

**Oracle® Communications
Diameter Signaling Router**

Transport Manager User's Guide

E73321 Revision 01

August 2016

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: Introduction.....	7
Overview.....	8
Scope and Audience.....	8
Manual Organization.....	8
Documentation Admonishments.....	8
Related Publications.....	9
Locate Product Documentation on the Oracle Help Center Site.....	9
Customer Training.....	10
My Oracle Support (MOS).....	10
Emergency Response.....	10
Chapter 2: User Interface Introduction.....	12
User Interface Organization.....	13
User Interface Elements.....	14
Main Menu Options.....	15
Missing Main Menu options.....	19
Common Graphical User Interface Widgets.....	20
Supported Browsers.....	20
System Login Page.....	20
Main Menu Icons.....	22
Work Area Displays.....	23
Customizing the Splash Page Welcome Message.....	26
Column Headers (Sorting).....	26
Page Controls.....	26
Clear Field Control.....	27
Optional Layout Element Toolbar.....	27
Filters.....	28
Pause Updates.....	31
Max Records Per Page Controls.....	31
Chapter 3: Transport Manager Overview.....	32
Overview.....	33
Multihoming.....	33

Transport Validation.....	34
SCTP Validation.....	34
Chapter 4: Transport Manager Configuration.....	36
Configuration Overview.....	37
Adjacent Node.....	37
Adjacent Node elements.....	38
Inserting an Adjacent Node.....	38
Deleting an Adjacent Node.....	39
Configuration Sets.....	39
Transport Manager Configuration Set elements.....	40
Inserting a Transport Manager Configuration Set.....	43
Editing a Transport Manager Configuration Set.....	43
Deleting a Transport Manager Configuration Set.....	44
Transport Configuration.....	44
Transport Configuration elements.....	45
Inserting a Transport.....	47
Editing a Transport.....	48
Deleting a Transport.....	49
Generating a Report on Transport Configuration Data.....	49
Viewing the Status of a Transport.....	50
Chapter 5: Transport Maintenance.....	51
Transport Maintenance Overview.....	52
Transport Maintenance Elements.....	52
Transport Admin State, Operational Status, and Operational Reason.....	53
Enabling a Transport.....	54
Disabling a Transport.....	55
Blocking a Transport.....	56
Appendix A: Transport Manager Use Cases.....	57
Use Case Overview.....	58
SS7+SCTP Multihomed Use Cases.....	59
Glossary.....	65

List of Figures

Figure 1: Oracle System Login.....	21
Figure 2: Paginated Table.....	23
Figure 3: Scrollable Table.....	24
Figure 4: Form Page.....	24
Figure 5: Tabbed Pages.....	25
Figure 6: Tabbed Pages.....	25
Figure 7: Report Output.....	25
Figure 8: Sorting a Table by Column Header.....	26
Figure 9: Clear Field Control X.....	27
Figure 10: Optional Layout Element Toolbar.....	27
Figure 11: Automatic Error Notification.....	28
Figure 12: Examples of Filter Styles.....	29

List of Tables

Table 1: Admonishments.....	9
Table 2: User Interface Elements.....	14
Table 3: Main Menu Options.....	15
Table 4: Main Menu Icons.....	22
Table 5: Example Action Buttons.....	26
Table 6: Submit Buttons.....	27
Table 7: Filter Control Elements.....	29
Table 8: SCTP Transport Address Validation.....	34
Table 9: Adjacent Node Elements.....	38
Table 10: Transport Manager Configuration Set Elements.....	40
Table 11: Transport Configuration Elements.....	45
Table 12: Transport Maintenance Elements.....	53
Table 13: Transport Admin State Relationships.....	54
Table 14: Use Case Overview.....	58
Table 15: SS7+SCTP Multihomed Use Cases.....	59

Chapter 1

Introduction

Topics:

- [Overview.....8](#)
- [Scope and Audience.....8](#)
- [Manual Organization.....8](#)
- [Documentation Admonishments.....8](#)
- [Related Publications.....9](#)
- [Locate Product Documentation on the Oracle Help Center Site.....9](#)
- [Customer Training.....10](#)
- [My Oracle Support \(MOS\).....10](#)
- [Emergency Response.....10](#)

The *Transport Manager User's Guide* and Help provide an overview of Transport Manager functions, and provide procedures to use to configure Adjacent Nodes, Configuration Sets, and Transports.

The contents of this chapter include sections on the scope, audience, organization of the documentation, and how to contact Oracle for assistance.

Overview

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 an SS7/Sigtran system.

Manual Organization





This manual is organized into the following chapters:

- *Introduction* contains general information about the *Transport Manager User's Guide*, the scope, audience, and organization of this document, and how to contact Oracle for assistance.
- *User Interface Introduction* describes the organization and usage of the application user interface.
- *Transport Manager Overview* provides an overview of Transport Manager functions, and describes multihoming and SCTP validation functions.
- *Transport Manager Configuration* describes the configuration of Transport Manager Adjacent Nodes and Configuration Sets, and Transports.
- *Transport Manager Maintenance* describes the information on the **Transport Manager > Maintenance > Transport** GUI page; and provides procedures for enabling, disabling, and blocking a Transport.
- *Transport Manager Use Cases* describes Use Cases in which the Transport Manager is involved.

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	Danger: (This icon and text indicate the possibility of <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)

Related Publications

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

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

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

<http://education.oracle.com/communication>

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Chapter 2

User Interface Introduction

Topics:

- [User Interface Organization.....13](#)
- [Missing Main Menu options.....19](#)
- [Common Graphical User Interface Widgets.....20](#)

This section describes the organization and usage of the application's user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction within an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

The core framework presents a common set of Main Menu options that serve various applications. The common Main Menu options are:

- Administration
- Configuration
- Alarm and Events
- Security Log
- Status & Manage
- Measurements
- Help
- Legal Notices
- Logout

Applications, such as DSR, build upon this framework to present features and functions. For example, the DSR Network OAM GUI may present the following Main Menu options in addition to the common options:

- Communication Agent
- Diameter Common
- Diameter
- Policy and Charging
- MAP-Diameter IWF
- SBR
- RADIUS

The DSR System OAM GUI may present even more Main Menu options as listed below. The end result is a flexible menu structure that changes according to the application needs and features activated.

- Transport Manager
- SS7/Sigtran
- RBAR
- FABR
- IPFE
- GLA
- Policy and Charging
- MAP-Diameter IWF
- SBR
- RADIUS
- Mediation

Note that the DSR System OAM Main Menu options differ from the Network OAM options. Some Main Menu options are configurable from the DSR Network OAM server and view-only from the System OAM server. This remains true for other applications.

User Interface Elements

Table 2: User Interface Elements describes elements of the user interface.

Table 2: User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.
Session Banner	Next bar across the top of the web page	<p>The left side of the banner just above the Main Menu provides the following session information:</p> <ul style="list-style-type: none"> • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. <p>The right side of the banner:</p> <ul style="list-style-type: none"> • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	<p>A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders.</p> <ul style="list-style-type: none"> • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	<p>Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area.</p> <ul style="list-style-type: none"> • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see Optional Layout Element Toolbar. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information

Element	Location	Function
		or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see Customizing the Login Message .

Main Menu Options

Table 3: Main Menu Options describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options do not appear on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the Network OAM and view-only on the System OAM; and some menu options are configurable only on the System OAM.

Note: Some features do not appear in the main menu until the features are activated.

