Oracle® Communications Tekelec HLR Router

SS7/Sigtran User's Guide

910-6589-001 Revision B

February 2014

ORACLE®

Oracle® Communications SS7/Sigtran User's Guide

Table of Contents

Chapter 1: Introduction.....10

Purpose of this documentation.....11
Scope and Audience.....11
Documentation Admonishments.....11
Document Organization.....12
Customer Care Center.....12
Emergency Response.....14
Related Publications.....15
Locate Product Documentation on the Customer Support Site.....16

Chapter 2: SS7 configuration.....17

Connecting to a SOAM.....18
SS7 network configuration overview.....18
Service-impacting actions.....19
Adjacent Server Groups.....20
Adjacent Server Groups elements.....20
Viewing Adjacent Server Groups.....20
Filtering using the display filter.....21
Inserting an Adjacent Server Group.....21
Editing an Adjacent Server Group.....22
Deleting an Adjacent Server Group.....22
Local Signaling Points.....23
Local Signaling Points elements.....23
Point code formats.....24
Viewing Local Signaling Points.....25
Inserting a Local Signaling Point.....25
Editing a Local Signaling Point.....25
Deleting a Local Signaling Point.....26
Generating a report on Local Signaling Points.....26
Local SCCP Users.....27
Local SCCP Users elements.....27
Viewing Local SCCP Users.....28
Inserting a Local SCCP User.....28
Deleting a Local SCCP User.....29

Generating a report on Local SCCP Users....29
Viewing the status of Local SCCP Users....30
Remote Signaling Points....30
Remote Signaling Point elements....30
Viewing Remote Signaling Points....31
Inserting a Remote Signaling Point....31
Deleting a Remote Signaling Point....32
Generating a report on Remote Signaling Points....32
Viewing the status of a Remote Signaling Point....32
Remote MTP3 Users....33
Remote MTP3 Users elements....33
Viewing Remote MTP3 Users....34
Inserting a Remote MTP3 User....34
Deleting a Remote MTP3 User....34
Viewing the status of Remote MTP3 Users....35
Link Sets....35
Link Sets elements....36
Viewing Link Sets....37
Inserting a Link Set....38
Deleting a Link Set....38
Generating a report on Link Sets....38
Viewing the status of Link Sets....39
Links....39
Links elements....40
Viewing Links....40
Inserting a Link....41
Deleting a Link....41
Generating a report on Links....41
Viewing the status of a Link....42
Routes....42
Routes elements....42
Viewing Routes....43
Inserting a Route....44
Editing a Route....44
Deleting a Route....44
Generating a report on Routes....45
Viewing the status of Routes....45
SCCP Options....45
SCCP Options elements....45
Viewing SCCP Options....46
Editing an SCCP Option....47

MTP3 Options....47
MTP3 Options elements....47
Viewing MTP3 Options....48
Editing MTP3 Options....48
M3UA Options....48
M3UA Options elements....49
Viewing M3UA Options....49
Editing M3UA Options....49
Local Congestion Options....50
Local Congestion Options elements....50
Viewing Local Congestion Options....53
Capacity Constraint Options....53
Capacity Constraint Options elements....53
Viewing Capacity Constraint Options....55

Chapter 3: SS7 maintenance....56

The SS7 Maintenance menu....57
Color codes on the Maintenance pages....57
Local SCCP Users Maintenance....58
Local SCCP Users Maintenance elements....58
Viewing Local SCCP Users status....59
Enabling a Local SCCP User....59
Disabling a Local SCCP User....60
Remote Signaling Points Maintenance....60
Remote Signaling Points Maintenance elements....61
Viewing Remote Signaling Points status....62
About resetting the Network Status of the routes....62
Remote MTP3 Users Maintenance....63
Remote MTP3 Users Maintenance elements....63
Viewing Remote MTP3 Users status....65
About resetting the subsystem and point code status....65
Link Set Maintenance....66
Link Set Maintenance elements....66
Link Set Operational Status and Reason....67
Viewing Link Set status....68
Link Maintenance....68
Links Maintenance elements....68
Link Operational Status and Reason....69
Viewing Link status....70
Enabling a Link....70

Disabling a Link....71

Chapter 4: Command Line Interface....72

Command Import elements....73
Validating commands....73
Command Validation Results....74
Command Validation Results elements....76
Executing commands....77
Command Execution Results....78
Command Execution Results elements....81
Command line interface import file....82
CLI command structure....82
File format....83
Sample command scripts....83
Managed objects....83
Remote Signaling Points....84
Remote MTP3 Users....85
Link Sets....87
Links....90
Routes....91
Local SCCP Users....93

Glossary....96

List of Figures

Figure 1: Example of Command Validation Results file....74

Figure 2: Example of Command Execution Results file....78

Figure 3: Insert commands....83

Figure 4: Delete commands....83

Figure 5: Edit commands....83

List of Tables

Table 1: Admonishments....11

Table 2: High-level Overview of SS7 Configuration....18

Table 3: Adjacent Server Groups Elements....20

Table 4: Local Signaling Points Elements....23

Table 5: Local SCCP Users Elements....27

Table 6: Remote Signaling Points Elements....30

Table 7: Remote MTP3 Users Elements....33

Table 8: Link Sets Elements....36

Table 9: Links Elements....40

Table 10: Routes Elements....43

Table 11: SCCP Options Elements....46

Table 12: MTP3 Options Elements....47

Table 13: M3UA Options Elements....49

Table 14: Alarm Severity for Onset and Abatement Thresholds....50

Table 15: Local Congestion Options Elements....50

Table 16: Capacity Constraint Options Elements....54

Table 17: SS7 Constraint Values....54

Table 18: Maintenance Page Color Codes....57

Table 19: Local SCCP Users Maintenance Elements....58

Table 20: Remote Signaling Points Maintenance Elements....61

Table 21: Remote MTP3 Users Maintenance Elements....64

Table 22: Link Sets Maintenance Elements....66

Table 23: Links Maintenance Elements....68
Table 24: Command Import Elements....73
Table 25: Command Validation Results....77
Table 26: Command Execution Results....81
Table 27: CLI command values....82
Table 28: Allowed operations....84
Table 29: Required Attributes....84
Table 30: Optional Attribute....85
Table 31: Allowed operations....86
Table 32: Required attributes....86
Table 33: Optional Attribute....87
Table 34: Allowed operations....87
Table 35: Required Attributes....88
Table 36: Optional Attributes....88
Table 37: Allowed operations....90
Table 38: Required Attributes....90
Table 39: Optional Attributes....91
Table 40: Allowed operations....92
Table 41: Required attributes....92
Table 42: Optional Attributes....93
Table 43: Allowed operations....94
Table 44: Required Attributes....94
Table 45: Optional Attributes....95

Chapter 1

Introduction

Topics:

- *Purpose of this documentation.....11*
- *Scope and Audience.....11*
- *Documentation Admonishments.....11*
- *Document Organization.....12*
- *Customer Care Center.....12*
- *Emergency Response.....14*
- *Related Publications.....15*
- *Locate Product Documentation on the Customer Support Site.....16*

Introduction provides a content overview of this guide with a brief summary about incidents, notifications, and the ID ranges for alarms and events. It also includes Tekelec contact information and how to locate product documentation on the Tekelec Customer Support site.

Purpose of this documentation

This documentation:

- Gives a conceptual overview of the application's purpose, architecture, and functionality
- Describes the pages and fields on the application GUI (Graphical User Interface)
- Provides procedures for using the application interface
- 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 managing a SS7/Sigtran system.

Documentation Admonishments

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

Table 1: Admonishments

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

Document Organization

This *SS7/Sigtran User Guide* is organized into the following chapters:

- *Introduction* contains general information about the *SS7/Sigtran User Guide*, the scope, audience, and organization of this document, how to contact Tekelec for assistance, and how to locate documentation on the Customer Support Site.
- *SS7 configuration* describes the SS7 menu that provides an interface for S7 network status, configuration, and maintenance.
- *SS7 maintenance* describes the SS7 maintenance menu, which provides maintenance and troubleshooting capabilities on Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, Links, and Associations.
- *Command Line Interface* describes a method for bulk loading SS7 configuration data and for validating and executing command scripts.

Customer Care Center

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

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

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

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

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

  TAC Regional Support Office Hours:

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

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

  Phone:

+1-919-460-2150

TAC Regional Support Office Hours (except Brazil):

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

- **Argentina**

  Phone:

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

- **Brazil**

  Phone:

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

  TAC Regional Support Office Hours:

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

- **Chile**

  Phone:

  1230-020-555-5468

- **Colombia**

  Phone:

  01-800-912-0537

- **Dominican Republic**

  Phone:

  1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552

- **Venezuela**

  Phone:

  0800-176-6497

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

Regional Office Hours:

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

- **Signaling**

  Phone:

  +44 1784 467 804 (within UK)

- **Software Solutions**

  Phone:

  +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

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

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

Related Publications

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

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

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

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

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

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

HLR Router Alarms, KPIs, and Measurements Reference Guide provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information. Available from the application GUI and on the documentation DVD.

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

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

Locate Product Documentation on the Customer Support Site

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

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

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

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

Chapter 2

SS7 configuration

Topics:

- *Connecting to a SOAM.....18*
- *SS7 network configuration overview.....18*
- *Service-impacting actions.....19*
- *Adjacent Server Groups.....20*
- *Local Signaling Points.....23*
- *Local SCCP Users.....27*
- *Remote Signaling Points.....30*
- *Remote MTP3 Users.....33*
- *Link Sets.....35*
- *Links.....39*
- *Routes.....42*
- *SCCP Options.....45*
- *MTP3 Options.....47*
- *M3UA Options.....48*
- *Local Congestion Options.....50*
- *Capacity Constraint Options.....53*

The **SS7/Sigtran** menu hosts the Signaling Network Interface for EAGLE XG applications. The **SS7/Sigtran** menu provides an interface for SS7 network status, configuration, and maintenance. The interface supports standards-based M3UA, MTP3, and SCCP signaling.

Connecting to a SOAM

If a user connects to a SOAM, the SS7 configuration pages are displayed. This includes the **Insert**, **Edit**, and **Delete** links on the page. If a page has **Report** and **Status** links, those links remain also enabled.

If a user is connected to an SOAM, data specific to the Signaling Network Element of the connected SOAM is shown.

Note that some pages are independent of the Signaling Network Element. Such pages show data pertaining to the system rather than to the Signaling Network Element. Those pages are as follows:

- **Remote Signaling Points** page
- **Remote MTP3 Users** page

SS7 maintenance is allowed from the SOAM. All maintenance links are active when the user is connected to the SOAM.

SS7 network configuration overview

The options on the **SS7/Sigtran>Configuration** menu are used to configure the SS7 networking. Each menu item aligns with an SS7 network configuration task. The options appear on the menu in the order that SS7 configuration must be performed. This section explains the use of the configuration options.

Any fields that require unique data for SS7/Sigtran configuration must be unique within the site but not across sites.

The table provides a high-level view of the SS7 network configuration and identifies the menu option that supports each task.

To bulk-load configuration data, see *Command Line Interface*.

If you are unfamiliar with any of the network components in the table, please use the links provided or consult the glossary.

Table 2: High-level Overview of SS7 Configuration

#	Task	Menu Option
1	Create signaling Network Element.	**Configuration>Network Elements**
2	Add MP and SOAM servers to the signaling Network Element.	**Configuration>Servers**
3	Create server groups for the MP servers.	**Configuration>Server Groups**
4	Create Adjacent Server Groups for each IP Signaling point that the EAGLE XG application will connect to. An example would be the EAGLE 5 ISS IP Signaling Gateway.	**SS7/Sigtran>Configuration>Adjacent Server Groups** (see *Adjacent Server Groups*)

#	Task	Menu Option
5	Create Local Signaling Points for each point code that identifies an MP server for the EAGLE XG application.	**SS7/Sigtran>Configuration>Local Signaling Points** (see *Local Signaling Points*)
6	Create a Local SCCP User for each SS7 application hosted by Tekelec MP servers.	**SS7/Sigtran>Configuration>Local SCCP Users** (see *Local SCCP Users*).
7	Create remote signaling points for each adjacent signaling point that the EAGLE XG application will connect to and each remote destination that the EAGLE XG will route to.	**SS7/Sigtran>Configuration>Remote Signaling Points** (see *Remote Signaling Points*)
8	Create Remote MTP3 Users for each Subsystem Number that the EAGLE XG application will route messages to.	**SS7/Sigtran>Configuration>Remote MTP3 Users** (see *Remote MTP3 Users*)
9	Create a Link Set for each LSP and for each Adjacent RSP.	**SS7/Sigtran>Configuration>Link Sets** (see *Link Sets*)
10	Create Links that reference each Association and Link Set.	**SS7/Sigtran>Configuration>Links** (see *Links*)
11	Create routes for each RSP and link set.	**SS7/Sigtran>Configuration>Routes** (see *Routes*)
12	Edit the SCCP, MTP3, and M3UA options as desired.	**SS7/Sigtran>Configuration>SCCP Options** (see *SCCP Options*) **SS7/Sigtran>Configuration>MTP3 Options** (see *MTP3 Options*) **SS7/Sigtran>Configuration>M3UA Options** (see *M3UA Options*)
13	Enable the LSUs.	**SS7/Sigtran/Maintenance>Local SCCP Users** (see *Local SCCP Users*)
14	Enable the Links.	**SS7/Sigtran>Maintenance>Links** (see *Link Maintenance*)

Service-impacting actions

The actions on the **SS7/Sigtran>Configuration** menu have built-in rules that prevent service impact from configuration changes. For example, the software will not let you delete an Adjacent Server that is referenced by an Adjacent Server Group. You would get an error message, and the delete action would fail. You would need to remove the Adjacent Server from the Adjacent Server Group prior to deleting the Adjacent Server. Such rules are discussed in the documentation for each **SS7/Sigtran>Configuration** menu option in a section titled "*Safeguards to prevent service impact from configuration changes*."

Adjacent Server Groups

An Adjacent Server Group is 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 RSP is associated with one Adjacent Server Group.

The Adjacent Server Groups page provides a means to group Adjacent Servers that belong to the same signaling gateway. For example, an Adjacent Server Group can refer to an Eagle 5 ISS STP with which this application is associated.

Safeguards to prevent service impact from configuration changes:

- The software will not allow you to remove a server from an Adjacent Server Group if the server is referenced by an Association.
- The software will not allow you to delete an Adjacent Server Group that is referenced by an RSP.

Adjacent Server Groups elements

This information appears on the **Adjacent Server Groups** page:

Table 3: Adjacent Server Groups Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Adjacent Server Group is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required.
Adjacent Server Group Identifier	Unique identifier used to label an Adjacent Server Group.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required.
Adjacent Server Group Member(s)	The list of Adjacent Servers that make up the Adjacent Server Group. Note that an Adjacent Server can be a member of only one Adjacent Server Group.	Range: 1 to 16 entries. This field is required.

