Local MP Congestion.	30 min
RxMaxTpsExceeded	Number of ingress SCCP messages that were discarded because of the Local MP Maximum TPS limit.	30 min
TxSCCPCongestion	Number of egress messages SCCP discarded because the RSP/Destination's congestion level was higher than the message's priority.	30 min
TxSCCPInvalidDPC	Number of egress messages SCCP discarded because the RSP/DPC is missing or invalid for an egress SCCP message.	30 min
TxSCCPInvalidSSN	Number of egress messages SCCP discarded because the remote SSN is missing or invalid for an egress SCCP message.	30 min
SCCPStackQueueFull	Number of ingress SCCP messages that were discarded because the SCCP Stack Event Queue was full.	30 min
TxSCCPUnavailDPC	RSP/affected DPC unavailable for an egress SCCP message.	30 min
TxSCCPUnknownDPC	RSP/affected DPC unknown (unequipped) for an egress SCCP message.	30 min
TxSCCPUnavailSSN	Remote/affected SSN unavailable for an egress SCCP message.	30 min
TxSCCPUnknownSSN	Remote/affected SSN unknown (unequipped) for an egress SCCP message.	30 min
TxSCCPInvUserMsgs	Invalid N-UnitDatareq received from the Local SCCP User/application.	30 min
RxSCCPUnavailSSN	Messages received for a prohibited Local/Affected SSN.	30 min

Measurement Tag	Description	Collection Interval
RxSCCPUnknownSSN	Messages received for an unequipped/unknown Local/Affected SSN.	30 min
SCMGErrors	Number of ingress/egress malformed or unsupported messages.	30 min
SCCPGTTFailure	Default action for `ri=rt-on-gtt` messages from the SS7 stack.	30 min

EvError

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of error trace conditions. This indicates that an expected but abnormal path was taken in the software, which warrants further investigation.

By default, error tracing is disabled. Non-zero values in this measurement indicate that something is occurring that would have generated an error trace, were error tracing enabled. These error trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

Contact the Tekelec *Customer Care Center* for assistance if any unexpected non-zero values in this measurement occur.

EvVital

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of vital trace conditions encountered. A vital trace indicates that an unexpected path was taken in the software, which warrants further investigation. These vital trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

During application start-up and shutdown, vital traces are used to show details that can aid in debugging of initialization and shutdown problems. These traces are always enabled and cannot be turned off.

It is a VITAL error condition for any other instance.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

Contact the Tekelec *Customer Care Center* for assistance if any unexpected non-zero values in this measurement occur.

RxMaxTpsExceeded

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress SCCP messages that were discarded because of the Local MP Maximum TPS limit.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

1. The MP is approaching or exceeding its engineered traffic handling capacity. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage>Server Status**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from the GUI main menu under **Status & Manage>KPI Display**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from the GUI main menu under **Status & Manage>KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The SS7 process may be experiencing problems. Examine the alarm log from the GUI main menu under **Alarms & Events**.
5. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxMPCongestion

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress SCCP messages that were discarded because of local MP congestion.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Control>Server Status**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from the GUI main menu under **Status & Control>KPI Display**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from the GUI main menu under **Status & Control>KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The SS7 process may be experiencing problems. The alarm log should be examined from the GUI main menu under **Alarms & Events**.
5. Contact the Tekelec *Customer Care Center* for assistance if needed.

RxSCCPInvalidDPC

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress messages SCCP discarded because the MTP point code was present but was not a TPC or CPC for the signaling standard of the message.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This count shows how many ingress messages SCCP discarded because the point code received in the MTP was not encoded correctly (same as TPC or CPC) for the signaling standard of the message. If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured. Contact the Tekelec *Customer Care Center* for assistance.

RxSCCPInvalidSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress messages SCCP discarded because the CdPA/CgPA SSN was present but had an invalid value (SSN< 1 or SSN >254).

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured.

RxSCCPInvalidMsg

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress messages SCCP discarded because the message type is not currently supported.

Note: Only the following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. Valid SCMG message types are SSA, SSP, and SST.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, then the originator of the message may be misconfigured.

RxSCCPInvalidHop

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of ingress messages SCCP discarded because of a Hop Counter violation associated with CdPA `RI=route on GT`.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

If this error occurs, then either the originator of the message is setting the initial value too low or the STPs are rerouting the message too many times due to a possible STP routing misconfiguration. Contact the Tekelec *Customer Care Center* for assistance.

RxSCCPInvalidClass

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress messages SCCP discarded because of an invalid protocol class.

Note: Only classes 0 and 1 are supported.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, then the originator of the message may be misconfigured or the network is misconfigured causing mis-routing of messages.

RxSCCPInvalidGTI

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress messages SCCP discarded because an invalid Global Title Indicator (GTI) value was received. This only applies to messages received with `RI=route on GT`.

Note: `GTI=0` is invalid.

Collection Interval: 30 min

Peg Condition:

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, then the originator of the message may be misconfigured.

RxSCCPReassFAIL

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of times the reassembly procedure failed.

Collection Interval: 30 min

Peg Condition: For each reassembly failure for ingress segmented XUDT message received from network

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of reassembly procedure failures encountered during the reporting interval.
2. Check for any related additional Events or Alarms from the server.

RxSCCPReassInternalFail

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of reassembly procedure failures due to internal error or resource limitation.

Collection Interval: 30 min

Peg Condition: N/A

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of reassembly procedure failures encountered due to errors encountered on server, during the reporting interval.
2. Non-zero value for this measurement tag represents resource usage issues on the server. Check for any related additional Events or Alarms from the server.

RxSCCPReassOOSFail

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of reassembly procedure failures due to out-of-sequence segments received from network.

Collection Interval: 30 min

Peg Condition: For each ongoing reassembly procedure failure as a result of out of order arrival of remaining segments.

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of reassembly procedure failures encountered due to "out of order arrival of remaining segments in a reassembly procedure" reason, during the reporting interval.
2. Non-zero value for this measurement tag represents sequencing issues in packet arrival from network or any other routing error or delays in network or on server. Check for any related additional Events or Alarms from the server.

RxSCCPReassTExp

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of reassembly procedure failures due to reassembly timer expiry.

Collection Interval: 30 min

Peg Condition: For each reassembly procedure failures due to reassembly timer expiry

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of reassembly procedure failures encountered due to "Reassembly Timer Expiry" reason, during the reporting interval.
2. Non-zero value for this measurement tag represents latency issues in packet arrival from network or any other delay on server resulting in reassembly timer expiry. Check for any related additional Events or Alarms from the server.

RxSCCPSegmentOOS

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of XUDT segments received out-of-sequence from network.

