Oracle® Communications Tekelec HLR Router

Transport Manager User's Guide

910-6590-001 Revision B

February 2014

ORACLE®

Oracle® Communications Transport Manager User's Guide

Table of Contents

List of Tables

Chapter 1

Introduction

Topics:

This chapter provides a brief summary of Transport Manager functions. It also includes Tekelec contact information and how to locate product documentation on the Tekelec Customer Support site.

Purpose of this documentation

This documentation:

- Describes the functions of Transport Manager configuration and maintenance
- Describes the pages and fields on the Transport Manager GUI (Graphical User Interface)
- Provides procedures for using the GUI
- Explains the organization of, and how to use, the documentation

Scope and Audience

This guide is intended for trained and qualified system operators and administrators who are responsible for configuration and maintenance of the Transport Manager in a SS7/Sigtran system.

Documentation Admonishments

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

Table 1: Admonishments

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

Document Organization

This *Transport Manager User Guide* is organized into the following chapters:

- *Introduction* contains general information about the *Transport Manager User Guide*, the scope, audience, and organization of this document, how to contact Tekelec for assistance, and how to locate documentation on the Customer Support Site.
- *Transport Manager Overview* provides an overview of the Transport Manager multihoming and validation functions.
- *Transport Manager Configuration* describes the configuration of Transport Manager Adjacent Nodes and Configuration Sets, and describes the **Transport Configuration** GUI page.
- *Transport Maintenance* describes the information on the **Transport Maintenance** page; and provides procedures for enabling, disabling, and blocking a Transport.

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

Transport Manager Overview

Topics:

Transport Manager enables the configuration of "Transports" (SCTP associations and UDP connections with remote hosts over an underlying IP network). It provides the interface to the adapter layer and manages the connections and data transmission from SCTP/UDP sockets.

The Transport Manager provides multihoming for SCTP associations and validation of SCTP and UDP addresses.

Multihoming

Multihoming is the ability of an SCTP association to support multiple IP paths to its peer endpoint. The benefit of multihoming associations is that it makes the association more fault-tolerant against physical network failures and other issues on the interfaces. It allows re-routing of packets in the event of failure and also provides an alternate path for retransmissions. Every MP supports two XSI IP addresses; therefore, the SCTP multihomed transport can have only two IPs. Transport Manager multihoming has the following characteristics:

- When there are multiple IPs for an endpoint, one address is designated as the primary address to receive data.
- A single port number is used across the entire address list at an endpoint.
- Endpoints exchange lists of addresses during initiation of the connection. The client informs the server about all its IP addresses in the INIT address parameters. The server provides all its IP addresses to the client in INIT-ACK .

For an SCTP Transports acting as an **Initiator**:

- Both Local IP addresses will be sent in INIT to Adjacent Node.
- Both the Remote IP addresses will be associated with ACE connect and if Primary Peer IP is down, then it will re-send INIT to Secondary Peer IP address.

For SCTP Transport acting as a **Listener**:

- Both Local IP addresses will be sent in INIT-ACK to Adjacent Node.
- A connect can be accepted from either the Primary or Secondary IP address and the connection established. It is expected that if the Primary Peer IP address is unreachable, the connection can be established via the secondary address.

For SCTP Transport acting as either an Initiator or Listener, validation mode of remote IP Address(es) received in INIT-ACK will be controlled by User. Validation modes/rules are defined in *SCTP Validation*.

Heartbeat chunks are used to monitor availability of alternate paths with thresholds set to determine failure of alternate and primary paths.

With the multihoming association support, Transport Manager will have potentially greater survivability of the sessions in case of network failures. There is no message loss if only single path fails, the in-flight data will be retransmitted via alternate path by LKSCTP.

Validation

One of the specific functions of Transport Manager is validation. When two endpoints are attempting to establish one or more paths between them using the available underlying local IP interfaces, each endpoint must determine whether the connection requests it receives are truly from the intended remote endpoint. Therefore, an endpoint must validate the IP addresses it receives from the far end in order to determine if the sender is the intended or configured one.

Validation is a service provided by Transport Manager and is adapter/protocol specific.

SCTP Validation

Transport Manager has two methods of SCTP validation: **Relaxed** and **Match**.

- Relaxed mode: one address in the incoming INIT/INIT-ACK received by an association must match either of the IP addresses provisioned for the Adjacent Node if two are provisioned. If only one is provisioned (the primary), one address must match it.
- Match mode: if the incoming INIT/INIT-ACK has multiple addresses, the number of IP addresses must match the number provisioned and the addresses themselves must match those provisioned for the Adjacent Node with that Transport. If only one is provisioned (the primary), one address must match it. Also, if only one is provisioned for the Adjacent Node, the incoming INIT/INIT-ACK should contain one address.