Table 3: Main Menu Options

Menu Item	Function
Administration	<p>The Administration menu allows the user to:</p> <ul style="list-style-type: none"> • General Options. Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • View the software versions report • Upgrade management including backup and reporting • Authenticate LDAP servers • Configure SNMP trapping services • Configure an export server • Configure DNS elements
Configuration	<p>On the NOAM, allows the user to configure:</p> <ul style="list-style-type: none"> • Network Elements • Network Devices • Network Routes

Menu Item	Function
	<ul style="list-style-type: none"> • Services • Servers • Server Groups • Resource Domains • Places • Place Associations • Interface and Port DSCP
Alarms and Events	<p>Allows the user to view:</p> <ul style="list-style-type: none"> • Active alarms and events • Alarm and event history • Trap log
Security Log	<p>Allows the user to view, export, and generate reports from security log history.</p>
Status & Manage	<p>Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, KPIs, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.</p>
Measurements	<p>Allows the user to view and export measurement data.</p>
Transport Manager (optional)	<p>On the SOAM, allows the user to configure adjacent nodes, configuration sets, or transports. A maintenance option allows the user to perform enable, disable, and block actions on the transport entries.</p>
Communication Agent (optional)	<p>Allows the user to configure Remote Servers, Connection Groups, and Routed Services. The user can perform actions to enable, disable, and block connections. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.</p>
SS7/Sigtran (optional)	<p>On the SOAM, allows the user to configure various users, groups, remote signaling points, links, and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data.</p>
Diameter Common (optional)	<p>Allows the user to view or configure:</p> <ul style="list-style-type: none"> • Dashboard, configure on the NOAM; view on both OAMs • Network Identifiers on the SOAM - MCC Ranges • Network Identifiers on the NOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile Assignments <p>The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.</p>
Diameter (optional)	<p>Allows the user to configure, modify, and monitor Diameter routing:</p> <ul style="list-style-type: none"> • On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration

Menu Item	Function
	<ul style="list-style-type: none"> • On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with IDIH, AVP Dictionary, and Diameter Mediation configuration
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: <ul style="list-style-type: none"> • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: <ul style="list-style-type: none"> • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only.
Policy and Charging (optional)	On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for: <ul style="list-style-type: none"> • General Options • Access Point Names • Policy DRA <ul style="list-style-type: none"> • PCRF Pools • PCRF Sub-Pool Selection Rules • Network-Wide Options • Online Charging DRA <ul style="list-style-type: none"> • OCS Session State • Realms • Network-Wide Options • Alarm Settings • Congestion Options Additionally on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for: <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> • SBR Database Status

Menu Item	Function
	<ul style="list-style-type: none"> • SBR Status • SBR Database Reconfiguration Status • Policy Database Query <p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • General Options • Access Point Names • Policy DRA <ul style="list-style-type: none"> • PCRFs • Binding Key Priority • PCRF Pools • PCRF Pool to PRT Mapping • PCRF Sub-Pool Selection Rules • Policy Clients • Suspect Binding Removal Rules • Site Options • Online Charging DRA <ul style="list-style-type: none"> • OCSs • CTFs • OCS Session State • Realms • Error Codes • Alarm Settings • Congestion Options
Gateway Location Application (optional)	<p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • Exceptions • Options <p>GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP).</p>
IPFE (optional)	<p>Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only.</p>
MAP-Diameter Interworking (optional)	<p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application:</p> <ul style="list-style-type: none"> • DM-IWF Options • Diameter Exception <p>On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application:</p>

Menu Item	Function
	<ul style="list-style-type: none"> • MD-IWF Options • Diameter Realm • Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping
RADIUS (optional)	<p>Allows the user to perform configuration tasks, edit system options, and view elements for:</p> <ul style="list-style-type: none"> • Network Options • Message Authenticator Configuration Sets • Shared Secret Configuration Sets • Ingress Status Server Configuration Sets • Message Conversion Configuration Sets • NAS Node
SBR (optional)	<p>Allows the user to perform configuration tasks, edit system options, and view elements for:</p> <ul style="list-style-type: none"> • SBR Databases • SBR Database Resizing Plans • SBR Data Migration Plans <p>Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> • SBR Database Status • SBR Status • SBR Database Reconfiguration Status
Help	Launches the Help system for the user interface
Legal Notices	Product Disclaimers and Notices
Logout	Allows the user to log out of the user interface

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the **Group Administration** page. The default group, **admin**, is permitted access to all GUI options and functionality. Additionally, members of the **admin** group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options do not appear on your screen if you do not have administrative

permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing the password upon login. The System Login page also features a date and time stamp reflecting the time the page was last refreshed. Additionally, a customizable login message appears just below the **Log In** button.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request to gain access.

Customizing the Login Message

Before logging in, the **System Login** page appears. You can create a login message that appears just below the **Log In** button on the **System Login** page.



Oracle System Login

Wed Jul 8 14:20:00 2015 EDT

Log In

Enter your username and password to log in

Username:

Password:

Change password

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2015, [Oracle](#) and/or its affiliates. All rights reserved.

Figure 1: Oracle System Login

1. From the **Main Menu**, click **Administration > General Options**.

The **General Options Administration** page appears.

2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.

A status message appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the login message text displays.

Accessing the DSR Graphical User Interface

In DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you need to access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM > Administration > Access Control > Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.







1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example `https://dsr-no.yourcompany.com`.
When using Single Sign-On, you cannot use the IP address of the server.
2. When prompted by the browser, confirm that the server can be trusted.
The System Login page appears.
3. Enter the Username and Password for your account.
The DSR GUI for the NOAM appears.
4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.
The DSR GUI for the SOAM appears





You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the **Main Menu**.

Table 4: Main Menu Icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.

Icon	Name	Description
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

Note: Screen shots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First** | **Prev** | **Next** | **Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see [Page Controls](#).

Displaying Records 1-1 of 1 | [First](#) | [Prev](#) | [Next](#) | [Last](#)

Action	System ID	IP Address	Permission	Action
Edit Delete	lisa	10.25.62.4	READ_WRITE	Edit Delete

Displaying Records 1-1 of 1 | [First](#) | [Prev](#) | [Next](#) | [Last](#)

Figure 2: Paginated Table

Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see [Page Controls](#).

Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	MiddleWare	procmgr	SOAMP	teks8011002	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5443	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011004	DB merging from a child Source Node has failed
5444	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011003	DB merging from a child Source Node has failed
5441	31209	2009-Jun-11 18:07:22.640 UTC	MINOR	MiddleWare	re.portmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the Nodeinfo table.
										Unable to resolve a

Export

Figure 3: Scrollable Table

Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of pulldown lists, buttons, and links.

Username: (5-16 characters)

Group:

Time Zone:

Maximum Concurrent Logins: Maximum concurrent logins for a user (0=no limit). [Default = 1; Range = 0-50]

Session Inactivity Limit: Time (in minutes) after which login sessions expire (0 = never). [Default = 120; Range = 0-120]

Comment: (max 64 characters)

Temporary Password: (8-16 characters)

Re-type Password:

Ok Apply Cancel

Figure 4: Form Page

Tabbed pages

Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields populate on the page. Retrieve is always the default for tabbed pages.

Entire Network *		System.CPU_CoreUtilPct_Average	System.CPU_CoreUtilPct_Peak				
NOAMP	SOAM	Timestamp	System CPU UtilPct Average	System CPU UtilPct Peak	System Disk UtilPct Average	System Disk UtilPct Peak	System RAM UtilPct Average
		10/22/2009 19:45	6.764068	44	0.520000	1	7.939407
		10/22/2009 20:00	7.143644	25	0.520000	1	8.523822

Figure 5: Tabbed Pages

Retrieve Add Update Delete

Fields marked with a red asterisk (*) require a value.

Field	Value	Description
Network Entity	<input type="text"/>	* Numeric identifier for the Network Entity 1-15 DIGITS

Retrieve

Figure 6: Tabbed Pages

Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking **Report**. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

```

=====
User Account Usage Report
=====
Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiadmin
-----
Username          Date of Last Login   Days Since Last Login  Account Status
-----
guiadmin          2009-06-19 19:00:17  0                       enabled
-----
End of User Account Usage Report
=====

```

Figure 7: Report Output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the splash page appears. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration > General Options**.

