Oracle® Communications Diameter Signaling Router

Transport Manager User's Guide

E53478 Revision 01

July 2014

ORACLE®

Oracle® Communications Transport Manager User's Guide

Copyright © 2014,

Oracle and/or its affiliates. All rights reserved.

Table of Contents

List of Tables

Chapter
1
Introduction

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, and organization of the documentation, and how to contact Oracle for assistance.

Purpose of this documentation

This documentation:

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

Scope and Audience

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

Documentation Admonishments

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

Table 1: Admonishments

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

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.
- *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 Maintenance* describes the information on the **Transport Manager > Maintenance > Transport** GUI page; and provides procedures for enabling, disabling, and blocking a Transport.

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 **2** for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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.

Related Publications

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

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter
2

Transport Manager Overview

Topics:

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.

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

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 will be sent in INIT to Adjacent Node.

• Both of the Remote IP addresses will be used. If the Primary Peer IP Address is down, then the Transport will re-send INIT to the Secondary Peer IP Address.

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

• Both Local IP addresses will be sent in INIT-ACK to Adjacent Node.
• A connect can be accepted from either the Primary or Secondary IP Address, and the connection 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 will be controlled by 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 in-flight data will be retransmitted by SCTP 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 tSCTP 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 2: 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 2: SCTP Transport Address Validation

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

			will be displayed as "Unavailable"	will be displayed as "Unavailable"
2	1	1	Association accepted	Association accepted
2	1	2	Association rejected, refusal event generated	Association accepted

Chapter

3

Transport Manager Configuration

Topics:

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 will listen 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 form 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 3: 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 3: 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:

Viewing Adjacent Nodes

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

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

The **Transport Manager > Configuration > Adjacent Node** page appears.\with the defined Adjacent Nodes listed. For field definitions, see *Adjacent Node elements*.

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**

   The **Transport Manager > Configuration > Adjacent Node** page appears.

2. Click **Insert**.

   The**Transport Manager > Configuration > Adjacent Node [Insert]** page appears.

3. Populate the fields with data (for field definitions, see *Adjacent Node elements*).

4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to exit this page without saving any data.

   When **OK** or **Apply** 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**.

   The **Adjacent Node** page appears.

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

   A delete confirmation message appears.

3. Click the **Delete** button at the bottom of the page.

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

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 will 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**.

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

  The **Transport Manager > Configuration > Configuration Sets [Insert]** page will 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 the **Edit** button.

  The **Transport Manager > Configuration > Configuration Sets [Edit]** page opens. 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 4: Transport Manager Configuration Set Elements describes the fields on the **Transport Manager > Configuration > Configuration Set** pages.

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

Table 4: Transport Manager Configuration Set Elements

Element (* indicates required field)	Description	Data Input Notes
* Configuration Set Name	A name that uniquely identifies the SCTP Transport Manager Configuration Set.	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. T his 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
* Retransmit Minimum Timeout	The minimum amount of time to wait for an acknowledgment for a message sent. This value prevents the retransmit timeout from becoming too small in networks with a very short round-trip time.	Format: Numeric Range: 10 - 1000 msec This minimum value cannot be greater than the maximum value. Default: 120
* Retransmit Maximum Timeout	The maximum amount of time to wait for an acknowledgment for a message sent. This value places an upper bound on the exponential back-off algorithm used by SCTP for retransmission timing. After this retransmit interval is reached, retransmits will be sent at a constant rate until an ACK is received or the maximum attempt is reached.	Format: Numeric Range: 10-10000 msec This maximum value cannot be less than the minimum value. Default: 120
* Number of Retransmits Triggering Association Failure	Number of consecutive retransmits that will cause an SCTP Association to be marked as failed.	Format: Numeric Range: 1- 12