Table 2: SCTP Transport Address Validation

IP Configured in Transport		Received in INIT/INIT-ACK	Transport Manager Behavior	
Local Node	Remote Node		Match Mode	Relaxed
1	1	1	Association will be accepted	Association will be accepted
1	1	2	Association rejected, refusal event generated	Association will be accepted
2	2	1	Association rejected, refusal event generated	Association will be accepted • Operation Reason updated as "Abnormal" for that Transport • Configured Adjacent IP status which has not been received in INIT/INIT-ACK chunk will be displayed as "Unavailable"
2	2	2	Association will be accepted	Association accepted
2	2	>2	Association rejected, refusal event generated	Association accepted
1	2	1	Association rejected, refusal event generated	Association accepted • Operation Reason updated as "Abnormal" for that Transport • Configured Adjacent IP status which has not been received in INIT/INIT-ACK chunk

				will be displayed as "Unavailable"
1	2	2	Association accepted • Operation Reason updated as "Abnormal" for that Transport • Configured Adjacent IP status which has not been received in INIT/INIT-ACK chunk will be displayed as "Unavailable"	Association accepted • Operation Reason updated as "Abnormal" for that Transport • Configured Adjacent IP status which has not been received in INIT/INIT-ACK chunk will be displayed as "Unavailable"
2	1	1	Association accepted	Association accepted
2	1	2	Association rejected, refusal event generated	Association accepted

UDP Validation

For UDP (User Datagram Protocol) validation, address validation can be performed by defining an Access Control List as a 'white list' or list of acceptable remote IP addresses. If a message's IP address is matched to an entry in this list, it will be accepted. Entries in the list consist of the address plus a network mask definition, and each entry defines a unique address space. Validation is performed by matching the candidate message's IP address for a list entry and searching list entries for the longest prefix match. Longest prefix match is defined at the most specific entry (the one with the highest subnet mask) that the candidate message's IP address can be matched to. If a message cannot be matched to an entry in the list, it will be rejected. If the list is empty, any message will be accepted.

Chapter 3

Transport Manager Configuration

Topics:

This chapter describes GUI pages and procedures for configuration of Adjacent Nodes, Configuration Sets, and Transports.

Adjacent Node

An Adjacent Node is a server acting as a signaling peer on a network. An Adjacent Node connects to one or more MP (message processing) Servers using reliable IP transport sessions, such as SCTP associations. In short, the Adjacent Node represents the far-end of an SCTP association. In the case of Eagle 5 ISS STP, an Adjacent Node is an E5-ENET card.

The Adjacent Nodes table lists all servers configured for direct connection to this SS7 node. An Adjacent Node is associated with the IP address on which the Adjacent Node will listen for M3UA signaling.

Safeguard to prevent service impact from configuration changes:

- The software will not allow you to delete an Adjacent Node that is referenced by an Adjacent Server Group.

Adjacent Node elements

This information appears on the **Adjacent Node** page:

Table 3: Adjacent Node Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required. Note: When the Adjacent Node configuration is mastered from the System OAM and this Insert screen is viewed from System OAM server, the Signaling Network Element Name drop down is disabled and contains the NE name of the connected System OAM server.
Adjacent Node Name	Unique identifier used to label an Adjacent Node. An adjacent node is a remote node serving as the far end of a Transport.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required.
IP Address 1	IP address 1 of an adjacent node. By default this will be configured as Primary IP address of an Adjacent Node.	Range: A valid IPv4 address: xxx.xxx.xxx.xxx This field is required.

Element	Description	Data Input Notes
IP Address 2	IP address 2 of an adjacent node. If this is configured then Adjacent Node can be configured as Multihomed if both the IP Addresses are selected in *Transport Configuration*	Range: A valid IPv4 address: xxx.xxx.xxx.xxx This field is required.

Viewing Adjacent Nodes

Use this procedure to view a list of defined Adjacent Nodes.

Select **Transport Manager>Configuration>Adjacent Nodes.**

The **Adjacent Nodes** page appears. For field definitions, see *Adjacent Node elements*.

To filter the information on this page, see *Filtering using the display filter*.

The page appears with the defined Adjacent Nodes listed.

Filtering using the display filter

Use this procedure to perform a filtering operation. This procedure assumes that you have a data table displayed on your page. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Select a field name from the **Display Filter** pulldown menu.

   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

   The selected field name displays in the **Display Filter** field.

2. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.

3. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify **Display Filter: Signaling Network Element Name** with the equals (**=**) operator and a value of **SO_ONE**, the table would show only records where the **Signaling Network Element Name=SO_ONE**.