Collection Interval: 30 min

Peg Condition: On received XUDT segments with F bit set as 0 and received segments could not be attached to any open reassembly procedure (i.e. reassembly procedure was not started for this and no key found to associate the segments to a in-process reassembly)

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of segmented XUDT messages received with sequence delivery option but arrived out of sequence at SCCP Layer, during the reporting interval.

2. For these out of sequence received XUDT segments, there is no ongoing reassembly procedure to attach these segments.
3. Non-zero value for this measurement tag represents in-sequence routing or reassembly key uniqueness issue. Check for any related additional Events or Alarms from the server.

RxSCCPSgmntsPartReassFAIL

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of partially reassembled segments discarded due to any errors.

Collection Interval: 30 min

Peg Condition: For each segmented XUDT message that was buffered and discarded due to reassembly procedure failure

Measurement Scope: Network, NE, Server

Recovery:

This value provides cumulative measure of ingress segmented XUDT messages which were buffered but discarded due to reassembly procedure failure.

RxSCCPUnavailSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of ingress messages (RI=SSN) SCCP discarded because the CdPA SSN (Local SSN for MPs TPC) was manually disabled.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many ingress (RI=SSN) messages SCCP discarded because the affected Local Subsystem status was manually disabled. The Status of Local Subsystems (Local SCCP Users, LSUs) for a Local Signaling Point can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Local SCCP Users'.

RxSCCPUnknownSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of ingress messages (RI=SSN) SCCP discarded because the CdPA SSN (Local SSN for MPs TPC) is not configured for the MTP DPC's signaling domain

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many ingress (RI=SSN) messages SCCP discarded because the affected Local Subsystem is not configured for the MTP DPC's signaling domain. The Local Subsystems (Local SCCP User, LSUs) for a Local Signaling Point can be configured via the following GUI menu: Main Menu: SS7/SIGTRAN -> Configuration -> 'Local SCCP Users' Insert.

RxSCCPXudtInvSgmnt

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of received XUDT segments resulted in protocol violation decode error.

Collection Interval: 30 min

Peg Condition: For protocol decoding errors while parsing ingress segmented XUDT

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of malformed segmented XUDT messages received from the network.

SCCPGTTFailure

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Count of SCCP GTT Failures due to default GTT handling in SS7Stack.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many "ri=rt-ongt" messages were subject to default Global Title Translation processing. This can occur when Application is using SS7 Stack for processing only "rt-on-ssn" messages OR "rt-on-gt" message handling is not implemented in Application.

SCCPStackQueueFull

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of ingress SCCP messages that were discarded because the SCCP Stack Event Queue was full.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP are significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

SCMGErrors

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of ingress/egress malformed or unsupported messages.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many malformed or unsupported SCCP management messages were discarded. Supported SCMG messages are SST, SSP and SSA. Any other SCCP Management message is pegged under this tag.

TxSCCPCongestion

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of egress messages SCCP discarded because the RSP/Destination's congestion level was higher than the message's priority.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

You can view the remote RSPs/Destinations to SCCP and their congestion status from the GUI main menu under **SS7/Sigtran>Maintenance>Remote MTP3 Users**.

TxSCCPInvUserMsgs

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: SCCP User submitted an Invalid/malformed/unsupported message for egress routing (SCCP User->SCCP N-UnitDataReq)

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress SCCP User messages encountered validation failure on SCCP. If a high number of these errors occur, then it indicates an encoding error at the originator or the originator of the message may be mis-configured.

TxSCCPInvalidDPC

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of egress messages SCCP discarded because the CdPA signaling point code is present but is not valid for the signaling standard of the message.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured.

TxSCCPInvalidSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of egress messages SCCP discarded because the CdPA/CgPA SSN was present but had an invalid value (SSN< 1 or SSN >254).

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured.

TxSCCPSegmentFAIL

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of times segmentation procedure failed.

Collection Interval: 30 min

Peg Condition: On failure in completion of segmentation procedure for each large egress user data message.

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of segmentation procedure completion failures for large egress user data messages. Segmentation Error Procedure is executed on each such failure.
2. Check for any related additional Events or Alarms from the server.

TxSCCPUnavailDPC

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of egress messages SCCP discarded because the affected DPC status was marked prohibited/unavailable.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress messages SCCP discarded because the RSP/Destination status was paused / prohibited at SCCP. Point code status is received from M3RL via the MTP-PAUSE and MTP-RESUME indications. The remote RSPs/Destinations known to SCCP and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote Signaling Points'.

TxSCCPUnavailSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of egress messages SCCP discarded because the CdPA or Affected SSN was either marked prohibited/unavailable.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress messages SCCP discarded because the Remote Subsystem status was Prohibited. Subsystem status is received from M3RL via the SS-STATUS indications or via SCMG SSA and SSP messages. The remote subsystems (RMUs) known to SCCP and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote MTP3 Users'.

TxSCCPUnknownDPC

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of egress messages SCCP discarded because the affected DPC in message is not configured or is unknown.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress messages SCCP discarded because the RSP or affected DPC in the message is not configured and is unknown at SCCP. The remote RSPs/affected

Destinations known to SCCP and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote Signaling Points'.

TxSCCPUnknownSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: Number of egress messages SCCP discarded because the CdPA or affected SSN was unknown.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress messages SCCP discarded because the Subsystem was unknown to SCCP. The remote subsystems (RMUs) can be configured from GUI menu:: Main Menu: SS7/SIGTRAN ->Configuration->Remote MTP3 Users and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote MTP3 Users'.

Server SCCP Performance measurements

Table 37: Server SCCP Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxSCCPMsgs	Egress messages sent by SCCP to M3RL (SCCP>M3RLMTP-TRANSFER request).	30 min
RxSCCPMsgs	Ingress messages received by SCCP from M3RL (M3RL>SCCP MTP-TRANSFER indication).	30 min
SCCPStackQueuePeak	Peak SCCP Stack Event Queue utilization (0-100%) measured during the collection interval.	30 min
SCCPStackQueueAvg	Average SCCP Stack Event Queue utilization (0-100%) measured during the collection interval.	30 min
TxSCCPUserMsgs	Valid N-UnitDatareq generated by local SCCP User and processed by SCCP.	30 min
TxSCMGMsgs	Number of valid egress SCMG messages.	30 min

Measurement Tag	Description	Collection Interval
RxSCCPUserMsgs	UDT/XUDT received and N-UnitDataInd Event delivered to Local SCCP.	30 min
RxSCCPUserNoticeMsgs	User UDTS/XUDTS received and NNotice-Ind sent to Local SCCP User.	30 min
RxSCMGMsgs	Number of valid ingress SCMG messages.	30 min

TxSCCPLargeMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of egress large user data messages for segmentation.

