



Dialogic® Vision™ Signaling Server Administration Manual

Copyright and legal notice

Copyright © 2009 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Brooktrout, Diva, Cantata, SnowShore, Eicon, Eicon Networks, NMS Communications, NMS (stylized), Eiconcard, SIPcontrol, Diva ISDN, TruFax, Exnet, EXS, SwitchKit, N20, Making Innovation Thrive, Connecting to Growth, Video is the New Voice, Fusion, Vision, PacketMedia, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation or its subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.

The names of actual companies and product mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Revision history

Revision	Release date	Notes
64-0407-02 Rev B	December 2009	BK, Dialogic® Vision™ CX Video Gateway 4.2 and Dialogic® Vision™ VX Integrated Media Platform 4.2
64-0407-02 Rev A	August 2009	BK, Dialogic® Vision™ CX Video Gateway 4.2 and Dialogic® Vision™ VX Integrated Media Platform 4.2
64-0407-01 Rev A	June 2009	DEH/BK, Dialogic® Vision™ CX Video Gateway 4.1 and Dialogic® Vision™ VX Integrated Media Platform 4.1

Last modified: November 16, 2009

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

Table Of Contents

Chapter 1: Introduction	9
Chapter 2: Overview of the Vision™ Signaling Server	11
Vision Signaling Server overview	11
Standalone deployment	11
Redundant deployment	11
Supported SS7 standards	13
Related documentation	14
Chapter 3: Configuring the Signaling Server	15
Overview of configuring the Signaling Server	15
TDM configuration file (txcfg1.txt)	15
IP configuration file (ipcfg1.txt)	16
SS7 configuration file (ss7_config_default.xml)	16
Configuring the Signaling Server	16
Configuring the server in a TDM network	17
Configuring the server in a SIGTRAN SS7 network	18
Reconfiguring the Signaling Server	19
Reconfiguring a standalone server	19
Reconfiguring a redundant server pair	19
Chapter 4: Configuring the physical interface for TDM	21
Overview of configuring the physical interface for TDM	21
Mapping trunk timeslots to SS7 ports	22
Chapter 5: Configuring the TDM SS7 network	23
Overview of configuring the TDM SS7 network	23
SS7 configuration types	24
Redundant direct-connected configuration	24
Redundant STP-connected configuration	24
Standalone direct-connected configuration	25
Standalone STP-connected configuration	25
Chapter 6: Managing the Signaling Server network	27
Overview of managing the Signaling Server network	27
Obtaining general information about a server	28
Determining which Signaling Server is active	29
Using the command line interface	29
Using SNMP	29
Switching control from an active to a backup server	30
Taking a Signaling Server out of service	31
Stopping a standalone Signaling Server	31
Stopping a Signaling Server in a redundant pair	31
Managing MTP links and linksets	32
Enabling or disabling a link	32
Inhibiting or uninhibiting a link	33
Obtaining status information for a link	34
Obtaining status information for a linkset	34
Obtaining statistical information for a link	35
Obtaining statistical information for a linkset	36

Stopping or restarting processes	37
Managing SS7 circuits and circuit groups	38
Blocking or unblocking a circuit	38
Blocking or unblocking a circuit group.....	39
Resetting a circuit.....	40
Resetting a circuit group.....	41
Obtaining status information for a circuit	41
Obtaining general information about a route	43
Obtaining route information using the command line interface	43
Obtaining route information using SNMP	43
Tracing SS7 data packets	44
Using ss7trace	44
Sample output	44
Chapter 7: Troubleshooting SS7 network problems	47
General techniques for troubleshooting SS7 network problems	47
Verifying the Signaling Server trunk status.....	47
Verifying the Signaling Server link status	47
Using the Signaling Server log file.....	47
Common SS7 network issues	49
Link fails to align at layer 2	49
Link aligns but does not become active.....	50
Link toggles in and out of service.....	50
ISUP circuits remain blocked after application starts	51
Chapter 8: ss7 command line interface	53
Using the SS7 command line interface (ss7cli).....	53
ss7cli command summary	54
Link and linkset commands	55
Route commands.....	56
Circuit and circuit group commands.....	56
Server commands	57
ss7cli SIGTRAN command summary.....	58
M3UA layer.....	58
SCTP layer.....	59
stats link.....	60
stats m3ua.....	62
stats psp.....	63
stats route	64
stats sctp.....	65
stats sctsap	66
status assoc	67
status circuit.....	68
status link	70
status linkset.....	72
status m3ua	73
status m3uasap	74
status nsap	75
status route.....	76
status sctp	78
status sctsap	79
status server	80
stats tsap.....	81

trace isup.....	82
trace m3ua.....	83
trace mtp.....	84
trace sctp.....	85
Chapter 9: SS7 configuration file parameters	87
Using the ss7_config_default.xml file	87
Structure of the ss7_config_default.xml file for a TDM configuration	88
Structure of the ss7_config_default.xml file for a SIGTRAN configuration	89
MTP parameters (<MtpConfig>)	90
MTP general parameters	90
MTP Network Service Access Point (NSAP) parameters	92
MTP link parameters	93
MTP linkset parameters	99
MTP route parameters	100
M3UA parameters <M3uaConfig>	102
Using M3UA	103
General M3UA configuration	104
Network configuration	105
NSAP configuration	107
SCT SAP configuration.....	107
Peer signaling process configuration	107
Peer server configuration.....	109
Routing entry configuration.....	110
SCTP parameters <SctpConfig>	111
General SCTP.....	111
SCT Upper SAP	112
SCT Lower SAP (TSAP)	113
ISUP parameters (<IsupConfig>)	114
ISUP general parameters.....	114
ISUP circuit group parameters.....	117
ISUP User Service Access Point (USAP) parameters	119
ISUP Network Service Access Point (NSAP) parameters.....	120
SSP parameters (<SspConfig>)	122
Chapter 10: Glossary	123

1

Introduction

The *Dialogic® Vision™ Signaling Server Administration Manual* provides information about configuring and managing a Dialogic® Vision™ Signaling Server (also referred to as Vision Signaling Server or Signaling Server in this manual).

This manual supplements the *Dialogic® Vision™ CX Video Gateway Administration Manual* and the *Dialogic® Vision™ VX Integrated Media Platform User's Manual*. It assumes that you have already read one of these manuals before using this one.

This manual also assumes that you are familiar with UNIX and SS7.

Note: The products to which this document pertains are part of the NMS Communications Platforms business that was sold by NMS Communications Corporation (“NMS”) to Dialogic Corporation (“Dialogic”) on December 8, 2008. Accordingly, certain terminology relating to the products has been changed. Below is a table indicating terminology that was formerly associated with the products, as well as the new terminology by which the products are now known.

Former terminology	Current terminology
Vision CX Gateway	Dialogic® Vision™ CX Video Gateway
Vision VoiceXML Server	Dialogic® Vision™ VX Integrated Media Platform

2

Overview of the Vision™ Signaling Server

Vision Signaling Server overview

The Vision™ Signaling Server provides an interface to the SS7 network for the Dialogic® Vision™ CX Video Gateway and the Dialogic® Vision™ VX Integrated Media Platform. The Vision™ Signaling Server can be configured to transport ISUP or BICC traffic over either MTP or SIGTRAN, and it supports the signaling protocol (MTP, SIGTRAN, ISUP, ANSI BICC, and ITU BICC) used in fixed line and wireless networks.

Note: The remainder of this manual uses the term Signaling Server to refer to the Vision™ Signaling Server, and the term Vision™ Server to refer to both the Dialogic® Vision™ CX Video Gateway and the Dialogic® Vision™ Integrated Media Platform collectively.

The Signaling Server has the following features:

- Operates in standalone or redundant configurations.
- Supports multiple gateway clients for scalable deployments.
- Supports up to four digital trunks per server, with software configurable for T1 or E1 operation.
- Supports up to 32 signaling links per node.
- Supports up to 16,384 ISUP circuits.
- Supports ANSI BICC and ITU BICC as an ISUP variant.
- In a SIGTRAN configuration, supports 256 SCTP associations.
- In a SIGTRAN configuration, can be an ASP or IPSP node.

Standalone deployment

In a standalone deployment, a single Signaling Server represents an entire signaling point with its own point code. The Signaling Server either terminates all signaling links (in a TDM configuration) or establishes SCTP associations (in a SIGTRAN configuration). The server provides signaling for one or more gateways.

The Signaling Server contains extensive fault detection, isolation, and recovery capabilities. A standalone server, however, may require a service outage to repair or reconfigure components. This type of deployment might not be suitable for applications with strict availability requirements.

Redundant deployment

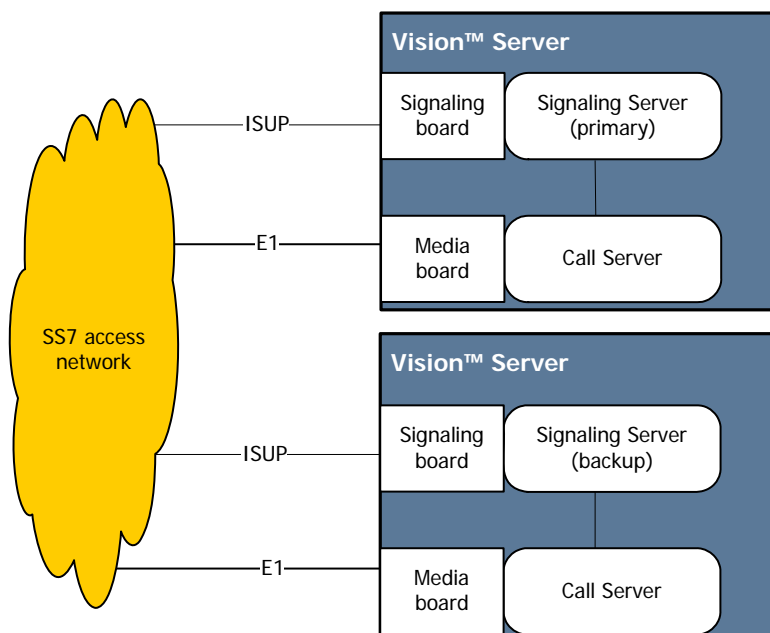
For high availability applications, Signaling Servers are deployed in redundant, mated pairs, using the Dialogic redundant SS7 technology. In redundant configurations, a pair of Signaling Servers represents a single signaling point, sharing a single point code.

Redundant server pairs have the following characteristics:

- At any point in time, one of the servers functions as the primary server and the other functions as the backup server. The servers negotiate the primary/backup roles between themselves at boot time. No operator intervention is required.
- In a TDM configuration, signaling links are spread between both servers. Links on both servers are active, and they fully load-share all traffic to and from the signaling point. All traffic from signaling links terminating on the backup server is backhauled over a private Ethernet link to the primary server for routing and distribution.
- In a SIGTRAN configuration, there are separate SCTP associations from primary and backup to the far endpoint. The association between the primary and far endpoint are active and there is no load-sharing of traffic.
- During operation, the primary server communicates network state information to the backup server. The backup is immediately ready to take over in case of a failure of the primary server or on operator command.

Each of the Vision™ Servers transparently connects with the Signaling Server pairs.

The following illustration shows how a redundant, mated pair of Signaling Servers work together to control signaling:



For identification purposes, one server in a mated pair is designated as the SS701 server and the other is designated as the SS702 server at installation time. This can be either the actual host name of the server or an alias host name. Each client machine must be able to resolve the SS701 and SS702 aliases into the IP addresses of the servers, either through DNS or through local configuration of the client machine.

The SS701 and SS702 aliases do not determine the primary or backup roles of each server. The first server in a mated pair to boot and initialize itself successfully becomes the primary server. The first server remains the primary server either until it fails or until an operator manually requests a switch-over.

Supported SS7 standards

The layers in the Signaling Server comply with the following SS7 standards:

Layer	Standards
MTP	ETS 300-008-1, 300-308-2, ETSI, 1997 GF001-9001 (SS7 for National Telephone Network of China) Q.701-702, ITU-T, 1992 Q.703-704, ITU-T, 1996 Q.707, ITU-T, 1992 Q.781-782, ITU-T, 1996 T1.111, 234, ANSI, 1992 TTC JJ-90.10 (future) NTT Q.701-704, Q.707 (future) GR-246-CORE GR-606-CORE
ISUP	China ISUP EN 300-356-1, ETSI ISUP V.3, 1998 ETS 300-121, ETSI ISUP V.1, 1992 ETS 300-356-1, ETSI ISUP V.2, 1995 ETS 300-356-33, ETSI Q.730-737, ITU-T, 1992 Q.761-764, ITU-T, 1997 Q.767, ITU-T, 1992 Q.784, ITU-T, 1996-1997 T1.113, 236, ANSI, 1995 NTT Q.761-764 (future)
SIGTRAN	SCTP (RFC 2960) and M3UA (RFC 4666)
BICC	Q.1901, ITU-T, 2000 Q.1902-6, ITU-T, 2001 ANSI T1.673-2002[R2007]

Related documentation

The following manuals provide information related to configuring and using the Signaling Server:

Document	Description
<i>Dialogic® Vision™ CX Video Gateway Administration Manual</i>	Describes how to configure and manage the CX Video Gateway. Also describes how to use the Vision™ Console to configure the Vision Signaling Server.
<i>Dialogic® Vision™ VX Integrated Media Platform User's Manual</i>	Describes how to configure and manage the VX Integrated Media Platform. Also describes how to use the Vision™ Console to configure the Vision Signaling Server.
<i>Dialogic® Vision™ SNMP Reference Manual</i>	Describes the management information bases (MIBs) and agents that support SNMP on the Vision™ Server.
<i>Dialogic® NaturalAccess™ Signaling Software Configuration Manual</i>	Describes how to configure the SS7 board and bring links into service.

3

Configuring the Signaling Server

Overview of configuring the Signaling Server

This document describes how to configure the Signaling Server manually. The manual method is intended for advanced users and should be used in consultation with Dialogic Services and Support.

Use the Vision™ Console to configure the Signaling Server, as this web-based tool is designed to handle most configuration needs. Only use the manual method when the Vision™ Console does not meet your configuration needs.

Note: Generating a configuration manually may render the configuration incompatible with the Vision™ Console. Subsequent configuration tasks will need to be performed manually.

The Signaling Server network configuration is based on the following configuration files:

File name	Description
<i>txcfg1.txt</i>	TDM configuration file, which defines the physical characteristics of the T1/E1 trunks. These characteristics include framing, clocking, and signaling link timeslot mappings. The TDM file also contains configuration parameters for the board interface or port number, including the IP addresses used for redundancy.
<i>ipcfg1.txt</i>	IP configuration file, which defines the board interface configuration, IP address and gateway configuration parameters for the SIGTRAN network connection.
<i>ss7_config_default.xml</i>	For TDM configurations, this configuration file defines the SS7 network configuration including signaling links, link sets, routes, and circuit groups. For SIGTRAN configurations, this file defines SCTP, M3UA, IP configurations, and circuit groups.

TDM configuration file (*txcfg1.txt*)

The *txcfg1.txt* file is used to define the four trunk ports as T1 trunks (ESF framing format and B8ZS line coding) or as E1 trunks (clear channel framing format and HDB3 line coding). It also defines a communications port for use as an SS7 link.

The *txcfg1.txt* is generated by the Vision™ Console and resides in */opt/nmstx/etc/cx*. For more information about this file, see the *Dialogic® NaturalAccess™ Signaling Software Configuration Manual*.

IP configuration file (ipcfg1.txt)

The *ipcfg1.txt* file is used to configure the TX board with explicit addressing information for both Ethernets. This file contains commented-out examples for defining interfaces with DHCP or for defining a redundant TX board mate. The sample IP configuration file shipped with the Signaling Server presents the most common type of TX board use.

The *ipcfg1.txt* file is generated by the Vision™ Console and resides in */opt/nmstx/etc/cx*. For more information about this file, see the *Dialogic® NaturalAccess™ Signaling Software Configuration Manual*.

SS7 configuration file (ss7_config_default.xml)

The *ss7_config_default.xml* file is an XML-formatted file that specifies the SS7 network configuration or SIGTRAN-specific configuration for the Signaling Server.

This file is generated by the Vision™ Console and resides in */opt/hs-data/raid/nms_hearsay/cfg/oam*.

Each Signaling Server is shipped with sample SS7 configuration files. These sample files reside in */opt/hs-data/raid/nms_hearsay/cfg/oam/defs*.

Note: In redundant configurations, both Signaling Servers use the identical *ss7_config_default.xml* configuration file. You can copy the configuration file from one server to the same location on the other server, rather than making identical edits to both servers.

For information about the parameters in the *ss7_config_default.xml* file, see *Using the ss7_config_default.xml file* on page 87.

Configuring the Signaling Server

Configure the Signaling Server before it is up and running. The configuration procedure varies depending on the network:

- Configuring the Signaling Server in a TDM network
- Configuring the Signaling Server in a SIGTRAN SS7 network

Configuring the server in a TDM network

To manually configure the Signaling Server in a TDM network, perform the following steps:

Step	Action	For more information, see...
1	Configure the SS7 physical interface, including T1/E1 trunks, clocking, signaling time slots, and the IP configuration for SS7 redundancy.	<i>Overview of configuring the physical interface for TDM on page 21 and Dialogic® NaturalAccess™ Signaling Software Configuration Manual.</i>
2	Configure the SS7 network for the Signaling Server, including setting point codes and protocol variants, and adding SS7 components such as links, circuit groups, and destinations. Only use one of the sample configuration files provided in <code>/opt/hs-data/raid/nms_hearsay/cfg/oam/defs</code> if the <code>ss7_config_default.xml</code> file generated by the Vision™ Console doesn't meet your needs.	<i>Overview of configuring the TDM SS7 network on page 23.</i>
3	Restart all processes on the Signaling Server using the Vision™ Console on the Services page of the Operations menu.	N/A
4	Make backups of all SS7 configuration files using the Vision™ Console Export option, and store them in a safe place.	N/A
5	If the server is part of a redundant pair, copy the configuration file from the active Signaling Server to the same location on the backup server.	N/A
6	If you plan to manage the Signaling Server with SNMP, configure SNMP access rights and trap destinations.	<i>Dialogic® Vision™ SNMP Reference Manual</i>

Configuring the server in a SIGTRAN SS7 network

To manually configure the Signaling Server in a SIGTRAN SS7 network, perform the following steps:

Step	Action	For more information, see...
1	Configure the board's interface, IP address, netmask, and gateway IP address, if needed for SIGTRAN network connectivity.	<i>Dialogic® NaturalAccess™ Signaling Software Configuration Manual</i>
2	Configure the SS7 network for the Signaling Server, depending on SS7 ANSI or ITU network connectivity. Only use one of the sample configuration files provided in <code>/opt/hs-data/raid/nms_hearsay/cfg/oam/defs</code> if the <code>ss7_config_default.xml</code> file generated by the Vision™ Console doesn't meet your needs.	<i>Using the <code>ss7_config_default.xml</code> file on page 87</i>
3	Restart all processes on the Signaling Server using the Vision™ Console on the Services page of the Operations menu.	N/A
4	Make backups of all SS7 configuration files using the Vision™ Console Export option, and store them in a safe place.	N/A
5	If the server is part of a redundant pair, copy the configuration file from the active Signaling Server to the same location on the backup server.	N/A
6	If you plan to manage the Signaling Server with SNMP, configure SNMP access rights and trap destinations.	<i>Dialogic® Vision™ SNMP Reference Manual</i>

Reconfiguring the Signaling Server

This topic describes how to modify the Signaling Server configuration once the server is up and running. The procedure differs depending on whether the server operates as a standalone server, or in a redundant server pair.