Viewing Adjacent Server Groups

Use this procedure to view the defined Adjacent Server Groups.

Select **SS7/Sigtran>Configuration>Adjacent Servers Groups.**

The Adjacent Server Groups page appears. For field definitions, see *Adjacent Server Groups elements*.

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

The page appears with the defined Adjacent Server Groups listed.

Filtering using the display filter

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

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

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

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

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

   The selected operator appears in the field.

3. Enter a value in the value field.

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

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

Records are displayed according to the specified criteria.

Inserting an Adjacent Server Group

1. Select **SS7/Sigtran>Configuration>Adjacent Server Groups**.

   The **Adjacent Server Groups** page appears. For field definitions, see *Adjacent Server Groups elements*.

2. Click **Insert**.

   The **Insert Adjacent Server Groups** page appears.

3. Select a **Signaling Network Element Name** from a pulldown list or in the case of SOAM, this option is grayed out.
4. Enter an Adjacent Server Group identifier.
5. To add an Adjacent Server, click the Adjacent Server name you want to add from the **Unassigned Adjacent Servers** list. You can select multiple individual items by holding down **ctrl** while clicking the item (**ctrl-click**). You can select all items by clicking **Add All**. To select a range, select **shift-click**.

   Note: If you need to add an Adjacent Server and no Adjacent Servers are available, you must first define one. Once you have defined an Adjacent Server, the **Unassigned Adjacent Servers** field will be populated.

6. Perform one of these actions:

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

The Adjacent Server Group is added.

Editing an Adjacent Server Group

The **Edit** operation lets you add or remove an Adjacent Server from an Adjacent Server Group.

The software will not allow you to remove a server from an Adjacent Server Group if the server is referenced by an Association.

1. Select **SS7/Sigtran>Configuration>Adjacent Server Groups**

   The **Adjacent Server Groups** page appears.

2. Click **Edit** next to the Adjacent Server Group you want to modify.

   The **Edit Adjacent Server Groups** page appears.

3. If you want to add or remove an Adjacent Server, perform these steps:

   - To add an Adjacent Server, click the name in the **Unassigned Adjacent Servers** list and click **Add**. You can select multiple individual items by holding down **ctrl** while clicking the item (**ctrl-click**). You can select all items by clicking **Add All**. To select a range, select **shift-click.**

     Note: If you need to add an Adjacent Server and no Adjacent Servers are available, you must first define one. Once you have defined an Adjacent Server, the **Unassigned Adjacent Servers** field is populated.

   - To remove an Adjacent Server from the Adjacent Server Group, click the name in the **Adjacent Servers in this Adjacent Server Group** list. You can select more than one Adjacent Server by holding down **ctrl** while clicking each name or clicking **Remove All**. To select a range, select **shift-click.**

4. Perform one of these actions

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

The Adjacent Server Group is updated.

Deleting an Adjacent Server Group

Deleting an Adjacent Server Group removes the group from the network configuration.

The software will not allow you to delete an Adjacent Server Group that is referenced by an RSP. If necessary, perform *Deleting a Remote Signaling Point* to remove the RSP.

1. Select **SS7/Sigtran>Configuration>Adjacent Server Groups**.

   The **Adjacent Server Groups** page appears.

2. Click **Delete** in the row of the Adjacent Server Group you want to remove.

   A delete confirmation message appears.

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

The Adjacent Server Group is deleted from the table.

Local Signaling Points

A Signaling Point is a set of signaling equipment represented by a unique point code within an SS7 domain (for example, ANSI, ITU-I, ITU-N). An LSP (Local Signaling Point) is a logical element representing an SS7 Signaling Point assigned to an MP server group.

A Point Code is a unique MTP3 (Message Transfer Part 3) address in a SS7 network. An LSP is uniquely identified by a point code and an SS7 domain.

The LSP assigns the SS7 identity to the MP server group. An LSP has an SS7 domain (ANSI, ITU-I, ITU-N) and a true point code. The LSP may optionally be assigned up to two CPCs (Capability Point Codes), which are point codes that can be shared with other LSPs. The LSP also has assigned a server group that hosts the point code.

The **Local Signaling Points** table contains a row for every point code that represents an MP server group.

Safeguards to prevent service impact from configuration changes:

- The software will not let you remove a server group from an LSP that is referenced by a Link Set.
- The software will not let you remove a Capability Point Code from an LSP that is referenced by a Link Set.
- The software will not let you delete an LSP that is referenced by a Link Set.

Local Signaling Points elements

This information appears on the **Local Signaling Points** page:

Table 4: Local Signaling Points Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Local Signaling Point is being added.	Format: Pulldown list Range: All configured LSPs. This field is required.
SS7 Domain	The SS7 domain in which the node resides.	Format: Pulldown list Range: ANSI, ITU International, or ITU National This field is required.
MTP True Point Code	The MTP point code that identifies this LSP. Only one LSP can have this MTP True point code.	Format: Text field requires point code format (see *Point code formats*). This field is required.

Element	Description	Data Input Notes
MTP Capability Point Code(s)	The MTP capability point code if this LSP shares a point code with one or more other LSPs.	Format: Checkbox and text field. The checkbox(es) must be checked to enable the field. The text field requires point code format (see *Point code formats*). The MTP Capability Point Code(s) cannot exist in the system as an MTP True Point Code. This field is optional unless the checkbox(es) are checked. If the checkbox(es) are checked, the text field(s) are required.
Local Signaling Point Name	Unique, case-sensitive name of the Local Signaling Point.	The default name is auto-generated and populated. You can overwrite the default name. Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required.
Server Group(s)	Server Groups that serve this LSP.	Range: 1 entry This field is required.

Point code formats

A point code is a unique (MTP3) address in an SS7 network. This application supports these point code formats based on the selected SS7 domain:

- **ANSI Point Code**

  Format: NNN-NNN-NNN

  Range: Point code must comply with ANSI T1.111.8.

- **ITU International Point Code**

  Format: J-NNN-J

  Range J can range from 0-7. NNN can range from 0-255.

- **ITU National Point Code**

  Format: NNNNN

  Range: NNNNN can range from 0-16383

Viewing Local Signaling Points

Use this procedure to view the configured LSPs.

Select **SS7/Sigtran>Configuration>Local Signaling Points.**

The L**ocal Signaling Points** page appears. For field definitions, see *Local Signaling Points elements*.

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

The page appears with the configured LSPs listed.

Inserting a Local Signaling Point

Use this procedure to insert an LSP.

1. Select **SS7/Sigtran>Configuration>Local Signaling Points.**

   The **Local Signaling Points** page appears.

2. Click **Insert**.

   The Insert Local Signaling Points page appears.

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

The LSP is added to the configuration.

Editing a Local Signaling Point

The **Edit** operation lets you add or remove the MTP Capability Point Code and the assigned Server Group from an LSP configuration.

Use this procedure to edit an LSP.

1. Select **SS7/Sigtran>Configuration>Local Signaling Points.**

   The **Local Signaling Points** page appears.

2. Click **Edit**.

   The **Edit Local Signaling Points** page appears.

3. (Optional) To delete an MTP Capability Point Code from the LSP, uncheck the checkbox.

   The software will not allow you remove a Capability Point Code from an LSP that is referenced by a Link Set. If necessary, perform *Viewing the status of Link Sets* to remove the reference.

4. (Optional) To add an MTP Capability Point Code, check the checkbox and then enter the MTP Capability Point Code as described in *Local Signaling Points elements*.

5. (Optional) To add a Server Group, click the name in the **Unassigned Server Group** list and click **Add**. You can select more than one by holding down **ctrl** while clicking a name or clicking **Add All**. Use **shift-click** to select a range.
6. (Optional) To remove a Server Group, click the name in the **Server Groups included in this Local Signaling Point** list and click **Remove**. You can select more than one by holding down **ctrl** while clicking a name or clicking **Remove All**.

   The software will not let you remove a server group from an LSP that is referenced by a Link Set. If appropriate, perform *Viewing the status of Link Sets*.

7. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The LSP is updated.

Deleting a Local Signaling Point

Deleting an LSP removes the LSP from the SS7 network configuration.

The software will not let you delete an LSP that is referenced by a Link Set. If appropriate, perform *Viewing the status of Link Sets*.

1. Select **SS7/Sigtran>Configuration>Local Signaling Points.**

   The **Local Signaling Points** page appears.

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

   A delete confirmation message appears.

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

The LSP is deleted from the configuration.

Generating a report on Local Signaling Points

1. Select **SS7/Sigtran>Configuration>Local Signaling Points.**

   The **Local Signaling Points** page appears.

2. Perform one of these actions:
   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Local SCCP Users

An LSU (Local SCCP User) is an application configured with a subsystem number to handle `rt-on-ssn` traffic for a local signaling point code hosted on an MP server.

Adding, deleting, or changing the status of an LSU affects the routing to configured Local SCCP Users. SCCP is notified when an operator creates a local subsystem via the GUI and assigns a Local SCCP User to the local subsystem. This assignment entry is added to SCCP's internal database with a default status of `Disabled`. The assignment enables SCCP to track the status of locally provisioned LSUs for messages that are routed on the SSN.

The Local SCCP Users table contains a row for each SS7 application hosted by Tekelec MP servers. The fields in this table are used to indicate which SSN is associated with an application.

Safeguards to prevent service impact from configuration changes:

- The software will not let you insert an LSU if an identical LSU already exists with a Subsystem Number corresponding to the same LSP (point code and domain).
- The software will prompt you to disable an LSU prior to its deletion or to confirm that you want to force its deletion if the LSU state reported by the MP server is not **Disabled** or if the MP server is unable to determine the state of the LSU. Deletion of an LSU that is not disabled may result in a loss of signaling data.

Local SCCP Users elements

This information appears on the **Local SCCP Users** page:

Table 5: Local SCCP Users Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element Name to which the Local SCCP User is being added.	Format: Pulldown list. of all provisioned Signaling Network Elements. Range: 1 entry This field is required.
SSN	The specific subsystem number served by this Local SCCP User. This field is used to route incoming messages to the application hosting this SSN.	Format: Numeric Range: 2 - 254 This field is required.
(Local Signaling Point) Point Code	The Local Signaling Point Code associated with this Local SCCP User. Local signaling points are defined at **SS7/Sigtran>Configuration>Local Signaling Points** (see *Local Signaling Points*).	Format: Pulldown list of all configured LSPs associated with the selected **Signaling Network Element Name**. Range: 1 entry This field is required.

Element	Description	Data Input Notes
(Local Signaling Point) SS7 Domain	The SS7 domain of the selected Local Signaling Point.	Format: View only. This field is populated when the **(Local Signaling Point) Point Code** is selected.
Application Name	Application Name to configure as the Local SCCP User.	Format: Pulldown list.of all configured applications. If there is only one application configured, the **Application Name** appears in this field as a view-only entry. Range: 1 entry This field is required.

Viewing Local SCCP Users

Use this procedure to view the configured LSUs.

Select **SS7/Sigtran>Configuration>Local SCCP Users.**

The **Local SCCP Users** page appears. For field definitions, see *Local SCCP Users elements*.

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

The page appears with the configured LSUs listed.

Inserting a Local SCCP User

Use this procedure to insert an LSU.

The software will not let you add an LSU if an identical LSU already exists with an SSN corresponding to the same LSP (point code and domain).

1. Select **SS7/Sigtran>Configuration>Local SCCP Users.**

   The **Local SCCP Users** page appears.

2. Click **Insert**.

   The **Insert Local SCCP Users** page appears.

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

The LSU is added to the configuration. By default, the LSU is in the **Disabled** state. To enable the LSU, see *Enabling a Local SCCP User*.

Deleting a Local SCCP User

Deleting an LSU removes the LSU from the SS7 network configuration.

Caution: Deletion of an LSU that is in the **Enabled** state may result in the loss of signaling data. To disable an LSU, see *Disabling a Local SCCP User*.

1. Select **SS7/Sigtran>Configuration>Local SCCP Users.**

   The **Local SCCP Users** page appears.

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

   A delete confirmation message appears.

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

   If the LSU is **Enabled**, an additional confirmation message appears.

4. Perform one of the following actions if the LSU is in the **Enabled** state:

   - If the confirmation message says that the LSU state reported by the MP server is not disabled, click **Cancel** to close the confirmation message and then disable the LSU.
   - If the confirmation message says that the MP server cannot determine the LSU state, click **Cancel** to close the confirmation message and look on the GUI main menu under **Status & Manage>Servers** to investigate.
   - On either confirmation message, click **OK** to force the deletion of the LSU.

     

     Caution: Deletion of an LSU that is **Enabled** may result in the loss of signaling data. See *Disabling a Local SCCP User* to disable the LSU.

The LSU is removed from the SS7 network configuration.

Generating a report on Local SCCP Users

1. Select **SS7/Sigtran>Configuration>Local SCCP Users.**

   The **Local SCCP Users** page appears.

2. Perform one of these actions:

   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Viewing the status of Local SCCP Users

The **Status** link launches the **Local SCCP Users Maintenance** page. The status information is the same information shown under **SS7/Sigtran>Maintenance>Local SCCP Users** (see *Viewing Local SCCP Users status*).

Use one of the following methods to access status information from the **SS7/Sigtran>Configuration>Local SCCP Users** menu:

1. Select **SS7/Sigtran>Configuration>Local SCCP Users.**

   The **Local SCCP Users** page appears.

2. Perform one of these actions:

   - Click **Status** next to an entry in the table to view the status of the entry.
   - Click the **Status** link at the bottom of the table to view the status of all entries.

The **Local SCCP Users Maintenance** page appears in a browser window.

Remote Signaling Points

An RSP (Remote Signaling Point) represents an SS7 network node (point code) that signaling must be sent to from an EAGLE XG node. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.

An Adjacent Server Group is configured if the remote signaling point is an *adjacent* remote signaling point. An STP to which an EAGLE XG node is connected via an Association is an adjacent RSP.

The **Remote Signaling Points** table must contain a row for every point code that is directly connected to the SS7 application and any remote destination that the SS7 application originates messages toward.

The **Remote Signaling Points** table provides a link to the **Remote Signaling Points Maintenance** page where you can view the status of each configured RSP. You can also manually reset the network status of an RSP.

Safeguards to prevent service impact from configuration changes:

- The software will not allow you to delete an RSP that is referenced by a Remote MTP3 User, a Link Set, or a Route.