The **General Options** page appears.

2. Locate **WelcomeMessage** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.

A status message appears at the top of the page to inform you if the operation was successful.

The next time you log in to the user interface, the new welcome message text is displayed.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See [Figure 8: Sorting a Table by Column Header](#). Clicking the column header again reverses the direction of the sort.

Local Node Name	Realm	FQDN	SCTP Listen Port	TCP Listen Port	Connection Configuration Set	CEX Configuration Set	IP Addresses
-----------------	-------	------	------------------	-----------------	------------------------------	-----------------------	--------------

Figure 8: Sorting a Table by Column Header

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in **Group Administration**, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

[Table 5: Example Action Buttons](#) contains examples of Action buttons.

Table 5: Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.

Action Button	Function
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in [Table 6: Submit Buttons](#), are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The Submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 6: Submit Buttons

Submit Button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

Click the X next to a pulldown list to clear the field.

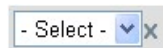


Figure 9: Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar appears in the Page Control Area of the GUI.

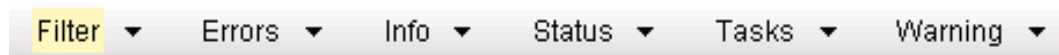


Figure 10: Optional Layout Element Toolbar

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear include:

- Filter – Allows you to filter data in a table.
- Errors – Displays errors associated with the work area.
- Info – Displays information messages associated with the work area.
- Status – Displays short status updates associated with the main work area.

- Warning – Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

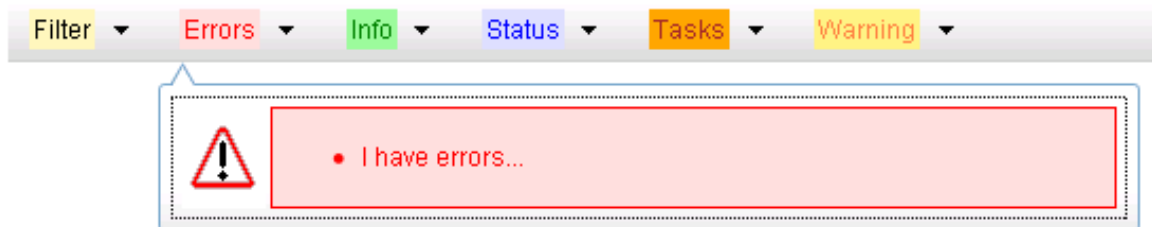


Figure 11: Automatic Error Notification

Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.
The selected element opens and overlays the work area.
2. Click **X** to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see [Optional Layout Element Toolbar](#).

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element – When enabled, the Network Element filter limits the data viewed to a single Network Element.
Note: Once enabled, the Network Element filter affect all pages that list or display data relating to the Network Element.
- Collection Interval – When enabled, the collection interval filter limits the data to entries collected in a specified time range.

- Display Filter – The display filter limits the data viewed to data matching the specified criteria. Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.



Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter Control Elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of Is Null in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators are available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once

enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
The filter tool appears.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
The filter tool appears.
2. Enter a duration for the **Collection Interval** filter.
The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.
The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering Using the Display Filter

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

1. Click **Filter** in the optional layout element toolbar.
The filter tool appears.
2. 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.
3. Select an operator from the operation selector pulldown menu.
The selected operator appears in the field.
4. Enter a value in the value field.
This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.
5. For data tables that support compound filtering, click **Add** to add another filter condition. Then repeat steps 2 through 4.

Multiple filter conditions are joined by an AND operator.

6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, click **Administration > General Options**.

The **General Options Administration** page appears.

2. Change the value of the **MaxRecordsPerPage** variable.

Note: Maximum Records Per Page has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

OK saves the change and returns to the previous page.

Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Chapter 3

Transport Manager Overview

Topics:

- [Overview.....33](#)
- [Multihoming.....33](#)
- [Transport Validation.....34](#)

Transport Manager enables the configuration of Transports (SCTP associations with remote hosts over an underlying IP network). Transport Manager provides the interface to the Adaptation Layer (M3UA) and manages the connections and data transmission from SCTP sockets.

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

Overview

A Transport Manager is a thin layer acting as an interface between a User Adaptation Layer and the IP Transport Layer. The Transport Manager that is used with the MAP-to-Diameter Interworking Function (MD-IWF) SS7 Application supports the MTP3 User Adaptation Layer (M3UA) and the Stream Control Transmission Protocol (SCTP) IP Transport Layer.

Note: The terms Association, connection, and Transport are used interchangeably in this document.

The Transport Manager performs the following activities:

- Handles Transport establish and tear down requests from the User.
- Manages Transport state and its User Adaptation Layer states for each Transport.
- Processes Transmit and Receive data.
- Provides multihoming for SCTP associations and validation of SCTP IP addresses.

The Transport Manager provides connection-based services, including IP-based addresses, to the MD-IWF SS7 Application on a physical MP server. Each MP has two Signaling IP Addresses. The Transport Manager uses these Signaling IP Addresses as Local IP Addresses for Transports.

Limitations

Transport Manager has the following limitations:

- Transport Manager does not support Transport Layer Security (TLS) and IPsec connections over SCTP.
- Transport Manager does not support IPv6 IP 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 IP addresses.

Transport Manager multihoming has the following characteristics:

- When there are multiple IP addresses for an endpoint, one address is designated as the Primary IP 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 Transport acting as an Initiator:

- Both Local IP addresses are sent in INIT to Adjacent Node.
- Both of the Remote IP addresses are used. If the Primary Peer IP Address is down, then the Transport re-sends INIT to the Secondary Peer IP Address.

For an SCTP Transport acting as a Listener:

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

For an SCTP Transport acting as either an Initiator or Listener, validation mode of remote IP Address(es) received in INIT-ACK is controlled by the User. Validation modes/rules are defined in [Transport 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 has potentially greater survivability of the sessions in case of network failures. There is no message loss if only a single path fails, the SCTP retransmits the in-flight data using an alternate path.

Transport 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

For SCTP, each endpoint advertises its reachable IP addresses to the far or remote end during the association formation. After SCTP signals that a candidate association has been formed, the Transport Manager validates the candidate.

Transport Manager has two methods of SCTP validation: Relax and Match. The effect of each validation method on the provisioning combinations versus the number of IP addresses exchanged by SCTP with the far end and any special action taken are described in [Table 8: SCTP Transport Address Validation](#).

- Relax 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 8: SCTP Transport Address Validation

IP Configured in Transport	Received in INIT/INIT-ACK	Transport Manager Behavior
----------------------------	---------------------------	----------------------------

Transport Manager Overview

Local Node	Remote Node		Match Mode	Relaxed
1	1	1	Association is accepted	Association is accepted
1	1	2	Association rejected, refusal event generated	Association is accepted
2	2	1	Association rejected, refusal event generated	Association is accepted <ul style="list-style-type: none"> • Operation Reason updated as Abnormal for that Transport • Configured Adjacent IP status, which has not been received in INIT/INIT-ACK chunk, is displayed as Unavailable
2	2	2	Association is accepted	Association accepted
2	2	>2	Association rejected, refusal event generated	Association accepted
1	2	1	Association rejected, refusal event generated	Association accepted <ul style="list-style-type: none"> • Operation Reason updated as Abnormal for that Transport • Configured Adjacent IP status, which has not been received in INIT/INIT-ACK chunk is displayed as Unavailable
1	2	2	Association accepted <ul style="list-style-type: none"> • Operation Reason updated as Abnormal for that Transport • Configured Adjacent IP status, which has not been received in INIT/INIT-ACK chunk is displayed as Unavailable 	Association accepted <ul style="list-style-type: none"> • Operation Reason updated as Abnormal for that Transport • Configured Adjacent IP status, which has not been received in INIT/INIT-ACK chunk is displayed as Unavailable
2	1	1	Association accepted	Association accepted
2	1	2	Association rejected, refusal event generated	Association accepted

Transport Manager Configuration

Topics:

- [Configuration Overview.....37](#)
- [Adjacent Node.....37](#)
- [Configuration Sets.....39](#)
- [Transport Configuration.....44](#)

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

Configuration Overview

The Transport Manager provides connection-based services, including IP-based addresses, to the MAP-to-Diameter Interworking Function (MD-IWF) SS7 Application on a physical MP server. Each MP has two Signaling IP Addresses. The Transport Manager uses these Signaling IP Addresses as Local IP Addresses for Transports.