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

Element (* indicates required field)	Description	Data Input Notes
	Setting the heartbeat interval to zero disables heartbeating (not recommended).	
* Connection Retry Interval (sec)	The interval in seconds between connection attempts when the connection is unsuccessful.	Format: Numeric Range: 5 - 60 sec Default: 10
* Socket Send Buffer Size (bytes)	The socket send buffer size for outgoing SCTP messages. The send buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.	Format: Numeric Range: 65535 - 5000000 bytes Default: 2000000
* Socket Receive Buffer Size (bytes)	The socket receive buffer size for incoming SCTP messages. The receive buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.	Format: Numeric Range: 65535 - 5000000 bytes Default: 2000000
* SCTP Multihoming Mode	The SCTP Multihoming mode allows the user to configure remote host validation mode setting for SCTP. If the Adjacent Node is Multihomed for a specified Transport, Adjacent Node IP Addresses received in INIT/INIT-ACK chunk will be validated based on this parameter. SCTP Multihoming Mode = **Relax**: One of the IP Address received from Adjacent Node in an INIT/INIT-ACK chunk must match any of the configured Adjacent Node IP Address associated with that Transport. SCTP Multihoming Mode = **Match**: All of the IP Address received from Adjacent Node in an INIT/INIT-ACK chunk must	format: Pulldown list Range: Relax, Match Default: Relax

Element (* indicates required field)	Description	Data Input Notes
	match all of the configured Adjacent Node IP Address associated with that Transport.	

Viewing Transport Manager Configuration Sets

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

The **Transport Manager > Cofiguration > Configuration Sets** page appears with the Configuration Sets listed (for field definitions, see *Transport Manager Configuration Set elements*).

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.**

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

2. Click **Insert**.

    The **Transport Manager > Configuration > Configuration Sets [Insert]** page appears.

    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** 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 *Transport Manager Configuration Set elements* 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**.

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

2. Click **Edit** next to the Transport Manager Configuration Set you wish to modify.

   A **Configuration Set Name** cannot be changed.

   The **Transport Manager > Configuration > Configuration Sets [Edit]** page appears.

3. Make the desired changes. For field definitions, see *Transport Manager Configuration Set elements*.

4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - 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.**

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

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

3. Click **OK** to remove the Configuration Set.

The Transport Manager Configuration Set is removed from the list.

Transport Configuration

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 the **Edit** button.

  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 the **Status** button 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 5: 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 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 will host 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 will be bound to this Transport. If the MP Server is configured with more than one Signaling Network IP address, this field	Format: Pulldown list Range: IP Addresses of configured MP Servers

Element (* indicates required field)	Description	Data Input Notes
	allows selection of the desired IP address to be used for this Transport.	
MP Server IP Address (Secondary)	The Secondary IP Address hosted by the MP Server that will be bound to this Transport. If the MP Server is configured with more than one Signaling Network IP address, this field allows the Transport to be Multihomed.	Format: Pulldown list Range: IP Addresses of configured MP Servers
MP Server Listen Port	Listen port number of the MP Server for this Transport. This port will be used if the Transport Type is configured as "Listener". If the MP server hosts multiple "Listener" Transports, each Transport may listen on a different port.	Format: Text box Range: 1024 - 65535 Default: 5060
MP Server Initiate Port	Initiate port number of the MP Server for this Transport. This port will be used if the Transport Type is configured as "Initiator". If the MP server hosts multiple Transports, a unique initiate port number must be configured for each IP address.	Format: Text box Range: 1024 - 65535 Default: 2905
Adjacent Node	The Adjacent Node that will host 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.	Format: Pulldown list Range: IP Addresses of configured Adjacent Nodes

Element (* indicates required field)	Description	Data Input Notes
	This is a display-only field populated automatically when the Adjacent Node is selected.	
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

Viewing Transports

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

The **Transport Manager > Configuration > Transport** page appears with the configured Transports listed. For field definitions, see *Transport Configuration elements*.

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**.

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

2. Click **Insert**.

   The **Transport Manager > Configuration > Transport [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Transport Configuration elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Clack **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**.

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

2. Click **Edit**.

   The **Transport Manager > Configuration > Transport [Edit]** page appears.

3. Make the desired changes. For field definitions, see *Transport Configuration elements*.
4. Perform one of the following actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Clack **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**.

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

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

   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 prior to 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."

3. 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 > Transports>.**

   The **Transport Manager > Configuration > Transports** page appears.