Collection Interval: 30 min

Peg Condition: For each large user data message submitted by SCCP User for egress routing.

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of how many large user data messages are submitted to SCCP layer for egress routing during the reporting interval. This measurement peg value divided by the interval yields the average rate of large egress user data messages for the server.

TxSCCPMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Egress messages sent by SCCP to M3RL (SCCP->M3RL MTP-TRANSFER request). This value provides a measure of how many egress SCCP messages are being processed by the MP server.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

No action required.

TxSCCPSegmentsPerMsg

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of segments created for each large egress user data message.

Collection Interval: 30 min

Peg Condition: When the segmentation procedure is completed on each large egress user data packet, using "number of segments" as index.

Measurement Scope: Network, NE, Server

Recovery:

1. Values in this arrayed measurement provides a measure of number of XUDT messages created each time a large user data messages is segmented by SCCP layer.
2. This arrayed measurement can be used for heuristics on segments created during the reporting interval and the SS7 traffic rate impact due to large egress user data size traffic.

TxSCCPSegmentSUCC

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of times segmentation procedure completed successfully.

Collection Interval: 30 min

Peg Condition: On successful completion of segmentation procedure for each large egress user data message (i.e. user data length is greater than SCCP Option Configured value).

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of number of successful segmentation procedure completion for large egress user data messages are successfully segmented and corresponding XUDT messages are forwarded by SCCP layer for egress routing during the reporting interval.

TxSCCPUserMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Egress messages sent by SCCP User to SCCP to M3RL (SCCPUser-> SCCP N-UnitDataReq->M3RL MTP-TRANSFER request)

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many egress SCCP User messages are being processed by the MP server.

TxSCMGMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of valid egress SCMG messages.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of egress SCCP Management messages This could be due to local or remote SCCP/SCCP Users status. The Status of Local or Remote Subsystems can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Local SCCP Users' or "Remote MTP3 Users".

RxSCCPMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Ingress messages received by SCCP from M3RL (M3RL> SCCP MTP TRANSFER indication).

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

No action required.

RxSCCPReassSUCC

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of times reassembly procedure successfully completed.

Collection Interval: 30 min

Peg Condition: On successful completion of reassembly procedure using a number of ingress segmented XUDT messages.

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of number of successful reassembly procedure (using a number of ingress segmented XUDT messages) completion during the reporting interval. The reassembled user data is forwarded as single packet to SCCP User.

RxSCCPRtGtFrwdAppl

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of Rt On Gt Messages forwarded to Local Application.

Collection Interval: 30 min

Peg Condition: N/A

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of number of messages received with CDPA RI=GT and are forwarded to Local Application due to configured SCCP Option.

RxSCCPRtGtXudtSgmnt

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of Rt on Gt segmented XUDT messages received from network

Collection Interval: 30 min

Peg Condition: N/A

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of number of Rt on Gt segmented XUDT messages received from the network.

RxSCCPRtSsnXudtSgmnt

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of Rt on Ssn segmented XUDT messages received from network.

Collection Interval: 30 min

Peg Condition: N/A

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of number of Route on SSN segmented XUDT messages received from the network.

RxSCCPSegmentSrvcMsg

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of Segmented XUDTS messages received from network.

Collection Interval: 30 min

Peg Condition: For each segmented XUDTS messages received from network

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of number of segmented XUDTS messages received from the network.

RxSCCPSgmntReassPerMsg

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of segments reassembled to create one large ingress user data message.

Collection Interval: 30 min

Peg Condition: This is an arrayed measurement with "number of XUDT segments assembled" as index. Peg this measurement using "number of XUDT segments assembled" as index, when reassembly procedure is completed using more than one ingress segmented XUDT message.

Measurement Scope: Network, NE, Server

Recovery:

1. Values in this arrayed measurement provides a measure of number of segmented XUDT messages were reassembled for each reassembly procedure before forwarding a large user data messages to SCCP User.
2. This arrayed measurement can be used for heuristics on number of segments network used for segmenting large message during the reporting interval and the SS7 traffic rate impact due to segmented XUDT messages on overall SCCP processing rate.

RxSCCPSgmntsReassSUCC

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of XUDT segments reassembled successfully.

Collection Interval: 30 min

Peg Condition: For each well-formed ingress segmented XUDT message resulting in a successful reassembly procedure

Measurement Scope: Network, NE, Server

Recovery:

This value provides a measure of well-formed ingress segmented XUDT messages that are reassembled successfully.

RxSCCPSgmntXudtMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of ingress segmented XUDT messages received from network.

Collection Interval: 30 min

Peg Condition: For each segmented XUDT message received from network.

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of how many segmented XUDT messages are received by SCCP layer during the reporting interval. SCCP will execute reassembly procedure for each such received message.
2. This measurement peg value divided by the interval yields the average rate of new segmented XUDT messages received from the network.

RxSCCPUserMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Ingress SCCP UDT/XUDT messages sent by SCCP to Configured and available SCCP Users using a local SSN (SCCP->SCCP User N-UnitDataInd)

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many ingress SCCP User (RI=SSN) messages are being forwarded to SCCP User application hosted by the MP server.

RxSCCPUserNoticeMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Ingress SCCP UDTS/XUDTS (RI=SSN) messages converted into N-Notice-Ind by SCCP and sent to the configured and available SCCP Users using a local SSN (SCCP->SCCP User N-NoticeInd)

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

1. This value provides a measure of how many ingress SCCP UDTS/XUDTS (RI=SSN) messages were received and converted into N-Notice-Ind and forwarded to SCCP User application hosted by the MP server.
2. If a high number of these errors occur, then it indicates the remote SCCP/SCCP Application could not process the message as expected and resulted in executing sccp error handling procedure. It's normally associated with an event/alarm condition. If a high number of these errors occur, then check the event history under "Main Menu:: Alarms & Events-> View History".

RxSCMGMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of valid ingress SCMG messages.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of ingress SCCP Management messages. This could be due to local or remote SCCP/SCCP Users status. The Status of Local or Remote Subsystems can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Local SCCP Users' or "Remote MTP3 Users".

SCCPStackQueuePeak

Measurement Group: Server SCCP Performance

Measurement Type: Max

Description: The peak SCCP Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The maximum SCCP Stack Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP are significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

SCCPStackQueueAvg

Measurement Group: Server SCCP Performance

Measurement Type: Average

Description: The average SCCP Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The average of all SCCP Stack Event Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact the Tekelec *Customer Care Center* for assistance if needed.