Remote Signaling Point elements

This information appears on the **Remote Signaling Points** page:

Table 6: Remote Signaling Points Elements

Element	Description	Data Input Notes
SS7 Domain	The SS7 domain in which the RSP resides.	Format: Pulldown list

Element	Description	Data Input Notes
		Range: ANSI, ITU International, or ITU National This field is required.
MTP Point Code	The unique MTP point code that identifies this RSP. Only one RSP can have this MTP point code.	Text field requires point code format (see *Point code formats*). This field is required.
Remote Signaling Point Name	An optional name that uniquely identifies the Remote Signaling Point. RSP names are case sensitive. If this field displays dashes, it indicates that a name has not been configured for this RSP.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is optional.
Adjacent Server Group	The Adjacent Server Group associated with this RSP. Populate this field if this RSP represents an Adjacent Server. An Adjacent Server Group can be referenced by more than one RSP. An RSP, however, can reference one and only one Adjacent Server Group.	Format: Pulldown list Range: All configured Adjacent Server Groups. Default: None (this RSP will not be used to signal to an Adjacent Server). This field is optional.

Viewing Remote Signaling Points

Use this procedure to view the configured RSPs.

Select **SS7/Sigtran>Configuration>Remote Signaling Points.**

The **Remote Signaling Points** page appears. For field definitions, see *Remote Signaling Point elements*.

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

The **Remote Signaling Points** page appears listing all of the configured RSPs.

Inserting a Remote Signaling Point

1. Select **SS7/Sigtran>Configuration>Remote Signaling Points.**

   The **Remote Signaling Points** page appears.

2. Click **Insert**.

   The **Insert Remote Signaling Points** page appears.

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

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

The RSP is added.

Deleting a Remote Signaling Point

Deleting an RSP removes the RSP from the SS7 network configuration.

The software will not allow you to delete an RSP that is referenced by a Remote MTP3 User, a Link Set, or a Route. If necessary, perform *Deleting a Remote MTP3 User*, *Viewing the status of Link Sets*, or *Deleting a Route* prior to attempting this procedure.

1. Select **SS7/Sigtran>Configuration>Remote Signaling Point**.

   The **Remote Signaling Point** page appears.

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

   A delete confirmation message appears.

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

The Remote Signaling Group is deleted from the table.

Generating a report on Remote Signaling Points

1. Select **SS7/Sigtran>Configuration>Remote Signaling Points.**

   The **Remote Signaling Points** page appears.

2. Perform one of these actions:

   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

The report is displayed in a browser window.

Viewing the status of a Remote Signaling Point

The **Status** link launches the **Remote Signaling Points Maintenance** page. The status information is the same information shown under **SS7/Sigtran>Maintenance>Remote Signaling Points** (see *Remote Signaling Points Maintenance*).

Use one of the following methods to access status information from the **SS7/Sigtran>Configuration** menu:

1. Select **SS7/Sigtran>Configuration>Remote Signaling Points.**

   The **Remote Signaling Points** page appears.

2. Perform one of these actions:

- Click **Status** next to an entry in the table to view the status of the entry.
- Click the **Status** link at the bottom of the table to view the status of all entries.

The **Remote Signaling Points Maintenance** page is displayed in a browser window.

Remote MTP3 Users

An RMU (Remote MTP3 User) represents a remote SCCP subsystem to which the Signaling Network Interface forwards signaling. When a message is forwarded from an MSC to an EAGLE XG node, an RMU must be configured for the subsystem on the EAGLE XG node.

There are two configuration scenarios for remote subsystems to which only service messages will be sent. A service message is a failure indication such as UDTS and XUDTS.

- If an MP must route signaling for UDT, XUDT, UDTS, or XUDTS to an RMU (i.e., remote SCCP peer), then an RMU must be configured for that remote SCCP subsystem.
- For a remote SCMG (SCCP Management) subsystem, it is not necessary or possible to create an RMU. SCCP Management uses subsystem 1 instead. Subsystem 1 is automatically created at the time the message is forwarded.

If an RMU exists, the subsystem status is tracked and used for routing SS7 messages (including service messages).

STPs generally do not have subsystems and therefore do not need RMUs. An exception would be an application such as LNP (Local Number Portability) that can be hosted on an STP.

The **Remote MTP3 Users** table contains an entry for each MTP3 user to which SS7 SCCP signaling is sent, or for which status tracking is desired. The fields in this table are used to populate the called party address parameters.

The **Remote MTP3 Users** table also provides a link to the **Remote MTP3 Users Maintenance** page where you can view the status of each configured RMU.The GUI also provides an option to reset the subsystem and point code status of an RMU.

Safeguards to prevent service impact from configuration changes:

- Not applicable.

Remote MTP3 Users elements

This information appears on the **Remote MTP3 Users** page:

Table 7: Remote MTP3 Users Elements

Element	Description	Data Input Notes
Remote Point Code	The Remote Point Code configured in the Remote Signaling Point associated with this Remote MTP3 User. Remote Signaling Points are defined at	Format: Pulldown list All configured Remote Signaling Points. This field is required.

Element	Description	Data Input Notes
	SS7/Sigtran>Configuration>Remote Signaling Points.	
SS7 Domain	The SS7 domain of the selected Remote Signaling Point.	Format: This is a display-only field populated when a Remote Signaling Point is selected.
Remote SSN	The specific subsystem number to track the status of the RMU. The combination of point code and SSN must be unique.	Format: Numeric Range: 2-254 This field is required.
Remote MTP3 User Name	An optional name that uniquely identifies the RMU. An RMU must be created for each MTP3 user whose status should be tracked by SCCP. The RMU name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Viewing Remote MTP3 Users

Select **SS7/Sigtran>Configuration>Remote MTP3 Users.**

The **Remote MTP3 Users** page appears. For field definitions, see *Remote MTP3 Users elements*.

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

The page appears with the configured RMUs listed.

Inserting a Remote MTP3 User

1. Select **SS7/Sigtran>Configuration>Remote MTP3 Users.**

   The **Remote MTP3 Users** page appears.

2. Click **Insert** .

   The **Insert Remote MTP3 Users** page appears.

3. Populate the fields with data. For field definitions, see *Remote MTP3 Users elements*.
4. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The RMU is added.

Deleting a Remote MTP3 User

1. Select **SS7/Sigtran>Configuration>Remote MTP3 Users**.

The **Remote MTP3 Users** page appears.

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

   A delete confirmation message appears.

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

The RMU is deleted from the database and no longer appears in the table.

Viewing the status of Remote MTP3 Users

The **Status** link launches the **Remote MTP3 Users Maintenance** page. The status information is the same information shown under **SS7/Sigtran>Maintenance>Remote MTP3 Users** (see *Remote MTP3 Users Maintenance*).

Use one of the following methods to access status information from the **SS7/Sigtran>Configuration** menu:

1. Select **SS7/Sigtran>Configuration>Remote MTP3 Users.**

   The **Remote MTP3 Users** page appears.

2. Perform one of these actions:

   - Click **Status** next to an entry in the table to view the status of the entry.
   - Click the **Status** link at the bottom of the table to view the status of all entries.

The **Remote MTP3 Users Maintenance** page is displayed in a browser window.

Link Sets

A Link Set represents a logical signaling connection from one local point code (LSP) to one adjacent remote point code (adjacent RSP).

A Link Set can span Associations. For example, an STP point code can be distributed across multiple servers such as Eagle 5 ISS E5-ENET cards. A Link Set cannot span MP servers because each MP server has its own point code.

A Link Set is typically configured for each combination of LSPs and adjacent RSPs with these parameters specified:

- The point code (the True Point Code or Capabililty Point Code) from the LSP that this Link Set serves.
- The adjacent RSP.
- (Optional) the routing context.

The **Link Sets** page lists Link Sets for each combination of Local Signaling Point and adjacent Remote Signaling Point.

The **Links Sets** page also provides a link to the **Link Sets Maintenance** page where you can view the status of each configured Link Set.

Safeguards to prevent service impact from configuration changes:

- If the SS7 domain of the LSP differs from the SS7 domain of the Adjacent Remote Signaling Point, the software will not allow you to add the Link Set.
- The software will not allow you to delete a Link Set that is referenced by a Link or a Route.

Link Sets elements

This information appears on the Link Sets page:

Table 8: Link Sets Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Link Set is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required.
Link Set Name	A name that uniquely identifies this Link Set. The Link Set name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required.
Mode	Defines the desired relationship between the local and remote peer for this Link Set. The mode specifies whether the Message Processor implements client or server procedures for session management. In this release, one mode is supported: **AS (Application Server) to SG (Signaling Gateway)**. The local side is the client; the remote side is the server. The local side has LMU and LSP; the remote side has RSP and optionally RMU.	Format: Pulldown list Select **AS->AG** if the local side of the connection is an Application Server and the remote side is a Signaling Gateway. Default: AS->AG This field is required.
Local Signaling Point	Specifies the LSP served by this Link Set. Each Local Signaling Point entry is a hyperlink to the Local Signaling Point table filtered by this LSP.	Format: Pulldown list Range: All configured LSPs. This field is required.
SS7 Domain	The SS7 domain of the selected Local Signaling Point.	Format: This is a display-only field populated when a Local Signaling Point is selected.

Element	Description	Data Input Notes
LSP Point Code	The point code of the selected Local Signaling Point to be served by this Link Set.	Format: Pulldown list A selection of **All** means that the Link Set will accept signaling destined for the selected Local Signaling Point's True Point Code or Capability Point Code, if one is assigned. Default: All This field is required.
Adjacent Remote Point Code	The point code of the Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway to be served by this Link Set. Each entry is a hyperlink to the Remote Signaling Point table filtered by this Adjacent Remote Point Code.	Format: Pulldown list Range: The list is based on the domain of selected **Local Signaling Point**. This field is required.
Assign Routing Context (appears on Insert Link Set page only)	Indicates whether a Routing Context applies to this Link Set. A Routing Context must be specified if links from this Link Set will share an association with links from at least one other Link Set.	Format: Pulldown list Range: Yes, No Select **Yes** if a Routing Context Applies. If you select **No**, the Routing Context field is cleared and disabled. Default: No
Routing Context	Message parameter used to uniquely identify the application context. This value is only used if Assign Routing Context is set to **Yes**. This Routing Context must be configured to match the Routing Context value configured for this Link Set at the signaling gateway.	Format: Numeric Range: 32-bit unsigned Default: First unused integer value greater than zero.

Viewing Link Sets

Select **SS7/Sigtran>Configuration>Link Sets**.

The **Link Sets** page appears. For field definitions, see *Link Sets elements* .

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

The page appears with the configured Link Sets listed.

Inserting a Link Set

1. Select **SS7/Sigtran>Configuration>Link Sets**.

   The **Link Sets** page appears.

2. Click **Insert**.

   The **Insert Link Sets** page appears.

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

The Link Set is added.

Deleting a Link Set

Deleting a Link Set removes the Link Set from the configuration.

The software will not let you delete a Link Set that is referenced by a Link or a Route. If necessary, perform *Deleting a Link* or *Deleting a Route* before proceeding.

1. Select **SS7/Sigtran>Configuration>Link Sets**.

   The **Link Sets** page appears.

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

   A delete confirmation message appears.

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

The Link Set is deleted from the table.

Generating a report on Link Sets

1. Select **SS7/Sigtran>Configuration>Link Sets**.

   The Link Sets page appears.

2. Perform one of these actions:
   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Viewing the status of Link Sets

The **Status** link launches the **Link Sets Maintenance** page. The status information is the same information shown under **SS7/Sigtran>Maintenance>Link Sets** (see *Link Set Maintenance*).

Use one of the following methods to access status information from the **SS7/Sigtran>Configuration** menu:

1. Select **SS7/Sigtran>Configuration>Link Sets.**

   The **Link Sets** page appears.

2. Perform one of these actions:
   - Click **Status** next to an entry in the table to view the status of the entry.
   - Click the **Status** link at the bottom of the table to view the status of all entries.

The **Link Sets Maintenance** page is displayed in a browser window.

Links

A Link carries signaling within a Link Set using a specific Association. A Link can belong to only one Link Set and one Association.

An EAGLE XG site can host up to 1024 Links.

If a Link fails, the Signaling Network Interface attempts to divert signaling traffic to another Link in the same Link Set.

The **Links** page shows all configured M3UA links.

The **Links** page also provides a link to the **Links Maintenance** page where you can view the status of all configured Links. You can also manually enable and disable Links.

Safeguards to prevent service impact from configuration changes:

- The software will not let you delete a Link if it is enabled. The Link must first be disabled.

The software will not let you insert a Link if any of the following is true:

- The Local MP Server that hosts the selected Association does not exist in the Server Group that hosts the Local Signaling Point associated with the selected Link Set.
- A Link already exists with the same combination of Link Set and Association.
- The selected Association already hosts at least one Link from another Link Set that has the same Routing Context as the Routing Context in the selected Link Set.
- The Adjacent Server that hosts the selected Association does not exist in the Adjacent Server Group that represents the Remote Signaling Point associated with the selected Link Set.
- The selected Association already hosts at least one Link from another Link Set but at least one of the Link Sets has no Routing Context configured.

Links elements

This information appears on the **Links** page:

Table 9: Links Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Link is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required.
Link Name	A name that uniquely identifies the Link. The name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required.
Link Set	The Link Set to which the Link is being added. A Link Set supports up to 16 links. Each Link Set entry is a hyperlink to the Link Set table filtered by this Link Set.	Format: Pulldown list Range: All Link Sets associated with the selected Signaling Network Element. This field is required.
Association	The SCTP Association that will host the Link. If the Link shares an Association with Links from other Link Sets, each Link Set using the Association must be configured with a unique routing context. Only one Link can be created for a given Link Set and Association. Each Association entry is a hyperlink to the Associations table filtered by this Association.	Format: Pulldown list Range: All configuration Associations associated with the selected Signaling Network Element. This field is required.

Viewing Links

Use this procedure to view the configured links.

Select **SS7/Sigtran>Configuration>Links.**

The **Links** page appears listing all of the configured links. For field definitions, see *Links elements*.

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

The page appears with the configured links listed.

Inserting a Link

1. Select **SS7/Sigtran>Configuration>Links.**
   The **Links** page appears.
2. Click **Insert**.

   The **Insert Links** page appears.

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

The Link is added and is placed in the **Disabled** administrative state. See *Viewing Link status* to view the administrative state of the link. To enable the link, see *Enabling a Link*.

Deleting a Link

Deleting a Link removes the Link from the database.

The software will not let you delete a Link if it is in-service. Disable the Link before you attempt this procedure (see *Disabling a Link*).

1. Select **SS7/Sigtran>Configuration>Links.**

   The **Links** page appears.

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

   A delete confirmation message appears.

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

The Link is deleted from the table.

Generating a report on Links

1. Select **SS7/Sigtran>Configuration>Links**.

   The **Links** page appears.

2. Perform one of these actions:
   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Viewing the status of a Link

The **Status** link launches the **Link Maintenance** page. The status information is the same information shown under **SS7/Sigtran>Maintenance>Links** (see *Link Maintenance*).

Use one of the following methods to access status information from the **SS7/Sigtran>Configuration** menu:

1. Select **SS7/Sigtran>Configuration>Links.**

   The **Links** page appears.