4. Click **Go** to filter on the selection or set the **Display Filter** to **None** to clear the selection.

Records are displayed according to the specified criteria.

Inserting an Adjacent Node

1. Select **Transport Manager>Configuration>Adjacent Node**

   The **Adjacent Nodes** page appears.

2. Click **Insert**.

The **Insert Adjacent Node** page appears.

3. Populate the fields with data (for field definitions, see *Adjacent Node elements*).
4. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The Adjacent Node is added to the configuration.

Deleting an Adjacent Node

Deleting an Adjacent Node removes the Adjacent Node from the configuration.

The software will not allow you to delete an Adjacent Node that is referenced by an Adjacent Server Group. If necessary, perform remove the Adjacent Node from the Adjacent Server Group.

1. Select **Transport Manager>Configuration>Adjacent Node**.

   The **Adjacent Node** page appears.

2. Click on the row of the Adjacent Node you want to remove.

   A delete confirmation message appears.

3. Click the Delete button at the bottom of the page.
4. Click **OK** to confirm the deletion.

The Adjacent Node is deleted from the table.

Configuration Sets

The **Transport Manager > Configuration > Configuration Sets** page shows all configured sets of SCTP association parameter values and lets you create new Configuration Sets.

A Default Configuration Set is provided with the software. The Default Configuration Set is pre-populated with values appropriate for a typical signaling network. The pre-populated values are shown in *Transport Manager Configuration Set elements*.

Transport Manager Configuration Set elements

Table 4: Transport Manager Configuration Set Elements describes the fields on the **Transport Manager > Configuration > Configuration Set** pages.

Many of the fields in the table use the value configured in the Default Configuration Set as their default. If the defaults have been modified, the new values are shown on the **Transport Manager > Configuration > Configuration Set** pages. The original default values are shown in *Table 4: Transport Manager Configuration Set Elements*.

Table 4: Transport Manager Configuration Set Elements

Element	Description	Data Input Notes
Configuration Set Name	A name that uniquely identifies the SCTP Transport Manager Configuration Set. The name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required and must be unique.
Retransmit Initial Timeout	The expected average network round-trip time in milliseconds. This value is used to initialize the round-trip time value when an association is first started and the round-trip time has not yet been measured. The round-trip time is used by SCTP in calculating when to retransmit chunks.	Format: Numeric Range: 10 - 5000 msec Default: 120 This field is required.
Retransmit Minimum Timeout	The minimum amount of time to wait for an acknowledgment for a message sent. This value prevents the retransmit timeout from becoming too small in networks with a very short round-trip time.	Format: Numeric Range: 10 - 1000 msec Default: 120 This field is required.
Retransmit Maximum Timeout	The maximum amount of time to wait for an acknowledgment for a message sent. This value places an upper bound on the exponential back-off algorithm used by SCTP for retransmission timing. Once this retransmit interval is reached, retransmits will be sent at a constant rate until an ACK is received or the maximum attempt is reached.	Format: Numeric Range: 10-10000 msec Default: 120 This field is required.
Number of Retransmits Triggering Association Failure	Number of consecutive retransmits that will cause an SCTP Association to be marked as failed. This value indicates how many SCTP retransmission attempts should be made to all destinations for an SCTP association before marking the association as failed. This value	Format: Numeric Range: 1- 12 Default: 5 This field is required.

Element	Description	Data Input Notes
	should not be greater than the sum of the retransmit attempts for all destinations within the association.	
Number of Retransmits Triggering Init Failure	Number of consecutive retransmits for INIT and COOKIE-ECHO chunks that will cause an SCTP Association to be marked as failed. This value indicates how many retransmission attempts should be made to the primary SCTP address for INIT and COOKIE-ECHO chunks before marking the association as failed.	Format: Numeric Range: 1 - 12 Default: 8 This field is required.
SACK Delay (ms)	The number of milliseconds to delay after receiving a DATA chunk and prior to sending a SACK. A non-zero value for SACK Delay gives the application time to bundle DATA chunks in the same SCTP datagram with the SACK, thereby reducing the number of packets in the network. Setting SACK Delay to zero disables this delay so that SACKs are sent as quickly as possible.	Format: Numeric Range: 0 - 200 msec Default: 10 This field is required.
SCTP Heartbeat Interval (ms)	The interval in milliseconds between sending SCTP HEARTBEAT messages to a peer. HEARTBEAT messages are only sent when no user data has been sent for the duration of the heartbeat interval. Setting the heartbeat interval to zero disables heartbeating (not recommended).	Format: Numeric Range: 0, 100 - 300000 msec Default: 1000 This field is required.
Connection Retry Interval (sec)	The interval in seconds between connection attempts when the connection is unsuccessful.	Format: Numeric Range: 5 - 60 sec Default: 10 This field is required.
Socket Send Buffer Size (bytes)	The socket send buffer size for outgoing SCTP messages. The send buffer size should be	Format: Numeric Range: 65535 - 5000000 bytes