Transport Manager Measurements

Table 38: Measurement Summary

Meas-ID	Measurement Tag	Measurement Description	Collection Interval	Report Accumulation Interval(s)	Scope		Group
					NE	MP	
Per MP Server Measurements							
9400	RxTrFarEndClose	Number of times the far-end closed the association	30 min	30 min, Daily	X	X	Transport Exception
9401	EvTrManClose	Number of times the Trasnport was manually closed. This includes manual changes of the transport administrative state that cause the transport to transition from APP-UP to Disabled.	30 min	30 min, Daily	X	X	Transport Exception
9402	EvTrNoRespClose	Number of times the Transport was closed due to lack of response from the	30 min	30 min, Daily	X	X	Transport Exception

		far-end. This includes lack of response to any signaling sent on the transport.					
9403	EvTrCnxSuccess	The number of times the SCTP connection was successfully established on the Transport. The number of times the UDP socket in Listen Mode was opened successfully on the Transport.	30 min	30 min, Daily	X	X	Transport Usage
9404	EvTrCnxFail	The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections. The number of times open attempt on UDP socket in	30 min	30 min, Daily	X	X	Transport Exception

		Listen Mode failed on the Transport.					
9405	TxTrSendFail	The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.	30 min	30 min, Daily	X	X	Transport Exception
9406	RxTrRcvFailed	The number of times an SCTP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.	30 min	30 min, Daily	X	X	Transport Exception
9407	EvTrSockInitFail	Number of times the socket initialization failed	30 min	30 min, Daily	X	X	Transport Exception
9408	TxTrOctets	The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min	30 min, Daily	X	X	Transport Performance

9409	RxTrOctets	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min	30 min, Daily	X	X	Transport Performance
9410	TmTrEnaNotUp	The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.	30 min	30 min, Daily	X	X	Transport Usage
9411	RxTmSctpBufAvg	The Average Value of the number of bytes in	5 min	5 min, Daily	X	X	Transport Usage

		SCTP RX Window.					
9412	RxTmSctpBufPeak	The Peak Value of the number of bytes in SCTP RX Window	5 min	5 min, Daily	X	X	Transport Usage
9413	TmSingleTransQueuePeak	The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval	30 min	30 min, Daily	X	X	Transport Performance
9414	TmSingleTransQueueAvg	The average single Transport Writer Queue utilization (0-100%) measured during the collection interval	30 min	30 min, Daily	X	X	Transport Performance
9415	TmSingleTransQueueFull	The number of egress messages that were discarded because the singleTransport Writer Queue was full.	30 min	30 min, Daily	X	X	Transport Exception
9416	SctpTransPeerCWNDPeak	The peak value of congestion window size recorded for the peer of a SCTP transport	30 min	30 min, Daily	X	X	Transport Performance

		during the collection interval.					
9417	SctpTransPeerCWNDAvg	The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.	30 min	30 min, Daily	X	X	Transport Performance
9418	SctpTransPeerSRTTPeak	The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.	30 min	30 min, Daily	X	X	Transport Performance
9419	SctpTransPeerSRTTAvg	The average value of smoothed round trip time for the SCTP Transport address during the collection interval.	30 min	30 min, Daily	X	X	Transport Performance
9420	SctpTransUnAckedDataPeak	The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.	30 min	30 min, Daily	X	X	Transport Performance

9421	SctpTransUnAckedDataAvg	The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.	30 min	30 min, Daily	X	X	Transport Performance
9422	SctpTransRTOPeak	The peak value of retransmission timeout in use for the SCTP Transport address	30 min	30 min, Daily	X	X	Transport Performance
9423	SctpTransRTOAvg	The average value of retransmission timeout in use for the SCTP Transport address	30 min	30 min, Daily	X	X	Transport Performance
9424	EvSctpAdjIPToDwn	Number of time configured IP Address of an Adjacent Node goes from Available to Unavailable.	30 min	30 min, Daily	X	X	Transport Exception
9425	EvSctpTransRej	Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP	30 min	30 min, Daily	X	X	Transport Exception

		Multihoming mode. This is valid only for SCTP Transports.					

Per Transport Measurements

Table 39: Meas-ID 9400 Details

Measurement Tag	RxTrFarEndClose
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	Number of times the far end closed the SCTP connection
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • the far-end of the association closes the association by sending either SHUTDOWN or ABORT
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If the closing of the association was expected, no further action is necessary - the association will be recovered as soon as the far-end is ready to connect again. If the closing of the association was not expected: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Look in the event history at **Main Menu** > **Alarms & Events** > **View History** for event id 19404 to determine exactly when the far-end closed the association. • Look for other events for the association or MP server in the event history. • Verify that IP connectivity still exists between the MP server and the SG.

	• Verify whether the far-end of the association is undergoing maintenance. • Contact Tekelec for assistance if needed.

Table 40: Meas-ID 9401 Details

Measurement Tag	EvTrManClose
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times the Transport was manually closed. This includes manual changes of the transport administrative state that cause the transport to transition from APP-UP to Disabled.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • A manual change is made to the transport administrative state from Enabled to Blocked or from Enabled to Disabled, causing the transport to transition out of APP-UP protocol state. **Note:** This has a special meaning for SS7/M3UA where it is linked with ASP-UP.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If the transport is known to be under maintenance, then no further action is necessary. If the transport was not known to be under maintenance: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • View the event history at Main Menu -> Alarms & Events -> View History looking for event id 19406. Event id 19406 shows the manual transport state transitions and contains a time-stamp of when the change occurred. • The security logs at **Main Menu** > **Log Files** > **Security Logs** can be searched using the

	time-stamp from the event history log to determine which login performed the manual state change on the association. • Contact Tekelec for assistance if needed.

Table 41: Meas-ID 9402 Details

Measurement Tag	EvTrNoRespClose
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times the transport was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the transport.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • An established Transport is closed by the MP server due to lack of response at the SCTP level from the far-end of the association
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. If non-zero, the association has been closed due to lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the SG. Troubleshooting: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Look in the event history at **Main Menu** > **Alarms & Events** > **View History** for event id 19405. • Verify IP connectivity between the MP server and the SG. • Determine if the far-end of the association is congested, possibly causing slow response times on the association.

	• Check the IP network between the MP server and the SG for excessive retransmissions. • Contact Tekelec for assistance if needed.

Table 42: Meas-ID 9403 Details

Measurement Tag	EvTrCnxSuccess
Measurement Group (64 chars)	Transport Usage
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times the SCTP connection was successfully established on the transport. The number of times the UDP socket in Listen Mode was opened successfully on the Transport.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • the SCTP association reaches the APP-UP protocol state (i.e. the connection is successfully ESTABLISHED) • UDP socket in Listen Mode was opened successfully.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise… Troubleshooting: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Look in the event history at **Main Menu** > **Alarms & Events** > **View History** for events related to the association or the MP server to determine what may have caused the Transport to fail. • Contact Tekelec for assistance if needed.