Note: The terms Association, connection, and Transport are used interchangeably in this document.

Transport Manager configuration is performed on an Active SOAM.

The **Transport Manager > Configuration** GUI pages provide fields for entering the information needed to configure Adjacent Nodes, Configuration Sets, and Transports (SCTP associations with remote hosts over an underlying IP network).

Configuration Sequence

Configured Adjacent Nodes and Configuration Sets are required in the configuration of Transports. Therefore, Adjacent Nodes and Configuration Sets must be configured before Transports can be configured.

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. (There must be a connection from every MP to every Adjacent Node.)

Note: In SS7/Sigtran, an Adjacent Node is referred to as an Adjacent Server, which can be assigned as a member of an Adjacent Server Group.

The **Transport Manager > Configuration > Adjacent Node** page 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 listens for M3UA signaling.

On the **Transport Manager > Configuration > Adjacent Node** page, you can perform the following actions:

- Filter the list of Adjacent Nodes, to display only the desired Adjacent Nodes.
- Sort the list by a column in ascending or descending order, by clicking the column heading
- Click **Insert**.

The **Transport Manager > Configuration > Adjacent Node [Insert]** page appears. You can add a new Adjacent Node.

- Select an Adjacent Node in the list, and click **Delete**. You can delete the selected Adjacent Node.

Note: An Adjacent Node that is referenced by an Adjacent Server Group cannot be deleted from the list until it is removed from the Adjacent Server Group. Refer to the "Editing an Adjacent Server Group" procedure in the *SS7/Sigtran User's Guide* and Help.

- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Adjacent Node elements

[Table 9: Adjacent Node Elements](#) describes the fields on the **Transport Manager > Configuration > Adjacent Node** View and Insert pages. Data Input Notes apply only to the Insert page; the View page is read-only.

Table 9: Adjacent Node Elements

Element (* indicates required field)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.	Format: Pulldown list Range: SOAM Signaling Network Element Note: On the SOAM, the Signaling Network Element Name pulldown list is disabled and contains the NE name of the connected SOAM server.
* Adjacent Node Name	Unique identifier used to label an Adjacent Node. An Adjacent Node is a remote node that serves 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
* IP Address 1	Primary IP address of an Adjacent Node.	Format: IPv4 P address xxx.xxx.xxx.xxx Range: A valid IPv4 address
IP Address 2	IP address 2 of an Adjacent Node. If this is configured, then the Transport for which this Adjacent Node hosts the remote end can be configured as Multihomed if both the IP Addresses are selected in Transport Configuration .	Format: IPv4 P address xxx.xxx.xxx.xxx Range: A valid IPv4 address

Inserting an Adjacent Node

Use this task to configure a new Adjacent Node.

The fields are described in [Adjacent Node elements](#).

1. Select **Transport Manager > Configuration > Adjacent Node**
2. Click **Insert**.
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.
- Click **Cancel** to exit this page without saving any data.

When **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any field contains a value that is not valid or is out of the allowed range.
- Any required field is empty (not entered).
- A value that must be unique is not unique.
- A selected value no longer exists (has been deleted)
- Adding the new Adjacent Node would cause the maximum number of Adjacent Nodes per site (128) to be exceeded

The Adjacent Node is added to the configuration.

Deleting an Adjacent Node

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

Note: An Adjacent Node that is referenced by an Adjacent Server Group cannot be deleted until it is removed from the Adjacent Server Group. Refer to the "Editing an Adjacent Server Group" procedure in the *SS7/Sigtran User's Guide* and Help to remove the Adjacent Node from the Adjacent Server Group.

1. Select **Transport Manager > Configuration > Adjacent Node**.
2. Click on the row of the Adjacent Node you want to remove.

A delete confirmation message appears.

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

If **OK** is clicked and the selected Adjacent Node has been deleted by another user, an error message appears.

The Adjacent Node is deleted from the table.

Configuration Sets

A Transport configuration Set is a collection of SCTP association parameter values that are used in connection management signaling on a specific Transport.

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 as the Default values in *Transport Manager Configuration Set elements*. The pre-populated values can be changed if needed; changed values appear on the **Transport Manager > Configuration > Configuration Sets** pages instead of the pre-populated values.

The **Transport Manager > Configuration > Configuration Sets** page lists all configured sets of SCTP association parameter values, including the Default Configuration Set. The parameter values are described in *Transport Manager Configuration Set elements*.

On the **Transport Manager > Configuration > Configuration Sets** page, you can perform the following actions:

- Filter the list of Configuration Sets to display only the desired Configuration Sets.
- Sort the list by a column in ascending or descending order by clicking the column heading.
- Click **Insert**.

You can add a new Configuration Set on the **Transport Manager > Configuration > Configuration Sets [Insert]** page.

The **Transport Manager > Configuration > Configuration Sets [Insert]** page does not open if the maximum number of Configuration Sets per system (20) already exists in the system.

- Select a **Configuration Set Name** in the list and click **Edit**.

The **Transport Manager > Configuration > Configuration Sets [Edit]** page appears. You can edit the selected Configuration Set.

- Select a Configuration Set in the list and click **Delete**.

You can delete the selected Configuration Set.

- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Transport Manager Configuration Set elements

Table 10: 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 10: Transport Manager Configuration Set Elements*.

Table 10: Transport Manager Configuration Set Elements

Element (* indicates required field)	Description	Data Input Notes
* Configuration Set Name	A name that uniquely identifies the SCTP Transport Manager Configuration Set. The Configuration Set Name field is required, must be unique, and cannot be edited after it is created.	Format: A case-sensitive string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: Up to 32 characters.
* 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

Element (* indicates required field)	Description	Data Input Notes
* Retransmit Minimum Timeout	<p>The minimum amount of time to wait for an acknowledgment for a message sent.</p> <p>This value prevents the retransmit timeout from becoming too small in networks with a very short round-trip time.</p>	<p>Format: Numeric</p> <p>Range: 10 - 1000 msec</p> <p>This minimum value cannot be greater than the maximum value.</p> <p>Default: 120</p>
* Retransmit Maximum Timeout	<p>The maximum amount of time to wait for an acknowledgment for a message sent.</p> <p>This value places an upper bound on the exponential back-off algorithm used by SCTP for retransmission timing. After this retransmit interval is reached, retransmits are sent at a constant rate until an ACK is received or the maximum attempt is reached.</p>	<p>Format: Numeric</p> <p>Range: 10 - 10000 msec</p> <p>This maximum value cannot be less than the minimum value.</p> <p>Default: 120</p>
* Number of Retransmits Triggering Association Failure	<p>Number of consecutive retransmits that cause an SCTP Association to be marked as failed.</p> <p>This value indicates how many SCTP retransmission attempts should be made to all destinations for an SCTP association before marking the association as failed.</p> <p>This value should not be greater than the sum of the retransmit attempts for all destinations within the association.</p>	<p>Format: Numeric</p> <p>Range: 1 - 12</p> <p>Default: 5</p>
* Number of Retransmits Triggering Init Failure	<p>Number of consecutive retransmits for INIT and COOKIE-ECHO chunks that cause an SCTP Association to be marked as failed.</p> <p>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.</p>	<p>Format: Numeric</p> <p>Range: 1 - 12</p> <p>Default: 8</p>
* SACK Delay	<p>The number of milliseconds to delay after receiving a DATA chunk and prior to sending a SACK.</p> <p>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.</p> <p>Setting SACK Delay to zero disables this delay so that SACKs are sent as quickly as possible.</p>	<p>Format: Numeric</p> <p>Range: 0 - 200 msec</p> <p>Default: 10</p>