Reconfiguring a standalone server

If the server is configured for standalone operation, use the procedure described in *Configuring the server in a TDM network* on page 17 or *Configuring the server in a SIGTRAN SS7 network* on page 18. This requires restarting Signaling Server processes, which results in a service outage.

Reconfiguring a redundant server pair

For redundant Signaling Servers, use the following procedure to reconfigure the physical interface or SS7 network configuration. This procedure allows for configuration changes without a service outage.

Step	Action	For more information, see...
1	Determine which server is the active server and which is the backup server.	<i>Determining which Signaling Server is active</i> on page 29.
2	For TDM configurations, determine which links terminate on the backup server.	<i>Obtaining status information for a link</i> on page 34.
3	For TDM configurations, if there are redundant paths to all destinations through links on both servers, disable the links that terminate on the backup server. This forces all traffic to links that terminate on the active server with no message loss. If there is a link terminated on the backup server that is the only path to a destination, omit this step. Note: Omitting this step can lead to message loss when the Signaling Server is reloaded with the new configuration (applies only to TDM configurations).	<i>Enabling or disabling a link</i> on page 32.
4	Make the necessary configuration changes to the backup server depending on TDM or SIGTRAN network connectivity.	<i>Overview of configuring the physical interface for TDM</i> on page 21. <i>Overview of configuring the TDM SS7 network</i> on page 23.
5	Restart all processes on the backup server using the Vision™ Console on the Services page of the Operations menu.	N/A
6	Make backups of all SS7 configuration files using the Vision™ Console Export option, and store them in a safe place.	N/A
7	For TDM configurations, on the primary server, enable the backup server's signaling links that were disabled in Step 2, if any.	<i>Enabling or disabling a link</i> on page 32.
8	On either server, request a server switchover to make the newly re-configured server the primary Signaling Server.	<i>Switching control from an active to a backup server</i> on page 30.

Step	Action	For more information, see...
9	Copy the configuration file from the active Signaling Server to the same location on the backup server.	<i>Dialogic® NaturalAccess™ Signaling Software Configuration Manual</i>
10	Repeat Steps 5 - 8 for the new backup server in the mated-pair to make the new configuration active.	N/A

4 Configuring the physical interface for TDM

Overview of configuring the physical interface for TDM

The Signaling Server physical interface includes T1/E1 trunks, clocking, and signaling timeslots. Configure this interface by editing the TDM configuration file (*txcfg1.txt*), which resides in */opt/nmstx/etc/cx*.

This section discusses the following topic:

- Mapping trunk timeslots to SS7 ports

For more information about other configuration tasks related to the TDM physical interface, see the *Dialogic® NaturalAccess™ Signaling Software Configuration Manual*.

Mapping trunk timeslots to SS7 ports

The *txcfg1.txt* port command defines a full-duplex connection between the Signaling Server communication controller and a remote SS7 connection over one of the server's T1/E1 trunks. The mapping between an SS7 MTP link number and the Signaling Server's trunk/timeslot is created by:

- Specifying a port number in a link configuration block in the SS7 configuration file (*ss7_config_default.xml*) as

```
<PortNumber>n</PortNumber>
```

- Mapping the port number *n* to a T1/E1 trunk/timeslot with a port command in the *txcfg1.txt* file.

The Signaling Server supports up to 32 low speed (64/56/48 kbps) SS7 ports or up to four high speed (2.048/1.544 Mbps) SS7 ports, subject to restrictions imposed by the license purchased for the Signaling Server. High speed links and low speed links cannot be mixed on the same Signaling Server.

5

Configuring the TDM SS7 network

Overview of configuring the TDM SS7 network

The Signaling Server SS7 network includes the MTP and ISUP layers. Configure these layers by editing the *ss7_config_default.xml* file in */opt/hs-data/raid/nms_hearsay/cfg/oam*. Or choose one of the sample configuration files that most closely matches the desired network configuration. The sample configuration files reside in */opt/hs-data/raid/nms_hearsay/cfg/oam/defs*.

In redundant server configurations, the SS7 configuration files must be identical for both servers.

This section contains the following topic:

- SS7 configuration types

For information about the elements and attributes in the *ss7_config_default.xml* file, see *Using the ss7_config_default.xml file* on page 87.

SS7 configuration types

The Signaling Server has eight sample SS7 configuration files to use as a starting point for configuring the SS7 MTP and ISUP layers. The sample configuration files can create the following types of configurations:

- Redundant direct-connected
- Redundant STP-connected
- Standalone direct-connected
- Standalone STP-connected

Redundant direct-connected configuration

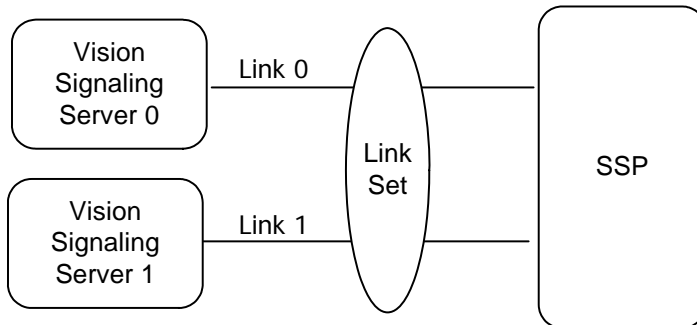
The Signaling Server has two configuration files that create a redundant direct-connected configuration:

- *ss7_ansi_dir_cfg.xml*, for ANSI networks
- *ss7_itu_dir_cfg.xml*, for ITU networks

These configuration files create an SS7 network with the following characteristics:

- Single link set that contains one link for each server in the redundant pair.
- The links in the link set connect directly to an SS7 service switching point (SSP).
- Four circuit groups terminate at the same SSP.

The following illustration shows the redundant direct-connected configuration:



Redundant STP-connected configuration

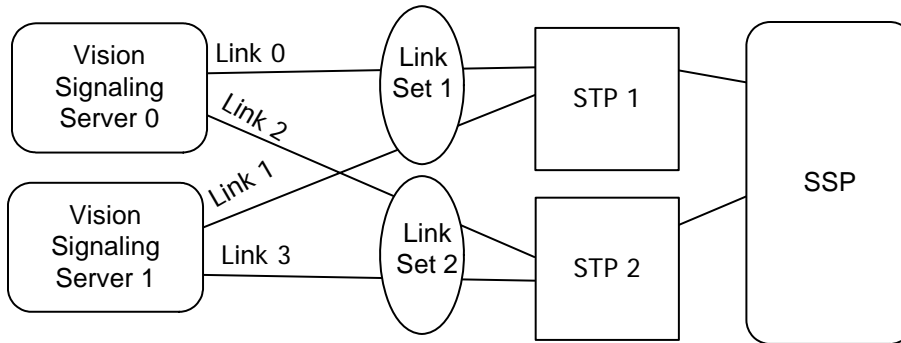
The Signaling Server has two configuration files that create a redundant STP-connected configuration:

- *ss7_ansi_stp_cfg.xml*, for ANSI networks
- *ss7_itu_stp_cfg.xml*, for ITU networks

These configuration files create an SS7 network with the following characteristics:

- Two link sets, with each link set containing one link from each Signaling Server in the redundant pair.
- The links in each link set connect to one of two signal transfer points (STPs).
- The two STPs connect to one SSP.
- Four circuit groups terminate at the same SSP.

The following illustration shows the redundant STP-connected configuration:



Standalone direct-connected configuration

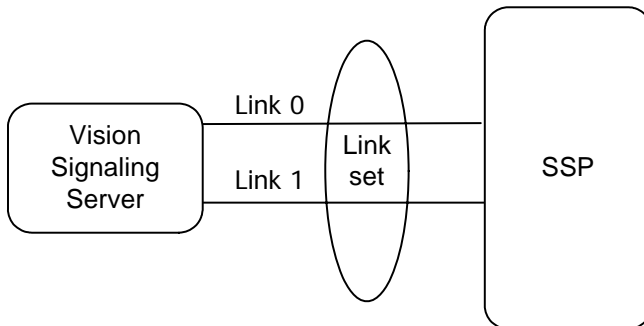
The Signaling Server has two configuration files that create a standalone direct-connected configuration:

- *ss7_stndaln_ansi_dir_cfg.xml*, for ANSI networks
- *ss7_stndaln_itu_dir_cfg.xml*, for ITU networks

These configuration files create an SS7 network with the following characteristics:

- One link set that contains two links from the Signaling Server.
- The links in the link set connect directly to the SSP.
- Four circuit groups terminate at the same SSP.

The following illustration shows the standalone direct-connected configuration:



Standalone STP-connected configuration

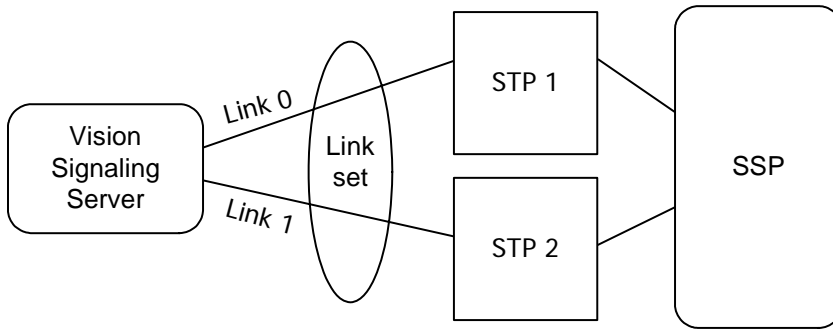
The Signaling Server has two configuration files that create a standalone STP-connected configuration:

- *ss7_stndaln_ansi_stp_cfg.xml*, for ANSI networks
- *ss7_stndaln_itu_stp_cfg.xml*, for ITU networks

These configuration files create an SS7 network with the following characteristics:

- Two link sets, each with a single link from the Signaling Server to one of the mated-pair STPs.
- The two STPs connect to one SSP.
- Four circuit groups terminate at the same SSP.

The following illustration shows the standalone STP-connected configuration:



6

Managing the Signaling Server network

Overview of managing the Signaling Server network

Once the Signaling Server is up and running, you can perform the following actions to manage the Signaling Server network:

- Obtain general information about a server.
- Determine which Signaling Server is active.
- Switch control from an active to a backup server.
- Take a Signaling Server out of service.
- Obtain general information about a process.
- Stop or restart processes.
- Manage MTP links and linksets.
- Manage SS7 circuits and circuit groups.
- Obtain general information about a route.
- Trace SS7 data packets.

Obtaining general information about a server

Use the command line interface to obtain information about the overall state of the Signaling Server. To obtain server information using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	<p>Enter the status server command.</p> <p>The command line interface displays state information for the Signaling Server.</p> <p>For example:</p> <pre>ss7cli] > status server SS7 ME State Info : SSP connection unavailable; Board HA State : Primary Board Interconnect State : Available</pre> <p>For more information, see <i>Status server</i> on page 80.</p>

Determining which Signaling Server is active

You can configure Signaling Servers in two ways:

- In a redundant configuration where one server is the primary server and the other is the backup server.
- As a standalone server.

For software maintenance procedures on the Signaling Servers, you often need to determine the current roles of the Signaling Servers. Determine the role of a Signaling Server by using the command line interface or the SNMP interface.

Using the command line interface

To determine which Signaling Server is active using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command: <pre>status server</pre> <p>The command line interface displays server status information. The Board HA State field indicates whether the server is starting, standalone, primary, or backup. A status of starting means that the system has not yet determined whether the server status is primary or backup.</p>

For more information about returned data, see *status server* on page 80.

Using SNMP

To determine which Signaling Server is active using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Perform an SNMP get operation on Vision-SignalingServer-Manager.mib > ss7Group ss7StateTable. <p>The ss7RmgBoardHaState variable in ss7StateTable contains state information for the specified server. If both Signaling Servers in a redundant configuration are up and running, the primary server has a value of primary (4), and the backup server has a value of backup (5). For more information, see the <i>Dialogic® Vision™ SNMP Reference Manual</i>.</p>

Switching control from an active to a backup server

When Signaling Servers are configured in a redundant configuration, one server is the active server and the other server is the backup server.

The backup server monitors the active server, and takes over the active server's duties immediately if the active server fails or is stopped. The backup server becomes the active server.

For maintenance purposes, you can switch control from an active to a backup server and then service the formerly active server. You can then restart the formerly active server as the backup server that is ready to take control if the active server goes offline.

To switch the active and backup servers using the command line interface, follow these steps:

Step	Action
1	Access the command line interface for either server, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to switch the servers in a redundant pair: <pre>switch</pre> <p>The command line interface switches the servers in a redundant pair. The primary server becomes the backup server, and the backup server becomes the primary server.</p>

To switch the active and backup servers using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to a Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ApplyActionSwitchover action variable to 1.
4	Set the ss7ActionMEIndex action variable to 1.
5	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Taking a Signaling Server out of service

The process for taking a Signaling Server out of service differs, depending on whether the Signaling Server is standalone or in a redundant pair.

Stopping a standalone Signaling Server

To stop a standalone Signaling Server, follow these steps:

Step	Action
1	Block all circuits controlled by the server by using the command line interface or SNMP. This prevents new incoming calls while preserving active calls. For information, see <i>Blocking or unblocking a circuit group</i> on page 39.
2	Monitor the status of call circuits by using the command line interface or SNMP. For information, see <i>Obtaining status information for a circuit</i> on page 41.
3	Once all active calls have been completed (all circuits are idle), stop all processes on the server by using the Vision™ Console on the Services page of the Operations menu.
4	Stop the Signaling Server's signaling board by doing either of the following: <ul style="list-style-type: none"> • Use the command line interface Halt board command. • Set the Vision-SignalingServer-Manager.mib > ss7Group > SS7ApplyActionHalt action variable to 1.

Stopping a Signaling Server in a redundant pair

To stop a Signaling Server in a redundant pair, follow these steps:

Step	Action
1	If the server to be stopped is the primary server, make it the backup server. For information, see <i>Switching control from an active to a backup server</i> on page 30.
2	From the new primary server, disable all links that terminate on the Signaling Server being taken out of service. This terminates all traffic to the server being taken out of service without message loss. For information, see <i>Enabling or disabling a link</i> on page 32.
3	Stop the Signaling Server's signaling board by doing either of the following: <ul style="list-style-type: none"> • Use the command line interface Halt board command. • Set the Vision-SignalingServer-Manager.mib > ss7Group > SS7ApplyActionHalt action variable to 1.
4	Stop all processes on the server by using the Vision™ Console on the Services page of the Operations menu.

Managing MTP links and linksets

The embedded SS7 software in the Signaling Server assigns a link number in the range 0 - 31 to each link. The SS7 command line interface link commands (status, stats, enable, inhibit, and so forth) require this link number to identify the link on which to perform the requested operation.

Each link also has a link index associated with it, in the range 1 – 32. The link index is assigned in the SS7 configuration file (*ss7_config_default.xml*). The link index for a particular link is always 1 greater than the link number. For example, link number zero uses link index 1, and link number 1 uses link index 2. SNMP uses the link index to identify the link on which to perform the requested operation

You can perform the following actions to manage the MTP links and linksets in your SS7 network:

- Enable or disable a link
- Inhibit or uninhibit a link
- Obtain status information for a link
- Obtain status information for a linkset
- Obtain statistical information for a link
- Obtain statistical information for a linkset

You can perform all of these actions by using either the command line interface or the SNMP interface. Unless specified otherwise, you must perform all of these actions on the active Signaling Server. For information, see *Determining which Signaling Server is active* on page 29.

Enabling or disabling a link

Enable or disable a link using the command line interface or the SNMP interface.

To enable or disable a link using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to enable a link: <pre>enable link <i>n</i></pre> Enter the following command to disable a link: <pre>disable link <i>n</i></pre> For both of these commands, <i>n</i> is the number of the link that you want to enable or disable.

To enable or disable a link using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ActionParameterLinkNumber action variable to the index of the link you want to enable or disable.
4	Set the ss7ActionMEIndex action variable to 1.
5	Do either of the following: <ul style="list-style-type: none"> To enable a link, set the s7ApplyActionEnableLink action variable to 1. To disable a link, set the ss7ApplyActionDisableLink action variable to 1.
6	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Inhibiting or uninhibiting a link

Inhibit or uninhibit a link by using the command line interface or the SNMP interface.

To inhibit or uninhibit a link using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to inhibit a link: <pre>inhibit link n</pre> Enter the following command to uninhibit a link: <pre>uninhibit link n</pre> For both of these commands, n is the number of the link that you want to inhibit or uninhibit.

To inhibit or uninhibit a link using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ActionParameterLinkNumber action variable to the MTP link index for the link you want to inhibit or uninhibit.
4	Set the ss7ActionMEIndex action variable to 1.
5	Set the appropriate action variable to 1 to inhibit or uninhibit a link: <ul style="list-style-type: none"> To inhibit a link, set the ss7ApplyActionInhibitLink action variable to 1. To uninhibit a link, set the ss7ApplyActionUninhibitLink action variable to 1.
6	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Obtaining status information for a link

Obtain status information for a link using the command line interface or SNMP interface. Perform this action on the primary server, unless you want to obtain layer 2 status information for a link. In this case, perform this action on the server at which the link terminates, even if it is the backup server.

Note: Links that terminate on the backup server appear with an L2 state of Remote when viewed on the primary server.