2. Perform one of these actions:
   - Click **Status** next to an entry in the table to view the status of the entry.
   - Click the **Status** link at the bottom of the table to view the status of all entries.

The **Links Maintenance** page is displayed in a browser window.

Routes

A Route represents a signaling path from a local (LSP) point code to a remote signaling point (RSP) point code using a given Link Set. Routes are needed for adjacent RSPs to route network management signaling. A route consists of an RSP, a Link Set, and a relative cost.

There can be up to two routes between a local point code and a remote point code.

Each route has a cost. The Signaling Network Interface attempts to route signaling over the lower cost route. If two routes have the same cost, signaling is load-shared across both routes.

The Signaling Network Interface supports 1024 routes per site.

The **Routes** page shows all configured Routes. Each Remote Signaling Point can have a maximum of two Routes.

The **Routes** page also provides a link to the **RSP Maintenance** page where you can view the status of all configured routes and destinations. You can also manually reset the network status of a route.

Safeguards to prevent service impact from configuration changes:

The software will not let you insert a Route if any of the following is true:

- A Route already exists with the selected Remote Signaling Point and Link Set.
- The SS7 domain of the selected Remote Signaling Point does not match the SS7 domain of the Local Signaling Point configured for the selected Link Set.

Routes elements

This information appears on the **Routes** page:

Table 10: Routes Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the route is being added.	Format: Pulldown list Range: All configured routes. This field is required.
Remote Point Code	The point code configured in the remote signaling point that identifies the destination of this route	Format: Pulldown list Range: All configured point codes at the destination RSP. This field is required.
SS7 Domain	The SS7 domain of the selected Remote Point Code.	This field is read-only. The field is populated automatically when a Remote Point Code is selected.
Link Set	The Link Set to be used by this route. The choice of Link Set implies the LSP of the Route.	Format: Pulldown list Range: All configured Link Sets. This field is required.
Adjacent Point Code	The point code configured in the Adjacent RSP being used by the selected Link Set.	This field is read-only. The field is populated automatically when a Link Set is selected.
Relative Cost	The relative cost assigned to this route. Lower cost routes are preferred over higher cost routes.	Format: Numeric Default: 20 Range: 0 - 99 This field is required.
Route Name	An optional name that uniquely identifies the route. The name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Viewing Routes

Use this procedure to view the configured routes.

Select **SS7/Sigtran>Configuration>Routes**.

The **Routes** page appears. For field definitions, see *Routes elements*.

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

The page appears with the configured routes listed.

Inserting a Route

1. Select **SS7/Sigtran>Configuration>Routes**.

   The **Routes** page appears.

2. Click **Insert** .

   The **Insert Routes** page appears.

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

The Route is added.

Editing a Route

The **Edit** operation lets you change the relative cost associated with a Route. All other fields on the page are read only.

1. Select **SS7/Sigtran>Configuration>Routes**.

   The **Routes** page appears.

2. Click **Edit**.

   The **Edit Routes** page appears. For field definitions, see *Routes elements*.

3. Change the value in the **Relative Cost** field.
4. Click **OK**.

   A confirmation message appears.

5. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The relative cost associated with the Route is updated. Changes to the RMU take effect in the next outgoing message after the **OK** button is clicked on the confirmation dialog.

Deleting a Route

Deleting a Route removes the Route from the database.

1. Select **SS7/Sigtran>Configuration>Routes**.

   The **Routes** page appears.

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

   A delete confirmation message appears.

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

The Route is deleted from the table.

Generating a report on Routes

1. Select **SS7/Sigtran>Configuration>Routes**.

   The **Routes** page appears.

2. Perform one of these actions:

   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Viewing the status of Routes

The **Status** link launches the **Remote Signaling Points Maintenance** page. The status information is the same information shown under **SS7/Sigtran>Maintenance>Remote Signaling Links** (see *Remote Signaling Points Maintenance*).

Use one of the following methods to access status information from the **SS7/Sigtran>Configuration** menu:

1. Select **SS7/Sigtran>Configuration>Routes.**

   The **Routes** page appears.

2. Perform one of these actions:

   - Click **Status** next to an entry in the table to view the status of the entry.
   - Click the **Status** link at the bottom of the table to view the status of all entries.

The **Remote Signaling Points Maintenance** page is displayed in a browser window.

SCCP Options

The **SCCP Options** page shows all of the configured SCCP options.

SCCP Options elements

This information is provided on the **SCCP Options** page:

Table 11: SCCP Options Elements

Variable	Description	Data Input Notes
Subsystem Test Interval	The number of seconds to delay after sending an SST (Subsystem Test) before sending the next SST.	Format: Numeric Range: 1 - 600 Default: 30
ANSI Default GTT Point Code	Default ANSI Global Title STP point code in format NNN-NNN-NNN. If the egress SCCP message request does not contain a destination point code and the CDPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Pulldown Range: Point Code must comply with ANSI T1.111.8 Default: n/a
ITUI Default GTT Point Code	Default ITUI Global Title STP point code in format J-NNN-J. If the egress SCCP message request does not contain a destination point code and the CDPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Pulldown Range: 'J' can range from 0-7, 'NNN' can range from 0-255 Default: n/a
ITUN Default GTT Point Code	Default ITUN Global Title STP point code in format NNNNN. If the egress SCCP message request does not contain a destination point code and the CDPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Pulldown Range: 'NNNNN' can range from 0 - 16383 Default: n/a
ITUN24 Default GTT Point Code	Default ITUN24 Global Title STP point code in format NNN-NNN-NNN. If the egress SCCP message request does not contain a destination point code and the CDPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Pulldown Range: Each 'NNN' can range from 0 - 255 Default: n/a

Viewing SCCP Options

Use this procedure to view the SCCP Options.

Select **SS7/Sigtran>Configuration>SCCP Options**.

The **SCCP Options** page appears. For field definitions, see *SCCP Options elements*.

The **SCCP Options** page appears with the SCCP Options listed.

Editing an SCCP Option

Use this procedure to edit the values of the variables on the **SCCP Options** page.

1. Select **SS7/Sigtran>Configuration>SCCP Options**.

   The **SCCP Options** page appears.

2. In the **Value** field, make the desired changes. For field definitions, see *SCCP Options elements*.
3. Click **Apply** to save the data.

The new value is added to the configuration.

MTP3 Options

The **MTP3 Options** page shows the MTP3 timers and their current values. The page enables you to change the value association with a timer.

MTP3 Options elements

This information appears on the **MTP3 Options** page:

Table 12: MTP3 Options Elements

Element	Description	Data Input Notes
Timer T1	Changeover timer. This timer introduces a delay to help prevent message mis-sequencing on link changeover.	Format: Numeric Range: 10 - 2000 msecs Default: 60 msecs
Timer T3	Change-back timer. This timer introduces a delay to help prevent message mis-sequencing on link change-back.	Format: Numeric Range: 10 - 2000 msecs Default: 60 msecs
Timer T6	Controlled Rerouting timer. This timer introduces a delay to help prevent message mis-sequencing on controlled rerouting.	Format: Numeric Range: 10 - 2000 msecs Default: 60 msecs
Timer T10	Destination Audit interval. This timer controls the interval at which RST/DAUD messages are sent when destination audit is activated. Destination audit is activated on receipt of a	Format: Numeric Range: 1000 - 120000 msecs Default: 60000 msecs

Element	Description	Data Input Notes
	TFP/DUNA. If a TFA/DAVA is received, destination audit is deactivated.	
Timer T15	Destination Congestion Test Delay. This timer controls the length of the wait prior to starting the signaling route set congestion test.	Format: Numeric Range: 100 - 10000 msecs Default: 2000 msecs
Timer T16	Destination Congestion Test Timeout. This timer controls the length of the wait for the route set congestion status update.	Format: Numeric Range: 100 - 10000 msecs Default: 1000 msecs
SLS Rotation	This value specifies whether the SLS rotation procedure is enabled for egress messages. If SLS rotation is **Enabled**, the SLS value of messages will be rotated before routing the messages to network.	Format: Pulldown list Range: Disabled, Enabled Default: Enabled

Viewing MTP3 Options

Select **SS7/Sigtran>Configuration>MTP3 Options**.

The **MTP3 Options** page appears. For field definitions, see *MTP3 Options elements*.

The page appears with the MTP3 options listed.

Editing MTP3 Options

1. Select **SS7/Sigtran>Configuration>MTP3 Options**.

   The **MTP3 Options** page appears.

2. Make the desired changes. For field definitions, see *MTP3 Options elements*.
3. Click **Apply** to save the data.

The new value is added to the configuration and will be used the next time a timer is started.

M3UA Options

The **M3UA Options** page shows the M3UA timers and their current values. The page enables you to change the value associated with a timer.

M3UA Options elements

This information appears on the **M3UA Options** page:

Table 13: M3UA Options Elements

Element	Description	Data Input Notes
State Management ACK Timer	This timer controls how long M3UA waits for ASP state and traffic management message acknowledgements. If this timer expires, the message may be retransmitted. In the case of M3UA heartbeats, if no BEAT-ACK is received in two-times this value, the SCTP association will be restarted.	Format: Numeric Range: 200 - 1200 msecs Default: 800 msecs
M3UA Heartbeating	This value specifies whether M3UA heartbeating is enabled for all M3UA associations. If M3UA heartbeating is enabled, the **M3UA Heartbeat Interval** field specifies the rate at which M3UA heartbeats are sent.	Format: Pulldown list Range: Enabled, Disabled Default: Disabled.
M3UA Heartbeat Interval	This value is the interval at which M3UA BEAT messages will be sent on each association when M3UA heartbeating is enabled. This value has no meaning when M3UA heartbeating is disabled.	Format: Numeric Range: 100 - 10000 msecs Default: 5000 msecs

Viewing M3UA Options

Use this procedure to view M3UA options:

Select **SS7/Sigtran>Configuration>M3UA Options**.

The **M3UA Options** page appears. For field definitions, see *M3UA Options elements*.

The page appears with the M3UA Options listed.

Editing M3UA Options

1. Select **SS7/Sigtran>Configuration>M3UA Options**.

   The **M3UA Options** page appears.

2. Make the desired changes. For field definitions, see *M3UA Options elements*.
3. Click **Apply** to save the data.

The new value(s) is added to the configuration. The new timer value will be used the next time the timer is started.

Local Congestion Options

The **Local Congestion Options** page is a view-only list of the congestion management configuration parameters. There are two sets of parameters:

- The parameters that define the maximum capacities of the resources which will be monitored by congestion management. The system automatically calculates the alarm onset and abatement thresholds from these maximum capacities. These parameters are the first nine parameters listed in the table (through **SCTP Aggregate Association Writer Queue Utilization**).
- The parameters that define the message treatment percentages for each MP congestion level. There are nine view-only configuration parameters; three for each MP congestion level (labeled CL1, CL2, and CL3).

Thresholds for minor, major, and critical alarms are based on a fixed percentage of the maximum configured value in the Local Congestion Options table:

Table 14: Alarm Severity for Onset and Abatement Thresholds

Severity	Onset %	Abate %
Minor	60	50
Major	80	70
Critical	95	90

Local Congestion Options elements

This information appears on the **Local Congestion Options** page:

Table 15: Local Congestion Options Elements

Element	Description
Maximum SS7 Process CPU Utilization	The SS7 process is responsible for all SS7 processing on an MP. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 90%
Maximum Ingress Message Rate	The ingress message rate measures the data messages (SI > 0) per second that the MP receives from the network. Thresholds for minor, major

Element	Description
	and critical alarms are based on a fixed percentage of this maximum value. Default: 15,000 msgs/sec.
Maximum PDU Buffer Pool Size for ANSI	A Protocol Data Unit (PDU) buffer is allocated for each ANSI message that arrives at an MP and is de-allocated when message processing completes. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 11000 PDUs
Maximum PDU Buffer Pool Size for ITUI	A Protocol Data Unit buffer is allocated for each ITUI message that arrives at an MP and is de-allocated when message processing completes. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 11000 PDUs
Maximum PDU Buffer Pool Size for ITUN	A Protocol Data Unit buffer is allocated for each ITUN message that arrives at an MP and is de-allocated when message processing completes. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 11000 PDUs
Maximum SCCP Stack Event Queue Size	The internal event queue to the SCCP Stack which is responsible for all SCCP sublayer processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 4,000 events
Maximum M3RL Stack Event Queue Size	The internal event queue to the M3RL stack, which is responsible for all M3RL non-management (SI > 0) processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 4,000 events
Maximum M3RL Network Management Event Queue Size	The internal event queue to M3RL Network Management which is responsible for all M3RL management (SI = 0) processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value.

Element	Description
	Default: 1000 events
Maximum M3UA Stack Event Queue Size	The internal egress event queue to the M3UA Stack which is responsible for all M3UA Stack processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 2,000 events
Maximum SCTP Single Association Writer Queue Size	The internal egress event queue to an SCTP Association Handler which is responsible for all non-Linux SCTP sublayer processing for a individual SCTP association. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 1,000 events
Maximum SCTP Aggregate Association Writer Queue Size	The internal egress event queue used to limit the maximum number of egress messages queued on all SCTP Association Handler Threads. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 10,000 events
CL1 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL1. Default: 80%
CL1 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and an SCCP UDTS/XUDTS response is sent (when requested by the originator) when the local MP congestion level is CL1. Default: 10%
CL1 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL1. Default: 10%
CL2 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL2. Default: 70%
CL2 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and an SCCP UDTS/XUDTS response

Element	Description
	is sent (when requested by the originator) when the local MP congestion level is CL2. Default: 10%
CL2 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL2. Default: 20%
CL3 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL3. Default: 60%
CL3 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and an SCCP UDTS/XUDTS response is sent (when requested by the originator) when the local MP congestion level is CL3. Default: 0%
CL3 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL3. Default: 40%

Viewing Local Congestion Options

Select **SS7/Sigtran>Configuration>Local Congestion Options**

The **Local Congestion Options** page appears. For field definitions, see *Local Congestion Options elements*.

The page appears with the configured links listed.

Capacity Constraint Options

The **Capacity Constraint Options** page shows the maximum and current capacity of each constraint. Use this page to configure the value at which the alarm for the particular constraint is raised. You can also use this page to configure the alarm severity and enable the specified alarm.

Capacity Constraint Options elements

This information appears on the **Capacity Constraint Options** page:

Table 16: Capacity Constraint Options Elements

Element	Description
SS7 Constraint values	List of available constraint values: • Adjacent Server Groups Per Site • Adjacent Servers Per Adjacent Server Group • Adjacent Servers Per Site • SCTP Association Configuration Sets Per Site • SCTP Association Per Site • SCTP Association Per MP Server • LSPs Per Site • Links Per Association • Links Per Linkset • Links Per Site • Linksets Per Site • RMUs Per Site • RSPs Per Site • Routes Per RSP Per MP • Routes Per Site • Server Groups Per LSP • Server Groups Per Site • Servers Per MP Server Group
Maximum Capacity	Maximum capacity supported by the system.
Current Capacity	Capacity used by the current system configuration.
Alarm At	Use this field to set the value at which the specified alarm will be raised.
Alarm Severity	Use this dropdown menu to select the alarm severity value.
Alarm Enabled	Use this checkbox to enable the specified alarm.
Submit	Use this button to apply your selections.