2. Use the **Report** button 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 **Repot** 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]

================================================================================
<APPLICATION NAME>   T r a n s p o r t s   R e p o r t
================================================================================
Report Generated: Tue Jan 25 23:10:55 2011 UTC
From: Active Network OAM&P on host XGNO
Report Version: 1.0
User: guiadmin

--------------------------------------------------------------------------------

Transports Summary
------------------

Test

Signaling Network Element Name      : Sig_OAM
MP Server Hostname                  : XGMP
Adapter                             : SIP
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             : 2906
Adjacent Node                       : AdjServer
Adjacent Node IP Address (Primary)  : 100.100.100.100
Adjacent Node IP Address (Secondary) : 100.100.105.100
Adjacent Node Port                  : 3333
Configuration Set Name              : Default

------------------------------------------------------------------------

End of <APPLICATION NAME>  T r a n s p o r t s   R e p o r t
========================================================================
```

Chapter

4

Transport Maintenance

Topics:

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 the **Status** button on the **Transport Manager > Congiuration > 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 6: Transport Maintenance Elements describes the fields on the **Transport Manager > Maintenance > Transport** page.

Table 6: 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 will host the local end of the Transport.
Adapter	Identifies the Transport User for which the Transport is being added.
Transport Name	A name that uniquely identifies this Transport.
Transport Protocol	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:** Clicking on the "+" button in the Adjacent Node field shows the IP addresses for the Adjacent Node.
Admin State	The Administrative State of the Transport (the manual maintenance state that the network operator has specified).: Enabled, Disabled, or Blocked. See *Transport Admin State, Operational Status, and Operational Reason*.
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 *Transport Admin State, Operational Status, and Operational Reason*.
Up/Down Since	The date and time that the Transport came up or went down. For a newly added Transport, the time is when the Transport was configured. After a database restart, reboot, or initial startup before the Transports and Links are initialized, the value is the time when the application initialization runs.

Transport Admin State, Operational Status, and Operational Reason

Table 7: 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 7: 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

Admin State	Operational Status	Operational Reason	Description
			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 will not be sent afterwards.
	Down	Blocked	**M3UA:** SCTP Transport has been established, but it has been blocked for any M3UA traffic.

Viewing the Status of a Transport

The **Transport Manager > Maintenance > Transport** GUI page displays the Administrative State, Operational Status, and Operational Reason of configured Transports.

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

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 on the "+" button 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*.

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**.

   The **Transport Manager > Maintenance > Transport** page appears.

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

   The **Enable** button 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 will disregard the command if the Transport is already in the selected Administrative State.

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

   A confirmation message appears.

4. Click **OK** to confirm.

   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.
   • The **Enable** button 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**.

   The **Transport Manager > Maintenance > Transport** page appears.

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.

   The **Disable** button 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 will disregard the command if the Transport is already in the selected Administrative State.

4. Click **Disable**
   A confirmation message appears.

5. Click **OK** to confirm.
   If the Transport is successfully disabled,

   • The **Operational Status** field shows **Down**.
   • The **Admin State** field shows **Disabled**.

- The **Disable** button at the bottom of the page 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**.

   The **Transport Manager > Maintenance > Transport** page appears.

2. Click the **Pause updates** check box (lower right corner) so that 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 the **Block** button.

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

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

   A confirmation message appears.

5. Click **OK** to confirm.

   The **Operational Status** field shows **Blocked**.

   The **Admin state** column now indicates when the Transport transitioned into the **Blocked** status.

   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:

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

Use Case Overview

Table 8: Use Case Overview summarizes the main (but not all possible) use cases that involve the Transport Manager.

Table 8: 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 9: SS7+SCTP Multihomed Use Cases describes Transport Manager SS7+SCTP Multihomed Use Cases.

Table 9: SS7+SCTP Multihomed Use Cases

UC#	DESCRIPTION
1.	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 for both Relax and Match validation modes. PRE CONDITIONS: • 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) DESCRIPTION: • 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 will generate an INIT to the Adjacent Node containing both the local addresses configured in the association via its primary interface • Adjacent Node will respond 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 POST CONDITIONS • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged. ALTERNATE COURSE: • Validation fails and association is rejected. Refusal event is generated, refusal count is pegged, and alarm is raised.