Element	Description	Data Input Notes
	greater than or equal to the product of the bandwidth and the round trip delay for the Association.	Default: 2000000 This field is required.
Socket Receive Buffer Size (bytes)	The socket receive buffer size for incoming SCTP messages. The receive buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.	Format: Numeric Range: 65535 - 5000000 bytes Default: 2000000 This field is required.
SCTP Multihoming Mode	The SCTP Multihoming mode allows the user to configure remote host validation mode setting for SCTP. If the Adjacent Node is Multihomed for a specified Transport, Adjacent Node IP Addresses received in INIT/INIT-ACK chunk will be validated based on this parameter. SCTP Multihoming Mode = **Relax**: One of the IP Address received from Adjacent Node in an INIT/INIT-ACK chunk must match any of the configured Adjacent Node IP Address associated with that Transport. SCTP Multihoming Mode = **Match**: All of the IP Address received from Adjacent Node in an INIT/INIT-ACK chunk must match all of the configured Adjacent Node IP Address associated with that Transport.	Default: Relax Allowed Values: Relax, Match This field is required.

Viewing Transport Manager Configuration Sets

Select **Transport Manager>Configuration>Configuration Sets.**

The **Transport Manager Configuration Sets** page appears (for field definitions, see *Transport Manager Configuration Set elements*).

To filter the information on this page, see *Filtering using the display filter*.

The **Transport Manager Configuration Sets** page appears with the Configuration Sets listed.

Inserting Transport Manager Configuration Set

1. Select **Transport Manager>Configuration>Configuration Sets.**

   The **Transport Manager Configuration Sets** page appears.

2. Click **Insert**.

   The **Insert Transport Manager Configuration Sets** page appears.

   The default values that appear on the Transport Manager Configuration Set page match whatever values are configured in the default Transport Manager Configuration Set. The original default values are shown in *Transport Manager Configuration Set elements*.

3. Populate the fields with data. For field definitions, see *Transport Manager Configuration Set elements*.
4. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The Transport Manager Configuration Set is added.

Editing a Transport Manager Configuration Set

Note: Although the software provides the capability to edit the Default Transport Manager Configuration Set, any changes to the default values should be evaluated carefully. The Default values shown in *Transport Manager Configuration Set elements* are recommended.

The software will not allow you to edit a configuration set that is referenced by an active Transport. To disable a Transport, see *Disabling a Transport*.

1. Select **Transport Manager>Configuration>Configuration Sets**.

   The **Transport Manager Configuration Sets** page appears.

2. Click **Edit** next to the Transport Manager Configuration Set you wish to modify. Note that you cannot change a Configuration Set Name.

   The **Edit Transport Manager Configuration Sets** page appears.

3. Make the desired changes. For field definitions, see *Transport Manager Configuration Set elements*.
4. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The Transport Managers Configuration Set is updated. For the changes to take effect, the disabled Transport Manager must be placed back in service (see *Enabling a Transport*).

Deleting a Transport Manager Configuration Set

Deleting a Transport Manager Configuration Set removes the configuration set from the database.

The software will not let you remove a Transport Manager Configuration Set that is referenced by an active Transport. To disable a Transport, see *Disabling a Transport*.

The *Default* Transport Manager Configuration Set cannot be deleted.

1. Select **Transport Manager>Configuration>Configuration Sets.**

   The **Transport Manager Configuration Sets** page appears (for field definitions, see *Transport Manager Configuration Set elements*).

2. Click **Delete** in the row you want to remove.
   A Delete confirmation message appears.
3. Click **OK** to remove the configuration set.

The Transport Manager Configuration Set is removed from the list.

Transport Configuration

The **Transport Configuration** page lists all SCTP Transports for all MP servers and Adjacent Nodes.

The **Transport Configuration** page also provides a link to the **Transport Maintenance** page where you can view the status of an Transport.

Safeguards to prevent service impact from configuration changes:

- The software will not let you edit or delete an Transport unless it is in the **Disabled** administrative state.
- The software will not let you specify an MP Server IP Address and Local SCTP Port combination that already exists as a Transport.
- The software will not let you delete an Transport referenced by a Link.

Note: There is dependency between the Transport Manager and ENUM UDP Adapter managed objects that dictate the order of Transport provisioning. When configuring a listening Transport for ENUM, the order of provisioning and the object dependencies are defined in the following: *Table 5: Order of Managed Object Provisioning*.