Element (* indicates required field)	Description	Data Input Notes
* Sctp Heartbeat Interval	<p>The interval in milliseconds between sending Sctp HEARTBEAT messages to a peer.</p> <p>HEARTBEAT messages are only sent when no user data has been sent for the duration of the heartbeat interval.</p> <p>Setting the heartbeat interval to zero disables heartbeating (not recommended).</p>	<p>Format: Numeric</p> <p>Range: 0, 100 - 300000 msec</p> <p>Default: 1000</p>
* Connection Retry Interval	<p>The interval in seconds between connection attempts when the connection is unsuccessful.</p>	<p>Format: Numeric</p> <p>Range: 5 - 60 sec</p> <p>Default: 10</p>
* Socket Send Buffer Size	<p>The socket send buffer size (in bytes) for outgoing Sctp messages.</p> <p>The send buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.</p>	<p>Format: Numeric</p> <p>Range: 65535 - 5000000 bytes</p> <p>Default: 2000000</p>
* Socket Receive Buffer Size	<p>The socket receive buffer size (in bytes) for incoming Sctp messages.</p> <p>The receive buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.</p>	<p>Format: Numeric</p> <p>Range: 65535 - 5000000 bytes</p> <p>Default: 2000000</p>
* Sctp Multihoming Mode	<p>The Sctp Multihoming mode allows the user to configure remote host validation mode setting for Sctp.</p> <p>If the Adjacent Node is Multihomed for a specified Transport, Adjacent Node IP Addresses received in INIT/INIT-ACK chunk are validated based on this parameter.</p> <p>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.</p> <p>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.</p>	<p>format: Pulldown list</p> <p>Range: Relax, Match</p> <p>Default: Relax</p>

Inserting a Transport Manager Configuration Set

Use this task to configure a new Transport Manager Configuration Set.

The fields are described in [Transport Manager Configuration Set elements](#).

1. Select **Transport Manager > Configuration > Configuration Sets**.
2. Click **Insert**.

The default values that appear on the **Transport Manager Configuration Set [Insert]** 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.
 - Click **Cancel** to exit this page without saving any data.

When **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any field contains a value that is not valid or is out of the allowed range.
- Any required field is empty (not entered).
- A value that must be unique is not unique.
- The Retransmit Minimum Timeout value is greater than Retransmit Maximum Timeout value.
- The Retransmit Maximum Timeout value is less than Retransmit Minimum Timeout value.
- Adding the new Configuration Set would cause the maximum number of Configuration Sets per system (20) to be exceeded.

The Transport Manager Configuration Set is added.

Editing a Transport Manager Configuration Set

Use this task to edit a Transport Manager Configuration Set.

Note: Although the Default Transport Manager Configuration Set can be edited, any changes to the default values should be evaluated carefully. The default values shown in are recommended.

A Configuration Set that is referenced by an active (Enabled) Transport cannot be edited. To disable a Transport, see [Disabling a Transport](#).

1. Select **Transport Manager > Configuration > Configuration Sets**.
2. Click **Edit** next to the Transport Manager Configuration Set you wish to modify.
A **Configuration Set Name** cannot be changed.
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.
 - Click **Cancel** to exit this page without saving any data.

If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any field contains a value that is not valid or is out of the allowed range.
- Any required field is empty (not entered).
- A value that must be unique is not unique.
- The edited entry no longer exists (has been deleted by another user).
- The Retransmit Minimum Timeout value is greater than Retransmit Maximum Timeout value.
- The Retransmit Maximum Timeout value is less than Retransmit Minimum Timeout value.
- The Transport Admin State could not be obtained from the MP server: Refer to the **Status & Manage > Server** GUI page for possible causes.

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

Deleting a Transport Manager Configuration Set

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

A Transport Manager Configuration Set that is referenced by an active Transport cannot be deleted. To disable a Transport, see [Disabling a Transport](#).

The Default Transport Manager Configuration Set cannot be deleted.

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

A Transport defines an SCTP association or connection that is used for communicating with a remote host over an underlying IP network.

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

On the **Transport Manager > Configuration > Transport** page, you can perform the following actions:

- Filter the list of Transports to display only the desired Transports.
- Sort the list by a column in ascending or descending order, by clicking the column heading.
- Click **Insert**.

The **Transport Manager > Configuration > Transport [Insert]** page appears. You can add a new Transport.

- Select a Transport in the list and click **Edit**.

The **Transport Manager > Configuration > Transport [Edit]** page opens. You can edit the selected Transport if it is in the Disabled Admin State.

- Select a Transport in the list and click **Delete**.

You can delete the selected Transport if it is in the Disabled Admin State and not referenced by a Link.

- Select no, one, or more than one Transport in the list, and click **Report** to generate a report that contains a summary of Transport configuration data.
 - With no Transports selected, the report contains a summary of the configuration data for all configured Transports.
 - With one Transport selected, the report contains a summary of the configuration data for the selected Transport.
 - With more than one Transport selected, the report contains a summary of the configuration data for each selected Transport.
- Select no, one, or more than one Transport in the list, and click **Status** to open the **Transport Manager > Maintenance > Transport** page, where you can view the status of configured Transports. See [Viewing the Status of a Transport](#)
 - With no Transports selected, the page displays status for all configured Transports.
 - With one Transport selected, the page displays status only for the selected Transport.
 - With more than one Transport selected, the page displays status only for each selected Transport.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Transport Configuration elements

[Transport Configuration elements](#) describes the fields on the **Transport Manager > Configuration > Transport** View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 11: Transport Configuration Elements

Element (* indicates required field)	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.
* Adapter	Identifies the Transport User for which the Transport is being added.	Format: Pulldown list Range: M3UA
* Transport Name	A name that uniquely identifies the Transport.	Format: Test box.. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: Up to 32 characters.
* Transport Protocol	Identifies the Transport protocol to be used by this Transport.	Format: Pulldown list Range: SCTP

Transport Manager Configuration

Element (* indicates required field)	Description	Data Input Notes
		This field populates automatically when M3UA is selected for the Adapter .
* Transport Type	Identifies the Transport type to be used by this Transport.	Format: Pulldown list Range: Initiator This field populates automatically when M3UA is selected for the Adapter .
* MP Server Hostname	The hostname of the MP server that hosts the local end of the Transport.	Format: Pulldown list Range: hostnames of configured MP servers
* MP Server IP Address (Primary)	The Primary IP Address hosted by the MP server that is 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 address to be used for this Transport.	Format: Pulldown list Range: IP Addresses of configured MP servers Only IPv4 addresses are supported for Transport configuration.
MP Server IP Address (Secondary)	The Secondary IP Address hosted by the MP server that is 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 Range: IP Addresses of configured MP servers Only IPv4 addresses are supported for Transport configuration.
MP Server Listen Port	Listen port number of the MP server for this Transport. This port is used if the Transport Type is configured as Listener. If the MP server hosts multiple Listener Transports, each Transport may listen on a different port.	Format: Text box Range for UDP protocol: 1 - 65535 Range for SCTP protocol: 1024 - 65535 Default: 5060
* MP Server Initiate Port	Initiate port number of the MP server for this Transport. This port is 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.	Format: Text box Range: 1024 - 65535 Default: 2905

Element (* indicates required field)	Description	Data Input Notes
* Adjacent Node	The Adjacent Node that hosts the remote end of this Transport.	Format: Pulldown list Range: All configured Adjacent Nodes
* 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 Range: IP Addresses of configured Adjacent Nodes
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 Range: IP Addresses of configured Adjacent Nodes
* Adjacent Node Port	Adjacent Node port number for this Transport. This port number must match the port number configured on the Adjacent Node as the listening or initiator port for the configured Transport Type. If the Adjacent Node hosts multiple Transports, each Transport may listen on a different Remote port number.	Format: Numeric Range: 1024 - 65535 Default: 2905
Configuration Set Name	The configuration parameter set to be used for this Transport. Configuration Sets are defined on the Transport Manager > Configuration > Configuration Sets page (see Configuration Sets).	Format: Pulldown list Range: All configured Configuration Set Names Default: Default

Inserting a Transport

Use this task to create a new **Transport**. The fields are described in [Transport Configuration elements](#).