Table 43: Meas-ID 9404 Details

Measurement Tag	EvTrCnxFail
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections. The number of times open attempt on UDP socket in Listen Mode failed on the Transport.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • An SCTP connect attempt fails • An UDP open attempt in Listen mode fails • An SCTP open attempt in Listen mode fails
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Peer IP Address at least once and failed to establish the SCTP connection. Troubleshooting: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Check the event history log at **Main Menu** > **Alarms & Events** > **View History**, looking for event id 19402. Event id 19402 provides more details as to the actual cause of the failure. • Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**. • Verify that the remote port configured at **Main Menu** > **Transport Manager** >

	Configuration > **Transport** for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections. • Verify the IP network connectivity between the MP server and the Adjacent Node. • If the SG must be configured to connect to the MP server's IP address and port, verify that the SG configuration matches the association configuration at **Main Menu** > **Transport Manager** > **Configuration** > **Transport**. • Contact Tekelec for assistance if needed.

Table 44: Meas-ID 9405 Details

Measurement Tag	TxTrSendFail
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • an attempt to send signaling DATA fails for any reason and the information being sent cannot be mapped to a specific transport
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this Transport has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association. Troubleshooting: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.

	• Look in the event history log at **Main Menu** > **Alarms & Events** > **View History** for event id 19407. Event id 19407 gives more information about exactly what caused the failure to send. • Verify that the IP network between the MP server and the Adjacent Node is functioning as expected. • Contact Tekelec for assistance if needed.

Table 45: Meas-ID 9406 Details

Measurement Tag	RxTrRcvFailed
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed. Troubleshooting: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Look in the event history log at **Main Menu** > **Alarms & Events** > **View History** for event id 19403. Event id 19403 gives more information about exactly what caused the failure.

	• Try to bring the sockets back into alignment by manually Disabling and Enabling the Transport. • Contact Tekelec for assistance if needed.

Table 46: Meas-ID 9407 Details

Measurement Tag	EvTrSockInitFail
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of times the socket initialization failed.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • one or more socket options cannot be set according to the settings in the transport's configuration set
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. A non-zero value indicates some problem with association setup prior to attempting to connect the association. If this occurs, look in **Main Menu** > **Alarms & Events** > **View History** for event id 19401. Event 19401 provides details about exactly what part of the configuration failed. Please contact Tekelec for further assistance.

Table 47: Meas-ID 9408 Details

Measurement Tag	TxTrOctets
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple

Measurement Description (255 chars)	The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by the number of octets in the message each time: • A DATA/non-DATA message is successfully sent on the transport.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	None. This measurement indicates the level of signaling octets that have been sent over the association during the reporting interval.

Table 48: Meas-ID 9409 Details

Measurement Tag	RxTrOctets
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by the number of octets in the message each time: • A DATA/non-DATA message is successfully received on the transport
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	None. This measurement indicates the level of signaling octets that have been received over the association during the reporting interval.

Table 49: Meas-ID 9410 Details

Measurement Tag	TmTrEnaNotUp
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Duration
Measurement Description (512 chars)	The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	Time shall be accumulated for this measurement during the collection interval when all of the following are true: • the association is in the ENABLED administrative state • the association is not in the ASP-UP protocol state for M3UA and APP-UP for other Plugins.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, the value of this measurement should be zero or very low value. A high value indicates that the association was set to the Enabled administrative state, but was not able to reach the desired protocol state (APP-UP) due to some problem. Troubleshooting: • Association status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**. • Verify that the remote port configured at **Main Menu** > **Transport Manager** > **Configuration** > **Transport** > **Configure** for

	the association correctly identifies the port that the SG is listening on for SCTP connections. • Verify the IP network connectivity between the MP server and the SG. • If the Adjacent Node must be configured to connect to the MP server's IP address and port, verify that the Adjacent Node configuration matches the association configuration at **Main Menu** > **Transport Manager** > **Configuration** > **Transport**. • Contact Tekelec for assistance if needed.

Table 50: Meas-ID 9411 Details

Measurement Tag	RxTmSctpBufAvg
Measurement Group (64 chars)	Transport Usage
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Average
Measurement Description (255 chars)	The Average Value of the number of bytes in SCTP RX Window
Collection Interval	5 min
Report Accumulation Interval(s)	5 min, Daily
Peg Condition	Every Second, retrieve the Rx socket buffer occupancy by using the "getsockopt" functions and then calculates and peg the Average buffer occupancy, during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface

Table 51: Meas-ID 9412 Details

Measurement Tag	RxTmSctpBufPeak
Measurement Group (64 chars)	Transport Usage
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport

Measurement Type (Simple, Average, Min, Max, Duration)	Max
Measurement Description (255 chars)	The Peak Value of the number of bytes in SCTP RX Window.
Collection Interval	5 min
Report Accumulation Interval(s)	5 min, Daily
Peg Condition	Every Second, retrieve the Rx socket buffer occupancy by using the "getsockopt" functions and then calculates and peg the Maximum buffer occupancy during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface

Table 52: Meas-ID 9413 Details

Measurement Tag	TmSingleTransQueuePeak
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Max
Measurement Description (255 chars)	The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec).
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	Transport's Queue is registered as a Stack Resource, StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*

Customer Action	"Transport single queue utilization depicts the SCTP or UDP Transport Writer Queues utilization." This is a measure of how fast the Transport queue is being processed. It indicates the maximum depth of queue over the monitored interval. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist. Contact Tekelec for assistance if needed.

Table 53: Meas-ID 9414 Details

Measurement Tag	TmSingleTransQueueAvg
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Average
Measurement Description (255 chars)	The average single Transport (SCTP/UDP) Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec).
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	Transport's Queue is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*

Customer Action	This is a measure of how fast the Transport queue is being processed. It indicates the Average depth of queue over the monitored interval. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist. Contact Tekelec for assistance if needed.

Table 54: Meas-ID 9415 Details

Measurement Tag	TmSingleTransQueueFull
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	The number of egress messages that were discarded because the single Transport Writer Queue was full.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	Check whether the single peers transmit data queue limit has reached its max limit (1000). If max limit is reached or exceeded then peg the measurement and discard the low priority events.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	It indicates that the Transport is backed up and there could be messages that will get discarded. If it's above the defined critical threshold, it results in generating Alarm. Contact Tekelec customer service.

Table 55: Meas-ID 9416 Details

Measurement Tag	SctpTransPeerCWNDPeak
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Max
Measurement Description (255 chars)	The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS), It indicates Peak of congestion window recorded for the peer address.