Table 5: Order of Managed Object Provisioning

Order of Managed Object Provisioning	Must be Available Beforehand
1. Local Node	Server Group
3. Configuration Set	Default is configured through initialization loaders
3. Listening Transport for ENUM	**Steps for Listening Transport:** a. Signaling Network Element b. Local MP server HostName c. Local MP Server IP Address/port

Transport Configuration elements

This information appears on the **Transport Configuration** page:

Table 6: Transport Configuration elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required.
Adapter	Identifies the Transport User for which the Transport is being added.	Default: n/a Options: ENUM, M3UA This field is required.
Transport Name	A name that uniquely identifies the Transport.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required and must be unique.
Transport Protocol	Identifies the Tranport protocol to be used by this Transport.	Format: Pulldown list Default: n/a This field is required.
Transport Type	Identifies the Transport type to be used by this Transport.	Format: Pulldown list Default: n/a This field is required.
MP Server Hostname	The hostname of the MP server that will host the local end of the Transport.	Format: Pulldown list Default: n/a This field is required.
MP Server IP Address (Primary)	The Primary IP Address hosted by the MP Server that will be bound to this Transport. If the MP Server is configured with more than one signaling network IP address, this field allows selection of the desired IP	Format: Pulldown list Default: n/a This field is required.

Element	Description	Data Input Notes
	address to be used for this Transport.	
MP Server IP Address (Secondary)	The Secondary IP Address hosted by the MP Server that will be bound to this Transport. If the MP Server is configured with more than one signaling network IP address, this field allows the Transport to be Multihomed.	Format: Pulldown list Default: n/a This field is required.
MP Server Listen Port	Listen port number of the MP Server for this Transport. This port will be used if the Transport Type is configured as "Listener". If the MP server hosts multiple "Listener" Transports, each Transport must listen on a different port.	Default: 5060; Range: 1024 - 65535
MP Server Initiate Port	Initiate port number of the MP Server for this Transport. This port will be used if the Transport Type is configured as "Initiator". If the MP server hosts multiple Transports, a unique initiate port number must be configured for each IP address.	Default: 2905; Range: 1024 - 65535
Adjacent Node	The Adjacent Node that will host the remote end of this Transport.	Format: Pulldown list Default: n/a
Adjacent Node IP Address (Primary)	The Primary IP Address configured for the Adjacent Node to host the remote end of the Transport.	This is a display-only field populated automatically when the Adjacent Node is selected. Format: Pulldown list Default: n/a
Adjacent Node IP Address (Secondary)	The Secondary IP Address configured for the Adjacent Node to host the remote end of the Transport. This field allows the Adjacent Node of a Transport to be Multihomed.	This is a display-only field populated automatically when the Adjacent Node is selected. Format: Pulldown list Default: n/a
Adjacent Node Port	Adjacent Node port number for this Transport. This port number	Format: Numeric Default: 2905

Element	Description	Data Input Notes
	must match the port number configured on the Adjacent Node as the listening or initiator port as per the Transport Type configured. If the Adjacent Node hosts multiple Transports, each Transport may listen on a different Remote port number.	Range: 1024 - 65535
Configuration Set Name	The configuration parameter set to be sused for this Transport. Configuraton sets are defined on the **Configuration Sets** page (see *Configuration Sets*).	Format: Pulldown list Range: All Configuration Set names Default: Default

Viewing Transports

Select **Transport Manager>Configuration>Transport>.**

The **Transport Configure** page appears. For field definitions, see *Transport Configuration elements*.

To filter the information on this page, see *Filtering using the display filter*.

The page appears with the configured Transports listed.

Inserting a Transport

1. Select **Transport Manager>Configuration>Transport.**

   The **Transport** page appears.

2. Click **Insert**.

   The **Insert Transport** page appears.

3. Populate the fields with data. For field definitions, see *Transport Configuration elements*.
4. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The Transport is added.

Editing a Transport

The **Edit** operation lets you change the following parameters on the **Transport** page:

- Transport Type
- MP Server IP Address
- MP Server Listen Port

- MP Server Initiate Port
- Adjacent Node
- Adjacent Node Port
- Configuration Set Name

The remaining parameters are grayed-out and cannot be edited.

Note: The software will not let you edit an Transport unless it is in the **Disabled** administrative state. For instructions on disabling the Transport, see *Disabling a Transport*.

1. Select **Transport Manager>Configuration>Transport.**

   The **Transports** page appears.

2. Click **Edit**.

   The **Edit Transports** page appears.

3. Make the desired changes. For field definitions, see *Transport Configuration elements*.
4. Perform one of the following actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The edited Transport data is written to the database. The Transport remains in the **Disabled** administrative state. To view or enable the Transport, see *Viewing Transports* or *Enabling a Transport*.