To obtain status information for a link using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to obtain status information for a specific link: <pre>status link n</pre> where <i>n</i> is the number of the link for which you want to obtain status information. Enter the following command to obtain status information for all links on the Signaling Server: <pre>status link *</pre>

For information about the data that gets returned, see *status link* on page 70.

To obtain status information for a link using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Perform an SNMP get operation on Vision-SignalingServer-Manager.mib > ss7Group > ss7MtpLinkTable. The ss7MtpLinkTable is indexed by the following attributes: <ul style="list-style-type: none"> • ss7MtpLinkMEIndex, which is always set to 1 for Signaling Servers • ss7MtpLinkIndex The ss7MtpLinkTable contains status information for the specified link, including the link state and whether or not the link is congested or inhibited. For more information, see the <i>Dialogic® Vision™ SNMP Reference Manual</i> .

Obtaining status information for a linkset

Obtain status information for a linkset using the command line interface or the SNMP interface.

To obtain status information for a linkset using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to obtain status information for a specific linkset: <pre>status linkset n</pre> where <i>n</i> is the link number of the linkset for which you want to obtain status information.

Step	Action
	Enter the following command to obtain status information for all linksets on the primary Signaling Server and backup server, if any: <pre>status linkset *</pre>

For information about the data that gets returned, see *status linkset* on page 72.

To obtain status information for a linkset using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Perform an SNMP get operation on Vision-SignalingServer-Manager.mib > ss7Group > ss7MtpLinksetTable. The ss7MtpLinksetTable is indexed by the following attributes: <ul style="list-style-type: none"> • ss7MtpLinksetMEIndex, which is always set to 1 for Signaling Servers • ss7MtpLinksetIndex The ss7MtpLinksetTable contains status information for the specified link, including the linkset state and whether or not all links in the linkset are congested. For more information, see the <i>Dialogic® Vision™ SNMP Reference Manual</i> .

Obtaining statistical information for a link

Obtain statistical information for a link by using the command line interface or the SNMP interface. Perform this action on the primary server, unless you want to obtain layer 2 statistical information. In this case, perform this action on the server at which the link terminates, even if it is the backup server.

To obtain statistical information for a link using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to obtain statistical information for a specific link: <pre>stats link n</pre> where <i>n</i> is the link number of the link for which you want to obtain status information.

For more information, see *stats link* on page 60.

To obtain statistical information for a link using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the Signaling Server for which you want to obtain link statistics.
2	<p>Perform an SNMP get operation on Vision-SignalingServer-Manager.mib > ss7Group > ss7MtpLinkTable.</p> <p>The ss7MtpLinkTable is indexed by the following attributes:</p> <ul style="list-style-type: none"> • ss7MtpLinkMEIndex, which is always set to 1 for Signaling Servers • ss7MtpLinkIndex <p>The ss7MtpLinkTable contains statistical information for the specified link, including the number of dropped transmit messages and the current number of messages in the layer 2 and layer 3 transmit queues.</p> <p>For more information, see the <i>Dialogic® Vision™ SNMP Reference Manual</i>.</p>

Obtaining statistical information for a linkset

To obtain statistical information for a linkset using the SNMP interface:

Step	Action
1	Connect the SNMP management software to the Signaling Server for which you want to obtain link statistics.
2	<p>Perform an SNMP get operation on Vision-SignalingServer-Manager.mib > ss7Group > s7MtpLinksetTable.</p> <p>The ss7MtpLinksetTable is indexed by the following attributes:</p> <ul style="list-style-type: none"> • ss7MtpLinksetMEIndex, which is always set to 1 for Signaling Servers • ss7MtpLinksetIndex <p>The ss7MtpLinksetTable contains statistical information for the specified linkset, including the current number of active and congested links in the linkset.</p> <p>For more information, see the <i>Dialogic® Vision™ SNMP Reference Manual</i>.</p>

Stopping or restarting processes

You can stop or restart processes on the Services page of the Operations menu in the Vision™ Console. For more information, see the *Dialogic® Vision™ CX Video Gateway Administration Manual* or the *Dialogic® Vision™ VX Integrated Media Platform User's Manual*.

Managing SS7 circuits and circuit groups

Circuit groups are identified by a circuit group index (range 1 – 4095) assigned in the *ss7_config_default.xml* file. A circuit group contains a maximum of 32 (ITU/E1) or 24 (ANSI/T1) circuits, and usually corresponds to a single E1 or T1 trunk carrying the corresponding circuits.

Individual circuits are assigned a circuit ID value based on the starting circuit ID value assigned to its circuit group in the *ss7_config_default.xml* file. For example, if a circuit group is assigned the starting circuit ID 1 and includes 31 circuits, then those circuits are assigned circuit IDs 1 – 31.

Circuit IDs are unique across all configured circuits on a Signaling Server or server pair. This contrasts with ISUP circuit identification codes (CICs) which are only unique to a particular destination point code. In other words, if a Signaling Server is connected to multiple SSPs, their CIC ranges can overlap. In configurations where the Vision Signaling Server is not connected to multiple SSPs with overlapping CIC ranges, you should configure the circuit index to be identical to the CIC for each circuit.

You can perform the following actions to manage the circuits and circuit groups in the SS7 network:

- Block or unblock a circuit
- Block or unblock a circuit group
- Reset a circuit
- Reset a circuit group
- Obtain status information for a circuit

You can perform most of these actions by using either the SNMP interface or the command line interface. You must perform these actions on the active Signaling Server. For information about determining which Signaling Server is active, see *Determining which Signaling Server is active* on page 29.

Blocking or unblocking a circuit

Note: Blocking or unblocking an individual BICC circuit is not supported.

To block or unblock a circuit using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	To block a circuit, enter: <pre>block circuit n</pre> To unblock a circuit, enter: <pre>unblock circuit n</pre> For both of these commands, n is the circuit ID of the circuit that you want to block or unblock.

To block or unblock a circuit using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ActionParameterCircuitNumber action variable to the ID of the circuit to be blocked or unblocked.
4	Set the ss7ActionMEIndex action variable to 1.
5	Do either of the following: <ul style="list-style-type: none"> To block the specified circuit, set the ss7ApplyActionBlockCircuit action variable to 1. To unblock the specified circuit, set the ss7ApplyActionUnblockCircuit action variable to 1.
6	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Blocking or unblocking a circuit group

Block or unblock a circuit group using the command line interface or SNMP. These procedures block or unblock all circuits in the circuit group. To block or unblock a subset of circuits in the circuit group, you must individually block or unblock each of those circuits.

To block or unblock a circuit group using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command to block a circuit group: <pre>block group n</pre> Enter the following command to unblock a circuit group: <pre>unblock group n</pre> For both of these commands, n is the circuit ID of any circuit in the group you want to block or unblock.

To block or unblock a circuit group using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ActionParameterCircuitNumber action variable to the circuit group ID of the circuit group that you want to block or unblock.
4	Set the ss7ActionMEIndex action variable to 1.
5	Do either of the following: <ul style="list-style-type: none"> To block the specified circuit group, set the ss7ApplyActionBlockCircuitGroup action variable to 1. To unblock the specified circuit group, set the ss7ApplyActionUnblockCircuitGroup action variable to 1.
6	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Resetting a circuit

To reset a circuit using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command <pre>reset circuit <i>n</i></pre> where <i>n</i> is the ID of the circuit that you want to reset.

To reset a circuit using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ActionParameterCircuitNumber action variable to the circuit group ID of the circuit that you want to reset.
4	Set the ss7ActionMEIndex action variable to 1.
5	Set the ss7ApplyActionResetCircuit action variable to 1.
6	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Resetting a circuit group

To reset a circuit group using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command <pre>reset group n</pre> where n is the circuit ID of any circuit in the group that you want to reset. Note: This procedure resets all circuits in the group. To reset a subset of circuits in the circuit group, you must individually reset each circuit in the subset.

To reset a circuit group using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Access Vision-SignalingServer-Manager.mib > ss7Group.
3	Set the ss7ActionParameterCircuitNumber action variable to the circuit group ID of any circuit in the circuit group that you want to reset. Note: This procedure resets all circuits in the group. To reset a subset of circuits in the circuit group, you must individually reset each circuit in the subset.
4	Set the ss7ActionMEIndex variable to 1.
5	Set the ss7ApplyActionResetCircuitGroup action variable to 1.
6	Submit the changes.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Obtaining status information for a circuit

To obtain status information for a circuit using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	Enter the following command: <pre>status circuit n</pre> where n is the number of the circuit for which you want to obtain status information.

For information about the data that gets returned, see *status circuit* on page 68.

To obtain status information for a circuit using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	Perform an SNMP get operation on Vision-SignalingServer-Manager.mib > ss7Group > ss7IsupCircStateTable. The ss7IsupCircStateTable contains status information for the specified circuit, including its circuit state and the state of any calls on the circuit.

For more information, see the *Dialogic® Vision™ SNMP Reference Manual*.

Obtaining general information about a route

Use either the command line interface or SNMP to get information about routes.

Obtaining route information using the command line interface

To obtain route information using the command line interface, follow these steps:

Step	Action
1	Access the command line interface, as described in <i>Using the SS7 command line interface (ss7cli)</i> on page 53.
2	<p>Enter the following command to obtain information about a specific route:</p> <pre>status route <i>n</i></pre> <p>where <i>n</i> is the index of the route for which you want to obtain information, as specified in the SS7 configuration file (<i>ss7.config.default.xml</i>).</p> <p>Note: You cannot retrieve status for an up route, which typically has route index 1.</p> <p>Enter the following command to obtain information about all routes in the SS7 network:</p> <pre>status route *</pre>

For information about the returned data, see *status route* on page 76.

Obtaining route information using SNMP

To obtain status information for routes using the SNMP interface, follow these steps:

Step	Action
1	Connect the SNMP management software to the primary Signaling Server.
2	<p>Perform an SNMP get operation on the Vision-SignalingServer-Manager.mib > ss7Group > ss7MtpRouteTable. The ss7MtpRouteTable is indexed by the following attributes:</p> <ul style="list-style-type: none"> ss7MtpRouteMEIndex, which is always set to 1 for Signaling Servers ss7MtpRouteIndex <p>The ss7MtpRouteTable contains status information for the specified route, including its state and whether or not all of its links are congested.</p> <p>For more information, see the <i>Dialogic® Vision™ SNMP Reference Manual</i>.</p> <p>Note: You cannot retrieve status for an up route, which typically has route index 1.</p>

Tracing SS7 data packets

Use the `ss7trace` utility to trace SS7 data packets when monitoring or troubleshooting SS7 signaling. `ss7trace` displays any debug data tracing turned on through the command line interface or the SNMP interface. It does not accept commands; it only displays the tracing.

Note: In a configuration with redundant Signaling Servers, run `ss7trace` on the active Signaling Server to display live traffic tracing.

`ss7trace` is located in `/opt/nmstx/bin`.

Using `ss7trace`

To use `ss7trace`, follow these steps:

Step	Action
1	Enable tracing for MTP packets and ISUP packets as follows: <ul style="list-style-type: none"> To trace MTP packets, enable MTP tracing and specify which component to trace by using the <code>trace mtp</code> command in the SS7 command line interface. For information, see <i>trace mtp</i> on page 84. To trace ISUP packets, enable ISUP tracing and specify which component you want to trace by using the <code>trace isup</code> command in the SS7 command line interface. For information, see <i>trace isup</i> on page 82.
2	Use SSH to access the active Signaling Server, and log on as root.
3	Access the Dialogic environment shell: <pre>bash</pre>
4	Start <code>ss7trace</code> by entering the following command: <pre>ss7trace</pre>

Sample output

The output of `ss7trace` differs depending on the trace data. If MTP has data tracing on, `ss7trace` shows a hexadecimal display of all messages passed between MTP layer 2 and layer 3. If ISUP data tracing is on, `ss7trace` shows a hexadecimal display of all ISUP messages.

The following example shows the output generated for a single received packet followed by a single transmitted packet when both MTP and ISUP layer tracing are enabled. This example shows hexadecimal dumps of the actual packets sent and received. You must be familiar with the detailed encodings of ISUP or MTP packets to decode the trace data.

The packets in this example were collected from an ANSI configuration:

```

14:46:36.0 MTP3.1 <-- : Link # 1
85 01 00 00 02 00 00 05 06 00 01 00 20 01 0A 03 .....
06 0B 03 C0 90 A2 05 03 10 01 01 01 0A 05 03 10 .....
04 22 04 00 00
."...
14:46:36.0 ISUP.1 <-- 0.0.2:
06 00 01 00 20 01 0A 03 06 0B 03 C0 90 A2 05 03 ....
10 01 01 01 0A 05 03 10 04 22 04 00 .....".
14:46:36.0 ISUP.1 --> 0.0.2:
06 00 06 14 14 00 .....
14:46:36.0 MTP3.1 --> : Link # 1
85 02 00 00 01 00 00 09 06 00 06 14 14 00 00 .....

```

Note: The point code length in the routing label is different for ITU or Japan protocol variants.

The output of *ss7trace* contains the following sections:

Section	Description
MTP heading	Shows the following information: <ul style="list-style-type: none"> • Time the packet was sent or received. • Layer generating the trace. • Direction of the message (--> indicates a transmitted packet, <-- indicates a received packet). • Link number for the link on which the packet was sent or received.
MTP packet trace	Contains the content of the packet starting with the service information octet (SIO) followed by the routing label (DPC, OPC, and SLS). The data portion of the packet then follows.
ISUP heading	Shows the following information: <ul style="list-style-type: none"> • Time the packet was sent or received. • Direction of the message (--> indicates a transmitted packet, <-- indicates a received packet). • Destination point code to which the packet was sent or from which it was received.
ISUP packet trace	ISUP portion of the packet being sent or received, starting with the circuit identification code (CIC), followed by the message type and parameters.

7 Troubleshooting SS7 network problems

General techniques for troubleshooting SS7 network problems

This topic describes how to use the following techniques to troubleshoot SS7 network problems:

- Verify the Signaling Server trunk status
- Verify the Signaling Server link status
- Use the Signaling Server log file

Verifying the Signaling Server trunk status

Use the `cpcon` utility `frstatus` command to check the status of trunks on the signaling board. The trunk carrying SS7 links should show a state of SYNC and no RX or TX alarms for the links to come into service.

For example:

```
1) [con] > frstatus
```

Trunk	State	RX Alarms	TX Alarms	Loop	B C	Testing
1	SYNC	NO ALARMS	NO ALARMS			NONE
2	SYNC	NO ALARMS	NO ALARMS			NONE
3	NO CONNECT	R	NO ALARMS			NONE
4	NO CONNECT	R	NO ALARMS			NONE

Verifying the Signaling Server link status

Use the SS7 command line interface to check link status and statistics. The status link `<n>` command provides the current status of a signaling link, including its MTP layer 3 state, layer 2 state, congestion status, and inhibiting status. Use the status link `*` command to get a summary status of all configured links.

For example:

```
[ss7cli] > status link *
```

Link	L3 State	L2 State	Inh	Blk	CongestLvl	L2FlowCtlLvl
0	Active	In Service			0	0
1	Active	In Service			0	0

Using the Signaling Server log file

The Signaling Server log file (`/opt/hs-data/log/log_service/localsystem.log`) is the primary troubleshooting tool for link alignment problems once the trunk's status has been verified. Check the log file on the server where the link physically terminates for messages related to the link. This server might be the backup server in a redundant configuration.

The following shows a sample set of log messages for a normal link that correctly comes into service:

```

...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Starting Alignment (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Sent SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@isup     1 Primary received from MTP [USAP=0].
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Sent SIE (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIE (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Timer 4 Expired (LINK 0 ALIGNED at layer 2).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 MTP3 Resume for DPC 0.0.2 (0x2).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Setting link 0 ACTIVE from SLTA.
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 MTP3 Link 0 Up.
    
```

Common SS7 network issues

This topic describes how to troubleshoot the following SS7 network issues:

- Link fails to align at layer 2
- Link aligns but does not become active
- Link toggles in and out of service
- ISUP circuits remain blocked after application starts

Link fails to align at layer 2

An SS7 link can fail to align at layer 2 for a variety of reasons, ranging from physical connection problems to configuration errors. To troubleshoot link problems, first verify that the trunk carrying the link is synchronized and alarm-free.

If the trunk is not synchronized or shows RX alarms, check that the physical connection between the Signaling Server and the switch or STP is correct. If the physical connection is correct, check that the trunk configuration (framing and coding) in the *txcfg1.txt* file matches the trunk configuration on the switch or STP.

If the physical connection is correct, follow these steps:

Step	Action
1	Check that the trunk configuration (framing and coding) in the <i>txcfg1.txt</i> file matches the trunk configuration on the switch or STP.
2	<p>If the trunk configuration is correct, use the Signaling Server log file to verify that the SS7 MTP layer on the server is receiving LSSUs for the link. If no packets are received, the log might look like this:</p> <pre>@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Starting Alignment (Lnk 0). @INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Sent SIO (Lnk 0). @INFO@SS_SS7_TX@txalarm@txboard@mtp 1 ALIGN TIMER 2 EXPIRED iacSt=8 (Lnk 0). @INFO@SS_SS7_TX@txalarm@txboard@mtp 1 LinkFailure (Lnk 0): Alignment Not Possible. @INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Sent SIOS (Lnk 0).</pre> <p>Possible causes of not receiving packets on the link are:</p> <ul style="list-style-type: none"> • The link is not provisioned or is not activated at the switch or STP side. • The switch or STP has the link provisioned on a different trunk or on the same trunk but on a different timeslot. • The switch or STP is configured for a different link speed (that is, for 56 or 64 kbps).
3	<p>If the log file indicates that the Signaling Server is receiving SIOS and SIO packets from the network but never a SIE or SIN packet, then the network side is not recognizing LSSUs from the Signaling Server. In this case, the log might look like this:</p> <pre>...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Starting Alignment (Lnk 0). ...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Sent SIO (Lnk 0). ...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Rcvd SIO (Lnk 0). ...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Sent SIE (Lnk 0). ...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Rcvd SIOS (Lnk 0). ...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 LinkFailure (Lnk 0): Alignment Not Possible. ...@INFO@SS_SS7_TX@txalarm@txboard@mtp 1 Sent SIOS (Lnk 0).</pre> <p>Note: This type of error is a rare occurrence. Most network equipment accepts both 1- and 2-byte LSSUs.</p> <p>Possible solutions are:</p>

Step	Action
	<ul style="list-style-type: none"> Change the <LssuLen> parameter for the link to 1. (The Signaling Server transmits 2-byte LSSUs by default.) If this does not correct the problem, check the configuration on the network side to verify that the link is transmitting and receiving on the same timeslot.