1. Select **Transport Manager > Configuration > Transport**.
2. Click **Insert**.
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.
- Click **Cancel** to exit this page without saving any changes.

When **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any field contains a value that is not valid or is out of the allowed range.
- Any required field is empty (not entered).
- A value that must be unique is not unique.
- The value combination of IP Address 1 and port, or IP Address 2 and port, is not unique.
- A selected value no longer exists (has been deleted).
- Adding the new Transport would cause the maximum number of Transports per site (1024) to be exceeded.

The Transport is added to the database. The Transport is in the **Disabled** Administrative State. To enable the Transport, see [Enabling a Transport](#).

Editing a Transport

Use this procedure to change fields for a configured Transport.

Fields that are not grayed-out can be edited.

Fields that are grayed-out cannot be edited.

The fields are described in [Transport Configuration elements](#).

When the **Transport Manager > Configuration > Transport [Edit]** page opens, the fields are populated with the current configured values.

Note: A Transport cannot be edited unless it is in the **Disabled** Administrative State. To disable the Transport, see [Disabling a Transport](#)

1. Select **Transport Manager > Configuration > Transport**.
2. Click **Edit**.
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.
 - Click **Cancel** to exit this page without saving any changes.

When **OK** or **Apply** is clicked and any or the following conditions exist, an error message appears:

- Any field contains a value that is not valid or is out of the allowed range.
- Any required field is empty (not entered).
- A value that must be unique is not unique.
- IP Address 1 and IP Address 2 are the same address.
- The value combination of IP Address 1 and port, or IP Address 2 and port, is not unique.
- A selected value no longer exists (has been deleted).
- The Transport Admin State could not be obtained from the MP server: Refer to the **Status & Manage > Server** GUI page for possible causes.

The edited Transport data is written to the database. The Transport remains in the **Disabled** Administrative State. To enable the Transport, see [Enabling a Transport](#).

Deleting a Transport

Use this task to delete a configured Transport.

Deleting a Transport removes the Transport from the configuration.

A Transport cannot be deleted unless:

- It is in the **Disabled** Administrative State. To disable the Transport, see [Disabling a Transport](#).
- It is not referenced by any Link. Refer to "Links" in the *SS7/Sigtran User's Guide* and Help.

1. Select **Transport Manager > Configuration > Transport**.
2. Select the Transport you want to remove.
3. Click **Delete**.

A delete confirmation message appears.

If the Transport is not in the **Disabled** Admin State, the following message appears:

"The transport state reported by the MP server is not Disabled. Please disable the transport from Main Menu: **Transport Manager > Maintenance > Transport** before deleting the transport. Deletion of a transport that is not disabled may result in loss of signaling data. If you wish to force deletion of the transport even though the transport may not be disabled, click **OK**, otherwise click **Cancel**."

If the Transport Admin State could not be determined, the following message appears:

"The Transport state on the MP server could not be determined. Please refer to Main Menu: **Status & Manage > Servers** for the cause of the problem. Deletion of a transport that is not disabled may result in loss of signaling data. If you wish to force deletion of the transport even though the transport may not be disabled, click **OK**, otherwise click **Cancel**."

4. Click **OK** to confirm the deletion, or **Cancel** to stop the delete.

When **OK** is clicked and the selected Transport no longer exists (has been deleted by another user), an error message appears.

The Transport is deleted from the list.

Generating a Report on Transport Configuration Data

1. Select **Transport Manager > Configuration > Transport**.
2. Click **Report** at the bottom of the page to generate a report of Transport configuration data.
 - With no Transports selected, click **Report** to generate a report containing configuration data for all configured Transports.
 - Select one or more Transports and click **Report** to generate a report containing configuration data only for the selected Transports
3. You can click **Print** to print a copy of the report, or click **Save** to save the report as a text file.

Example Report

```

Main Menu: Transport Manager > Configuration > Transport [Report]
=====
d s r   T r a n s p o r t s   R e p o r t
=====
Report Generated: Tue Nov 03 9:55:30 2015 EST
From: System OAM on host MutiAppl-SOAM2
Report Version: 7.1.1.0.0-71.29.0
User: guiadmin

-----

Transports Summary
-----

pc1110916

Signaling Network Element Name      : NE_MultiAppl_SOAMP
MP Server Hostname                   : MultiAppl-SS7-MP1
Adapter                              : M3UA
Transport Protocol                   : SCTP
Transport Type                       : Initiator
MP Server IP Address (Primary)       : 192.168.66.13
MP Server IP Address (Secondary)     : 192.168.67.13
MP Server Listen Port                : ----
MP Server Initiate Port              : 2905
Adjacent Node                        : pc1110916_VM1
Adjacent Node IP Address (Primary)   : 100.100.100.100
Adjacent Node IP Address (Secondary) : 100.100.105.100
Adjacent Node Port                   : 32905
Configuration Set Name                : Default

-----

End of d s r   T r a n s p o r t s   R e p o r t
=====

```

Viewing the Status of a Transport

Use this procedure to view Status of the configured Transport.

1. Select **Transport Manager > Configuration > Transport**.
2. Select the **Transport Name** to check the status.
3. Click **Status**.

The **Transport Manager > Maintenance > Transport** page appears listing all configured Transports and their Admin State and Operational Status.

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

For a description of the Admin State relationships with Operational Status and Operational Reason, see *Transport Admin State, Operational Status, and Operational Reason*. See *Enabling a Transport*, *Disabling a Transport*, and *Blocking a Transport* for the procedures.

Chapter 5

Transport Maintenance

Topics:

- *Transport Maintenance Overview.....52*
- *Transport Maintenance Elements.....52*
- *Transport Admin State, Operational Status, and Operational Reason.....53*
- *Enabling a Transport.....54*
- *Disabling a Transport.....55*
- *Blocking a Transport.....56*

The **Transport Manager > Maintenance > Transport** GUI 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 Manager > Maintenance > Transport** page shows the Transport Status for each configured Transport, including the Administrative State and Operational Status of each Transport. The Administrative State can be **Enabled**, **Blocked**, or **Disabled**. The Operational Status can be **Up** or **Down**.

The **Transport Manager > Maintenance > Transport** page can be accessed by selecting **Transport Manager > Maintenance > Transport** in the left-hand GUI menu, or by clicking **Status** on the **Transport Manager > Configuration > Transport** GUI page.

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

Status information is obtained on the system through the collection process, whereby the SOAM server collects data from the MP servers.

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

When the active server's collection status is **Unknown**, cells with gray text indicate the last known information about the Transport.

The **Transport Manager > Maintenance > Transport** values are helpful under alarm conditions as a starting point for gathering additional information. For example, a timestamp is recorded when a Transport goes down. The timestamp can be used to narrow the search in the event history log and measurements reports.