The following table lists the SS7 constraint value details:

Table 17: SS7 Constraint Values

Value	Description
AdjSvrGrpsPerSite	Number of Adjacent Server Groups (STPs) supported per SOAM pair.
AdjSvrsPerAdjSvrGrp	Number of Servers (Cards) supported in a Adjacent Server group STP).

Value	Description
AdjSvrsPerSite	Number of Servers (STP Cards) supported per SOAM pair.
LinksetsPerSite	Number of SS7 linksets supported per SOAM pair.
LinksPerAssociation	Number of SS7 links supported per SCTP association.
LinksPerLinkset	Number of links supported per linkset.
LinksPerSite	Numbers of SS7 links supported per SOAM pair.
LSPsPerSite	Number of LSPs supported per SOAM pair.
RMUsPerSite	Numbers of RMUs supported per SOAM pair
RoutesPerRSPPerMP	Number of SS7 Routes supported per RSP on one MP..
RoutesPerSite	Number of SS7 Routes supported per SOAM pair.
RSPsPerSite	Number of RSPs supported per SOAM pair.
SCTPAssocConfigsPerSystem	Number of Configuration sets supported per System.
SCTPAssocPerMP	Number of SCTP associations supported per MP.
SCTPAssocPerSite	Number of SCTP associations supported per SOAM pair.
ServerGroupsPerLSP	ServerGroupsPerLSP
ServerGroupsPerSite	Number of Server groups (MPs) supported per SOAM pair.
ServersPerMP	Number of servers per MP.

Viewing Capacity Constraint Options

Select **SS7/Sigtran>Configuration>Capacity Constraint Options**

The **Capacity Constraint Options** page appears. For field definitions, see *Capacity Constraint Options elements*.

The page appears with a list of configurable constraint values.

Chapter 3

SS7 maintenance

Topics:

- *The SS7 Maintenance menu.....57*
- *Color codes on the Maintenance pages.....57*
- *Local SCCP Users Maintenance.....58*
- *Remote Signaling Points Maintenance.....60*
- *Remote MTP3 Users Maintenance.....63*
- *Link Set Maintenance.....66*
- *Link Maintenance.....68*

SS7 Maintenance provides maintenance and troubleshooting capabilities on Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, Links, and Associations.

The SS7 Maintenance menu

The **SS7/Sigtran>Maintenance** menu provides maintenance and troubleshooting capabilities on Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, Links, and Associations.

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

Errors, warnings, and the possible need for maintenance activity are shown in the GUI in colored cells so that the conditions are readily identifiable. The colored cells are the same entries that appear when the **Show Errors** button is pressed from a **Maintenance** page.

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

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

- Enabling and disabling Links.
- Enabling, blocking, and disabling Associations.
- Resetting the network status of Routes.
- Resetting the MP's SCCP status of the subsystem and point code.
- Enabling and disabling LSUs.

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

A user group must have permissions to view or execute any of the procedures on the **SS7/Sigtran Maintenance** menu. If a group does not have permissions for the **Maintenance** menu options for **Local SCCP Users**, **Remote Signaling Points**, **Remote MTP3 Users**, **Link Sets**, **Links**, or **Associations**, these options will not appear in the GUI.

SS7 maintenance is allowed from the SOAM. All maintenance links are active when the user is connected to the SOAM.

Color codes on the Maintenance pages

The colors on the **Maintenance** pages alert the network operator to potential problems:

Table 18: Maintenance Page Color Codes

Color	Description
Red background	Indicates an error.
Orange background	Indicates maintenance activity.

Color	Description
Yellow background	Used for warnings such as congestion or some of a link set's links are down.
Gray background	Indicates that conditions are normal.
Gray text	If status cannot be collected from an MP server, cells with gray text indicate the last known information reported from the server.

Local SCCP Users Maintenance

The **Local SCCP Users Maintenance** page shows the status of each configured LSU.

Colored cells may indicate the need for maintenance activity. If status cannot be collected from a server, cells with gray text indicate the last known information reported from the server.

Local SCCP Users Maintenance elements

This information appears on the **Local SCCP Users Maintenance** page:

Table 19: Local SCCP Users Maintenance Elements

Element	Description
Show Errors/Show All button	Toggles the display to show only entries with errors (**Show Errors**) or to show all entries whether they have errors or not (**Show All**). The default resets when you exit the page. By default, all entries are shown (similar to the results of **Show All**).
Signaling Network Element Name	The Signaling Network Element Name to which the Local SCCP User is associated.
SSN	The subsystem number served by this Local SCCP User.
(Local Signaling Point) Point Code	The point code of the Local Signaling Point associated with this Local SCCP User.
(Local Signaling Point) SS7 Domain	The SS7 domain of the Local Signaling Point.
Application Name	Application Name associated with the Local SCCP User.
SSN Status	The SSN Status. Possible values are **Enabled** and **Disabled**. These values indicate whether the Local SCCP subsystem is enabled or disabled.

Element	Description
	The user can manually disable an LSU (see *Disabling a Local SCCP User*).The Local SCCP subsystem will also be automatically disabled under the following conditions: • When SCCP receives a notification from the OAM subsystem that a Local Subsystem and SCCP User have been added to the MP's database. • In some cases, when SCCP receives a notification from the OAM Subsystem that an enabled Local Subsystem and SCCP User have been deleted from the MP database. The user can manually enable an LSU (see *Enabling a Local SCCP User*). When SCCP receives a notification from the OAM subsystem that a local SCCP user has been enabled, SCCP sets the subsystem status to **Enabled**.
Up/Down Since	Indicates the time when the LSU status was changed.

Viewing Local SCCP Users status

Use this procedure to view status information on LSUs.

1. Select **SS7/Sigtran>Maintenance>Local SCCP Users**.

   The **Local SCCP Users Maintenance** page appears. For field definitions, see *Local SCCP Users Maintenance elements*.

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

2. (Optional) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the data updates. You can also click the menu option on the main menu to manually update the page.
3. (Optional) Click **Show Errors** to view only the entries with errors.

The page shows LSU status.

Enabling a Local SCCP User

The **Enable** command causes SCCP to set the Local SCCP subsystem status to **Enabled**.

LSUs must be enabled one LSU at a time.

1. Select **SS7/Sigtran>Maintenance>Local SCCP Users**.

   The **Local SCCP Users Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to **15** so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
3. Click **Enable** in the row of the appropriate LSU.

   The MP server will disregard the command if the LSU is already in the **Enabled** state.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **SSN Status** field changes to **Enabled**.

The LSU is enabled. The **Up/Down Since** column now indicates when the LSU transitioned into the **Enabled** state.

Disabling a Local SCCP User

The **Disable** command causes the status of the Local SCCP subsystem to change to **Disabled**.

LSUs must be disabled one LSU at a time.

1. Select **SS7/Sigtran>Maintenance>LSU**.

   The **Local SCCP User Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to **15** so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
3. Click **Disable** in the row of the appropriate LSU.

   The MP server will simply disregard the command if the LSU is already in the **Disabled** state.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **SSN Status** field changes to **Disabled**, and the cell turns red.

The LSU is disabled. The **Up/Down Since** column now indicates when the LSU transitioned into the **Disabled** state.

Remote Signaling Points Maintenance

The **Remote Signaling Points Maintenance** page shows the status of each configured RSP and the Routes to that RSP. The status information is shown from the perspective of each MP at the site.

Each RSP can have up to two routes. The route status is divided into link set status and network status. The network status is the status of the RSP as reported from the network via the STP.

The **Reset** action resets the MP's view of both routes' network status to available. This action allows the network operator to attempt signalilng on the routes.

Colored cells may indicate the need for maintenance activity. If status cannot be collected from a server, cells with gray text indicate the last known information reported from the server.

Remote Signaling Points Maintenance elements

This information appears on the **Remote Signaling Points Maintenance** page:

Table 20: Remote Signaling Points Maintenance Elements

Element	Description
Show Errors/Show All button	Toggles the display to show only entries with errors (**Show Errors**) or to show all entries whether they have errors or not (**Show All**). The default resets when you exit the page. By default all entries are shown (similar to the result of clicking **Show All**).
Remote Point Code	The point code for this RSP.
SS7 Domain	The SS7 domain of the RSP.
RSP Status	RSP Status is an aggregation of the statuses for Route 1 and Route 2. The intent is to display the MP server's ability to signal to the RSP. Possible values are: • **Available**-at least one route is available. • **Unavailable**-both routes are down/unavailable. • **Congested**-a report has been received from the network that the RSP is congested, but not unavailable. • **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state. • **Non-Preferred**-the lower cost route is down/unavailable, causing signaling to use the non-preferred route. • **Application Disabled**-the application has been manually disabled via the **Server Status** page.
Route X Status, where Route X is Route 1 or Route 2	Route Status is an aggregation of **Link Set Status** and **Network Status**. If either the **Link Set Status** is **Down** or the **Network Status** is **Unavailable**, the route is **Unavailable**.
Link Set Status	Corresponds to the status of the Link Set that the Route is configured to use, as shown on the **Link Set Maintenance** page. Possible values are **Up** or

Element	Description
	Down. If **Down**, more information can be found on the **Link Set Maintenance** page. For information on Link Set Maintenance, see *Link Set Maintenance elements*.
Network Status	Indicates the Route status reported from the network. Possible values are **Available** or **Unavailable**. **Unavailable** means that a DUNA/TFP was received from a signaling gateway indicating that the RSP is not accessible from that signaling gateway. A restricted route is displayed as available.
Time of Last Status Change	Indicates the last time when any status change occurred on this row, including changes for the RSP status and the link set and network status for Route 1 and Route 2.
MP Server Hostname	The hostname of the MP server reporting the status.
Route X Details, where Route X is Route 1 or Route 2	Route Details provides detailed information about Route 1 and Route 2.
Route Cost	The cost associated with the Route.
Link Set Name	The Link Set associated with the Route.
Adjacent Point Code	The Adjacent Point Code associated with the Route.

Viewing Remote Signaling Points status

Use this procedure to view status information on RSPs.

1. Select **SS7/Sigtran>Maintenance>Remote Signaling Points**.

   The **Remote Signaling Points Maintenance** page appears. For field definitions, see *Remote Signaling Points Maintenance elements*.

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

2. (Optional) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the data updates. You can also click the menu option on the main menu to manually update the page.
3. (Optional) Click **Show Errors** to view only the entries with errors.

The page shows all configured RSPs.

About resetting the Network Status of the routes

The **Reset** action allows the network operator to reset the MP server's view of the **Network Status** for both Routes to **Available**. If the **Link Set Status** values for the two Routes do not prevent signaling,

then both Routes (and the RSP) will become available for signaling. The **Link Set Status** is not affected by the **Reset** action. Resetting the **Network Status** for the Routes may cause the **RSP Status** to change.

Reset should only be used in cases in which the network operator suspects that a DAVA/TFA management message may have been lost so that the MP has a stale view of the true network status. If **Reset** is used and the **Network Status** was correct (was unavailable), then response method signaling will set the **Network Status** back to the correct value. Clicking **Reset** when the route **Network Status** is already available has no effect.

Reset can also be used to reset the MP's view of the RSP's congestion status. In other words, **Reset** will make the MP server think that the RSP is no longer congested. Again, if the RSP really is congested, response method signaling may set it back to congested.

Reset has no effect on an RSP for which both Routes are Up/Available and the RSP is not congested.

Resetting the Network Status of the Routes

1. Select **SS7/Sigtran>Maintenance>Remote Signaling Links**.

   The **Remote Signaling Links Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
3. Click **Reset** in the row of the appropriate route.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Network Status** field shows **Available**.

The **Network Status** is reset to **Available**.

Remote MTP3 Users Maintenance

The **Remote MTP3 Users Maintenance** page shows the operational status of each configured RMU. The subsystem statuses are shown from the perspective of each MP server.

The **Reset** action causes the MP's view of the remote subsystem to be reset, allowing signaling attempts to occur.

Colored cells may indicate the need for maintenance activity. If status cannot be collected from a server, cells with gray text indicate the last known information reported from the server.

Remote MTP3 Users Maintenance elements

This information appears on the **Remote MTP3 Users Maintenance** page:

Table 21: Remote MTP3 Users Maintenance Elements

Element	Description
Show Errors/Show All button	Toggles the display to show only entries with errors (**Show Errors**) or to show all entries whether they have errors or not (**Show All**). By default all entries are shown. The default resets when you exit the page.
Remote Point Code	The Remote Point Code associated with the RMU.
SS7 Domain	The SS7 domain of the RMU.
Remote SSN	The Remote Subsystem Number whose status is being tracked.
MP Server Hostname	The hostname of the MP server reporting the status.
Operational Status	RMU status is an aggregation of the Remote PC and Remote SSN status that indicates the MP's ability to signal to the specified RMU. Possible values are: • **Available**-the RMU is *available* (none of the conditions for **Unavailable** is true). A congested point code can have a status of **Available**. • **Unavailable**-the SSN is prohibited or the point code is unavailable.
Operational SSN Reason	Shows one of these values: • **Normal**-the MP server thinks the RMU's subsystem is fully accessible for SCCP signaling. • **Prohibited**-an SSP was received for the point code and subsystem. • **Unknown**- DUPU/UPU was received for the point code indicating that SCCP is unavailable on that RSP. • **Application Disabled** -the application has been manually disabled via the **Server Status** page. • **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state. A value of ITU subsystem congestion (SSC) is not yet supported.

Element	Description
Operational Point Code Reason	Shows one of these values: • **Normal**-the point code is *normal* (none of the other conditions listed in this section is true). • **User Part Unavailable**-an MTP-Status indicating user part unavailable or unknown is received from the signaling gateway. • **Point Code Paused**-SCCP received an MTP-Pause indicating that the point code is inaccessible for signaling. • **Congested**-an MTP-Status message is received indicating that the point code is congested. • **Application Disabled** -the application has been manually disabled via the **Server Status** page. • **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.
Available/Unavailable Since	Indicates the last time when the operational status changed.

Viewing Remote MTP3 Users status

Use this procedure to view status information on RMU.

1. Select **SS7/Sigtran>Maintenance>Remote MTP3 Users**.

   The **Remote MTP3 Users Maintenance** page appears. For field definitions, see *Remote MTP3 Users Maintenance elements*.

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

2. (Optional) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the data updates. You can also click the menu option on the main menu to manually update the page.
3. (Optional) Click **Show Errors** to view only the entries with errors.