Link aligns but does not become active

If a link aligns successfully but does not come into service at MTP layer 3, then the link is failing the signaling link test that occurs after alignment but prior to link activation. In this case, the log looks like this:

```

...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Starting Alignment (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Sent SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@isup      1 Primary received from MTP [USAP=0].
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Sent SIE (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIE (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Timer 4 Expired (LINK 0 ALIGNED at layer 2).
...
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 MTP3 Link 0 DOWN.
    
```

Note: The MTP3 Link <n> DOWN message appears only on the primary Signaling Server log.

Possible causes of signaling link test failure are:

- Signaling Server OPC and DPC do not match the point codes configured on the network side.
- SLC value assigned to the link does not match the SLC assigned to the link on the network side.
- SS7 MTP layer at the Signaling Server does not have a route configured for the DPC at the other end of the link.

Link toggles in and out of service

If a link frequently toggles into and out of service at layer 3, the log file at the primary server usually contains the following sequence, repeated periodically:

```

...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Starting Alignment (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Sent SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@isup      1 Primary received from MTP [USAP=0].
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Sent SIE (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIO (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Rcvd SIE (Lnk 0).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Timer 4 Expired (LINK 0 ALIGNED at layer 2).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 MTP3 Resume for DPC 0.0.2 (0x2).
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Setting link 0 ACTIVE from SLTA.
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 MTP3 Link 0 Up.
...
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 Layer1: SUERM Threshold Reached.
...@INFO@SS_SS7_TX@txalarm@txboard@mtp      1 MTP3 Link 0 Down.
    
```

The cause of this is usually a clocking problem. To find the cause of the clocking problem, check that the:

- Signaling Server main or fallback clock reference is a trunk that is synchronized and alarm-free.

- Network is configured to be the master clock reference for the trunk. By default, the Signaling Server is configured to be the clock slave for all trunks. If the Signaling Server should be the clock master for the trunk, set the loop master parameter for the trunk to true in the *txcfg1.txt* file.

ISUP circuits remain blocked after application starts

At startup, the Signaling Server locally blocks all ISUP circuit groups in its configuration until an application opens and starts each circuit. In some cases, circuits remain blocked after the circuit is started due to network or configuration problems. Possible causes of this are:

Cause	Action																
No network path is available to the destination switch	<p>Check that there is a route configured to the destination switch by using the SS7 command line interface status route command:</p> <pre>[ss7cli] > status route *</pre> <p>The following returned data shows that there is a route configured to DPC 2.</p> <table border="1"> <thead> <tr> <th>Rte</th> <th>DPC</th> <th>OPC</th> <th>RteState</th> <th>Cong</th> <th>Nmb of Cong LS</th> <th>Nmb of Act LS</th> <th>Adj SP Rst</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>2</td> <td>1</td> <td>Available</td> <td>false</td> <td>0</td> <td>1</td> <td>false</td> </tr> </tbody> </table> <p>If no route is configured to that DPC, add a route for it and assign it to at least one link set in the SS7 configuration file. If a route is configured but is not in the available state, check that it is assigned to a link set and that the link set has at least one link that is active.</p> <p>For more information, see <i>Using the SS7 command line interface (ss7cli)</i> on page 53.</p>	Rte	DPC	OPC	RteState	Cong	Nmb of Cong LS	Nmb of Act LS	Adj SP Rst	2	2	1	Available	false	0	1	false
Rte	DPC	OPC	RteState	Cong	Nmb of Cong LS	Nmb of Act LS	Adj SP Rst										
2	2	1	Available	false	0	1	false										
Circuit is remotely blocked	<p>Check the circuit blocking status by using the SS7 command line interface status circuit command:</p> <pre>[ss7cli] > status circuit n</pre> <p>where <i>n</i> is the number of the circuit you are checking.</p> <p>The following returned data shows that circuit 1 is remotely blocked at the network side:</p> <pre>[ss7cli] > status circuit 1 Circuit State : RemBlkd Call State : Idle</pre> <p>Check with network operations to verify that the circuit is physically connected and activated at the remote switch, or if it has been remotely blocked for operational reasons.</p> <p>For more information, see <i>Using the SS7 command line interface (ss7cli)</i> on page 53.</p>																
Circuit identification code (CIC) is not defined at the switch side	<p>Check the log file for ISUP messages related to the blocked circuits. If the log contains the ISUP message "Circuit unequipped [CIRCUIT n]" or "No response to management message [CIRCUIT n]", then the affected circuit may not be defined or activated at the switch side.</p> <p>In some cases, you might have to examine the contents of the ISUP messages sent or received (or both) by the Signaling Server to determine the cause of the problem. Use the SS7 command line interface trace isup command to enable tracing of ISUP packets. Then use the <i>ss7trace</i> utility to capture and view the raw signaling packets, as described in <i>Tracing SS7 data packets</i> on page 44. Turn tracing off with the trace isup data off command, for performance reasons, once you have identified the problem.</p>																

8

ss7 command line interface

Using the SS7 command line interface (ss7cli)

Use the Signaling Server command line interface (*ss7cli*) to monitor and control the operations of the Signaling Servers in the system.

ss7cli provides the following functionality, depending on the Signaling Server configuration:

Signaling Server configuration	ss7cli functionality
MTP/TDM	<ul style="list-style-type: none">• Status information for circuits, circuit groups, links, linksets and routes• Statistical information for links and routes• Commands (actions) for tracing server information and for controlling signaling links, circuits, and servers
SIGTRAN	<ul style="list-style-type: none">• Status information for SCTP, M3UA, SCTP associations, SCTP SAP, and M3UA SAP• Statistical information for SCTP, SCTP SAPs, TSAPs, M3UA, and PSPs• Commands for enabling/disabling trace for layers such as SCTP, M3UA and ISUP

Run the *ss7cli* locally from the standard UNIX prompt on the Signaling Server, or remotely via telnet or remote login. To run the *ss7cli*, follow these steps:

Step	Action
1	<p>From the UNIX prompt, type ss7cli.</p> <p>For an MTP configuration, the following prompt appears:</p> <pre>[ss7cli] ></pre> <p>For a SIGTRAN configuration, the following prompt appears:</p> <pre>[sigtrancli] ></pre>
2	<p>Enter any of the following:</p> <ul style="list-style-type: none">• An <i>ss7cli</i> command, as described in <i>ss7cli command summary</i> on page 54 and <i>ss7cli SIGTRAN command summary</i>.• ? to display a list of valid commands• ? command to get help for a specific command, where command is any valid <i>ss7cli</i> command.

ss7cli command summary

ss7cli uses the following types of commands for an MTP/TDM SS7 configuration:

Command type	Description
Action	Causes actions to be performed on links, linksets, routes, circuits, circuit groups, and Signaling Server boards. All action commands display Action complete upon successful return. If a command is not successful, the command displays an error code and an error message. Action commands do not return any data.
Statistics	Displays statistical information about SS7 entities.
Status	Displays current status information for SS7 entities.

ss7cli provides commands that act on the following entities in an MTP/TDM SS7 configuration:

- Links and linksets
- Routes
- Circuit and circuit groups
- Server

Link and linkset commands

Command	Type	Syntax	Description
disable link	Action	disable link <i>n</i>	Disables link number <i>n</i> . MTP takes the link out of service and does not attempt realignment with the far exchange until the link is manually enabled.
enable link	Action	enable link <i>n</i>	Enables link number <i>n</i> . MTP aligns the link with the far exchange, making it available to carry traffic.
inhibit link	Action	inhibit link <i>n</i>	Inhibits link number <i>n</i> so that it cannot carry normal traffic. You typically inhibit a link to test its quality through special test messages. An inhibit request is denied if it could cause any destination to become unavailable (for example, if the link is the last available link in a linkset). <i>ss7cli</i> returns a successful response even when an inhibit request is denied. You can use status link to determine if the link is inhibited.
uninhibit link	Action	uninhibit link <i>n</i>	Uninhibits link number <i>n</i> , which allows normal traffic to flow over the link. An uninhibit link request succeeds only if the link was locally inhibited. The request is denied if the link is only remotely inhibited. <i>ss7cli</i> returns a successful response even when an uninhibit request is denied. You can use status link to determine if the link is uninhibited.
stats link	Statistics	stats link <i>n</i>	Displays statistical information about links. For more information, see <i>stats link</i> on page 60.
status link	Status	status link <i>n</i> or status link *	Displays status information about link number <i>n</i> or about all links in the SS7 system (*). For more information, see <i>status link</i> on page 70.
status linkset	Status	status linkset <i>n</i> or status linkset *	Displays status information about linkset number <i>n</i> or about all linksets in the SS7 system (*). For more information, see <i>status linkset</i> on page 72.

Route commands

Command	Type	Syntax	Description
stats route	Statistics	stats route <i>n</i>	Displays statistical information about route number <i>n</i> . For more information, see <i>stats route</i> on page 64.
status route	Status	status route <i>n</i> or status route *	Displays status information about route number <i>n</i> or about all routes in the SS7 system (*). For more information, see <i>status route</i> on page 76.

Circuit and circuit group commands

Command	Type	Syntax	Description
block circuit	Action	block circuit <i>n</i>	Blocks the circuit with ID <i>n</i> . Note: Blocking an individual BICC circuit is not supported.
unblock circuit	Action	unblock circuit <i>n</i>	Unblocks the circuit with ID <i>n</i> . Note: Unblocking an individual BICC circuit is not supported.
block group	Action	block group <i>n</i>	Blocks all circuits in the group containing the circuit with ID <i>n</i> .
unblock group	Action	unblock group <i>n</i>	Unblocks all circuits in the group containing the circuit with ID <i>n</i> .
reset circuit	Action	reset circuit <i>n</i>	Resets the circuit with ID <i>n</i> .
reset group	Action	reset group <i>n</i>	Resets all circuits in the group containing the circuit with ID <i>n</i> .
status circuit	Status	status circuit <i>n</i>	Displays status and configuration information for the circuit with ID <i>n</i> . For more information, see <i>status circuit</i> on page 68.

Server commands

Command	Type	Syntax	Description
halt board	Action	halt board	Stops the local Signaling Server's signaling board by performing a reset. This loads only the operating system, and not the SS7 software. Use this command before installing a new configuration or to stop a faulty server.
load board	Action	load board	Loads the SS7 software onto the local Signaling Server's signaling board. Use this command after a configuration change or to start a halted server.
status server	Status	status server	Displays the current state of the Signaling Server. For more information, see <i>status server</i> on page 80.
switch	Action	switch	Switches the servers in a redundant pair. The primary server becomes the backup server, and the backup server becomes the primary server.
trace mtp	Action	trace mtp type indicator link_n	Controls MTP tracing on the Signaling Server. For more information, see <i>trace mtp</i> on page 84.
trace isup	Action	trace isup type indicator	Controls ISUP tracing on the Signaling Server. For more information, see <i>trace isup</i> on page 82.

ss7cli SIGTRAN command summary

ss7cli uses the following types of commands for a SIGTRAN configuration:

Command type	Description
Statistics	Displays counters and statistical information about SS7 entities.
Status	Displays current status information for SS7 entities.
Trace	Enables/disables trace for specified layers of the SS7 network.

ss7cli provides commands that act on the following entities in a SIGTRAN configuration:

- M3UA layer
- SCTP layer

M3UA layer

The following *ss7cli* commands act on the M3UA layer in a SIGTRAN configuration:

Command	Type	Syntax	Description
stats m3ua	Statistics	stats m3ua	Displays MTP 3 counters, M3UA counters, data statistics, and error statistics for the M3UA layer. For more information, see <i>stats m3ua</i> on page 62.
stats psp	Statistics	stats psp <i>pspld</i>	Displays counters, data statistics, and error statistics for the associations with the peer signaling process (PSP) specified by <i>pspld</i> . For more information, see <i>stats psp</i> on page 63.
status m3ua	Status	status m3ua	Displays MTP 3 counters, M3UA counters, data statistics, and error statistics for the M3UA layer. For more information, see <i>status m3ua</i> on page 73.
status assoc	Status	status assoc <i>associd</i>	Displays status information and configuration values for the specified SCTP association specified by <i>associd</i> . For more information, see <i>status assoc</i> on page 67.
status m3uasap	Status	status m3uasap <i>sapld</i>	Displays status information and configuration values for the SCT SAP specified by <i>sapld</i> . For more information, see <i>status m3uasap</i> on page 74.
status nsap	Status	status nsap <i>sapld</i>	Displays counters, data statistics, and error statistics for the NSAP specified by <i>sapld</i> . For more information, see <i>status nsap</i> on page 75.
status sctsap	Status	status sctsap <i>sapld</i>	Displays status information and configuration values for the SCT SAP specified by <i>sapld</i> . For more information, see <i>status sctsap</i> on page 79.
trace m3ua	trace	trace m3ua	Enables or disables data tracing for the M3UA layer. For more information, see <i>trace m3ua</i> on page 83.

SCTP layer

The following *ss7cli* commands act on the SCTP layer in a SIGTRAN configuration:

Command	Syntax	Description
stats sctp	stats sctp	Displays data chunk counters for the SCTP layer. For more information see <i>stats sctp</i> on page 65.
stats sctsap	stats sctsap sapid	Displays transmitted, received, and re-transmitted message statistics for the SCT SAP specified by sapid . For more information, see <i>stats sctsap</i> on page 66.
stats tsap	stats tsap sapid	Displays transmitted, received, and re-transmitted message statistics for the TSAP specified by sapid . For more information, see <i>stats tsap</i> on page 81.
status sctsap	status sctp sappid	Displays status information and configuration values for the SCT SAP specified by sapid . For more information, see <i>status sctsap</i> on page 79.
trace sctp	trace sctp	Enables or disables data tracing for the SCTP layer. For more information, see <i>trace sctp</i> on page 85.

stats link

Displays MTP2 and MTP3 statistical information for a link.

Syntax

stats link *n*

Option	Description
<i>n</i>	Link for which you want to obtain statistical information.

Details

MTP2-related statistics cannot be displayed for a remote link (a link originating on the mate server in a redundant pair). To see MTP2-related statistics, run *ss7cli* from the server where the link originates. MTP3-related statistics are always displayed for a link, whether the link terminates locally or on the mate server.

Returned fields

The following fields are returned for MTP3 statistics:

Field	Description
Tx MSU	Number of messages transmitted by MTP3.
Rx MSU	Number of messages received by MTP3.
Tx Queue Count	Current number of messages in the MTP3 transmit queue. This is zero, unless high congestion is occurring and MTP2 has invoked flow control.
High Tx Queue Count	Highest threshold the MTP3 transmit queue has reached since the Vision Signaling Server was loaded. This is non-zero if high congestion occurred in the past or is occurring now.
Tx Dropped	Number of messages dropped for any reason during transmit. Messages can be dropped due to bad format, congestion, local restart, or no links available.
Tx Dropped Congestion	Number of messages dropped due to congestion during transmit.

The following fields are returned for MTP2 statistics:

Field	Description
Tx Queue Count	Current number of messages in the MTP2 transmit queue.
High Tx Queue Count	Highest threshold the MTP2 transmit queue has reached since the Vision Signaling Server was loaded.
Sap Queue Count	Number of messages currently in the MTP2 receive queue waiting to be passed up to MTP 3.
High Sap Queue Count	Highest threshold the MTP2 receive queue has reached since the Vision Signaling Server was loaded.

Related command

stats route

Example

```
[ss7cli] > stats link 0
```

MTP3 Stats

```
Tx MSU           : 117
Rx MSU           : 106
Tx Queue Count   : 0
High Tx Queue Count : 0
Tx Dropped       : 0
Tx Dropped Congestion : 0
```

MTP2 Stats

```
Tx Queue Count   : 0
High Tx Queue Count : 1
Sap Queue Count   : 0
High Sap Queue Count : 0
```

stats m3ua

Displays general statistical information for the M3UA layer.

Syntax

```
stats m3ua
```

Related command

```
stats link
```

Example

```
[sigtrancli] > stats m3ua

M3UA General Statistics:
Counter      Tx              Rx
=====
DATA         8              8
DUNA         0              0
DUVA         0              0
DAUD         0              0
SCON         0              0
SCON         0              0
DRST         0              0
REGS         0              0
DREG         0              0
REGRSP       0              0
DREGRSP      0              0
ASPUP        1              0
ASPUPACK     0              1
ASPDN        0              0
ASPDNACK     0              0
ASPAC        1              1
ASPACACK     1              1
ASPIA        0              0
ASPIAACK     0              0
HBEAT        0              0
HBEATAACK   0              0
ERROR        0              0
NTFY         1              2
Error Statistics:
Error          Down            Up
=====
No Route      0              0
PC Unavail    0              0
PC Congested  0              0
No PSP Avail  0              0
No NSAP Avail 0              0
LoadShare Fail 0              0
MMH Fail      0              0
Queue Cong    0              0
AS Pending    0              0
```

stats psp

Displays counters, data statistics, and error statistics for the associations with the specified peer signaling process (PSP).

Syntax

stats PSP *pspid*

Option	Description
<i>pspid</i>	Identifies the PSP for which you want to obtain statistical information.

Related commands

stats link

Example

```
Stats psp - M3UA PSP statistics (Psp Id required)
```

```
[sigtrancli] > stats psp 1
```

```
PSP Statistics:
```

Counter	Tx	Rx
DATA	8	8
DUNA	0	0
DUVA	0	0
DAUD	0	0
SCON	0	0
DUPU	0	0
DRST	0	0
REGS	0	0
DREG	0	0
REGRSP	0	0
DREGRSP	0	0
ASPUP	1	0
ASPUPACK	0	1
ASPDN	0	0
ASPDNACK	0	0
ASPAC	1	1
ASPACACK	1	1
ASPIA	0	0
ASPIAACK	0	0
HBEAT	0	0
HBEATAACK	0	0
ERROR	0	0
NTFY	1	2

```
Error Statistics
```

```
Error Message Dropped
```

No Route	0
No PC Avail	0
PC Congested	0
No PSP Avail	0
No NSAP Avail	0
LoadShare Fail	0
MMH Fail	0
Queue Cong	0
AS Pending	0

stats route

Displays statistical information about a route.

Syntax

stats route *n*

Option	Description
<i>n</i>	Identifies the route number for which you want to obtain statistical information.

Returned fields

Field	Description
Rx TFP	Number of transfer-prohibited messages received for this route.
Rx TFR	Number of transfer-restricted messages received for this route.