After rudimentary information for troubleshooting has been obtained, the network operator can continue investigating using the **Alarms & Events** and **Measurements** GUI pages.

On the **Transport Manager > Maintenance > Transport** page, you can perform the following actions:

- Filter the list of Transports to display only the desired Transports.
- Sort the list by a column in ascending or descending order by clicking the column heading. The default order is by **Transport Name** in ascending ASCII order.
- Select one or more rows, and click **Enable** to enable each selected Transport.
- Select one or more rows, and click **Disable** to disable each selected Transport.
- Select one or more rows, and click **Block** to block each selected Transport.
- Prevent the page from automatically refreshing by clicking the **Pause updates** check box.

Transport Maintenance Elements

Table 12: Transport Maintenance Elements describes the fields on the **Transport Manager > Maintenance > Transport** page.

Table 12: Transport Maintenance Elements

Element	Description
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.
MP Server Hostname	The hostname of the MP server that hosts 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	The Transport Protocol to be used by this Transport (SCTP).
Transport Type	The Transport Type to be used by this Transport (Initiator, Listener).
Adjacent Node	The Adjacent Node to host the remote end of the Transport. Note: Click + in the Adjacent Node field to show the IP addresses for the Adjacent Node.
Admin State	The Administrative State of the Transport (the manual maintenance state that the network operator has specified): Enabled, Disabled, or Blocked. See <i>Transport Admin State, Operational Status, and Operational Reason</i> .
Operational Status	The Operational Status of the Transport: Up or Down .
Operational Reason	The reason that a given Operational Status is shown. For information on a value listed in this field, see <i>Transport Admin State, Operational Status, and Operational Reason</i> .
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 Admin State, Operational Status, and Operational Reason

Table 13: Transport Admin State Relationships shows the possible values that may appear in the **Operational Status** and **Operational Reason** fields of the **Transport Manager > Maintenance > Transport** page, and shows the relationship between the Transport Admin States, Operational Status, and Operational Reasons.

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 **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 **Operational Status** is **Down**, the **Operational Reason** provides information about why it is Down.

Table 13: Transport Admin State Relationships

Admin State	Operational Status	Operational Reason	Description
Enabled	Down	Connecting	Trying to establish the SCTP connection in Initiator mode.
	Down	Listening	Trying to establish the SCTP connection in Listener mode.
	Down	Up Pending	M3UA: SCTP Transport has been established and ASP-UP has been sent, Waiting for ASP-UP-ACK.
	Up	Normal	M3UA: For SCTP Transport, it has reached the ASP-UP state and is available for enabling links.
	Up	Abnormal	If one of the Local IP address goes down in SCTP Transport for Multihomed Adjacent Nodes.
	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	M3UA: Trying to establish the SCTP connection, but ASP-UP is not sent afterwards.
	Down	Blocked	M3UA: SCTP Transport has been established, but it has been blocked for any M3UA traffic.

Enabling a Transport

When a Transport is put in the **Enabled** Administrative State, the MP server associated with the Transport 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**.
2. Click on the row to highlight the Transport you wish to enable.
Enable is not grayed out if the Transport's Administrative State is already **Enabled**.

Also, if collection on the server is not working, all buttons (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server disregards the command if the Transport is already in the selected Administrative State.

3. Click **Enable**.
A confirmation message appears.
4. Click **OK** to confirm.

If the Transport is successfully enabled,

- 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.
- **Enable** is now grayed out.

If **OK** is clicked and the selected Transport has been deleted by another user, an error message appears.

Disabling a Transport



CAUTION

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

When a Transport is put in the **Disabled** Administrative State, the MP server attempts to bring the Transport to the SCTP Closed state and the ASP-DOWN state.

1. Select **Transport Manager > Maintenance > Transport**.
2. Click on the **Pause updates** check box on the page (lower right corner) so you can view the results of your selections during this procedure. You can also click the **Transport Manager > Maintenance > Transport** on the main menu to manually update the page.
3. Click on the row that contains the Transport to highlight it.

Disable is not grayed out if the Transport's Administrative State is already **Disabled**.

Also, if collection on the server is not working, all buttons (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The Admin State, Operational Status, and Operational Reason fields are grayed out. The MP server disregards the command if the Transport is already in the selected Administrative State.

4. Click **Disable**.
5. Click **OK** to confirm.

If the Transport is successfully disabled,

- The **Operational Status** field shows **Down**.
- The **Admin State** field shows **Disabled**.
- **Disable** is now grayed out.

If **OK** is clicked and the selected Transport has been deleted by another user, an error message appears.

Blocking a Transport

Note: Blocking a Transport causes a 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 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 > Transport**.
2. Click the **Pause updates** check box (lower right corner) so you can view the results of your selection during this procedure. You can also click **Transport Manager > Maintenance > Transport** on the main menu to update the page.
3. Click on the row to highlight the transport you wish to block.
4. Click **Block**.

Block is not grayed out if the Transport's Administrative State is already **Blocked**.

Also, if collection on the server is not working, all buttons (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server disregards 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.

If **OK** is clicked and the Transport has been deleted by another user, an error message appears.

The Transport is blocked.

Appendix

A

Transport Manager Use Cases

Topics:

- [Use Case Overview.....58](#)
- [SS7+SCTP Multihomed Use Cases.....59](#)

This Appendix describes Use Cases in which the Transport Manger is involved.

Use Case Overview

Table 14: Use Case Overview summarizes the main (but not all possible) use cases that involve the Transport Manager.

Table 14: Use Case Overview

UC#	SS7 + Transport Protocol	Description
1	SS7-SCTP	SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation sent via primary IP port Initiate and establish an outgoing SCTP multihomed association to the Adjacent Node via IP address marked as primary.
2	SS7-SCTP	SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation received via primary IP port Receive and establish an incoming SCTP association from a remote destination with IP address marked as primary.
3	SS7-SCTP	SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation sent via alternate IP port Initiate and establish an outgoing SCTP multihomed association to a remote destination with IP address marked as alternate.
4	SS7-SCTP	SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation received via alternate IP port Receive and establish an incoming SCTP multihomed association from a remote destination with IP address marked as alternate.
5	SS7-SCTP	SCTP Multihomed Association Rejection – DNS SCTP association is provisioned as multihomed and incoming INITs contain DNS names rather than IP addresses.
6	SS7-SCTP	SCTP Multihomed Association Primary Path Fail
7	SS7-SCTP	SCTP Multihomed Association Primary Path Restored
8	SS7-SCTP	SCTP Multihomed Association Alternate Path Fail
9	SS7-SCTP	SCTP Multihomed Association Alternate Path Restored
10	SS7-SCTP	SCTP Multihomed Association Both Paths Failure
11	SS7-SCTP	SCTP Multihomed Association Both Paths Restored

SS7+SCTP Multihomed Use Cases

Table 15: SS7+SCTP Multihomed Use Cases describes Transport Manager SS7+SCTP Multihomed Use Cases.