2.	SCTP Multihomed Association Establishment - XSI1/XSI2 IP ports - Initiation received via primary IP port 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 . PRE CONDITIONS:

UC#	DESCRIPTION
	• 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) DESCRIPTION: • 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 will receive an INIT from the Adjacent Node containing both its local addresses via its primary interface • Association will respond 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. POST CONDITIONS • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged. ALTERNATE COURSE: • Validation fails and association is rejected. Refusal event is generated; refusal count is pegged.
3.	SCTP Multihomed Association Establishment - XSI1/XSI2 IP ports - Initiation sent via alternate IP port I nitrate and establish an outgoing SCTP multihomed association to the Adjacent Node via IP address marked as alternate for both Relax and Match validation modes. PRE CONDITIONS: • 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) DESCRIPTION: • 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 will generate an INIT to the Adjacent Node containing both the local addresses configured in the association via its alternate interface • Adjacent Node will respond with INIT-ACK containing both its local addresses

UC#	DESCRIPTION
	• Adjacent Node's addresses are successfully validated according to validation mode and rules in *SCTP Validation* • Establishment procedure continues. POST CONDITIONS • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged ALTERNATE COURSE: • Validation fails and association is rejected. Refusal event is generated, refusal count is pegged.
4.	SCTP Multihomed Association Establishment - XSI1/XSI2 IP ports - Initiation received via alternate IP port 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. PRE CONDITIONS: • 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) DESCRIPTION: • 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 will receive an INIT from the Adjacent Node containing both its local addresses via its alternate interface • Association will respond 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. . POST CONDITIONS • Association is accepted and established/normal. Both paths are established, and adapter traffic may now be exchanged. ALTERNATE COURSE: • Validation fails and association is rejected. Refusal event is generated, refusal count is pegged, and alarm is raised.

UC#	DESCRIPTION
5.	SCTP Multihomed Association Rejection - XSI1/XSI2 IP ports - DNS SCTP association is configured as multihomed and incoming INITs contain DNS names rather IPv4 addresses PRE CONDITIONS: • 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) DESCRIPTION: • 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 will receive an INIT from the Adjacent Node containing one or more addresses as Domain Names. • INIT is rejected. • Establishment procedure is halted. . POST CONDITIONS • Association is not accepted and remains in unestablished state. ALTERNATE COURSE: • None
6.	SCTP Multihomed Association - Primary Path Fail With all paths of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the primary path is failed. PRE CONDITIONS: • Multihomed association in established state, both paths established • Traffic is being exchanged with the Adjacent Node DESCRIPTION: • 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 POST CONDITIONS • Association remains established although in degraded/abnormal state • No loss of traffic occurred ALTERNATE COURSE: • None

UC#	DESCRIPTION
7.	SCTP Multihomed Association - Primary Path Restored
	With only the alternate path of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the primary path is restored.
	PRE CONDITIONS:
	• Multihomed association in established state, only the alternate paths established • Traffic is being exchanged with the Adjacent Node
	DESCRIPTION:
	• 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
	. POST CONDITIONS
	• Association remains established • No loss of traffic occurred
	ALTERNATE COURSE:
	• None
8.	SCTP Multihomed Association - Alternate Path Fail
	With all paths of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the alternate path is failed.
	PRE CONDITIONS:
	• Multihomed association in established state, both paths established • Traffic is being exchanged with the Adjacent Node
	DESCRIPTION:
	• The alternate path is failed • Event is generated indicating loss of path and Adjacent Node's alternate address is marked as unreachable
	POST CONDITIONS
	• Association remains established although in degraded/abnormal state • Traffic is unaffected
	ALTERNATE COURSE:
	• None
9.	SCTP Multihomed Association - Alternate Path Restored
	With only the primary path of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, the alternate path is restored.
	PRE CONDITIONS:
	• Multihomed association in established state, only the primary path established

UC#	DESCRIPTION
	• Traffic is being exchanged with the Adjacent Node DESCRIPTION: • The alternate path is restored • Alternate path is restored and Adjacent Node's alternate address is marked as reachable POST CONDITIONS • Association remains established • Traffic is unaffected ALTERNATE COURSE: • None
10.	SCTP Multihomed Association - Both Paths Failure With all paths of a multihomed SCTP association established and traffic being exchanged with the Adjacent Node, both paths are failed. PRE CONDITIONS: • Multihomed association in established state, both paths established DESCRIPTION: • 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 POST CONDITIONS • Association remains in down state ALTERNATE COURSE: • None
11.	SCTP Multihomed Association - Both Paths Restored With all paths of a multihomed SCTP association failed, both paths are restored. PRE CONDITIONS: • Multihomed association in established state, both paths established DESCRIPTION: • 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 POST CONDITIONS • Association remains in down state ALTERNATE COURSE:

UC#	DESCRIPTION
	• None

Glossary

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 provide the user 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

S

SCTP

Stream Control Transmission Protocol

An IETF transport layer protocol, similar to TCP that sends a message in one operation.

The transport layer for all standard IETF-SIGTRAN protocols.

SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

SS7

Signaling System #7

A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

T

T

Transport

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