Related command

stats link

Example

```
[ss7cli] > stats route 2
```

```
Rx TFP          : 0  
Rx TFR          : 0
```

stats sctp

Displays general statistical information for the SCTP layer.

Syntax

```
stats sctp
```

Related command

```
stats link
```

Example

```
[sigtrancli] > stats sctp
```

Counter	Tx	Rx	ReTx
INIT	1	0	0
INITACK	0	1	n/a
SDOWN	0	0	0
COOKIE	1	0	0
COOKACK	0	1	n/a
DATA	12	13	0
DATAACK	7	8	n/a
SDNCOMP	0	0	n/a
DNS_QRY	0	0	0
BYTES	464	432	n/a

```

Stat sctsap          - SCTP SCT SAP statistics (Sap Id required)
[sigtrancli] > stats sctsap 0
Total Bytes Received : 432
Total Bytes Transmitted : 432
Stats tsap          - SCTP TSAP statistics (Sap Id required)
[sigtrancli] > stats tsap 0
SCTP transport sap Statistics:

```

Counter	Tx	Rx	ReTx
INIT	1	0	0
INITACK	0	1	n/a
SDOWN	0	0	0
COOKIE	1	0	0
COOKACK	0	1	n/a
DATA	12	13	0
DATAACK	7	8	n/a
SDNCOMP	0	0	n/a
DNS_QRY	0	0	0
BYTES	0	0	n/a
BIND ReTx	n/a	n/a	0

stats sctsap

Displays transmitted, received, and re-transmitted message statistics for the specified SCT SAP.

Syntax

stats sctsap *sapid*

Option	Description
<i>sapid</i>	Identifies the SCT SAP for which you want to obtain statistical information.

Related commands

stats link

Example

```
sigtrancli] > stats sctsap 0  
Total Bytes Received      : 432  
Total Bytes Transmitted  : 432
```

status assoc

Displays the status of a single M3UA association.

Syntax

status assoc *associd*

Option	Description
<i>associd</i>	Identifies the M3UA association for which you want to obtain information.

Related commands

status m3ua, status m3uasap, status nsap

Example

The following example returns status information for M3UA association 0:

```
[sigtrancli] > status assoc 0  
  
Association State      : ESTABLISHED  
Destination Address   : 192.168.1.2  
Source Address        : 192.168.1.1  
Primary Net Address   : 192.168.1.2  
Destination Port      : 2905  
Source Port           : 2905
```

status circuit

Displays the status of a single circuit.

Syntax

status circuit *n*

Option	Description
<i>n</i>	Identifies the circuit for which you want to obtain status information

Returned fields

Field	Description
Circuit State	<p>Current state of the circuit. Valid values:</p> <ul style="list-style-type: none"> BothBlkd: Locally and remotely blocked. Idle: Idle and ready for a call. LBWaitForBlkResp: Locally blocked. Waiting for a block response. LBWaitForUnblkResp: Locally blocked. Waiting for an unblock response. LocBlkd: Locally blocked. LocUnequipped: Locally unequipped. RBWaitForBlkAck: Remotely blocked. Waiting for a block acknowledgment. RBWaitForUnblkAck: Remotely blocked. Waiting for an unblock acknowledgment. RemBlkd: Remotely blocked. RemUnequipped: Remotely unequipped. WaitForBlkAck: Waiting for a block acknowledgment. WaitForBlkAckAndBlkResp: Waiting for a block acknowledgment and a block response. WaitForBlkAckAndUnblkResp: Waiting for a block acknowledgment and an unblock response. WaitForBlkResp: Waiting for a block response. WaitForUnblkAck: Waiting for an unblock acknowledgment. WaitForUnblkAckAndBlkResp: Waiting for an unblock acknowledgment and a block response. WaitForUnblkAckAndUnblkResp: Waiting for an unblock acknowledgment and an unblock response. WaitForUnblkResp: Waiting for an unblock response.
Call State	<p>Current state of the call. Valid values:</p> <ul style="list-style-type: none"> Transient: Call is being terminated. Idle: No call in progress. BusyIn: Inbound call in progress. BusyOut: Outbound call in progress.

Related commands

status link, status linkset, status route, status server

Example

```
[ss7cli] > status circuit 1
```

```
Circuit State    : Idle  
Call State      : Idle
```

status link

Displays the status of a single link or all links in the SS7 network.

Syntax

status link *n*

Option	Description
<i>n</i>	Identifies the link for which you want to obtain status information. Use an asterisk (*) instead of a number to return status information for all links in the SS7 network.

Returned fields

The returned field names differ, depending on whether you specify a specific link (*n*) or all links (*). The following table shows both sets of field names where appropriate:

Field	Description
Link	Identifies a link.
MTP3 State (specific link) L3 State (all links)	<p>MTP3 state of the link. Valid values:</p> <p>Inactive: Link is manually disabled or internally disabled by MTP. The link typically stays inactive until manual intervention.</p> <ul style="list-style-type: none"> Connecting: MTP is aligning the link. Active: Link is aligned and in service. Failed: Link failed. Typically a transient state until MTP realigns the link. Binding: Link is binding to MTP2. Typically a transient state until the bind succeeds. Unbinding: Link is unbinding from MTP2. Typically a transient state until the unbind succeeds. Unbound: MTP3 has unbound from MTP2 for this link.
MTP2 State (specific link) L2 State (all links)	<p>MTP2 state of locally-terminated links. Valid values:</p> <ul style="list-style-type: none"> Aligned Ready: Link is aligned at layer two. Aligned Not Ready: Link is aligned at layer two, but a processor outage condition exists. In Service: Link is fully available. Initial Alignment: Attempting to align the link. Out of Service: Received a power on request. Not attempting to align the link. Power Off: Initial state. Processor Outage: Processor outage occurred after being in service. <p>For remote links, the value of this field is always Remote.</p>

Field	Description
Inhibited (specific link) Inh (all links)	Indicates whether the link is inhibited. Valid values: <ul style="list-style-type: none"> • None: Link is not inhibited. • Local or L: Link is locally inhibited. • Remote or R: Link is remotely inhibited. • Both: Link is locally and remotely inhibited.
Blocked (specific link) Blk (all links)	Indicates whether the link is blocked (a local or remote processor outage condition). Valid values: <ul style="list-style-type: none"> • None: Link is not blocked. • Local or L: Link is locally blocked. • Remote or R: Link is remotely blocked. • Both: Link is locally and remotely blocked.
Congested	Indicates whether the link is congested. Valid values: <ul style="list-style-type: none"> • True: Link is congested. • False: Link is not congested.
L2 Flow Control Level (specific link) L2FlowCtlLvl (all links)	For locally-terminated links, flow control imposed by MTP2 due to outbound queue thresholds being reached. Valid values: <ul style="list-style-type: none"> • 0: No flow control • 2: Maximum flow control. MTP3 is no longer allowed to send to MTP2. For remote links, the value of this field is always Remote .

Related commands

status circuit, status linkset, status route, status server

Example

The following example returns status information for link 0:

```
[ss7cli] > status link 0
```

```
MTP3 State      : Active
MTP2 State:     : In Service
Inhibited       : None
Blocked         : None
Congested:      : false
```

The following example returns status information for all links in the SS7 network:

```
[ss7cli] > status link *
```

```
L2 Flow Control Level: 0
```

Link	L3 State	L2 State	Inh	Blk	Congested	L2FlowCtlLvl
0	Active	In Service			false	0
1	Active	Remote			false	Remove
2	Active	In Service			false	0
3	Active	Remote			false	Remote

status linkset

Displays the status of a single linkset or all linksets in the SS7 network.

Syntax

status linkset *n*

Option	Description
<i>n</i>	Identifies the linkset for which you want to obtain status information. Use an asterisk (*) instead of a number to return status information for all linksets in the SS7 network.

Returned fields

Field	Description
Linkset	Identifies the linkset.
State	State of the linkset. Valid values: Active Inactive
Congested	Indicates whether the linkset is congested. Valid values: true false
Active Links	Number of currently active links in the linkset.
Congested Links	Number of currently congested links in the linkset.

Related commands

status circuit, status link, status route, status server

Examples

The following example returns status information for linkset 1:

```
[ss7cli] > status linkset 1
State           : Inactive
Congested       : false
Active Links    : 0
Congested Links : 0
```

The following example returns linkset status information for all linksets in the SS7 network:

Linkset	State	Congested	Active Links	Congested Links
1	Active	false	2	0
2	Active	false	2	0

status m3ua

Displays general status information for the M3UA layer.

Syntax

status m3uasap

Related commands

status m3uasap, status nsap

Example

The following example returns general status information for the M3UA layer:

```
[sigtrancli] > status m3ua
Total Memory size in use   : 55451
Total Memory allocated    : 5255
HA State                   : STANDALONE
```

status m3uasap

Displays the status of a single M3UA SAP.

Syntax

status m3uasap *sapid*

Option	Description
<i>sapid</i>	Identifies the M3UA SAP for which you want to obtain information.

Related commands

status nsap

Example

The following example returns status information for M3UA SAP 0:

```
[sigtrancli] > status m3uasap 0  
High Level State      : READY  
Service Provider Id  : 0  
Active Associations   : 1
```

status nsap

Displays the status of a single M3UA NSAP.

Syntax

status nsap *sapid*

Option	Description
<i>sapid</i>	Identifies the NSAP for which you want to obtain information. The <i>sapid</i> should have been configured in the M3UA configuration.

Related commands

status m3uasap

Example

The following example returns status information for NSAP 0:

```
[sigtrancli] > status nsap 0
Local SAP Id       : 0
Remote SAP Id      : 0
High Level State   : BOUND
```

status route

Displays the current status of a single route or all routes in the SS7 network.

Syntax

status route *n*

Option	Description
<i>n</i>	Identifies the route for which you want to obtain status information. Use an asterisk (*) instead of a number to return status information for all routes in the SS7 network.

Returned fields

The returned field names differ, depending on whether you specify a specific route or all routes (*). The following table shows both sets of field names where appropriate:

Field	Description
DPC	Destination point code.
OPC	Originating (local) point code.
Rte State	Current state of the route. Valid values: Available Unavailable
Congested (specific route) Cong (all routes)	Indicates whether the route is congested. Valid values: true false
Num Congested Linksets (specific route) Num of Cong LS (all routes)	Number of congested linksets to this route.
Num Active Linksets (specific route) Num of Act LS (all routes)	Number of active linksets to this route.
Adjacent SP Restarting (specific route) Adj SP Rst (all routes)	Indicates whether the adjacent signaling point is restarting. Values include: true false

Related commands

status circuit, status link, status linkset, status server

Examples

The following example returns status information for route 1:

```
[ss7cli] > status route 1
DPC                : 2
OPC                : 1
Rte State          : Available
Congested          : false
Num Congested Linksets : 0
Num Active Linksets  : 1
Adjacent SP Restarting : false
```

The following example returns status information for all routes in the SS7 network:

```
[ss7cli] > status route *
Rte   DPC      OPC   RteState  Cong   Num of   Num of   Adj SP Rst
---   -
2     2        1    Available false   0        1        false
```

status sctp

Displays general status information for the SCTP layer.

Syntax

```
status m3uasap
```

Related commands

```
status nsap
```

Example

The following example returns general status information for the SCTP layer:

```
[sigtrancli] > status sctp
```

```
Number of Associations      : 1  
Number of Endpoints        : 1  
Number of Local Address    : 0  
Number of Peer Address     : 1
```

status sctsap

Displays the status of a single SCT SAP.

Syntax

status sctsap *sapid*

Option	Description
<i>sapid</i>	Identifies the SCT SAP for which you want to obtain information.

Related commands

status m3ua, status m3uasap, status nsap

Example

The following example returns status information for SCT SAP 0:

```
[sigtrancli] > status sctsap 0  
Protocol switch          : 1  
High Level State        : BOUND
```

status server

Displays the current state of the Signaling Server.

Syntax

status server

Return fields

Field	Description
SS7 ME State Info	State of the SS7 managed element. Valid values: Blank: All is well Configuration error ISUP connection unavailable MTP connection unavailable Logging unavailable RMG connection unavailable SSP connection unavailable Uninitialized ISUP License Failure Dialogic License success
Board HA State	High availability state of the Signaling Server. Valid values: Starting Primary Backup Standalone
Board Interconnect State	State of the Ethernet connection between Signaling Servers in a redundant system. Valid values: Available Unavailable

See also

status link, status linkset, status route, status circuit

Example

```
[ss7cli] > status server
SS7 ME State Info      :  SSP connection unavailable;
Board HA State         :  Primary
Board Interconnect State : Available
```

stats tsap

Displays transmitted, received, and re-transmitted message statistics for the specified TSAP.

Syntax

stats TSAP *sapid*

Option	Description
<i>sapid</i>	Identifies the TSAP for which you want to obtain statistical information.

Related commands

stats link

Example

```
[sigtrancli] > stats tsap 0
```

```
SCTP transport sap Statistics:
```

Counter	Tx	Rx	ReTx
INIT	1	0	0
INITACK	0	1	n/a
SDOWN	0	0	0
COOKIE	1	0	0
COOKACK	0	1	n/a
DATA	12	13	0
DATAACK	7	8	n/a
SDNCOMP	0	0	n/a
DNS QRY	0	0	0
BYTES	0	0	n/a
BIND ReTx	n/a	n/a	0

trace isup

Controls ISUP tracing on the Signaling Server.

Syntax

trace isup *type indicator*

Option	Description
<i>type</i>	<p>Determines what type of information gets traced. Valid values:</p> <ul style="list-style-type: none"> data element error event timer token warning <p>The output for all tracing types except data tracing goes to the SS7 Signaling Server log file, <i>/opt/hs-data/log/log_service/localssystem.log</i>. The output for data tracing goes to <i>ss7trace</i>.</p> <p>For more information, see <i>Using the Signaling Server log file</i> on page 47 and <i>Tracing SS7 data packets</i> on page 44.</p>
<i>indicator</i>	Turns tracing on or off.

See also

trace mtp

Examples

The following example turns ISUP tracing on:

```
trace isup data on
```

The following example turns ISUP tracing off:

```
trace isup data off
```

trace m3ua

Enables or disables data tracing for the M3UA layer.

Syntax

trace m3ua *indicator*

Option	Description
<i>indicator</i>	Turns tracing on or off. Valid values: ena: Enable data tracing. dis: Disable data tracing.

See also

trace mtp

Examples

The following example turns data tracing on for the M3UA layer:

```
trace m3ua ena
```

The following example turns M3UA tracing off for the M3UA layer:

```
trace m3ua dis
```

trace mtp

Controls packet tracing in the MTP layer of the SS7 network. The tracing output goes to the *ss7trace* utility. For more information, see *Tracing SS7 data packets* on page 44.

Syntax

trace mtp *type indicator linknumber*

Option	Description
<i>type</i>	Determines what type of information gets traced. Always set this value to data .
<i>indicator</i>	Turns tracing on or off for a single link or for all links, depending on the value of <i>linknumber</i> .
<i>link_n</i>	Optional. When specified, the Trace mtp command applies only to the specified link. Otherwise, it applies to all links in the SS7 system.

See also

trace isup

Examples

The following example traces all links:

```
trace mtp data on
```

The following example traces only link 1:

```
trace mtp data on 1
```

trace sctp

Enables or disables data tracing for the SCTP layer.

Syntax

trace m3ua *indicator*

Option	Description
<i>indicator</i>	Turns data tracing on or off. Valid values: ena: Enable data tracing. dis: Disable data tracing.

See also

trace mtp

Examples

The following example turns SCTP data tracing on:

```
trace sctp ena
```

The following example turns SCTP data tracing off:

```
trace sctp dis
```

9

SS7 configuration file parameters

Using the `ss7_config_default.xml` file

The `ss7_config_default.xml` is a standard XML format file that configures SS7 network entities. The Signaling Server stores this file on both the primary and backup Signaling Servers, in the `/opt/hs-data/raid/nms_hearsay/cfg/oam` directory. The file on one server is identical to the file on the other.

The SS7 configuration portion of the `ss7_config_default.xml` file is divided into several sections, each of which contains parameters that configure a certain aspect of the SS7 interface. The following table describes each section:

Section	Description	For information, see...
<code><MtpConfig></code>	MTP layer configuration parameters.	<i>MTP parameters (<MtpConfig>)</i> on page 90.
<code><M3uaConfig></code>	M3UA layer configuration parameters.	<i>M3UA parameters <M3uaConfig></i> on page 102
<code><SctpConfig></code>	SCTP layer configuration parameters.	<i>SCTP parameters <SctpConfig></i> on page 111
<code><IsupConfig></code>	ISUP configuration parameters.	<i>ISUP parameters (<IsupConfig>)</i> on page 114.
<code><SspConfig></code>	SSP parameters.	<i>SSP parameters (<SspConfig>)</i> on page 122.