Table 56: Meas-ID 9417 Details

Measurement Tag	SctpTransPeerCWNDAvg
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Average
Measurement Description (255 chars)	The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected

	Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS); It indicates Average of congestion window recorded for the peer address.

Table 57: Meas-ID 9418 Details

Measurement Tag	SctpTransPeerSRTTPeak
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Max
Measurement Description (255 chars)	The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Table 58: Meas-ID 9419 Details

Measurement Tag	SctpTransPeerSRTTAvg
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport

Measurement Type (Simple, Average, Min, Max, Duration)	Average
Measurement Description (255 chars)	The average value of smoothed round trip time for the SCTP Transport address during the collection interval.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Table 59: Meas-ID 9420 Details

Measurement Tag	SctpTransUnAckedDataPeak
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Max
Measurement Description (255 chars)	The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*

Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Table 60: Meas-ID 9421 Details

Measurement Tag	SctpTransUnAckedDataAvg
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Average
Measurement Description (255 chars)	The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Table 61: Meas-ID 9422 Details

Measurement Tag	SctpTransRTOPeak
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Max
Measurement Description (255 chars)	The peak value of retransmission timeout in use for the SCTP Transport address.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and

	updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Table 62: Meas-ID 9423 Details

Measurement Tag	SctpTransRTOAvg
Measurement Group (64 chars)	Transport Performance
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Average
Measurement Description (255 chars)	The average value of retransmission timeout in use for the SCTP Transport address.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Table 63: Meas-ID 9424 Details

Measurement Tag	EvSctpAdjIPToDwn
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple

Measurement Description (255 chars)	Number of time configured IP Address of an Adjacent Node goes from Available to Unavailable.
Collection Interval	30 min
Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • reachibility to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. A non-zero value indicates a path fault to that address was detected. Troubleshooting: • Check the event history log at **Main Menu** > **Alarms & Events** > **View History**, looking for event id 19410. Event id 19410 provides more details as to the actual cause of the failure. • Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**. • Verify the IP network connectivity between the MP server and the Adjacent Node's IP address using a ping or traceroute command. • Contact Tekelec for assistance if needed.

Table 64: Meas-ID 9425 Details

Measurement Tag	EvSctpTransRej
Measurement Group (64 chars)	Transport Exception
Measurement Dimension (Single, Arrayed)	Arrayed - per Transport
Measurement Type (Simple, Average, Min, Max, Duration)	Simple
Measurement Description (255 chars)	Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.
Collection Interval	30 min

Report Accumulation Interval(s)	30 min, Daily
Peg Condition	This measurement shall be incremented by one each time: • the association has been rejected due to IP address validation failure in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.
Measurement Scope (Network, NE, Server)	NE, Server
Merge Scope (Network, Site)	Default:: Network. Can be updated to Site by Application *(Implementation note: A/B-source)*
Customer Action	If all is well, this measurement should have a zero value. A non-zero value indicates that the Adjacent Node has attempted to connect to the Peer IP Address at least once and but the connection attempt was rejected because the IP addresses advertised by the Adjacent Node failed validation. Troubleshooting: • Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**. • Check the event history log at **Main Menu** > **Alarms & Events** > **View History**, looking for event ids 19411 or 19412. Event ids 19411 and/or 19412 provides more details as to the actual cause of the failure. • Verify that the SCTP validation mode is as desired. • Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**. • Verify that the remote port configured at **Main Menu** > **Transport Manager** > **Configuration** > **Transport** for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections. • Contact Tekelec for assistance if needed.

Throttling measurements

Table 65: Throttling Measurements

Measurement Tag	Measurement Description	Collection Interval
ThrottleAllow	The number of times a message was allowed	5 min
ThrottleDiscard	The number of messages that were discarded as a result of matching a rule with no response	5 min
ThrottleDiscardByName	The number of messages that were discarded as a result of matching a specific rule, by name	5 min
ThrottleDiscardTCAP	The number of times a TCAP error was returned in conjunction with a discard	5 min
ThrottleDiscardUDTS	The number of times a UDTS was returned in conjunction with a discard	5 min
ThrottleMatch	The number of messages that matched a rule	5 min
ThrottleMatchByName	The number of messages that matched a specific rule, by name	5 min
ThrottleSimulation	The number of times a message matched a rule in the 'Simulation' mode but was not acted upon	5 min
ThrottleWhitelistHit	The number of times a message matched a rule with Whitelist enabled, and the subscriber was in the Dn/Imsi Whitelist	5 min
ThrottleWhitelistMiss	The number of times a message matched a rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist	5 min

ThrottleAllow

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of times a message was allowed (for any reason)

Collection Interval: 5 mins

Peg Condition: The ThrottleAllow measurement shall be incremented by one each time when a new incoming message was allowed to reach the HLR (for any reason)

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

ThrottleDiscard

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of messages that were discarded as a result of a throttling rule

Collection Interval: 5 mins

Peg Condition: The ThrottleDiscard measurement shall be incremented by one each time when a new incoming message matches the criteria found in Rules table and shall be throttled accordingly.

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

ThrottleDiscardTCAP

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of times a TCAP error was returned in conjunction with a discard

Collection Interval: 5 mins

Peg Condition: The ThrottleDiscardTCAP measurement shall be incremented by one each time when a TCAP error was returned in conjunction with a discard

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

ThrottleDiscardUDTS

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of times a UDTS was returned in conjunction with a discard

Collection Interval: 5 mins

Peg Condition: The ThrottleDiscardUDTS measurement shall be incremented by one each time when a UDTS was returned in conjunction with a discard

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

ThrottleSimulation

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of times a message matched a rule but was not acted upon because the rule was in 'Simulation' mode

Collection Interval: 5 mins

Peg Condition: The ThrottleSimulation measurement shall be incremented by one each time when a new incoming message matches a rule but was not acted upon because the rule was in 'Simulation' mode

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

ThrottleWhitelistHit

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of times a message matches a throttling rule with Whitelist enabled, and the subscriber is in the Dn/Imsi Whitelist

Collection Interval: 5 mins

Peg Condition: The ExhrThrottleWhitelistHit measurement shall be incremented by one each time when a new incoming message matches the throttling rule with Whitelist enabled, and the subscriber is in the Dn/Imsi Whitelist

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

ThrottleWhitelistMiss

Measurement Group: Throttling

Measurement Type: Simple

Description: The number of times a message matched a rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist

Collection Interval: 5 mins

Peg Condition: The ThrottleWhitelistMiss measurement shall be incremented by one each time when a new incoming message matches the throttling rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist

Measurement Scope: Network, NE, Server

Recovery:

1. No action required

HLR Router Measurements

This section provides information about HLR Router measurement reports.