The page shows all configured RMUs.

About resetting the subsystem and point code status

The **Reset** action enables the network operator to reset the MP's SCCP view of the SSN status to allowed and the point code status to available.

Reset should only be used if the network operator suspects that an SSA or MTP-Resume management message may have been lost, resulting in the MP server having a stale view of the true network status. If **Reset** is used and the network status was correct (was really unavailable), then response method signaling will set the network status back to the correct value.

Reset can also be used to reset the MP's view of the point code's congestion status. In other words, **Reset** will make the MP server SCCP think that the point code is no longer congested. Again, if the point code really is congested, response method signaling may set it back to congested. **Reset** has no effect on an RMU for which both **SSN Reason** and **PC Reason** are normal.

Resetting the subsystem and point code status

1. Select **SS7/Sigtran>Maintenance>Remote MTP3 Users**.

   The **Remote MTP3 Users Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
3. Click **Reset** in the row of the appropriate route.

   A confirmation message appears.

4. Click **OK** to confirm.

The SSN status is reset to allowed. The point code status is reset to available.

Link Set Maintenance

The **Link Sets Maintenance** page shows status information for each Link Set as viewed by each MP server. Each MP server reports status only for Link Sets hosted by that MP server (i.e., Link Sets that include Links that use Associations hosted by the MP server).

Each Link Set's operational status and the reason for the operational status are shown.

The **Link Set Maintenance** page does not distinguish between links down for maintenance and links down due to errors. Colored cells may indicate the need for maintenance activity. When the server's collection status is Unknown, cells with gray text indicate the last known information about the Link Set.

For additional details on Link status, see *Link Maintenance*.

Link Set Maintenance elements

This information appears on the **Link Sets Maintenance** page:

Table 22: Link Sets Maintenance Elements

Element	Description
Show Errors/Show All button	Toggles the display to show only entries with errors (**Show Errors**) or to show all entries whether they have errors or not (**Show All**). By default all entries are shown. The default resets when you exit the page.

Element	Description
Signaling Network Element Name	The name of the Signaling Network Element associated with the Link Set.
Link Set Name	The name that identifies this Link Set.
MP Server Hostname	The hostname for the MP server.
Local Signaling Point	The LSP associated with the Link Set.
SS7 Domain	The SS7 domain of the LSP.
Adjacent Remote Point Code	The point code of the Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway to be served by this Link Set.
Operational Status	The operational status of the Link Set: **Down** or **Up**. Link Set status is reported per MP server, meaning each MP reports its view of the Link Set. There is no aggregated view.
Operational Reason	The reason a given operational status is shown. For information on a value listed in this field, see *Link Set Operational Status and Reason*.
MP Server HA Status	The high availability status of the MP server: **Active** or **Standby**.
Up/Down Since	The date and time that the Link Set came up or went down. After a database restart, reboot, or initial startup before the Associations and Links are initialized, the value is the time when the application initialization runs.

Link Set Operational Status and Reason

This list shows the possible values that may appear in the **Operational Status** and **Reason** fields of the **Link Set Maintenance** page.The **Operational Status** is either **Up** or **Down**. **Up** indicates that the Link Set can be used for signaling. **Down** indicates that the Link Set cannot be used for signaling. If the **Status** is **Down**, the **Operational Reason** provides information about why it is down.

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

- **Application Disabled**-the MP server's application administrative state has been manually **Disabled** via the **Server Status** page.
- **All Links Normal**-this status occurs when all of the configured Links that reference this Link Set are reporting an operational reason of **Normal**.
- **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.
- **0 of N Links Normal**-all Links configured on this MP for this Link Set are reporting an operational reason other than **Normal**.

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

- **All Links Normal**-this is the desired status of the server. This status occurs when all of the configured Links that reference this Link Set are reporting an operational reason of **Normal**.
- **M of N Links Normal**-some of the configured Links on an MP server that reference this Link Set are reporting an operational reason of **Normal**. **N** represents the sum of Links on the MP server that belong to the Link Set. **M** represents the subset of **N** that are reporting an operational reason of **Normal**.

Viewing Link Set status

Use this procedure to view information on the operational status of a Link Set.

1. Select **SS7/Sigtran>Maintenance>Link Sets**.

   The **Link Sets Maintenance** page appears. For field definitions, see *Link Set Maintenance elements*.

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

2. (Optional) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the data updates. You can also click the menu option on the main menu to manually update the page.
3. (Optional) Click **Show Errors** to view only the entries with errors.

The page shows all configured Link Sets.

Link Maintenance

The **Links Maintenance** page shows the administrative state and operational status of each SS7 Link. The administrative state is either **Enabled** or **Disabled**. The operational status is either **Up** or **Down**.

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

Colored cells may indicate the need for maintenance activity. Red cells indicate failures. Orange cells indicate maintenance conditions. When the active server's collection status is Unknown, cells with gray text indicate the last known information about the Link.

You can obtain additional information about the Link status by viewing the status of the Association that hosts the link (see Transport Manager).

Links Maintenance elements

These elements appear on in the **Links Maintenance** page:

Table 23: Links Maintenance Elements

Element	Description
Show Errors/Show All button	Toggles the display to show only entries with errors (**Show Errors**) or to show all entries whether they have errors or not (**Show All**). By default all entries are shown. The default resets when you exit the page.

Element	Description
Signaling Network Element Name	The Signaling Network Element associated with the Link.
Link Name	The name that identifies this Link.
Link Set	The name that identifies this Link Set.
MP Server Hostname	The hostname for the MP server associated with this Link.
Admin State	Shows the Link's administrative state: **Enabled** or **Disabled**. In the **Enabled** administrative state, the Link is in the ASP-Active state on an active MP server or the ASP-INACTIVE state on a standby MP server. In the **Disabled** administrative state, the Link is in the ASP-INACTIVE state on the MP server and is unavailable for Sigtran signaling. When a new Link is configured, the Link is in the **Disabled** administrative state. The Link must be placed in the **Enabled** administrative state to bring the Link up. Orange color highlights the administrative state when it is **Disabled**.
Operational Status	The operational status of the Link: **Up** or **Down**.
Operational Reason	The reason a given operational status is shown. For information on a value listed in this field, see *Link Operational Status and Reason*.
MP Server HA Status	The high availability status of the MP server: **Active** or **Standby**.
Up/Down Since	The date and time that the Link came up or went down. For a newly added Link, the time is when the Link was configured. After a database restart, reboot, or initial startup before the Associations and Links are initialized, the value is the time when the application initialization runs.

Link Operational Status and Reason

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

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

- **Disabled**-the Link's administrative state is **Disabled**. This is the initial operational status and reason for a newly configured Link. This reason is also shown when a link is manually disabled.

- **Application Disabled**-the Link's administrative state is **Enabled** and the server's application administrative state has been manually **Disabled** via the **Server Status** page.
- **Association Down**-the Link's administrative state is **Enabled**, but the Link's Association is in any of these **Down** states: Down/Disabled, Down/Connecting, Down/Blocked, or Down/Up Pending.
- **Forced Standby**-the Link's administrative state is **Enabled** and the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.
- **Up Pending**-the Link's administrative state is **Enabled**, but the ASP-ACTIVE-ACK has not yet been received.

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

- **Normal**-this status occurs when the administrative state is **Enabled** and the ASP-ACTIVE-ACK has been received.

Viewing Link status

Use this procedure to view information on the administrative state and operational status of a Link.

1. Select **SS7/Sigtran>Maintenance>Links**.

   The **Links Maintenance** page appears. For field definitions, see *Links Maintenance elements*.

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

2. (Optional) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the data updates. You can also click the menu option on the main menu to manually update the page.
3. (Optional) Click **Show Errors** to view only the entries with errors.

The page shows Link status information.

Enabling a Link

When a Link is put in the **Enabled** administrative state, the MP server begins attempts to bring the Link to the ASP-ACTIVE state on an active MP server or the ASP-INACTIVE state on a standby MP server.

Links must be enabled one Link at a time.

1. Select **SS7/Sigtran>Maintenance>Links**.

   The **Links Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to **15** so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
3. Click **Enable** in the row of the appropriate Link.

   The MP server will disregard the command if the Link is already in the selected administrative state.

   If the link you wish to enable is missing or displayed in gray text, it indicates a management network problem between the MP server and the SOAM server from which your GUI session is hosted.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Link transitioned into the **Up** status. The **Enable** action is now grayed out.

The Link is enabled.

Disabling a Link

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

When a Link is put in the **Disabled** administrative state, the MP server begins attempts to place the Link in the ASP-INACTIVE state. Placing a Link in the **Disabled** administrative state makes the Link unavailable for Sigtran signaling.

Links must be disabled one Link at a time.

1. Select **SS7/Sigtran>Maintenance>Links**.

   The **Links Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to **15** so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
3. Click **Disable** in the row of the appropriate Link.

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

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Link transitioned into the **Up** status. The **Enable** action is now grayed out.

The Link is disabled.

Chapter 4

Command Line Interface

Topics:

- *Command Import elements.....73*
- *Validating commands.....73*
- *Command Validation Results.....74*
- *Command Validation Results elements.....76*
- *Executing commands.....77*
- *Command Execution Results.....78*
- *Command Execution Results elements.....81*
- *Command line interface import file.....82*
- *Managed objects.....83*

The **Command Line Interface > Command Import** page provides a method for bulk loading SS7 configuration data. The Command Import page allows you to validate and execute command scripts. Validation and execution results are written to log files in the file management area.

The **Command Import** page allows configuration of the following types of data:

- Remote signaling points
- Remote MTP3 users
- Links
- Link Sets
- Routes
- Local SCCP users

Command Import elements

This information appears on the **Command Import** page:

Table 24: Command Import Elements

Element	Description	Data Input Notes
Command Script Location	A file selection field used to locate commands.	Format: Text box
Validate	Validates the command script when the user selects **Submit**.	Format: Radio button **Note:** Validate is the default value.
Execute	Executes the command script when the user selects **Submit**.	Format: Radio button
Submit	Initiates either the validation or execution of the selected command script.	Format: Button

Validating commands

Use this procedure to validate commands. Validation only validates the syntax of input commands. For example, it validates command format, verifies that the operation is supported for the managed object, and confirms that all required attributes are present. It does not validate field values.

1. Select **SS7/Sigtran>Command Line Interface>Command Import.**
   The **Command Import** page appears.
2. Click **Browse** to select a file.

   The file browse dialog appears.
3. Select the file you want to validate.
4. Click **Open**.
   The file appears in the **Command Script Location** field.
5. Select the **Validate** radio button and click **Submit**.
   The file is validated and results are exported to a Command Validation Results TXT file, which is stored in the file management area. The results can also be accessed through the link in the work area of the **Command Import** page.
6. Click the link that appears in the work area of the **Command Import** page to view the Command Validation Results file.

   If the link is clicked immediately after submit, the validation may not be complete, and a partial file may be displayed.

   Note: If you navigate away from the Command Import page, the link will no longer be available.

The Command Validation Results file opens. For more information see *Command Validation Results elements*.

Command Validation Results

Results from command script validation are written to a TXT file. The naming convention of the file is <*filename*>.<*timestamp*>.txt, where <*filename*> is the name portion of the selected command script file and <*timestamp*> is the time the results file was created in UTC.

```
================================================================================
Command Validation Results
================================================================================
Report Generated: Fri Aug 06 17:20:18 2010 UTC
From: Active NETWORK_OAMP on host XGNO
Report Version: 3.0.0-3.0.0_30.5.0
User: guiadmin

--------------------------------------------
Command Validation Details

08/06/2010 17:20:18:883 1 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=
08/06/2010 17:20:18:883 1 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:883 2 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=10.250.52.54
08/06/2010 17:20:18:884 2 ***ERROR*** [Error Code 10096] - Managed object not yet
 supported: adjserver

08/06/2010 17:20:18:884 4 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
ADJSERVERS=
08/06/2010 17:20:18:884 4 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:885 5 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
ADJSERVERS=AS_01
08/06/2010 17:20:18:885 5 ***ERROR*** [Error Code 10096] - Managed object not yet
 supported: asgroup

08/06/2010 17:20:18:886 7 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=
08/06/2010 17:20:18:886 7 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:887 8 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=SG_MP
08/06/2010 17:20:18:887 8 ***ERROR*** [Error Code 10096] - Managed object not yet
 supported: lsp

08/06/2010 17:20:18:888 10 FAILED: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=
08/06/2010 17:20:18:888 10 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:889 11 SUCCESS: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=TCAP
08/06/2010 17:20:18:890 13 FAILED: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=
08/06/2010 17:20:18:890 13 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:891 14 SUCCESS: INSERT: RSP: name=STP_01: pointcode=6-6-6:
```

```
domain=itui: asgroup=AdjServGrp1
08/06/2010 17:20:18:892 16 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-006-6:DOMAIN=ITUI: SSN=
08/06/2010 17:20:18:892 16 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:893 17 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN= : SSN=5
08/06/2010 17:20:18:893 17 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:894 18 SUCCESS: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN=ITUI: SSN=5
08/06/2010 17:20:18:895 20 FAILED: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
LSP=ITUI_1_001_1: POINTCODE
08/06/2010 17:20:18:895 20 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:896 21 SUCCESS: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
 LSP=ITUI_1_001_1: POINTCODE=6-006-6: DOMAIN=ITUI: ASSIGNRC=no
08/06/2010 17:20:18:897 23 FAILED: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=
08/06/2010 17:20:18:897 23 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:898 24 SUCCESS: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=192.168.67.151
08/06/2010 17:20:18:899 26 FAILED: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=
08/06/2010 17:20:18:899 26 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:900 27 SUCCESS: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=LS_01: ASSOCIATION=AssocTest1
08/06/2010 17:20:18:901 29 FAILED: INSERT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-006-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:18:901 29 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:902 30 SUCCESS: INSERT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-6-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=5
08/06/2010 17:20:18:903 32 FAILED: EDIT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-006-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:18:903 32 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:904 33 SUCCESS: EDIT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-006-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=10
08/06/2010 17:20:18:905 35 FAILED: DELETE: ROUTE: POINTCODE=
08/06/2010 17:20:18:905 35 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:906 36 SUCCESS: DELETE: ROUTE: POINTCODE=6-006-6: DOMAIN=ITUI:
 LINKSET=LS_01
08/06/2010 17:20:18:907 38 FAILED: DELETE: LINK: NAME=
08/06/2010 17:20:18:907 38 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:908 39 SUCCESS: DELETE: LINK: NAME=Link1: FORCE=1
08/06/2010 17:20:18:909 41 FAILED: DELETE: ASSOCIATION: NAME=
08/06/2010 17:20:18:909 41 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:910 42 SUCCESS: DELETE: ASSOCIATION: NAME=AssocTest1: FORCE=1
08/06/2010 17:20:18:911 44 FAILED: DELETE: LINKSET: NAME=
08/06/2010 17:20:18:911 44 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:912 45 SUCCESS: DELETE: LINKSET: NAME=LS_01
08/06/2010 17:20:18:913 47 FAILED: DELETE: RMU: POINTCODE=6-006-6: DOMAIN=ITUI:
08/06/2010 17:20:18:914 47 ***ERROR*** [Error Code 001] - Missing Field Value:
ssn

08/06/2010 17:20:18:914 48 SUCCESS: DELETE: RMU: POINTCODE=6-6-6: DOMAIN=ITUI:
SSN=5
```

```
08/06/2010 17:20:18:915 50 FAILED: DELETE: RSP: pointcode=6-6-6
08/06/2010 17:20:18:916 50 ***ERROR*** [Error Code 001] - Missing Field Value:
domain

08/06/2010 17:20:18:916 51 SUCCESS: DELETE: RSP: pointcode=6-006-6: domain=itui
08/06/2010 17:20:18:917 53 FAILED: Delete: Lsu: Pointcode=1-001-1: Domain=ITUI:
Ssn=
08/06/2010 17:20:18:917 53 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:918 54 SUCCESS: Delete: Lsu: Pointcode=1-1-1: Domain=ITUI:
Ssn=5: Force=1
08/06/2010 17:20:18:919 56 FAILED: DELETE: LSP: NAME=
08/06/2010 17:20:18:919 56 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:920 57 FAILED: DELETE: LSP: NAME=LSP_01
08/06/2010 17:20:18:920 57 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: lsp

08/06/2010 17:20:18:921 59 FAILED: DELETE: ASGROUP: NAME=
08/06/2010 17:20:18:921 59 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:922 60 FAILED: DELETE: ASGROUP: NAME=ASG_01
08/06/2010 17:20:18:922 60 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: asgroup

08/06/2010 17:20:18:923 62 FAILED: DELETE: ADJSERVER: NAME=
08/06/2010 17:20:18:923 62 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:924 63 FAILED: DELETE: ADJSERVER: NAME=AS_01
08/06/2010 17:20:18:924 63 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: adjserver


------------------------------------------
Command Validation Summary

Input File: cli_commands.txt
Number of Commands Executed:    43
Number of Commands Succeeded:   15
Number of Commands Failed:      28

--------------------------------------------------------------------------------
End of Command Validation Results
================================================================================
```