The following topics describe the structure of the `ss7_config_default.xml` file:

- Structure of the `ss7_config_default.xml` file for a TDM configuration
- Structure of the `ss7_config_default.xml` file for a SIGTRAN configuration

Structure of the `ss7_config_default.xml` file for a TDM configuration

The following table shows the structure of the `ss7_config_default.xml` file for a TDM configuration, with the highest-level section names and descriptions in bold:

<MtpConfig>	MTP configuration section
<GenConfig>	MTP general configuration section
<NsapConfig Index= <i>n</i> >	MTP NSAP <i>n</i> configuration section
<LinkConfig Index=1>	MTP link 1 configuration section
<LinkConfig Index= <i>n</i> >	MTP link <i>n</i> configuration section
<LinksetConfig Index=1>	MTP linkset 1 configuration section
<LinksetConfig Index= <i>n</i> >	MTP linkset <i>n</i> configuration section
<RouteConfig = 1>	MTP route 1 configuration section
<RouteConfig = <i>n</i> >	MTP route <i>n</i> configuration section
<IsupConfig>	ISUP configuration section
<GenConfig>	ISUP general configuration section
<CircConfig Index=1>	ISUP CircGrp 1 configuration section
<CircConfig Index= <i>n</i> >	ISUP CircGrp <i>n</i> configuration section
<UsapConfig Index=1>	ISUP USAP 1 configuration section
<UsapConfig Index= <i>n</i> >	ISUP USAP <i>n</i> configuration section
<NsapConfig Index= 1>	ISUP NSAP 1 configuration section
<NsapConfig Index= <i>n</i> >	ISUP NSAP <i>n</i> configuration section
<SspConfig>	SSP configuration section
<GenConfig>	SSP general configuration section

Structure of the `ss7_config_default.xml` file for a SIGTRAN configuration

The following table shows the structure of the `ss7_config_default.xml` file for a SIGTRAN configuration, with the highest-level section names and descriptions in bold:

<IsupConfig>	ISUP configuration section
<GenConfig>	ISUP general configuration section
<CircConfig Index=1>	ISUP CircGrp 1 configuration section
<CircConfig Index= <i>n</i> >	ISUP CircGrp <i>n</i> configuration section
<UsapConfig Index=1>	ISUP USAP 1 configuration section
<UsapConfig Index= <i>n</i> >	ISUP USAP <i>n</i> configuration section
<NsapConfig Index= 1>	ISUP NSAP 1 configuration section
<NsapConfig Index= <i>n</i> >	ISUP NSAP <i>n</i> configuration section
<M3uaConfig>	M3UA configuration section
<GenConfig>	General M3UA configuration
<NetworkConfig Index = 1>	Network configuration
<M3uaNsapConfig Index = 1>	NSAP configuration
<SctSapConfig Index = 1>	SCT SAP configuration
<PspConfig Index = 1>	Peer signaling process configuration
<PsConfig Index = 1>	Peer server configuration
<RteConfig Index = 1>	Routing entry configuration
<SctpConfig>	SCTP configuration section
<GenConfig>	General SCTP
<SctSapConfig Index = 1>	SCT Upper SAP configuration
<TSapConfig Index = 1>	SCT Lower SAP (TSAP) configuration
<SspConfig>	SSP configuration section
<GenConfig>	SSP general configuration section

MTP parameters (<MtpConfig>)

The MTP parameters section of the *SS7_config_default.xml* file begins with the following XML tag:

```
<MtpConfig>
```

It contains the following parameter groups:

- General parameters
- Network Service Access Point (NSAP) parameters
- Link parameters
- Linkset parameters
- Route parameters

MTP general parameters

The MTP general parameters in the *SS7_config_default.xml* configuration file define and control the general operation of the signaling point (SP) that the Signaling Server implements.

The MTP general configuration section, which configures the general parameters, appears as a subsection within the <MtpConfig> section. Its XML tag is <GenConfig>.

The following table lists the configurable parameters in the MTP 3 general configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Note: For timer parameters, a value of zero disables the timer. The units for the timer parameters specified in this table depend on the Mtp3TimerRes parameter setting.

Parameter name	Default	Range	Usage
OPC	None	N/A	Point code of the Signaling Server node, specified as x.y.z (three bytes, decimal, separated by periods), as a hexadecimal value preceded by 0x (0x123), or as a decimal value.
DefaultVariant	ITU	ITU ANSI	Default SS7 variant used for links, linksets, and routes. Specifying a variant in the MTP link, linkset, and route configuration sections overrides the default variant. If you omit the DefaultVariant parameter, you must specify a variant in the MTP link, linkset, and route configuration sections.
DefaultDPC	None	N/A	Default destination point code used for all links, linksets, and circuit groups that do not have an explicit DPC or adjacent DPC specified. Specifying the DPC or adjacent DPC parameter within a link, linkset, or circuit group section overrides the DefaultDPC for that entity.

Parameter name	Default	Range	Usage
Mtp3TimerRes	tenths	tenths seconds	Specifies whether timer values in the configuration file are in seconds or tenths of a second. Note: Changing this parameter is not recommended. Changing the timer resolution to seconds can prevent the server from passing MTP conformance tests.
NodeType	STP	STP SP	If set to STP, the node includes the signal transfer function. If set to SP, the node does not include this function.
DisableUPU	false	true/yes false/no	If set to true, MTP never sends a user part unavailable message.
ValidateSsf	true	true/yes false/no	When set to true, MTP 3 validates incoming MTP 3 signaling network management (SNM) and test (SLTM/SLTA) messages. Any message is rejected whose sub-service field (SSF) does not match the value configured for the link on which the message was received. When set to false, the SSF is not checked for incoming MTP 3 management or test messages. Instead, any SSF value is accepted. MTP 3 does not validate the SSF in any incoming or outgoing user part messages.
RestartRequired	true	true/yes false/no	Set to true if a full restart procedure is required whenever the node becomes accessible. MTP restart procedures are specified in ANSI T1.111.4 section 9 and ITU-T Q.704 section 9.
MaxLinks	4	1 to 32	Maximum number of physical links. The actual maximum depends on the hardware configuration. If you add more than four links, increase this value.
MaxUsers	2	1 to 64	Maximum number of MTP 3 users (user parts).
MaxLinksets	2	1 to 32	Maximum number of linksets supported. If you add more than two linksets, increase this value.
MaxRoutes	32	1 to 32767	Maximum number of routes. If you add more than 32 routes, increase this value.
MaxRouteEntries	1024	1 to 32767	Maximum number of route instances.
TraceData	false	true false	When set to true, starts tracing of all data between MTP 2 and MTP 3.
OpcRouting	false	true false	If true, outbound routing takes into account OPC values, as well as DPC and SLS values. If false, outbound routing takes into account only DPC and SLS values.
TransparentMode	false	true false	If true, all inbound traffic is passed up to the SIO matching bound application regardless of DPC or OPC values. All outbound traffic is shared across all links regardless of DPC or OPC values. If false, normal routing is in effect.
NumberOfRouteMasks	0	0 to 8	Maximum number of routing masks. If zero, then all destination point codes in outgoing messages must exactly match a point code in a route entry.

Parameter name	Default	Range	Usage
RouteMask Index = n		0 to 0x00FFFFFF	A routing mask applied to the destination point code before matching it against route table entries. Can reduce the number of routes that must be configured or when remote destination point codes are not known at configuration time. Multiple route masks can be specified. They are applied in the order in which they appear in the configuration file.
T15	30	0 to 65535	Wait to start or repeat the route set congestion test.
T16	20	0 to 65535	Wait for route set congestion status update.
T18itu	300	1 to 65535	ITU restart timer for an STP during which links are restarted and TFA, TFR, and TFP messages are received.
T20itu	600	1 to 65535	ITU overall restart timer.
T22ansi	300	1 to 65535	ANSI restart timer at restarting SP waiting for links to become available.
T23ansi	300	1 to 65535	ANSI restart timer at restarting SP waiting for TRA messages.
T26ansi	130	1 to 65535	ANSI restart timer at restarting SP waiting to repeat TRW message.
T27ansi	30	1 to 65535	Minimum duration of unavailability for full restart.
TRtelnst	18000	0 to 65535	Internal route instance timer (how long a route instance is valid).

MTP Network Service Access Point (NSAP) parameters

The MTP NSAP parameters in the *SS7_config_default.xml* configuration file define an ISUP interface to MTP.

The MTP NSAP configuration sections, which configure the NSAP parameters, appear as subsections within the <MtpConfig> section. Each MTP NSAP configuration section has an <NsapConfig Index=*n*> XML tag, where *n* is a unique index. There is usually only one MTP NSAP configuration section.

The following table lists the configurable parameters in an MTP NSAP configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Parameter name	Default	Range	Usage
Variant (required if DefaultVariant is not specified)	None	ANSI ITU JNTT JTTC	MTP 3 protocol variant used by this MTP 3 user part. If the Variant parameter is not present, the DefaultVariant parameter from the MTP general parameters section is used. Either the Variant or DefaultVariant parameter must be present.
P0Queue	2	2 to 1024	Receive queue length threshold at which the congestion priority is raised to level 0.
P1Queue	512	(p0Qlen + 2) to 1024	Receive queue length threshold at which the congestion priority is raised to level 1.
P2Queue	768	(p1Qlen + 2) to 1024	Receive queue length threshold at which the congestion priority is raised to level 2.
P3Queue	896	(p2Qlen + 2) to 1024	Receive queue length threshold at which the congestion priority is raised to level 3.
DpcLength	14 (ITU) 16 (JNTT and JTTC) 24 (ANSI)	14 16 24	Number of bits in a point code. For most installations, this value defaults correctly based on the Variant or DefaultVariant parameter. Installations in Japan use the JNTT or JTTC variant and 16-bit point codes. In these installations, set DpcLength to 16. Installations in China use the ITU variant and 24-bit point codes. In these installations, set DpcLength to 24.
OPC	0.0.1	N/A	N/A

MTP link parameters

The MTP link parameters in the *SS7_config_default.xml* configuration file define the properties of the links connected to the SS7 network.

The MTP link configuration sections, which configure the link parameters, appear as subsections within the <MtpConfig> section. Each MTP link configuration section has a <LinkConfig Index=*n*> XML tag, where *n* is a unique index. Each MTP 3 link configuration section configures a single link.

The following table lists the configurable parameters in an MTP 3 link configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Note: The units for the timer parameters specified in this table depend on the Mtp3TimerRes parameter setting in the MTP general parameters section of the file.

Parameter name	Default	Range	Usage
AdjDpc (required if DefaultDPC is not specified)	None	N/A	Point code of the node on the other end of the link, usually the remote switch or an STP. Use dot notation (such as 2.45.76), a hex number (such as 0x101), or a decimal number. If the AdjDpc parameter is not present, the DefaultDPC parameter from the MTP general parameters section is used. Either the AdjDpc or the DefaultDPC parameter must be present.
Server	None	SS701 SS702 Server host name	Logical name (SS701 or SS702) or the physical host name of the Vision Signaling Server where this link physically terminates.
PortNumber	None	1 to 32	Corresponds to the port entry in the TDM configuration file.
OPC	0 (Use general OPC)	N/A	Originating point code of the link. Use for multiple OPC emulation and OPC routing.
LinkSLC	Link index - 1	N/A	Link selection code for signaling link testing. This value is used by both sides to reference this link. It must be unique for every link and match on both sides.
Variant (required if DefaultVariant is not specified)	DefaultVariant	ANSI ITU JNTT JTTC	MTP 3 protocol variant used on this link. If the Variant parameter is not present, the DefaultVariant parameter from the MTP general parameters section is used. Either the Variant or DefaultVariant parameter must be present.
P0Queue	16	2 to 1024	Transmit queue length threshold at which the congestion priority is raised to level 0.
P1Queue	32	(p0Qlen + 2) to 1024	Transmit queue length threshold at which the congestion priority is raised to level 1.
P2Queue	64	(p1Qlen + 2) to 1024	Transmit queue length threshold at which the congestion priority is raised to level 2.
P3Queue	128	(p2Qlen + 2) to 1024	Transmit queue length threshold at which the congestion priority is raised to level 3.
Linkset	1	1 to 32	Linkset to which this link belongs. This value should match the index of a linkset configuration section. For information, see <i>MTP linkset parameters</i> on page 99.
Disabled	false	true false	If false, the link is initially enabled and tries to align with the remote side immediately. If true, the link is initially disabled, and no attempt is made to align with the remote side.

Parameter name	Default	Range	Usage
Ssf	National (ANSI) International (ITU, JNTT, JTTC)	National International	Value used in the sub-service field (SSF) of the SIO.
DpcLength	14 (ITU) 16 (JNTT or JTTC) 24 (ANSI)	14 16 24	Number of bits in a point code. For most installations, this value defaults based on the Variant or DefaultVariant parameter. Installations in Japan use the JNTT or JTTC variant and 16-bit point codes. In these installations, set DpcLength to 16. A DpcLength value of 16 is only valid on links whose LinkType is JNTT or JTTC. Installations in China use the ITU variant and 24-bit point codes. In these installations, set DpcLength to 24.
LinkPrior	0	0 to 3	Priority of this link within the linkset. Priorities range from 0 (highest) to 3 (lowest).
MessageSize	272	64 to 1024	Maximum message length for this link.
UsePrior	true	true false	If true, message priorities generated by user parts are inserted into the SIO octet (spare bits) of outgoing messages; otherwise, the SIO spare bits are set to zero. This parameter is usually set to true in ANSI networks and false in ITU-T networks.
MgmtMsgPrior	3	0 to 3	Priority to use for MTP3 management messages. Priorities range from 0 (lowest) to 3 (highest).
SltmRetry	2	0 to 255	Maximum number of times to retry a signaling link test message (SLTM). A value of zero results in infinite retries.
DiscPrior	0	0 to 3	Congestion priority at which messages with priority below the current threshold are discarded.
TraceData	false	true false	When set to true, starts tracing all data between MTP 2 and MTP 3 on this link.
TestPattern	TST	1 to 15 ASCII characters	Link test pattern for SLTM messages.
MaxFrame	272	64 to 1024	Maximum frame length for MSU.
SuermThresh	64	1 to 255	Signal unit error rate monitor threshold (bad frames).
SuermDRate	256	1 to 65535	Signal unit error rate monitor decrement rate (frames).
AermThreshN	4	1 to 255	Alignment error rate monitor error rate threshold (normal alignment).
AermThreshE	1	1 to 255	Alignment error rate monitor error rate threshold (emergency alignment).

Parameter name	Default	Range	Usage
MaxRtbMsgs	127	1 to 255	Maximum number of MSUs for retransmission (when using PCR error correction only).
MaxRtbOctets	34544	1 to 65535	Maximum number of MSUs octets for retransmission (when using PCR error correction only).
MaxProvAbort	5	1 to 255	Maximum number of proving failures.
ErrType	Normal	Normal PCR	Error correction method: Normal or Preventive Cyclic Retransmission.
LssuLen	2	1 to 2	LSSU length.
IsoThresh	1000	1 to 65535	Number of messages queued to MTP 3 while isolated that causes MTP 2 to begin processor outage (SIPOs).
L2TxqThresh1	50	1 to 65535	Transmission queue length at which the outbound flow control level is raised to one.
L2TxqThresh1Abate	20	1 to 65535	Transmission queue length at which the outbound flow control level is lowered to zero.
L2TxqThresh2	200	1 to 65535	Transmission queue length at which the outbound flow control level is raised to two. The subsequent indication causes MTP 3 to cease all transmission to MTP 2 until the flow control level returns to one or zero.
L2TxqThresh2Abate	100	1 to 65535	Transmission queue length at which the outbound flow control level is lowered to one.
L2SapThresh	500	1 to 65535	Number of messages queued to MTP 3 while inbound flow control is in effect that causes MTP 2 to send busy indications (SIBs).
L2SapThreshAbate	100	1 to 65535	Number of messages queued to MTP 3 while inbound flow control is in effect that causes MTP 2 to stop sending busy indications (SIBs).
L2_T1	130 (ANSI) 400 (ITU-T)	1 to 65535	Timer aligned/ready.
L2_T2	115 (ANSI) 100 (ITU-T)	1 to 65535	Timer not aligned.
L2_T3	115 (ANSI) 15 (ITU-T)	1 to 65535	Timer aligned.
L2_T4N	23 (ANSI) 82 (ITU-T)	1 to 65535	Normal proving period.
L2_T4E	6 (ANSI) 5 (ITU-T)	1 to 65535	Emergency proving period.
L2_T5	1	1 to 65535	Timer sending SIB.

Parameter name	Default	Range	Usage
L2_T6	60	1 to 65535	Timer remote congestion.
L2_T7	20	1 to 65535	Timer excessive delay of acknowledgement.
L2_T10	30	1 to 65535	Amount of time MTP 2 can be isolated from a remote MTP 3 before sending processor outage (SIPO).
L2_T11	20	1 to 65535	Time to wait for a flow control acknowledgement from MTP 3 before sending another flow control indication.
L2_T12	20	1 to 65535	Time to wait for a status confirmation from MTP 3 before sending another status indication.
L2_T13	20	1 to 65535	Time to wait for a disconnect confirmation from MTP 3 before sending another disconnect indication.
DataEncoding	NRZ	NRZ NRZI	Data encoding (NRZ or NRZ inverted).
UseFlags	true	true false	Use flags (true) or idles (false) between frames.
ShareFlags	true	true false	Allow single flag to be shared between frames.
MinFlags	0	0 to 15	Minimum number of additional flags between frames (in addition to shared flag).
IdleFreq	0 (continuous)	0 65535	Frequency at which FISUs are sent by the software (in ms). Zero indicates that hardware constantly retransmits duplicate FISUs as is the norm. Typically used for Japan deployments.
RtFreq	0 (continuous)	0 65535	Frequency at which other retransmitted SUs (LSSUs) are sent by the software (in ms). Zero indicates that hardware constantly retransmits duplicate LSSUs as is the norm. Typically used for deployments in Japan.
T1	10	0 to 65535	Delay to avoid message mis-sequencing on changeover.
T2	10	0 to 65535	Wait for changeover acknowledgment.
T3	10	0 to 65535	Time controlled diversion - delay to avoid mis-sequencing on changeback.
T4	10	0 to 65535	Wait for first changeback acknowledgment (first attempt).
T5	10	0 to 65535	Wait for first changeback acknowledgment (second attempt).
T6	10	0 to 65535	Delay to avoid mis-sequencing on controlled rerouting.

Parameter name	Default	Range	Usage
T7	20	0 to 65535	Wait for data link connection acknowledgment.
T11	600	0 to 65535	Transfer restricted timer.
T12	10	0 to 65535	Wait for uninhibit acknowledgment.
T13	10	0 to 65535	Wait for forced uninhibit.
T14	30	0 to 65535	Wait for inhibition acknowledgment.
T17	10	0 to 65535	Delay to avoid oscillation of initial alignment failure and link restart.
T22	1100 (ANSI) 2400 (ITU, JNTT, JTTC)	0 to 65535	Wait to repeat local inhibit test (ANSI T20 value).
T23	1100 (ANSI) 2400 (ITU, JNTT, JTTC)	0 to 65535	Wait to repeat remote inhibit test (ANSI T21 value).
T24	40	0 to 65535	Reserved for future use (not ANSI T24).
T31	10	0 to 65535	Internal BSN Requested Timer (not ANSI T31).
T32	100	0 to 65535	Wait for response to SLTM timer (ANSI T1.111.7 timer T1 - not ANSI T32).
T33	30	0 to 65535	Signaling link connection timer (not ANSI T33).
T34	600	0 to 65535	Periodic signaling link test timer (ANSI T1.111.7 timer T2 - not ANSI T34).
T40	30	1 to 65535	Time to wait for a bind confirm from MTP 2 before sending another bind request.
T41	30	1 to 65535	Time to wait for a disconnect confirm from MTP 2 before sending another disconnect request.
T42	30	1 to 65535	Time to wait for a flow control confirm from MTP 2 before sending another flow control request.
T43	30	1 to 65535	Time to wait for a status confirm from MTP 2 before sending another status request.
T44	30	1 to 65535	Time to wait for an unbind confirm from MTP 2 before sending another unbind request.