EXHR measurements

Table 66: EXHR Measurement Report Fields

Measurement Tag	Description	Collection Interval
ExhrGttAlternateRoute	Number of GTTs performed where the preferred destination was not available	5 min
ExhrGttExceptionRouting	Number of times exception routing was used	5 min
ExhrGttFail	Number of Global Title Translation failures	5 min
ExhrGttFailIncorrectGTI	Number of Global Title Translation failures due to incorrect Global Title Indicator	5 min
ExhrGttFailNoTransForAddress	Number of Global Title Translation failures due to IMSI/DN not provisioned	5 min

Measurement Tag	Description	Collection Interval
ExhrGttFailTTNotFound	Number of Global Title Translation failures due to Translation Type not provisioned	5 min
ExhrGttPerformed	Number of Global Title Translations performed	5 min
ExhrGttExceptionRtgOverride	Total number of messages where Exception Routing was overridden	5 min
ExhrGttExceptionRtgOverrideErr	Total number of TCAP Response Failures when the Exception Routing Override feature is active and the response message fails during encode.	5 min
ExhrMlrDecodeFailed	Total number of messages that failed Map Layer Routing decode. HLRR failed to find IMSI/DN in the MAP layer.	5 min
ExhrMlrDecodeSuccessful	Total number of messages that were successfully Map Layer Decoded. HLRR found IMSI/DN in the MAP Layer.	5 min
ExhrMlrFailNoTransForAddress	Total number of MLR failures due to IMSI/DN not provisioned. IMSI/DN found in MAP Layer but not in Database.	5 min
ExhrMlrPerformed	Total number of messages that were MLR Performed. IMSI/DN found in MAP Layer and in Database plus the message was successfully routed.	5 min

EXHRTT measurements

Table 67: EXHRTT Measurement Report Fields

Measurement Tag	Description	Collection Interval
ExhrGttFailNoTransForAddressByTT	Number of Global Title Translation failures due to IMSI/DN not provisioned, by TT	5 min

Measurement Tag	Description	Collection Interval
ExhrGttPerformedByTT	Number of Global Title Translations performed, by TT	5 min
ExhrGttFailTTNotFoundByTT	Total number of GTT failures due to translation type not provisioned, per translation type	5 min

PDBI measurements

Table 68: PDBI Measurement Report Fields

Measurement Tag	Description	Collection Interval
NetSync RepAud ErrCnt	Number of errors detected	5 min
NetSync RepAud RecCnt	Number of records audited	5 min
PdbiConnectionIdleTimeouts	Total number of connections that have timed out and terminated due to idleness.	5 min
PdbiConnectsAccepted	Total number of client initiated connect attempts that have been accepted.	5 min
PdbiConnectsAttempted	Total number of client initiated connect attempts to establish a connection with the server.	5 min
PdbiConnectsDenied	Total number of client initiated connect attempts that have been denied due to clients not running on an authorized server, maximum number of allowed connections already established, or the PDBI interface is disabled.	5 min
PdbiConnectsFailed	Total number of client initiated connect attempts that failed due to errors during initialization.	5 min
PdbiDnSplitCreated	Number of DN records created by NPA split	5 min
PdbiDnSplitRemoved	Number of DN records removed by NPA split	5 min
PdbiEpapAuditCompleted	Number of completed EPAP audits	5 min
PdbiEpapAuditStarted	Number of started EPAP audits	5 min

Measurement Tag	Description	Collection Interval
PdbiExportsFailed	Total number of PDBI export requests that have failed due to errors.	5 min
PdbiExportsSuccessful	Total number of successful PDBI export requests.	5 min
PdbiImportsFailed	Total number of files that had failed to be imported to PDBI due to errors.	5 min
PdbiImportsSuccessful	Total number of files imported to PDBI successfully.	5 min
PdbiMsgsDiscarded	The total number of PDBI messages that have been discarded due to the connection being shutdown, server being shutdown, server's role switching from active to standby, or transaction not becoming durable within the allowed amount of time.	5 min
PdbiMsgsFailed	The total number of PDBI messages that have failed to be processed due to errors. See section 5.1 for a list and description of possible errors.	5 min
PdbiMsgsImported	The total number of PDBI messages that have been received from an import operation.	5 min
PdbiMsgsReceived	The total number of PDBI messages that have been received.	5 min
PdbiMsgsSent	The total number of PDBI messages that have been sent.	5 min
PdbiMsgsSuccessful	The total number of PDBI messages that have been successfully processed.	5 min
PdbiNpaSplitCompleted	Number of completed NPA splits	5 min
PdbiNpaSplitStarted	Number of started NPA splits	5 min
PdbiTxnAborted	Total number of transactions that have been successfully aborted.	5 min

Measurement Tag	Description	Collection Interval
PdbiTxnCommitted	The total number of transactions that have been successfully committed to the database (memory and on disk) on the active server of the primary NOAMP cluster.	5 min
PdbiTxnDurabilityTimeouts	The total number of committed, non-durable transaction that have failed to become durable within the amount of time specified by Transaction Durability Timeout.	5 min
PdbiTxnFailed	Total number of transactions that have failed to be started, committed, or aborted due to errors.	5 min
PdbiTxnTimeouts	Total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.	5 min
PdbiTxnTotal	Total number of transactions that have been attempted. It is the sum of pdbi.TxnCommitted, pdbi.TxnTimeouts, pdbi.TxnAborted, and pdbi.TxnFailed counters.	5 min
PdbiTxnWriteMutexTimeouts	The total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.	5 min

PDE measurements

Table 69: PDE Measurement Report fields

Measurement Tag	Description	Collection Interval
PdeFilesCreatedNO	Number of created files on NOAMP server	5 min
PdeFilesTransferredNO	Number of transferred files from NOAMP server	5 min

Measurement Tag	Description	Collection Interval
PdeFilesCreatedSO	Number of created files on SOAM server	5 min
PdeFilesTransferredSO	Number of transferred files from SOAM server	5 min

Glossary

A

ACK	Data Acknowledgement
ANSI	American National Standards Institute An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.
ASP	Abstract Service Primitive Application Server Process A process instance of an Application Server. An Application Server Process serves as an active or standby process of an Application Server (e.g., part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances of) MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP end-point, and may be configured to process signaling traffic within more than one Application Server. Application Service Part Application Server Process
Association	An association refers to an SCTP association. The association provides the transport for protocol

A

data units and adaptation layer peer messages.

B

BIOS

Basic Input-Output System

Firmware on the CPU blade that is executed prior to executing an OS.