Deleting a Transport

Deleting an Transport removes the Transport from the configuration.

The software will not let you delete an Transport unless it is in the **Disabled** administrative state. For instructions on disabling the Transport, see *Disabling a Transport*.

1. Select **Transport Manager>Configuration>Transport>**.

   The **Transports** page appears.

2. Click **Delete** in the row you want to remove.

   A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

The Transport is deleted from the table.

Generating a Report on Transports

1. Select **Transport Manager>Configuration>Transports>.**

   The **Transports** page appears.

2. Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens listing all of the transports and associated parameters. Click **Print** or **Save** to print a copy of the report or save the report as a text file.

Viewing the Status of a Transport

You can use the Transport Maintenance page to view the administrative status of transports.

Select **Transport Manager>Maintenance>Transport.**

The **Transport Maintenance** page appears listing all transports and their operational status.

Note: To see the IP addresses of the Adjacent Node, click on the "+" button in the Adjacent Node field.

For a description of the operational status and reason, see *Transport Operational Status and Reason*.

For a descripton of the administrative state relationships, see *Admin State Relationships*.

Chapter 4

Transport Maintenance

Topics:

The **Transport Maintenance** page shows the administrative state and operational status of each Transport, and provides functions for enabling, disabling, and blocking Transports.

Transport Maintenance Overview

The **Transport Maintenance** page shows the administrative state and operational status of each Transport. The administrative state may be **Enabled**, **Blocked**, or **Disabled**. The operational status may be **Up** or **Down**.

Each MP server reports status only for Transports hosted by that MP server.

Colored cells may indicate the need for maintenance activity. When the active server's collection status is **Unknown**, cells with gray text indicate the last known information about the Transport.

The **Maintenance** menu options are helpful under alarm conditions as a starting point for gathering additional information. For example, the maintenance options record the timestamp when a Transport goes down. The timestamp can then be used to narrow the search in the event history log and measurements reports.

Errors, warnings, and the possible need for maintenance activity are shown in the GUI in colored cells so that the conditions are readily identifiable.

Once rudimentary information for troubleshooting has been obtained, the network operator can continue investigating under the **Alarms & Events** and **Measurements** options on the GUI.

The menu also enables you to perform maintenance-related tasks such as:

- Enabling and disabling Transports.
- Blocking Transports.

Status information is obtained on the system through the collection process, whereby the SOAM server collects data from the MP servers.You can monitor the system's data collection functions under **Status & Manage>Collection**.

A user group must have permissions to view or execute any of the procedures on the **Transport Manager Maintenance** menu. If a group does not have permissions for the **Maintenance** menu options for **Transport**, this option will not appear in the GUI.

Transport maintenance is allowed from both the NOAMP and the SOAM. When the configuration is allowed from the SOAM, configuration and maintenance from the NOAMP is not allowed. All maintenance links are active whether the user is connected to the NOAMP or the SOAM. Maintenance data can be written to the standby NOAMP server.

Transport Maintenance Elements

This information appears on the **Transport Maintenance** page:

Table 7: Transport Maintenance elements

Element	Description
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.

Element	Description
MP Server Hostname	The hostname of the MP server that will host the local end of the Transport.
Adapter	Identifies the Transport User for which the Transport is being added.
Transport Name	A name that uniquely identifies this Transport.
Transport Protocol	Identifies the Transport protocol to be used by this Transport.
Transport Type	Identifies the Transport type to be used by this Transport.
Adjacent Node	The Adjacent Node to host the remote end of the Transport. Note: clicking on the "+" button in the Adjacent Node field shows the IP addresses for the Adjacent Node.
Admin State	The administrative state of the Transport. Transports can be either enabled, disabled, or blocked.
Operational Status	The operational status of the Transport: **Up** or **Down**.
Operational Reason	The reason a given operational status is shown. For information on a value listed in this field, see *Transport Operational Status and Reason*.
Up/Down Since	The date and time that the Transport came up or went down. For a newly added Transport, the time is when the Transport was configured. After a database restart, reboot, or initial startup before the Transports and Links are initialized, the value is the time when the application initialization runs.

Transport Administrative State

This list shows the possible values that may appear in the **Admin State** field of the **Transport Maintenance** page. A description of each state is also provided.

- **Enabled**- the MP server associated with the Transport begins attempts to bring the Transport to the SCTP Established state and the ASP-UP Operational State.
- **Blocked**-the SCTP connection should be up, but no M3UA signaling is allowed. The MP server associated with the Transport begins attempts to bring the Transport to the SCTP Established state and the ASP-DOWN state. The **Blocked** administrative state is useful for cases in which the network operator wishes to verify IP network connectivity without allowing any M3UA signaling.