Table 15: SS7+SCTP Multihomed Use Cases

UC#	Description
1	<p>SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation sent via primary IP port.</p> <p>Initiate and establish an outgoing SCTP multihomed association to the Adjacent Node via IP address marked as primary for both Relax and Match validation modes.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • MP XS1 and XS2 IP addresses configured • SCTP association is not established • MP and remote Adjacent Node are each configured with two IP addresses, and each remote address is reachable via one local IP port (but both remote IP addresses are not reachable by any one local IP port) <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Association is configured with both local MP addresses and addresses of Adjacent Node. One local MP address is marked as primary • Association is configured as an Initiator • Association is marked as open • Association generates an INIT to the Adjacent Node containing both the local addresses configured in the association via its primary interface • Adjacent Node responds with INIT-ACK containing both its local addresses • Adjacent Node's addresses are successfully validated according to validation mode and rules in SCTP Validation • Establishment procedure continues <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged. <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • Validation fails and association is rejected. Refusal event is generated, refusal count is pegged, and alarm is raised.
2	<p>SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation received via primary IP port.</p> <p>Initiate and establish an incoming SCTP multihomed association to the Adjacent Node via IP address marked as primary for both Relax and Match validation modes.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • MP XS1 and XS2 IP addresses configured

UC#	Description
	<ul style="list-style-type: none"> • SCTP association is not established • MP and remote Adjacent Node are each configured with two IP addresses, and each remote address is reachable via one local IP port (but both remote IP addresses are not reachable by any one local IP port) <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Association is configured with both local MP addresses and addresses of Adjacent Node. One local MP address is marked as primary. • Association is configured as an Responder • Association is marked as open • Association receives an INIT from the Adjacent Node containing both its local addresses via its primary interface • Association responds with INIT-ACK containing both local addresses configured in the association • Adjacent Node's addresses are successfully validated according to validation mode and rules in SCTP Validation • Establishment procedure continues <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged. <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • Validation fails and association is rejected. Refusal event is generated; refusal count is pegged.
3	<p>SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation sent via alternate IP port.</p> <p>Initiate and establish an outgoing SCTP multihomed association to the Adjacent Node via IP address marked as alternate for both Relax and Match validation modes.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • MP XS1 and XS2 IP addresses configured • SCTP association is not established • MP and remote Adjacent Node are each configured with two IP addresses, and each remote address is reachable via one local IP port (but both remote IP addresses are not reachable by any one local IP port) <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Association is configured with both local MP addresses and addresses of Adjacent Node. One local MP address is marked as primary. • Association is configured as an Inhalator • Association is marked as open • Association generates an INIT to the Adjacent Node containing both the local addresses configured in the association via its alternate interface • Adjacent Node responds with INIT-ACK containing both its local addresses • Adjacent Node's addresses are successfully validated according to validation mode and rules in SCTP Validation

UC#	Description
	<ul style="list-style-type: none"> • Establishment procedure continues <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • Validation fails and association is rejected. Refusal event is generated, refusal count is pegged.
4	<p>SCTP Multihomed Association Establishment – XSI1/XSI2 IP ports – Initiation received via alternate IP port.</p> <p>Initiate and establish an incoming SCTP multihomed association to the Adjacent Node via IP address marked as alternate for both Relax and Match validation modes.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • MP XS1 and XS2 IP addresses configured • SCTP association is not established • MP and remote Adjacent Node are each configured with two IP addresses, and each remote address is reachable via one local IP port (but both remote IP addresses are not reachable by any one local IP port) <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Association is configured with both local MP addresses and primary address of Adjacent Node. One local MP address is marked as primary. • Association is configured as an Responder • Association is marked as open • Association receives an INIT from the Adjacent Node containing both its local addresses via its alternate interface • Association responds with INIT-ACK containing both local addresses configured in the association • Adjacent Node's addresses are successfully validated according to validation mode and rules in SCTP Validation • Establishment procedure continues <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged. <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • Validation fails and association is rejected. Refusal event is generated, refusal count is pegged, and alarm is raised.
5	<p>SCTP Multihomed Association Rejection – XSI1/XSI2 IP ports – DNS SCTP association is configured as multihomed and incoming INITs contain DNS names rather IPv4 addresses.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • MP XS1 and XS2 IP addresses configured

UC#	Description
	<ul style="list-style-type: none"> • SCTP association is not established • MP and remote Adjacent Node are each configured with two IP addresses, and each remote address is reachable via one local IP port (but both remote IP addresses are not reachable by any one local IP port) <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Association is configured with both local MP addresses and primary address of Adjacent Node. One local MP address is marked as primary. • Association is configured as an Responder • Association is marked as open • Association receives an INIT from the Adjacent Node containing one or more addresses as Domain Names • INIT is rejected • Establishment procedure is halted <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association is not accepted and remains in unestablished state. <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None
6	<p>SCTP Multihomed Association – Primary Path Fail.</p> <p>With all paths of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the primary path is failed.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • Multihomed association in established state, both paths established • Traffic is being exchanged with the Adjacent Node <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • The primary path is failed • Traffic is moved to the alternate path • Event is generated indicating loss of path – Adjacent Node's primary address is marked as unavailable • Adjacent Node's primary address is marked as unreachable <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association remains established although in degraded/abnormal state • No loss of traffic occurred <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None
7	<p>SCTP Multihomed Association – Primary Path Restored.</p> <p>With only the alternate path of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the primary path is restored.</p> <p>PRE CONDITIONS:</p>

UC#	Description
	<ul style="list-style-type: none"> • Multihomed association in established state, only the alternate paths established • Traffic is being exchanged with the Adjacent Node <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • The primary path is restored • Traffic is moved back to the primary path • Primary path is restored – Adjacent Node's primary address is marked as available • Adjacent Node's primary address is marked as reachable <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association remains established • No loss of traffic occurred <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None
8	<p>SCTP Multihomed Association – Alternate Path Fail.</p> <p>With all paths of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the alternate path is failed.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • Multihomed association in established state, both paths established • Traffic is being exchanged with the Adjacent Node <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • The alternate path is failed • Event is generated indicating loss of path and Adjacent Node's alternate address is marked as unreachable <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association remains established although in degraded/abnormal state • Traffic is unaffected <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None
9	<p>SCTP Multihomed Association – Alternate Path Restored.</p> <p>With only the primary path of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the alternate path is restored.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • Multihomed association in established state, only the primary path established • Traffic is being exchanged with the Adjacent Node <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • The alternate path is restored • Alternate path is restored and Adjacent Node's alternate address is marked as reachable

UC#	Description
	<p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association remains established • Traffic is unaffected <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None
10	<p>SCTP Multihomed Association – Both Paths Failure.</p> <p>With all paths of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, both paths are failed.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • Multihomed association in established state, both paths established <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Both paths are failed • Events are generated indicating both paths failed and Adjacent Node's IP addresses are marked as unreachable. An alarm is generated indicating the Transport is down. • Association transitions to down state <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association remains in down state <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None
11	<p>SCTP Multihomed Association – Both Paths Restored.</p> <p>With all paths of a multihomed SCTP association failed, both paths are restored.</p> <p>PRE CONDITIONS:</p> <ul style="list-style-type: none"> • Multihomed association in established state, both paths established <p>DESCRIPTION:</p> <ul style="list-style-type: none"> • Both paths are failed • Events are generated indicating both paths failed and Adjacent Node's IP addresses are marked as unreachable. An alarm is generated indicating the Transport is down. • Association transitions to down state <p>POST CONDITIONS:</p> <ul style="list-style-type: none"> • Association remains in down state <p>ALTERNATE COURSE:</p> <ul style="list-style-type: none"> • None

A

Adjacent Server A server acting as a signaling peer for M3UA signaling. An Adjacent Server connects to one or more MP Servers using reliable IP transport sessions, such as SCTP associations. Only adjacent Remote Signaling Points and adjacent Remote MTP3 Users are hosted on Adjacent Servers.

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.

Association An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.

C

connection An SCTP association or a TCP connection.

G

GUI Graphical User Interface
The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

M

M3UA SS7 MTP3-User Adaptation Layer
M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.

MD-IWF MAP-Diameter Interworking SS7 Application, which translates MAP messages into Diameter messages

N

NOAM Network Operations, Administration, and Maintenance

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.

SOAM System Operations, Administration, and Maintenance

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

S

messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

T

Transport

An SCTP association with remote hosts over an underlying IP network.

TSA

Target Set Address

An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.