MTP linkset parameters

A linkset is a collection of all links on the Signaling Server that terminate at a particular SS7 network node. The MTP linkset parameters in the *SS7_config_default.xml* configuration file define the properties of the linkset, such as the DPC of the node that terminates the linkset and the list of routes (destinations) that are reachable through that linkset.

The MTP linkset configuration sections, which configure the linkset parameters, appear as subsections within the <MtpConfig> section. Each MTP linkset configuration section has a <LinksetConfig Index=*n*> XML tag, where *n* is a unique index. Each MTP 3 linkset configuration section configures a single linkset.

The following table lists the configurable parameters in an MTP linkset configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Parameter name	Default	Range	Usage
AdjDpc	None	N/A	Point code of the node on the other end of the link, usually either the remote switch or an STP. Use dot notation (such as 2.45.76) or a hex number (such as 0x101). This value should match the AdjDpc value for all links in this linkset.
OPC	0 (Use general OPC)	Any valid point code	Originating point code. Use for multiple OPC emulation and OPC routing.
TargetNmbActiveLinks	MAX_LINKS	1 to 32	Target number of links in this linkset to keep active at any given time. Set this value to the actual number of links in this linkset.

The <Route index=*n*> entries refer to routes defined in the MTP route configuration section that can be reached through the linkset. There is one <Route index=*n*> entry for each route. Each entry has a unique index. The following table lists the configurable parameters in a <Route index=*n*> subsection:

Parameter name	Default	Range	Usage
RouteNumber	None	0 to MaxRoutes	Matches the index of the route in the MTP route configuration section.
Priority	0		Priority of this linkset for carrying traffic to the route's destination in relation to other linksets that can reach that destination. 0 is the highest priority. Priorities cannot be skipped. For example, do not specify a priority of 2 for a route, unless you have also defined this destination as reachable through at least two other linksets with priorities 0 and 1. A typical use of route priority within a linkset is to specify priority 0 for the most direct path to that destination and priority 1 for a less direct path. The priority 1 linkset is only used for routing traffic to the destination when the priority 0 linkset is unavailable. If traffic to a destination is load-shared across two or more linksets, specify that destination route as priority 0 in each of those linksets.

MTP route parameters

MTP routes specify destination signaling endpoints or subnets. The MTP route parameters in the *SS7_config_default.xml* configuration file define the properties of the routes that are accessible from the Signaling Server.

The MTP route configuration sections, which configure the route parameters, appear as subsections within the <MtpConfig> section. Each MTP route configuration section has a <RouteConfig Index=*n*> XML tag, where *n* is a unique index. Each MTP 3 route configuration section configures a single route.

The following table lists the configurable parameters in a route configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Note: The units for the timer parameters specified in this table depend on the Mtp3TimerRes parameter setting in the MTP general parameters section of the file.

Parameter name	Default	Range	Usage
DPC	None	N/A	For down routes, set to the destination point code. For up routes, set to the local point code. Use dot notation (such as 2.45.76), a hex number (such as 0x101), or a decimal number.
Variant (Required if DefaultVariant is not specified)	None	ANSI ITU JNTT JTTC	MTP 3 protocol variant associated with this route. If the Variant parameter is not present, the DefaultVariant parameter from the MTP general parameters section is used. Either the Variant or DefaultVariant parameter must be present.
Ssf	National (ANSI) International (ITU, JNTT, JTTC)	National International	Value for the subservice field used in route management messages for this route.
Direction	Down	Up Down	Route direction. Up routes result in messages routed to user parts or applications on this node. Down routes are routes to remote signaling points. There must be one Up route configured to receive traffic at this node. All the other routes are Down and indicate destinations to which traffic can be sent.
AdjRoute	true	true/yes false/no	Indicates whether this is a route to an adjacent signaling point (a signaling point that is directly connected to this node). Set to true if the destination is directly connected, or false if it is reached through one or more hops.
OPC	0 (use general OPC)	Any valid point code	Originating point code. Use for multiple OPC emulation and OPC routing.
AdjCluster	false	true/yes false/no	Indicates whether this is a route to an adjacent cluster, allowing use of the cluster variant of route management messages (ANSI only).

Parameter name	Default	Range	Usage
T8	10	0 to 65535	Transfer prohibited inhibition timer.
T10	450	0 to 65535	Wait to start/repeat periodic route set test.
T19itu	680	1 to 65535	ITU restart timer to avoid ping-pong of TFP, TFR, or TRA messages.
T21itu	640	1 to 65535	Overall ITU restart timer at adjacent SP.
T25ansi	320	1 to 65535	ANSI restart timer at adjacent SP waiting for a TRA message.
T28ansi	300	1 to 65535	ANSI restart timer at adjacent SP waiting for a TRW message.
T29ansi	630	1 to 65535	ANSI restart timer started when a TRA is sent in response to an unexpected TRA or TRW.

M3UA parameters <M3uaConfig>

The M3UA parameters section of the *SS7_config_default.xml* file begins with the following XML tag:

```
<M3uaConfig>
```

This topic describes how to use M3UA and presents the M3UA configuration file parameters. To satisfy entity dependency, configuration sections must be loaded to the M3UA task in the following order:

- General M3UA configuration
- Network configuration
- NSAP configuration
- SCT SAP configuration
- Peer signaling process configuration
- Peer server configuration
- Routing entry configuration

It is not required that these sections appear in this order in the text file, provided that the configuration program reads and downloads the sections in the correct order, as the *m3uacfg* sample file does.

Using M3UA

M3UA implements services through the configuration of general parameters and the following entities:

Entity	Description
General M3UA	The general configuration parameters define and control the general operation of M3UA including maximum values of various layer resources, congestion levels, and protocol timers.
Network configuration	Defines the SS7 network context or appearance for potential use over multiple SS7 networks, including SSF, DPC length, and SLS length.
Network service access points (NSAPs)	Defines the upper layer SS7 applications that use M3UA. Each NSAP is associated with one application, as identified by the service indicator field of a message, and one protocol variant.
Service access points (M3UA SCT SAP)	Defines the lower layer interface between M3UA and SCTP. Only one SCT SAP can be defined.
Peer signaling process (PSP)	An instance of a peer server that can either be local or remote. A peer signaling process can process signaling traffic for multiple peer servers. A peer server process can be a signaling gateway process (SGP), an application server process (ASP), or an IP server process (IPSP).
Peer server (PS)	A logical entity that serves a specific routing key. For example, a peer server can be a virtual switch element that handles a signaling relation identified by DPC/OPC, or a virtual database element that handles all HLR transactions for a particular SIO/DPC/OPC combination. There is a one-to-one relationship between a peer server and a routing key. Because the application server effectively represents an MTP3 user, it has its own point code. A peer server can be an application server (AS) or signaling gateway (SG).
Routing entry	Set of M3UA parameters that uniquely define the range of signaling traffic to be handled by a particular peer server.

Configure M3UA as either an application server process (ASP) or an IP server process (IPSP). The following table shows the differences when configuring M3UA for ASP or IPSP:

Parameter name	ASP	IPSP
MODE (for remote peer servers)	Must be set to LOADSHARE.	Can be set to either LOADSHARE or ACTSTANDBY.
PSP_TYPE	Set to SGP.	Set to IPSP.

If M3UA is configured as an IPSP, the IPSP_MODE parameter must be configured as either singled-ended (SE) or double-ended (DE):

IPSP Mode	Description
Single-ended (SE)	A single exchange of the ASPAC (ASP Active) and ASPAC ACK (ASP Active Acknowledgement) messages, that initiated from either side, is sufficient to allow traffic to flow in both directions.
Double-ended (DE)	Each side must send and receive the ASPAC and ASPAC ACK messages before allowing traffic flow.

IPSP_MODE is valid only when IPSP is configured as the remote peer signaling process type.

The CLIENT_SIDE parameter is required in an IPSP configuration. This parameter tells M3UA whether or not to initiate an association to the peer. Setting the CLIENT_SIDE parameter to TRUE indicates that M3UA always initiates an association. Setting this parameter to FALSE indicates that the other side is expected to initiate the association. If configured as an ASP, M3UA always initiates the association.

The RTE_CTX parameter, in the PS configuration section of the M3UA configuration file, must match the peer side's configuration. For example, the route context for a remote PS must match that side's route context for a local PS, and vice versa. The route context is passed in most M3UA messages and is used to match incoming messages with their associated NSAPs and upper layers. For more information, see the *Dialogic® NaturalAccess™ Signaling Software Configuration Manual*.

General M3UA configuration

The following table lists the configurable parameters in the M3UA general configuration <GenConfig> section and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

The default values for all timers at the M3UA level are shown in milliseconds. A configuration value of zero for a timer disables that timer.

Parameter	Default	Description
NodeType	ASP	Type of M3UA. Application server process (ASP) is currently supported.
MaxNsap	2	Maximum number of NSAPs supported simultaneously.
MaxNetwork	2	Maximum number of network contexts supported. There is one network context per variant and network indicator.
MaxRoute	16	Maximum number of route entries supported, including local routes.
MaxDpc	32	Maximum number of destination point codes (DPC) supported, including configured and dynamically learned DPCs.
MaxPs	8	Maximum number of peer servers supported, including both local and remote peer servers.
MaxLps	4	Maximum number of local peer servers.
MaxPsp	16	Maximum number of peer signaling processes supported.
MaxMsg	128	Number of M3UA messages in transit supported.
MaxRoundRobinLs	4	Maximum number of peer servers that can use round-robin load sharing.
MaxSlsLs	4	Maximum number of peer servers that can use SLS-based (signaling link selector) load sharing.
MaxSls	128	Maximum number of SLS values that can be used by all peer servers.
QueueSize	256	Outgoing congestion queue size per association. Messages above this limit are dropped.
CongLevel1	64	Congestion level 1 in the queue; not valid in international networks.
CongLevel2	128	Congestion level 2 in the queue; not valid in international networks.

Parameter	Default	Description
CongLevel3	196	Congestion level 3 in the queue; not valid in international networks.
TmrRestart	1000	Restart hold-off time. This parameter is only used in an SGP configuration.
TmrAsPend	5000	Time for which a peer server can remain in an AS_PENDING state.
TmrAspUp1	2000	Initial time between ASPUP (ASP Up) retries.
TmrAspUp2	2000	Steady state time between ASPUP retries.
NmbAspUp1	3	Number of initial attempts at sending ASPUP messages at interval TMR_ASP_UP1 before sending them at interval TMR_ASP_UP2.
TmrAspDown	2000	Time between ASPDN (ASP Down) retries.
TmrAspm	2000	Time to wait before failing, after sending ASPAC (ASP Active) or ASPIA (ASP Inactive) messages.
TmrDaud	2000	Time between DAUD (Destination State Audit) messages.
TmrDrkm	2000	Time between DRKM (Dynamic Routing Key Registration Message).
NmbDrkm	3	Number of DRKM attempts before failing.
TmrSeqControl	1000	Delay used when diverting traffic to maintain sequencing.

Network configuration

The following table lists the configurable parameters in the M3UA network configuration <NetworkConfig> section and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
NetworkId	1	Network identifier. Valid range is 1 - 255.
NetworkAppear	1234	Network appearance code. Network appearance values are determined and configured by network operators on each side of an association. This value is used in M3UA messages only if the <UseNwkAppear> parameter is set to true in the Peer Signaling Process (PSP) configuration section. See <i>Peer signaling process configuration</i> on page 107.
Ssf	NAT	Subservice field. Valid values are: INTL = International NAT = National
DpcLength	24	DPC or OPC length. Valid values are: 14 = Length for ITU networks 16 = Length for Japanese networks 24 = Length for ANSI networks and other national variants
SlsLength	5	SLS length, in bits. Valid values are: 4 = SLS length 4 bits 5 = SLS length 5 bits 8 = SLS length 8 bits

Parameter	Default	Description
ServiceUserVar	ANS	Protocol variant of the M3UA service user, such as ISUP, SCCP, and TUP. Valid values are: ANSI = ANSI variant BICI = BICI ITU = CCITT variant China = China variant NTT = NTT Japan TTC = TTC Japan The protocol variant specified in <ServiceUserVar> can be modified in <i>ss7_config_default.xml</i> file depending on ANSI, ITU, and other protocol variants configured.
ServiceUserVar2	ANS	Protocol variant for user of the M3UA service user, such as TCAP, which uses SCCP. Valid values are: ANSI = TCAP type ANSI ETSI = TCAP type ETSI ITU = TCAP type ITU The protocol variant specified in <ServiceUserVar2> can be modified in <i>ss7_config_default.xml</i> file depending on ANSI, ITU, and other protocol variants configured.

Sample M3UA Network configuration for ITU

The following is a sample M3UA Network configuration for ITU:

```
<NetworkConfig Index="1">
  <NetworkId>1</NetworkId>
  <NetworkAppear>1234</NetworkAppear>
  <Ssf>INTL</Ssf>
  <DpcLength>14</DpcLength>
  <SlsLength>4</SlsLength> <!-- 4 / 5/ 8 -->
  <ServiceUserVar>ITU</ServiceUserVar>
  <ServiceUserVar2>ITU</ServiceUserVar2> <!-- TCAP user var -->
</NetworkConfig>
```

Sample M3UA Network configuration for ANSI

The following is a sample M3UA Network configuration for ANSI:

```
<NetworkConfig Index="1">
  <NetworkId>1</NetworkId>
  <NetworkAppear>1234</NetworkAppear>
  <Ssf>NAT</Ssf>
  <DpcLength>24</DpcLength>
  <SlsLength>5</SlsLength> <!-- 4 / 5/ 8 -->
  <ServiceUserVar>ANSI</ServiceUserVar>
  <ServiceUserVar2>ANSI</ServiceUserVar2> <!-- TCAP user var -->
</NetworkConfig>
```

NSAP configuration

The following table lists the configurable parameters in the M3UA NSAP configuration <M3uaNsapConfig> section and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
NsapId	0 for ISUP 1 for SCCP	Identifier for this NSAP.
NetworkId	1	Logical network identifier for this NSAP.
ServiceType	ISUP	Type of NSAP service user. Valid values are: ISUP = ISUP user SCCP = SCCP user TUP = TUP user BICC = BICC user

SCT SAP configuration

The following table describes the M3UA SCT SAP configuration <SctSapConfig> parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
SctSapId	0	M3UA identifier for this SCT SAP. This value must be 0.
SrcPort	2095	Source port for the listening endpoint.
Spld	0	SCTP identifier for this SCT SAP. This value must be 0.

Peer signaling process configuration

The following table describes the M3UA peer signaling process configuration <PspConfig> parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
PspId	1	Peer service process (PSP) identifier. Valid values range from 1 to the result of (Max Number of PSP -1).
PspType	IPSP	Remote peer signaling process type. Valid values are: SGP = Signaling gateway process. IPSP = IP service process.
IpspMode	SE	Valid when PSP_TYPE = IPSP. Indicates whether the IPSP mode is single-ended or double-ended. Valid values are: DE = Double-ended mode SE = Single-ended mode
DrkmAllowed	FALSE	Indicates whether this peer signaling process can send and receive dynamic routing key management (DRKM) messages. Valid values are: TRUE = Peer signaling process can send and receive DRKM messages. FALSE = Peer signaling process cannot send or receive DRKM messages.

Parameter	Default	Description
UseNwkAppear	FALSE	Determines whether the optional network appearance parameter is included when communicating with the remote peer. Valid values are: TRUE = Include the network appearance parameter. FALSE = Do not include the network appearance parameter.
AspldMand	NONE	Indicates whether an ASP identifier is required in sent and/or received ASPUP and ASPUP ACK (ASP Up Acknowledgement) messages. Valid values are: RX = Identifier is required in received ASPUP and ASPUP ACK messages. TX = Identifier is required in transmitted ASPUP and ASPUP ACK messages. BOTH = Identifier is required in transmitted and received ASPUP and ASPUP ACK messages. NONE = ASP ID not required in transmitted or received ASPUP and ASPUP ACK messages.
NetworkId	1	Default network context identifier for incoming messages, if the messages do not include one.
PrimeDetAddr	192.168.1.2	Primary destination address of the remote peer used in outgoing association requests.
DestPort	2905	Remote SCTP port.
ClientSide	TRUE	TRUE = Associations are automatically initiated from this PSP, if PSP_TYPE = IPSP. FALSE = Associations are not initiated from this PSP, if PSP_TYPE = IPSP. The other side is expected to initiate any associations.
NmbOutStreams	2	Number of streams supported by this association. Valid range is 1 - 255.

Peer server configuration

The following table describes the M3UA peer server configuration <PsConfig> parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
PsId	N/A	Peer server identifier.
NwkId	1	Peer server network identifier.
Mode	ACTSTANDBY	Peer server availability mode. Valid values are: ACTSTANDBY LOADSHARE BROADCAST (not supported)
Local	FALSE	Indicates whether the peer server is local or remote: TRUE = Local peer server FALSE = Remote peer server
PspId	1	Ordered list of PSP identifiers configured in the system that handle the routing key associated with this PS. Preference is given to earlier entries in the list when performing fail-over or fail-back procedures. Valid values are 1 to MAX_PSP.
RteCtx	0	Routing context. Allowed value is any unsigned 32-bit integer.

Routing entry configuration

The following table describes the M3UA routing configuration <RteConfig> entry parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
Dpc	N/A	Destination point code associated with this route.
DpcMask	0xFFFFFFFF	Wildcard mask for the DPC. In most cases, set to all 1 bits to use the entire DPC for routing.
Opc	0	Origination point code (OPC) associated with this route, if any.
OpcMask	0	Wildcard mask for the OPC. In most cases, set to all 1 bits (0xFFFFFFFF) to use the entire OPC for routing, if OPC routing is required. Otherwise, set to 0 to indicate that OPC routing is not used.
Sio	0	Service information octet (SIO) associated with this route, if any. Valid values are ISUP, SCCP, BICC, TUP, or a numeric value between 0 and 0xF. Note: If SIO is not specified, the default is 0, which indicates that SIO is not used for routing.
SioMask	0	Wildcard mask for the service information octet (SIO). If SIO is set, set SIO_MASK to 0xF to use the specified SIO value for routing. Set SIO_MASK to 0 if SIO routing is not used.
RouteType	PS	Route type. Valid value is PS.
NwkId	1	Network identifier. Valid range is 1 - 255.
NsapId	0	NSAP identifier configured in the system with which this route is associated. Used only for local (or up) routes. Do not specify for remote routes.
RoutePsId	0	Identifier of the peer server associated with this route.