- **Disabled**-the MP server associated with the Transport begins attempts to bring the Transport to the SCTP Closed state and the ASP-DOWN states.

The relationship between the **Admin State** and the protocol state is reflected in the **Transport Status** (*Viewing the Status of a Transport*).

Orange color in the **Admin State** field highlights the value when the value is anything other than **Enabled**.

When a new Association is configured, the Association is in the **Disabled** administrative state and must be manually placed in the **Enabled** administrative state.

Admin State Relationships

This section provides additional details about the **Admin State** field on the **Transport Maintenance** page.

The **Admin State** tells the MP server what protocol state the Transport should be in. If the Transport protocol state does not match what is expected for the **Admin State**, the MP server actively tries to resolve the problem until the **Admin State** and the protocol state match. The relationship between the **Admin State** and the protocol state is reflected in the **Transport Status**.

Table 8: Transport Admin State Relationships

Admin State	Operational Status	Operational Reason	Description
Enabled	Down	Connecting	Trying establishing the SCTP connection in Initiator mode.
	Down	Listening	Trying establishing the SCTP connection or opening UDP socket in Listener mode.
	Down	Up Pending	**Valid only for M3UA :** SCTP Transport has been established & ASP-UP has been sent, Waiting for ASP-UP-ACK.
	Up	Normal	**SIP** : • For SCTP Transports, SCTP Connection is established after exchanging SCTP Init handshake methods. • For UDP Transports, UDP Socket binds

Admin State	Operational Status	Operational Reason	Description
			and opened for Listen mode. **M3UA** : • For SCTP Transport, it has reached the ASP-UP state and is available for enabling links. **ENUM** : For UDP Transports, UDP Socket binds and opened for Listen mode.
	Up	Abnormal	If one of the Local IP address goes down in SCTP Transport for Multihomed Adjacent nodes.
	Down	BindFail	**Valid only for SIP/ENUM :** Socket bound fail.
	Down	Application Disabled	Application is down.
	Down	Forced Standby	If the application process was gracefully stopped and the server's HA status is set to Forced Standby.
Disabled	Down	Disabled	Transport is Disabled
Disabled	Down	Connecting	**Valid only for M3UA :** Trying establishing the SCTP connection. But ASP-UP will not be sent afterwards.
	Down	Blocked	**Valid only for M3UA :** SCTP Transport has been established. But is has been blocked for any M3UA traffic.

Transport Operational Status and Reason

This list shows the possible values that may appear in the **Operational Status** and **Reason** fields of the Transport Maintenance page. The **Operational Status** is either **Up** or **Down**. **Up** indicates that the Transport is ready for M3UA signaling. **Down** indicates that the Transport is not ready for M3UA signaling. If the **Status** is **Down**, the **Operational Reason** provides information about why it is down.

Possible values of the **Operational Reason** field where **Status=Down** are:

- **Disabled**-the Transports's administrative state is **Disabled**.This is the initial operational status and reason for a newly configured Transport. This reason is also shown when an Transport is manually disabled.
- **Application Disabled**-the Transport's administrative state is **Enabled** or **Blocked**, and the application state has been manually **Disabled** via the **Server Status** page.
- **Connecting**-the administrative state is **Enabled** or **Blocked**, but the SCTP 4-way handshake has not yet completed xxxxxxxxxxxxxx.
- **Up Pending**-the administrative state is **Enabled**, but the ASP-UP has not yet been acknowledged.
- **Blocked**-the administrative state is **Blocked**, and the SCTP 4-way handshake has completed successfully.
- **Forced Standby**-the administrative state is **Enabled** or **Blocked**, and the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.

Possible values of the **Operational Reason** field where **Status=Up** are:

- **Normal**-this is the desired status. This status occurs when the administrative state is **Enabled** and the ASP-UP has been ACKed.

Viewing the Status of a Transport

You can use the Transport Maintenance page to view the administrative status of transports.

Select **Transport Manager>Maintenance>Transport.**

The **Transport Maintenance** page appears listing all transports and their operational status.

Note: To see the IP addresses of the Adjacent Node, click on the "+" button in the Adjacent Node field.

For a description of the operational status and reason, see *Transport Operational Status and Reason*.

For a descripton of the administrative state relationships, see *Admin State Relationships*.

Enabling a Transport

When a Transport is put in the **Enabled** administrative state, the MP server associated with the Transport begins attempts to bring the Transport to the SCTP Established state and the ASP-UP state.

You can enable multiple transports at the same time.