C

CAPM

Computer-aided policy making

CdPA

Called Party Address

The field in the SCCP portion of the MSU that contains the additional addressing information of the destination of the MSU. Gateway screening uses this additional information to determine if MSUs that contain the DPC in the routing label and the subsystem number in the called party address portion of the MSU are allowed in the network where the EAGLE 5 ISS is located.

Charging Proxy Application

A DSR Application that is responsible for sending and receiving Diameter accounting messages.

CMOS

Complementary Metal Oxide Semiconductor

CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.

C

ComAgent	Communication Agent A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.
Communication Agent	See ComAgent.
CPA	Capability Point Code ANSI Charging Proxy Application The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.
CPC	Capability Point Code A capability point code used by the SS7 protocol to identify a group of functionally related STPs in the signaling network.
CSV	Comma-separated values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

DAVA	Destination Available

D

DB	Database Data bus
DNS	Domain Name Services Domain Name System A system for converting Internet host and domain names into IP addresses.
DRST	Destination Restricted
DUNA	Destination Unavailable
DUPU	Destination User Part Unavailable An M3UA management message.

F

FABR	Full Address Based Resolution Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.
Full Address Based Resolution	See FABR.

G

GLA	Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B by the

G

	Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.
GT	Global Title Routing Indicator
GTI	Global Title Indicator
GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA	High Availability High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.
HLR	Home Location Register A component within the Switching Subsystem of a GSM network. The HLR database is the central database within the GSM architecture. This is where information about the mobile communications subscribers who are assigned to a specific location area is stored. The subscriber data is used to establish connections and control services. Depending on the network size, the number of

H

	subscribers and the network organization, a number of HLRs can exist within a GSM network.
HP	Hewlett-Packard

I

IP	Intelligent Peripheral Internet Protocol IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
IPFE	IP Front End A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.
ITU	International Telecommunications Union An organization that operates worldwide to allow governments and the private telecommunications sector to coordinate the deployment and operating of telecommunications networks and services. The ITU is responsible for regulating, coordinating and developing

I

	international telecommunications, and for harmonizing national political interests.

K

KPI	Key Performance Indicator

L

LSP	Local Signaling Point A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique primary/true point code within a particular SS7 Domain to an MP server.

M

M3RL	M3UA Routing Layer A layer invented by Tekelec to enhance M3UA by adding a true routing layer.
M3UA	SS7 MTP3-User Adaptation Layer M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MP	Message Processor The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.
MTP	Message Transfer Part

M

	The levels 1, 2, and 3 of the SS7 protocol that control all the functions necessary to route an SS7 MSU through the network
	Module Test Plan
MTP3	Message Transfer Part, Level 3

N

NE	Network Element
	An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location.
	In a 2-Tiered DSR OAM system, this includes the NOAM and all MPs underneath it. In a 3-Tiered DSR OAM system, this includes the NOAM, the SOAM, and all MPs associated with the SOAM.
	Network Entity
NI	Network Indicator
NOAMP	Network Operations, Administration, Maintenance, and Provisioning
NTP	Network Time Protocol
NTP daemon	Network Time Protocol daemon – NTP process that runs in the background.

O

OAM	Operations, Administration, and Maintenance

O

	The application that operates the Maintenance and Administration Subsystem which controls the operation of many products.
OID	Object Identifier An identifier for a managed object in a Management Information Base (MIB) hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB OIDs belong to different standard organizations. Vendors define private branches that include managed objects for their own products.
OPC	Originating Point Code Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.

P

PDBI	Provisioning Database Interface The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDBA.
PDU	Protocol Data Unit
PM&C	Platform Management and Configuration Server with hardware management software that manages the

P

	remaining servers (System OAMs and MPs) in a network element. The terms PM&C and system manager are used synonymously in the online help documentation. PM&C functions include hardware monitoring and control, switch configuration, and software installation and upgrade.
	Provides hardware and platform management capabilities at the site level for Tekelec platforms. The PMAC application manages and monitors the platform and installs the TPD operating system from a single interface.

R

RBAR	Range Based Address Resolution
	A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, "Routing Entity" Type, and Routing Entity address ranges.
REPL	Replication
RI	Routing Indicator
RSP	Route Set Test - Prohibited message
	Remote Signaling Point
	Represents an SS7 network node (point code) that signaling must be sent to. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.
	Remote Signaling Point

R

	A logical element that represents a unique point code within a particular SS7 domain with which the SS7 application's Local Signaling Point interacts.

S

SBR	Subsystem Backup Routing Session Binding Repository - A highly available, distributed database for storing Diameter session binding data
SCCP	Signaling Connection Control Part The signaling connection control part with additional functions for the Message Transfer Part (MTP) in SS7 signaling. Messages can be transmitted between arbitrary nodes in the signaling network using a connection-oriented or connectionless approach.
SCMG	SCCP Management SCMG manages the status of subsystems and SCCP-capable signaling points (SPs). It maintains the status of remote SCCP SPs and that of local subsystems.
SCON	Signaling Congested
SCTP	Stream Control Transmission Protocol An IETF transport layer protocol, similar to TCP that sends a message in one operation. The transport layer for all standard IETF-SIGTRAN protocols.

S

	SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SG	Secure Gateway Signaling Gateway A network element that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be coresident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (e.g., signaling backhaul). A Signaling Gateway could be modeled as one or more Signaling Gateway Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers.
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed

S

	objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance Site Operations, Administration, and Maintenance
SOAP	Simple Object Access Protocol
SS7	Signaling System #7 A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE 5 ISS is an STP, which is a device that routes these messages through the network.
SSA	Subsystem Allowed
SSP	Subsystem Prohibited network management message. Subsystem Prohibited SCCP (SCMG) management message. (CER) Service Switching Point (SS7 Network) Signal Switching Point Signal Switching Points are switches that originate, terminate, or tandem calls. An SSP sends

S

	signaling messages to other SSPs to setup, manage, and release voice circuits required to complete a call.
SST	Secondary State The secondary state of the specified entity. Subsystem Status Test Subsystem Status Test network management message. Subsystem Status Test SCCP (SCMG) management message. (CER)
STP	Signal Transfer Point The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network. Spanning Tree Protocol
SW	Software Switch

T

TFA	TransFer Allowed (Msg)
TFC	Transfer Control TransFer Controlled (Msg)
TFP	TransFer Prohibited (Msg) A procedure included in the signaling route management (functionality) used to inform a

T

	signaling point of the unavailability of a signaling route.
TFR	Transfer Restricted
TPC	True Point Code

U

UDT	Unitdata Transfer
UDTS	Unitdata Transfer Service An error response to a UDT message.

X

XUDT	Extended Unit Data Extended User Data
XUDTS	Extended Unitdata Service message An error response to an XUDT message.