Figure 1: Example of Command Validation Results file

Command Validation Results elements

Results from command script validation are written to a TXT file. This table describes the elements of the command validation results file.

Table 25: Command Validation Results

Element	Description
Command Validation Results	Displays the following information: • Time the report was generated • Server name • Report version number • User name
Command Validation Details	Output in the details section of the results file displays: • UTC timestamp in millisecond format: MM/DD/YYYY hh:mm:ss:uuu • Corresponding line number from the input file • Command statements from the input file • Successfully validated commands are preceded by: SUCCESS • Failed commands are preceded by: FAILED • Failed commands are followed by a line that begins: ***ERROR*** [Error Code <number>] - <error code text> • Comments from the input file, if applicable • Comments are preceded by: Comment
Command Validation Summary	Output in the summary section of the file displays: • Name of the input file • Number of commands validated • Number of commands succeeded • Number of commands failed • If a fatal error occurs, the script is terminated, and the summary will contain this message: ***SCRIPT ABORTED DUE TO ERROR***

Executing commands

Use this procedure to execute commands.

1. Select **SS7/Sigtran>Command Line Inteface>Command Import.**
   The **Command Import** page appears.
2. Click **Browse** to select a file.

   The file browse dialog appears.
3. Select the file you want to execute.
4. Click **Open**.

The file appears in the **Command Script Location** field.

5. Select the **Execute** radio button and click **Submit**.
   The commands in the file are executed and results are exported to a Command Execution Results TXT file, which is stored in the file management area. The results can also be accessed through the link in the work area of the **Command Import** page.
6. Click the link that appears in the work area of the **Command Import** page to view the Command Execution Results file.

   If the link is clicked immediately after submit, the validation may not be complete, and a partial file may be displayed.

   Note: If you navigate away from the **Command Import** page, the link will no longer be available.

   The Command Execution Results file opens. For more information see *Command Execution Results elements*.

Command Execution Results

Results from command script execution are written to a TXT file. The naming convention of the file is <*filename*>.<*timestamp*>.txt, where <*filename*> is the name portion of the selected command script file and <*timestamp*> is the time the results file was created in UTC.

```
================================================================================
Command Execution Results
================================================================================
Report Generated: Fri Aug 06 17:20:56 2010 UTC
From: Active NETWORK_OAMP on host XGNO
Report Version: 3.0.0-3.0.0_30.5.0
User: guiadmin

--------------------------------------------
Command Execution Details

08/06/2010 17:20:57:544 1 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=
08/06/2010 17:20:57:544 1 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:546 2 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=10.250.52.54
08/06/2010 17:20:57:546 2 ***ERROR*** [Error Code 10096] - Managed object not yet
 supported: adjserver

08/06/2010 17:20:57:549 4 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
ADJSERVERS=
08/06/2010 17:20:57:549 4 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:551 5 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
ADJSERVERS=AS_01
08/06/2010 17:20:57:551 5 ***ERROR*** [Error Code 10096] - Managed object not yet
 supported: asgroup

08/06/2010 17:20:57:553 7 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=
08/06/2010 17:20:57:553 7 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:555 8 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=SG_MP
```

```
08/06/2010 17:20:57:555 8 ***ERROR*** [Error Code 10096] - Managed object not yet
 supported: lsp

08/06/2010 17:20:57:557 10 FAILED: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=
08/06/2010 17:20:57:557 10 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:576 11 SUCCESS: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=TCAP
08/06/2010 17:20:57:579 13 FAILED: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=
08/06/2010 17:20:57:579 13 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:593 14 SUCCESS: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=itui: asgroup=AdjServGrp1
08/06/2010 17:20:57:596 16 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-006-6:DOMAIN=ITUI: SSN=
08/06/2010 17:20:57:596 16 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:600 17 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN= : SSN=5
08/06/2010 17:20:57:600 17 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:615 18 SUCCESS: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN=ITUI: SSN=5
08/06/2010 17:20:57:617 20 FAILED: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
LSP=ITUI_1_001_1: POINTCODE
08/06/2010 17:20:57:617 20 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:637 21 SUCCESS: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
 LSP=ITUI_1_001_1: POINTCODE=6-006-6: DOMAIN=ITUI: ASSIGNRC=no
08/06/2010 17:20:57:639 23 FAILED: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=
08/06/2010 17:20:57:639 23 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:659 24 SUCCESS: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=192.168.67.151
08/06/2010 17:20:57:662 26 FAILED: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=
08/06/2010 17:20:57:662 26 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:683 27 SUCCESS: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=LS_01: ASSOCIATION=AssocTest1
08/06/2010 17:20:57:686 29 FAILED: INSERT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-006-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:57:686 29 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:705 30 SUCCESS: INSERT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-6-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=5
08/06/2010 17:20:57:707 32 FAILED: EDIT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-006-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:57:707 32 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:720 33 SUCCESS: EDIT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-006-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=10
08/06/2010 17:20:57:722 35 FAILED: DELETE: ROUTE: POINTCODE=
08/06/2010 17:20:57:722 35 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:735 36 SUCCESS: DELETE: ROUTE: POINTCODE=6-006-6: DOMAIN=ITUI:
 LINKSET=LS_01
08/06/2010 17:20:57:737 38 FAILED: DELETE: LINK: NAME=
08/06/2010 17:20:57:737 38 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:750 39 SUCCESS: DELETE: LINK: NAME=Link1: FORCE=1
```

```
08/06/2010 17:20:57:752 41 FAILED: DELETE: ASSOCIATION: NAME=
08/06/2010 17:20:57:752 41 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:765 42 SUCCESS: DELETE: ASSOCIATION: NAME=AssocTest1: FORCE=1
08/06/2010 17:20:57:767 44 FAILED: DELETE: LINKSET: NAME=
08/06/2010 17:20:57:767 44 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:780 45 SUCCESS: DELETE: LINKSET: NAME=LS_01
08/06/2010 17:20:57:783 47 FAILED: DELETE: RMU: POINTCODE=6-006-6: DOMAIN=ITUI:
08/06/2010 17:20:57:783 47 ***ERROR*** [Error Code 001] - Missing Field Value:
ssn

08/06/2010 17:20:57:797 48 SUCCESS: DELETE: RMU: POINTCODE=6-6-6: DOMAIN=ITUI:
SSN=5
08/06/2010 17:20:57:799 50 FAILED: DELETE: RSP: pointcode=6-6-6
08/06/2010 17:20:57:799 50 ***ERROR*** [Error Code 001] - Missing Field Value:
domain

08/06/2010 17:20:57:813 51 SUCCESS: DELETE: RSP: pointcode=6-006-6: domain=itui
08/06/2010 17:20:57:815 53 FAILED: Delete: Lsu: Pointcode=1-001-1: Domain=ITUI:
Ssn=
08/06/2010 17:20:57:815 53 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:828 54 SUCCESS: Delete: Lsu: Pointcode=1-1-1: Domain=ITUI:
Ssn=5: Force=1
08/06/2010 17:20:57:831 56 FAILED: DELETE: LSP: NAME=
08/06/2010 17:20:57:831 56 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:833 57 FAILED: DELETE: LSP: NAME=LSP_01
08/06/2010 17:20:57:833 57 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: lsp

08/06/2010 17:20:57:835 59 FAILED: DELETE: ASGROUP: NAME=
08/06/2010 17:20:57:835 59 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:837 60 FAILED: DELETE: ASGROUP: NAME=ASG_01
08/06/2010 17:20:57:837 60 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: asgroup

08/06/2010 17:20:57:839 62 FAILED: DELETE: ADJSERVER: NAME=
08/06/2010 17:20:57:839 62 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:841 63 FAILED: DELETE: ADJSERVER: NAME=AS_01
08/06/2010 17:20:57:841 63 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: adjserver


-----------------------------------------------
Command Execution Summary

Input File: cli_commands.txt
Number of Commands Executed:    43
Number of Commands Succeeded:   15
Number of Commands Failed:      28

-------------------------------------------------------------------------------
End of Command Execution Results
===============================================================================
```

Figure 2: Example of Command Execution Results file

Command Execution Results elements

Results from command script execution are written to a TXT file. This table describes the elements of the command execution results file.

Table 26: Command Execution Results

Element	Description
Command Execution Results	Displays the following information: • Time the report was generated • Server name • Report version number • User name
Command Execution Details	Output in the details section of the results file displays: • UTC timestamp in millisecond format: MM/DD/YYYY hh:mm:ss:uuu • Corresponding line number from the input file • Command statements from the input file • Successfully executed commands are preceded by: SUCCESS • Failed commands are preceded by: FAILED • Failed commands are followed by a line that begins with: ***ERROR*** [Error Code <number>] - <error code text> • Comments from the input file, if applicable • Comments are preceded by: Comment
Command Execution Summary	Output in the summary section of the file displays: • Name of the input file • Number of commands executed • Number of commands succeeded • Number of commands failed • If a fatal error occurs, the script is terminated, and the summary will contain this message: ***SCRIPT ABORTED DUE TO ERROR***

Command line interface import file

The CLI (Command Line Interface) import file enables you to create command scripts to insert, delete, and edit SS7 data. Using an import file facilitates the provisioning of large amounts of data. It also provides a convenient method for configuring data that is common to multiple sites.

CLI command structure

CLI commands are formatted as follows:

```
<operation>: <managed object>: <attribute>=<value>
```

Commands can contain multiple attribute value pairs. The format for commands that contain multiple attribute value pairs is:

```
<operation>: <managed object>: <attribute>=<value>: <attribute>=<value>
```

Table 27: CLI command values

Element	Valid Values	Data Input Notes
Operation	• insert • edit • delete	Operation names are not case-sensitive.
Managed object	• rsp • rmu • association • linkset • link • route • lsu	Managed object names are not case-sensitive.
Attributes	Attributes are specific to the commands. Some attributes are required; others are optional. For more information, see: • *Remote Signaling Points* • *Remote MTP3 Users* • *Link Sets* • *Links* • *Routes* • *Local SCCP Users*	Attribute names are not case-sensitive.

Element	Valid Values	Data Input Notes
Value	For more information about attribute values, see: • *Remote Signaling Point elements* • *Remote MTP3 Users elements* • *Link Sets elements* • *Links elements* • *Routes elements* • *Local SCCP Users elements*	Attribute values are case-sensitive.

File format

The following rules apply to the format of command script files:

- One command is allowed per line.
- Command lines that begin with the pound sign (#) are treated as comments. Comments are included in the results file, and they are counted, but are not validated or executed.
- Blank lines are skipped.

Sample command scripts

```
insert: rmu: pointcode=003-003-003: domain=ansi: ssn=5
insert: rmu: pointcode=004-004-004: domain=ansi: ssn=6
# This is a sample script that demonstrates how to use insert
```

Figure 3: Insert commands

```
delete: rsp: pointcode=100-1-1: domain=ansi
delete: rsp: pointcode=100-1-2: domain=ansi
# This is a sample script that demonstrates how to use delete
```

Figure 4: Delete commands

```
edit: Route: Pointcode=001-001-001: Domain=Ansi: Linkset=LS1: Relcost=10
edit: Route: Pointcode=001-001-002: Domain=Ansi: Linkset=LS1: Relcost=5
edit: Route: Pointcode=001-001-003: Domain=Ansi: Linkset=LS1: Relcost=3
# This is a sample script that demonstrates how to use edit
```

Figure 5: Edit commands

Managed objects

Command Import supports these managed objects:

- `rsp`

- `rmu`
- `association`
- `linkset`
- `link`
- `route`
- `lsu`

Remote Signaling Points

Managed object

`rsp`

GUI Page updated

Remote Signaling Points page

Allowed operations

The table shows the operations allowed on the **Remote Signaling Points** page. The operation is not case-sensitive, for example, `INSERT`, `insert` and `Insert` are valid.

Table 28: Allowed operations

Operation	Description
Insert	Adds an RSP to the configuration.
Delete	Deletes an RSP from the configuration.

Required attributes

This table lists the required attributes for the `rsp` managed object. The table maps the command attributes to their corresponding field names on the **Remote Signaling Points** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote Signaling Point elements*).

Table 29: Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
pointcode	MTP Point Code	• Insert • Delete	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0

Attribute Name	GUI Field Name	For Operation	Notes
domain	SS7 Domain	• Insert • Delete	Not applicable

Optional attribute

This table lists an optional attribute for the `rsp` managed object. The table maps the command attribute to its corresponding field name on the **Remote Signaling Points** page in the GUI.

The attribute name is not case sensitive; however, the attribute value is.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote Signaling Point elements*).