1. Select **Transport Manager>Maintenance>Transport**.

   The **Transport Maintenance** page appears.

2. Click on the row with the Transport you wish to enable to highlight it.

   The **Enable** link is not grayed out if the Transport's administrative state is already **Enabled**. Also if collection on the server is not working, all actions (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Transport is already in the selected administrative state.

3. Click the **Enable**button at the bottom of the screen.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Transport transitioned into the **Up** status. The orange color is removed from the **Admin State** field. The **Enable** action is now grayed out.

The Transport is enabled.

Disabling a Transport

Caution: Disabling an Transport causes an Transport alarm, and possibly, alarms for Links, Link Sets, Routes, or node isolation.

When an Transport is put in the **Disabled** administrative state, the MP server begins attempts to bring the Transport to the SCTP Closed state and the ASP-DOWN states.

1. Select **Transport Manager>Maintenance>Transports**.

   The **Transports Maintenance** page appears.

2. Click on the **Pause Updates** checkbock for the page (lower right corner) so 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.
3. Click on the row that contains the transport to highlight it. **Disable** in the row of the appropriate Transport.

   The **Disable** link is not grayed out if the Transport's administrative state is already **Disabled**. Also if collection on the server is not working, all actions (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Transport is already in the selected administrative state.

4. Click **Disable**

   A confirmation message appears.

5. Click **OK** to confirm.

The **Operational Status** field shows **Down**. The The **Admin State** field shows **Disabled**. The **Disable** button at the bottom of the page is now grayed out.

The Transport is disabled.

Blocking a Transport

Note: Blocking an Transport causes an Transport alarm, and possibly, alarms for Links, Link Sets, Routes, or node isolation.

When a Transport is put in the **Blocked** administrative state, the MP server begins attempts to bring the Transport to the SCTP Established protocol state and the ASP-DOWN state. The MP server does not attempt to send ASP-UP.

1. Select **Transport Manager>Maintenance>Transports**.

   The **Transports Maintenance** page appears.

2. Click the **Pause Updates** checkbox (lower right corner) so that you can view the results of your selection during this procedure. You can also click the menu option on the main menu to update the page.
3. Click on the row containing the transport you wish to block to highlight it.
4. Click the **Block** button.

   The **Block** button is not grayed out if the Transport's administrative state is already **Blocked**. Also if collection on the server is not working, all actions (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Transport is already in the selected administrative state.

   A confirmation message appears.

5. Click **OK** to confirm.

   The **Operational Status** field shows **Blocked**. The **Admin state** column now indicates when the Transport transitioned into the **Blocked** status. The **Block** button is no longer available.

The Transport is blocked.

Transport Maintenance Overview

The **Transport Maintenance** page shows the administrative state and operational status of each Transport. The administrative state may be **Enabled**, **Blocked**, or **Disabled**. The operational status may be **Up** or **Down**.

Each MP server reports status only for Transports hosted by that MP server.

Colored cells may indicate the need for maintenance activity. When the active server's collection status is **Unknown**, cells with gray text indicate the last known information about the Transport.

The **Maintenance** menu options are helpful under alarm conditions as a starting point for gathering additional information. For example, the maintenance options record the timestamp when a Transport goes down. The timestamp can then be used to narrow the search in the event history log and measurements reports.

Errors, warnings, and the possible need for maintenance activity are shown in the GUI in colored cells so that the conditions are readily identifiable.

Once rudimentary information for troubleshooting has been obtained, the network operator can continue investigating under the **Alarms & Events** and **Measurements** options on the GUI.

The menu also enables you to perform maintenance-related tasks such as:

- Enabling and disabling Transports.
- Blocking Transports.

Status information is obtained on the system through the collection process, whereby the SOAM server collects data from the MP servers.You can monitor the system's data collection functions under **Status & Manage>Collection**.

A user group must have permissions to view or execute any of the procedures on the **Transport Manager Maintenance** menu. If a group does not have permissions for the **Maintenance** menu options for **Transport**, this option will not appear in the GUI.

Transport maintenance is allowed from both the NOAMP and the SOAM. When the configuration is allowed from the SOAM, configuration and maintenance from the NOAMP is not allowed. All maintenance links are active whether the user is connected to the NOAMP or the SOAM. Maintenance data can be written to the standby NOAMP server.

Glossary

A

Adjacent Server Group	A collection of Adjacent Servers that implements a distributed IP signaling function.The group represents a set of Adjacent Servers that share a point code on the signaling gateway.An Adjacent Server Group has a name and a list of Adjacent Servers.

C

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).

G

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.

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.

S

S

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. 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.
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.

U

UDP	User Datagram Protocol
User Datagram Protocol	The User Datagram Protocol is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams to one another.