Table 30: Optional Attribute

Attribute Name	GUI Field Name	For Operation
name	Remote Signaling Point Name	• Insert
asgroup	Adjacent Server Group	• Insert

Samples

To insert RSP STP_01 with pointcode 100-1-1 for the ANSI Domain with the Adjacent Server Group as asg1, use any of the following commands:

```
insert: rsp: pointcode=100-1-1: domain=ansi: asgroup=asg1
Insert: RSP: pointcode=100-1-1: domain=ansi: asgroup=asg1
INSERT: RSP: name=STP_01: pointcode=100-1-1: domain=ansi: asgroup=asg1
```

To delete RSP STP_01, use any of the following commands:

```
delete: rsp: pointcode=100-1-1: domain=ansi
Delete: RSP: pointcode=100-1-1: domain=ansi
DELETE: RSP: pointcode=100-1-1: domain=ansi
```

Remote MTP3 Users

Managed object

`rmu`

GUI Page updated

Remote MTP3 Users page

Allowed operations

The table shows the operations allowed on the **Remote MTP3 Users** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 31: Allowed operations

Operation	Description
Insert	Adds an RMU to the configuration.
Delete	Deletes an RMU from the configuration.

Required attributes

This table lists the required attributes for the `rmu` managed object. The table maps the command attributes to their corresponding field names on the **Remote MTP3 Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote MTP3 Users elements*).

Table 32: Required attributes

Attribute Name	GUI Field Name	For Operation	Notes
domain	SS7 Domain	• Insert • Delete	Not applicable
pointcode	Remote Point Code	• Insert • Delete	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
ssn	Remote SSN	• Insert • Delete	CLI ignores leading zeros, for example: 001 = 01 = 1

Optional attributes

This table lists the optional attributes for the `rmu` managed object. The table maps the command attributes to their corresponding field names on the **Remote MTP3 Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote MTP3 Users*).

Table 33: Optional Attribute

Attribute Name	GUI Field Name	Operation
name	Remote MTP3 User Name	• Insert

Samples

To insert an RMU named RMU_01 with a point code of 3-3-3, the domain as ANSI, and an SSN of 5, use any of use any of these commands:

```
insert: rmu: pointcode=003-003-003: domain=ansi: ssn=5

Insert: RMU: Pointcode=3-3-3: Domain=ansi: Ssn=5

INSERT: RMU: NAME=RMU_01: POINTCODE=003-003-003: DOMAIN=ANSI: SSN=5
```

To delete the RMU RMU_01, use any of the following commands:

```
delete: rmu: pointcode=003-003-003: domain=ansi: ssn=5

Delete: RMU: Pointcode=3-3-3: Domain=ansi: Ssn=5

DELETE: RMU: POINTCODE=003-003-003: DOMAIN=ANSI: SSN=5
```

Link Sets

Managed object

`linkset`

GUI page updated

Link Sets page

Allowed operations

The table shows the operations allowed on the **Link Sets** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 34: Allowed operations

Operation	Description
Insert	Adds a Link Set to the configuration.
Delete	Deletes a Link Set from the configuration.

Required attributes

This table lists the required attributes for the `linkset` managed object. The table maps the command attributes to their corresponding field names on the **Link Sets** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Link Sets elements*).

Table 35: Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
name	Link Set Name	• Insert • Delete	Not applicable
lsp	Local Signaling Point	• Insert	Not applicable
pointcode	Adjacent Remote Point Code	• Insert	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 domain	• Insert	Not application
assignrc	Assign Routing Context	• Insert	If **assignrc = yes**, and the optional **routingcontext** attribute is not specified, then the default value of **routingcontext** prevails (i.e., the first unused integer value greater than zero).

Optional attributes

This table lists the optional attributes for the `linkset` managed object. The table maps the command attributes to their corresponding field names on the **Link Sets** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Link Sets elements*).

Table 36: Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	On EAGLE XG applications where configuration is performed from the SOAM, this parameter is optional.
routingcontext	Routing Context	• Insert	The following rules are applicable for routing context. The attribute value is not case-sensitive: • If you do not want a routing context to be assigned, specify **No** for the **assignrc** field. If the

Attribute Name	GUI Field Name	For Operation	Notes

			routingcontext attribute is specified and **assignrc=no**, then the routing context is ignored:
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=003-003-003: domain=ansi: assignrc=NO`
			or
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=3-3-3: domain=ansi: assignrc=no: routingcontext=55`
			• To specify the default routing context as the first unused integer value greater than zero, specify **assignrc=yes**, but do not specify **routingcontext**:
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=3-3-3: domain=ansi: assignrc=YES`
			• To define the routing context, specify **assignrc=yes** and specify a value for **routingcontext**:
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=003-003-003: domain=ansi:assignrc=YES: routingcontext=1000`

Samples

To insert Linkset LS_01 with the LSP as LSP_01 and the adjacent point code as 003-003-003 with no routing context, use any of the following commands:

```
insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=3-3-3:
domain=ansi: assignrc=no

Insert: Linkset: NeName=sig_oam: Name=LS_01: Lsp=LSP_01: Pointcode=003-003-003:
Domain=ansi: Assignrc=no

INSERT: LINKSET: NENAME=sig_oam: NAME=LS_01: LSP=LSP_01: POINTCODE=003-003-003:
DOMAIN=ANSI: ASSIGNRC=no
```

To delete Link Set LS_01, use any of the following commands:

```
delete: linkset: name=LS_01
```

```
Delete: Linkset: Name=LS_01

DELETE: LINKSET: NAME=LS_01
```

All attribute values are case sensitive. The following commands add two different Link Sets:

```
insert: linkset: name=LS_01: lsp=LSP_01: pointcode=003-003-003: domain=ansi:
assignrc=no

insert: linkset: name=ls_01: lsp=LSP_01: pointcode=003-003-002: domain=ansi:
assignrc=no
```

Links

Managed object

`link`

GUI page updated

Links page

Allowed operations

The table shows the operations allowed on the **Links** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 37: Allowed operations

Operation	Description
Insert	Adds a Link to the configuration.
Delete	Deletes a Link from the configuration.

Required attributes

This table lists the required attributes for the `link` managed object. The table maps the command attributes to their corresponding field names on the **Links** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Links elements*).

Table 38: Required Attributes

Attributes Name	GUI Field Name	For Operation
name	Link Name	• Insert • Delete
linkset	Link Set	• Insert
association	Association	• Insert

Optional attributes

This table lists the optional attributes for the `link` managed object. The table maps the command attributes to their corresponding field names on the **Link** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Links elements*).

Table 39: Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	On EAGLE XG applications where configuration is performed from the SOAM, this parameter is optional.
force	Not applicable	• Delete	The only valid value is **force=1**. The attribute is used to force the delete operation for an association, irrespective of its Admin State.

Samples

To insert a Link named Linkl with a Link Set of LS1 and an association of Assoc1 on Signaling Network Element NE_01, use any of the following commands: :

```
insert: link: nename=NE_01: name=Link1: linkset=LS1: association=Assoc1
Insert: Link: NeName=NE_01: Name=Link1: Linkset=LS1: Association=Assoc1
INSERT: LINK: NENAME=NE_01: NAME=Link1: LINKSET=LS1: ASSOCIATION=Assoc1
```

To delete the Link, Link1, use any of the following commands:

```
delete: link: name=Link1
Delete: Link: Name=Link1
DELETE: LINK: NAME=Link1
DELETE: LINK: NAME=Link1: FORCE=1
```

All attribute values are case sensitive. The following commands add two different Links:

```
insert: link: nename=NE_01: name=Link1: linkset=LS1: association=Assoc1
insert: link: nename=NE_01: name=LINK1: linkset=LS2: association=Assoc1
```

Routes

Managed object

`route`

GUI Page updated

Routes page

Allowed operations

The table shows the operations allowed on the **Routes** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 40: Allowed operations

Operation	Description
Insert	Adds a Route to the configuration.
Delete	Deletes a Route from the configuration.
Edit	Allows modification of the Route Cost for an existing Route.

Required attributes

This table lists the required attributes for the `route` managed object. The table maps the command attributes to their corresponding field names on the **Routes** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Routes elements*).

Table 41: Required attributes

Attribute Name	GUI Field Name	For Operation	Notes
pointcode	Remote Point Code	• Insert • Delete • Edit	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 Domain	• Insert • Delete • Edit	Not applicable
linkset	Link Set	• Insert • Delete • Edit	Not applicable
relcost	Relative Cost	• Insert • Edit	CLI ignores leading zeros, for example: 001 = 01 = 1

Optional attributes

This table lists the optional attributes for the `route` managed object. The table maps the command attributes to their corresponding field names on the **Routes** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Routes elements*).

Table 42: Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	On EAGLE XG applications where configuration is performed from the SOAM, this parameter is optional.
name	Route Name	• Insert	Not applicable.

Samples

To insert a Route with a point code of 1-1-1, the domain as ANSI, and a relative cost of 5, use any of the following commands:

```
insert: route: nename=sig_oam: pointcode=1-1-1: domain=ansi: linkset=LS1: relcost=5

Insert: Route: NeName=sig_oam: Pointcode=001-001-001: Domain=ansi: Linkset=LS1:
Relcost=5

INSERT: ROUTE: NENAME=sig_oam: POINTCODE=001-001-001: DOMAIN=ANSI: LINKSET=LS1:
RELCOST=5
```

To delete Route_01, use any of the following commands:

```
delete: route: pointcode=1-1-1: domain=ansi: linkset=LS1

Delete: Route: Pointcode=001-001-001: Domain=Ansi: Linkset=LS1

DELETE: ROUTE: POINTCODE=001-001-001: DOMAIN=ANSI: LINKSET=LS1
```

To update the Relative Cost for Route_01 with a value of 10, use any of the following commands:

```
edit: route: pointcode=1-1-1: domain=ansi: linkset=LS1: relcost=10

Edit: Route: Pointcode=001-001-001: Domain=Ansi: Linkset=LS1: Relcost=10

EDIT: ROUTE: POINTCODE=001-001-001: DOMAIN=ANSI: LINKSET=LS1: RELCOST=10
```

Local SCCP Users

Managed object

`lsu`

GUI page updated

Local SCCP Users page

Allowed operations

The table shows the operations allowed on the **Local SCCP Users** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 43: Allowed operations

Operation	Description
Insert	Adds an LSU to the configuration.
Delete	Deletes an LSU from the configuration.

Required attributes

This table lists the required attributes for the `lsu` managed object. The table maps the command attributes to their corresponding field names on the **Local SCCP Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Local SCCP Users elements*).

Table 44: Required Attributes

Attributes Name	GUI Field Name	For Operation	Note
pointcode	Local Signaling Point	• Insert • Delete	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 Domain	• Insert • Delete	Not applicable
ssn	SSN	• Insert • Delete	Not applicable
application	Application Name	• Insert	Not applicable

Optional attributes

This table lists the optional attributes for the `lsu` managed object. The table maps the command attributes to their corresponding field names on the **Local SCCP Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Local SCCP Users elements*).

Table 45: Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	On EAGLE XG applications where configuration is performed from the SOAM, this parameter is optional.
force	Not applicable.	• Delete	The only valid value is **force=1**. The attribute is used to force the delete operation for an association, irrespective of its Admin State.

Samples

To insert an LSU with a point code of 1-1-1, the domain as ANSI, and an SSN of 5, use any of the following commands:

```
insert: lsu: nename=NO_01: pointcode=1-1-1: domain=ansi: ssn=5:
application=LocalSCCPUser

Insert: Lsu: NeName=NO_01: Pointcode=001-001-001: Domain=Ansi: Ssn=5:
Application=LocalSCCPUser

INSERT: LSU: NENAME=NO_01: POINTCODE=001-001-001: DOMAIN=ANSI: SSN=5:
APPLICATION=LocalSCCPUser
```

To delete an LSU with a point code of 1-1-1, the domain as ANSI, and an SSN of 5, use any of the following commands:

```
delete: lsu: pointcode=1-1-1: domain=ansi: ssn=5

Delete: Lsu: Pointcode=001-001-001: Domain=Ansi: Ssn=5: Force=1

DELETE: LSU: POINTCODE=001-001-001: DOMAIN=ANSI: SSN=5
```

Glossary

A

Adjacent Server Group	A collection of Adjacent Servers that implements a distributed IP signaling function.The group represents a set of Adjacent Servers that share a point code on the signaling gateway.An Adjacent Server Group has a name and a list of Adjacent Servers.
ANSI	American National Standards Institute An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.

C

CLI	Command-line interface
CSV	Comma-separated values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

DAUD	Destination Audit

D

DAVA	Destination Available
DRST	Destination Restricted
DUNA	Destination Unavailable
DUPU	Destination User Part Unavailable An M3UA management message.

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.

I

ITU-I	ITU-International
ITU-N	ITU-National

L

Link	Signaling Link Carries signaling within a Link Set using a specific Association. A Link can belong to only one Link Set and one Association. There is generally one Link per Association in a Link Set.
LNP	Local Number Portability The ability of subscribers to switch local or wireless carriers and still retain the same phone number.

L

LSP	Local Signaling Point A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique primary/true point code within a particular SS7 Domain to an MP server.
LSU	Local SCCP User Refers to an Application Configured with a Subsystem Number to handle “rt-on-ssn” traffic for local signaling point code hosted on MP server.

M

M3RL	M3UA Routing Layer A layer invented by Tekelec to enhance M3UA by adding a true routing layer.
M3UA	SS7 MTP3-User Adaptation Layer M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MTP3	Message Transfer Part, Level 3

P

PDBI	Provisioning Database Interface The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDBA.

P

PDU	Protocol Data Unit

R

Remote MTP3 User	See RMU.
Remote Signaling Point	See RSP.
RMU	Remote MTP3 User Represents a remote SCCP subsystem to which the Signaling Network Interface forwards signaling. When a message is forwarded from an MSC to an HLR, an RMU must be configured for the subsystem on the HLR.
Route	A signaling path from an LSP to an RSP using a specified Link Set
RSP	Remote Signaling Point Represents an SS7 network node (point code) that signaling must be sent to. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.
RST	Routeset Prohibited Test (Msg)

S

SCCP	Signaling Connection Control Part The signaling connection control part with additional functions for the Message Transfer Part (MTP) in SS7 signaling. Messages can be transmitted between arbitrary nodes in the signaling network

S

	using a connection-oriented or connectionless approach.
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.
Sigtran	Signaling Transport
SLS	Signaling Link Selector
STP	Spanning Tree Protocol

T

TFA	TransFer Allowed (Msg)
TFP	TransFer Prohibited (Msg) A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.

U

UDT	Unitdata Transfer

U

UDTS	Unitdata Transfer Service An error response to a UDT message.

X

XUDT	Extended Unit Data
XUDTS	Extended Unitdata Service message An error response to an XUDT message.