SCTP parameters <SctpConfig>

The SCTP parameters section of the *SS7_config_default.xml* file begins with the following XML tag:

```
<SctpConfig>
```

It contains the following parameter groups:

- General SCTP
- SCT Upper SAP
- SCT Lower SAP (TSAP)

General SCTP

The following table describes the SCTP general configuration <GenConfig> parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
MaxAssoc	4	Maximum number of SCTP associations the service user can open simultaneously. Valid range is 1 - 65535.
MaxDestAddr	8	Maximum number of destination addresses that can be active simultaneously in SCTP. Valid range is 1 - 65535.
MaxTxQueue	256	Maximum number of datagrams that can be queued for sending to the peer. Valid range is 1 - the result of $(2^{32}-1)$.
MaxRxQueue	256	Maximum number of datagrams received from the peer that can be queue before being sent up to the service user. Valid range is 1 - the result of $(2^{32}-1)$.
MaxInStream	8	Maximum number of incoming streams per association. Valid range is 1 - 65545.
MaxOutstream	8	Maximum number of outgoing streams per association. Valid range is 1 - 65545.
MtuInitial	1400	Initial path max transmit unit (MTU) in bytes. Valid range is 1 - 1400.
MtuMax	1400	Maximum value in bytes to be used in searching for an optimal MTU size using the midpoint algorithm. This field is mandatory if the value of the PERFORM_MTU parameter is TRUE. Valid range is 1 - 1400.
MtuMin	500	Minimum value in bytes to be used in searching for an optimal MTU size using the midpoint algorithm. This field is mandatory if the value of the PERFORM_MTU parameter is TRUE. Valid range is 1 - 1400.
PerformMtu	FALSE	Indicates whether or not to perform MTU discovery. Valid values are: TRUE = Perform MTU discovery. FALSE = Do not perform MTU discovery.
HostName	NULL	Self-hostname.
UseHostName	FALSE	Whether or not to send hostname in INIT (Initiation) / INIT ACK (Initiation Acknowledgement).
MaxInitRetry	0	Maximum number of retries for INIT message to open an association. Valid range is 0 - 255. Set to 0 to retry indefinitely.
MaxAssocRetry	10	Maximum retransmissions for an association. Valid range is 0 - 255.

Parameter	Default	Description
MaxDestRetry	5	Maximum retransmissions for a destination address. Valid range is 0 - 255.
AcceptAlt	FALSE	TRUE = Accepts additional lifetime parameters from the peer to extend cookie lifetime. FALSE = Does not accept additional lifetime parameters from the peer to extend cookie lifetime.
TmrMd5Key	60000	Lifetime of an MD5 key. A new private key is generated every time this timer expires. Valid range is 1 - 65535.
RttAlpha	12	Used for round trip time (RTT) calculations. Valid range is 0 - 65535.
RttBeta	25	Used for RTT calculations. Valid range is 0 - 65535.

SCT Upper SAP

The following table describes the SCT upper SAP configuration <SctSapConfig> parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
SctSapId	0	SAP ID used by the upper layer (M3UA). This identifier must be specified and must be 0.
TmrAckDelay	200	Maximum time to wait before the SCTP layer must send a SACK (Selective Acknowledgement) message. Valid range is 1 - 165535.
NmbAckDelay	2	Maximum number of messages to receive before the SCTP layer must send a SACK message. Valid range is 1 - 165535.
TmrInitRto	3000	Initial value of the retransmission timeout (RTO). The SCTP layer retransmits data after waiting for feedback during this time period. Valid range is 1 - 65535.
TmrMinRto	1000	Minimum value used for the RTO. If the computed value of RTO is less than TMR_MIN_RTO, the computed value is rounded up to this value. Valid range is 1 - 65535.
TmrMaxRto	10000	Maximum value used for RTO. If the computed value of RTO is greater than TMR_MAX_RTO, the computed value is rounded down to this value. Valid range is 1 - 65535.
TmrBundle	200	Timer to bundle messages.
TmrCookieLife	60000	Base cookie lifetime for the cookie in the INIT ACK (Initiation Acknowledgement) message. Valid range is 1 - 65535.
TmrHbInterval	3000	Default heartbeat interval timer. Valid range is 1 - 65535.
MaxBurst	4	Maximum burst value. Valid range is 1 - 65535.
MaxHbBurst	1	Maximum number of heartbeats sent at each retransmission timeout (RTO). Valid range is 1 - 65535.
AbortOnStream	FALSE	Action to take when the receiver's number of incoming streams is less than the sender's number of outgoing streams. Valid values are: TRUE = Accept incoming stream and continue association. FALSE = Abort the association.

Parameter	Default	Description
EnableHeartbeat	TRUE	Whether to enable or disable heartbeat by default. Valid values are: TRUE = Enable heartbeat. FALSE = Disable heartbeat. Dialogic recommends that you enable heartbeats to allow earlier detection of loss of associations.
FlowStartThr	192	Numbers of messages waiting in queue, when flow control indication is sent to the service user to inform that the queue is nearly full. Valid range is FLOW_STOP_THR to MAX_TX_QUEUE.
FlowStopThr	64	Numbers of messages waiting in queue, when flow control indication is sent to the service user to inform that the queue is almost empty. Valid range is 0 to FLOW_START_THR.
TmrSdGuard	15000	Shutdown guard timer for graceful shutdowns. Valid range is 1 - 65535.

SCT Lower SAP (TSAP)

The following table describes the SCT lower SAP (TSAP) <TSapConfig> parameters and their default values. All parameters listed must be present in the *ss7_config_default.xml* file.

Parameter	Default	Description
TsapId	0	Service user ID for the TSAP being configured. This must be 0.
SapId	0	Service provider ID of the TSAP to which this TSAP binds. This must be 0.
MaxBindRetry	3	Maximum number of bind request retries allowed.
TmrCfm	200	Time interval for which the SCTP layer waits for bind or status confirmations from the lower layer.

ISUP parameters (<IsupConfig>)

The ISUP parameters section of the *SS7_config_default.xml* file begins with the following XML tag:

```
<IsupConfig>
```

It contains the following parameter groups:

- General parameters
- Circuit group parameters
- User Service Access Point (USAP) parameters
- Network Service Access Point (NSAP) parameters

ISUP general parameters

The ISUP general parameters control the ISUP layer as a whole, including maximums for resource allocation, the point code of the Signaling Server, and general timer values.

The ISUP general configuration section, which configures the ISUP general parameters, appears as a subsection within the <IsupConfig> section. Its XML tag is <GenConfig>.

The following table lists the configurable parameters in the ISUP general configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Note: All ISUP timer values are in seconds.

Parameter name	Default	Range	Usage
OPC	Value of the OPC field in the MTP general configuration section.	N/A	(Optional) Point code of this server, specified as x.y.z (three bytes, decimal, separated by periods), as a hexadecimal value preceded by 0x (0x123), or as a decimal value. If you omit this parameter, the OPC from the MTP general parameters is used. For information, see <i>MTP general parameters</i> on page 90.
DefaultVariant	None	ANSI88 ANSI92 ANSI95 ANSIBICC ETSIV2 ETSIV3 ITU ITUBICC ITUBLUE ITUWHITE ITU97 JNTT JTTC Q767	SS7 ISUP variant used for all ISUP circuit groups, USAPs, and NSAPs. Specifying a variant in the ISUP circuit group, USAP, and NSAP configuration sections overrides the default variant. If you omit DefaultVariant, specify a variant in the ISUP circuit group, USAP, and NSAP configuration sections.
MaxSaps	1	1	Maximum number of applications.
MaxNSaps	1	1 to 255	Maximum number of interfaces with the MTP 3 network layer.

Parameter name	Default	Range	Usage
MaxCircuits	2048	0 to 65535	Maximum number of circuits to be managed by the ISUP layer.
MaxGroups	32	0 to 65535	Maximum number of circuit groups managed by the ISUP layer.
MaxCallRefs	16	0 to 65535	Maximum number of call references, and hence connections, that ISUP can keep track of simultaneously.
PassAlong	false	true false	If set to true, messages are sent in pass-along format.
ExtElmts	false	true false	If set to true, allows the sending and receiving of extended elements.
RawMsgs	false	true false	If set to true, allows the sending of raw binary encoded ISUP messages with non-standard message type codes (that is, messages not directly interpreted by the Dialogic ISUP layer). This allows applications to implement new messages in national variants not directly supported by the Dialogic ISUP layer.
RmtUserUnavl	false	true false	If true, configures the stack to start in remote user unavailable mode.
GrpResetEvent	false	true false	If true, configures the stack to send up one group reset event instead of many separate circuit reset events.
SlsFromCICS	true	true false	If true, sets the ANSI SLS value to the bottom bits of the CIC.
DsblRmtUserUnavl	false	true false	If true, disables appropriate user part test procedure (for SSURN among others).
RestartT7	false	true false	If true, restarts T7 when an inbound INR is received.
DisableACL	false	true false	If true, disables automatic congestion control.
ClIiName	none	N/A	Common Language Location Identifier (CLLI) name assigned to this node (exactly 11 ASCII characters).
QCongOnset1	600	0 to 65535	When API sending queue size is increasing, the congestion level is set to 1 when the queue is this length.
QCongAbate1	400	0 to 65535	When API sending queue size is decreasing, the congestion level is set to 0 when the queue is this length.
QCongOnset2	900	0 to 65535	When API sending queue size is increasing, the congestion level is set to 2 when the queue is this length.
QCongAbate2	700	0 to 65535	When API sending queue size is decreasing, the congestion level is set to 1 when the queue is this length.

Parameter name	Default	Range	Usage
QCongOnset3	1200	0 to 65535	When API sending queue size is increasing, the congestion level is set to 3 when the queue is this length.
QCongAbate3	1000	0 to 65535	When API sending queue size is decreasing, the congestion level is set to 2 when the queue is this length.
MCongOnset1	20	0 to 100	When free memory is decreasing, the congestion level is set to 1 when the percentage remaining is this percentage.
MCongAbate1	25	0 to 100	When free memory is increasing, the congestion level is set to 0 when the percentage remaining is this percentage.
MCongOnset2	10	0 to 100	When free memory is decreasing, the congestion level is set to 2 when the percentage remaining is this percentage.
MCongAbate2	15	0 to 100	When free memory is increasing, the congestion level is set to 1 when the percentage remaining is this percentage.
MCongOnset3	5	0 to 100	When free memory is decreasing, the congestion level is set to 3 when the percentage remaining is this percentage.
MCongAbate3	8	0 to 100	When free memory is increasing, the congestion level is set to 2 when the percentage remaining is this percentage.
TraceEvent	false	true false	Enables event logging when true.
TraceData	false	true false	Enables data tracing when true.
TraceWarning	false	true false	Enables logging of unexpected information element value warnings when true.
TraceError	false	true false	Enables logging of message encoding errors when true.
T18	12	0 to 65535	Time to wait for a response to a group blocking message sent.
T19	60	0 to 65535	Time to wait for a response to initial group blocking message sent.
T20	12	0 to 65535	Time to wait for a response to a group unblocking message sent.
T21	60	0 to 65535	Time to wait for a response to initial group unblocking message sent.
T22	12	0 to 65535	Time to wait for a response to a circuit group reset message sent.
T23	60	0 to 65535	Time to wait for a response to initial circuit group reset message sent.
T28	10	0 to 65535	Time to wait for a CQR after sending a CQM.

Parameter name	Default	Range	Usage
Tgres	5	0 to 65535	Group reset timer.
Tfgr	5	0 to 65535	ANSI first group received timer.

ISUP circuit group parameters

The ISUP circuit group parameters in the *SS7_config_default.xml* configuration file specify the characteristics of each of the circuit groups to be managed by the ISUP layer. This includes the circuit identification codes (CICs), destination point code (DPC) at the other end of the circuits, and circuit type (incoming, outgoing, or both).

The circuit group configuration section, which configures the ISUP circuit group parameters, appears as a subsection within the <IsupConfig> section. Each circuit group configuration section has a <CircConfig Index=*n*> XML tag, where *n* is a unique index. Each circuit group configuration section configures a single circuit group. These groups should match the circuits defined for the SSP process. For more information, see *SSP parameters (<SspConfig>)* on page 122.

The following table lists the configurable parameters in a circuit group parameters section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Note: Timer default values in parentheses are ITU values. All ISUP timer values are in seconds.

Parameter name	Default	Range	Usage
Circuit	None	1 to MaxCircuits	Number of the first circuit in this group. Circuits in this group are numbered from this value to (value + NumCircuits - 1). This range must be unique for all circuits defined. Circuit numbers must start at 1 not 0. This value is used by the application and the ISUP layer to identify circuits, but has no meaning to the far exchange.
DPC (Required if DefaultDPC is not specified)	None	N/A	Destination point code to which this circuit group connects. If the DPC parameter is not present, the DefaultDPC parameter from the MTP general parameters section is used. Either the DPC or the DefaultDPC parameter must be present.
AltOPC	0 (Use general OPC)	N/A	When using multiple OPC capability, the OPC to be used for messages regarding this circuit group.

Parameter name	Default	Range	Usage
CIC	None	0 to 4095	Circuit identification code (CIC) of the first circuit in this group. This code is used by ISUP and the remote side to uniquely identify a circuit. Circuits in this group are assigned CICs from this value to (value + NumCircuits-1). The number range must agree with the CICs assigned to this circuit group at the far exchange. CIC codes can start at 0.
NumCircuits	None	1 to 32	Number of circuits in this circuit group.
Variant (Required if DefaultVariant is not specified)	None	ANSI88 ANSI92 ANSI95 ANSIBICC ETSIV2 ETSIV3 ITU ITUBICC ITUBLUE ITUWHITE ITU97 JNTT JTTC Q767	Protocol variant. If the Variant parameter is not present, the DefaultVariant parameter from the ISUP general parameters section is used. Either the Variant or the DefaultVariant parameter must be present.
Direction	Incoming	Incoming Outgoing Bothways	Direction of calls allowed on this circuit group.
UnusedCircuits	none	Each list member must be in the range: 0 to (NumCircuits - 1) or the keyword none.	A space-separated list of circuits within the range of this circuit group that are not controlled by ISUP. Each number in the list is a zero-based index from the starting Circuit/CIC and identifies a Circuit/CIC that is not used. For example, if Circuit and CIC for this group both start at 1, then the value 15 in the UnusedCircuits list means that Circuit/CIC 16 is not controlled by ISUP.
ControlType	NONE	NONE ALL ODDEVEN	Dual seizure control.
GroupChars	0	0 to 0xFF	This value, if non-zero, is placed in the Group Characteristics of the CVR message.
Ssf	Value of the Ssf field in the ISUP NSAP configuration section.	National International Reserved Spare	Putting a value in this field overrides the default for messages regarding this circuit group.
T4	0	0 to 65535	Time to wait for call modification complete message.
T12	12 (15)	0 to 65535	Time to wait for response to blocking message.

Parameter name	Default	Range	Usage
T13	60 (300)	0 to 65535	Time to wait for a response to the initial blocking message sent.
T14	12 (15)	0 to 65535	Time to wait for a response to an unblocking message sent.
T15	60 (300)	0 to 65535	Time to wait for a response to the initial unblocking message sent.
Tval	30	0 to 65535	ANSI circuit validation timer.
Tpause	60	0 to 65535	Time to wait after MTP pause before resetting circuits.

ISUP User Service Access Point (USAP) parameters

The ISUP USAP parameters defines the upper layer interfaces of the ISUP layer.

The ISUP USAP configuration section, which contains the ISUP USAP parameters, appears as a subsection within the <IsupConfig> section. Each ISUP USAP configuration section has a <UsapConfig Index=*n*> XML tag, where *n* is a unique index. Each ISUP USAP section configures a single interface. For the Signaling Server, there is usually only one ISUP USAP section.

The following table lists the configurable parameters in a USAP configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Note: All ISUP timer values are in seconds.

Parameter name	Default	Range	Usage
Variant (Required if DefaultVariant is not specified)	None	ANSI88 ANSI92 ANSI95 ANSIBICC ETSIV2 ETSIV3 ITU ITUBICC ITUBLUE ITUWHITE ITU97 JNTT JTTC Q767	Protocol variant employed for this application. Must match one of the switch types defined in the NSAP configuration section. The matching occurs as follows: <ul style="list-style-type: none"> • ITUWHITE/BLUE/97/BICC, ETSIV2/V3, and Q767 ISUP variants match the ITU MTP variant. • ANSI88/92/95/BICC variants match the ANSI MTP variant. • JNTT and JTTC ISUP variants match directly with the identical MTP variant. <p>If the Variant parameter is not present, the DefaultVariant parameter from the ISUP general parameters section is used. Either the Variant or the DefaultVariant parameter must be present.</p>
Mask	None	N/A	Not applicable to Signaling Servers.
MaxUserToUser	20	0 to 0xFF	Sets the maximum length of User to User information in an IAM.
T1	12 (15)	0 to 65535	Time to wait for a response to a release message sent.
T2	0	0 to 65535	Time to wait for a resume message after a suspend message received.

Parameter name	Default	Range	Usage
T5	60 (300)	0 to 65535	Time to wait for a response to initial release message sent.
T6	30	0 to 65535	Time to wait for a resume message after a suspend (network) message received.
T7	25	0 to 65535	Time to wait for a response (for example, ACM, ANS, or CON) to the latest address message sent.
T8	12	0 to 65535	Time to wait for a continuity message after receiving IAM requiring continuity check.
T9	180	0 to 65535	Time to wait for answer of outgoing call after ACM message received.
T16	12	0 to 65535	Time to wait for a response to a reset message sent.
T17	12 (300)	0 to 65535	Time to wait for a response to initial reset message sent.
T27	240	0 to 65535	Time to wait for a continuity check request after ensuing continuity check failure indication is received. See the Tccr field.
T31	0 (disabled)	0 to 65535	Time to wait before reusing call reference after a connection is cleared.
T33	15	0 to 65535	Time to wait for a response to information request message sent.
Tex	0 (disabled)	0 to 65535	Time to wait before sending ANSI exit message.
Tcrm	4	0 to 65535	Time to wait for a response to a circuit reservation message sent.
Tcra	10	0 to 65535	Time to wait for an IAM message after circuit reservation acknowledgment message sent.
Tccr	20 (240)	0 to 65535	Time to wait for CCR after the first COT indicating failure. See the T27 field.

ISUP Network Service Access Point (NSAP) parameters

The ISUP NSAP parameters define the characteristics of the ISUP interface to the MTP 3 layer.

The ISUP NSAP configuration sections appear within the <IsupConfig> section. Each ISUP NSAP configuration section has an <NsapConfig Index=*n*> XML tag, where *n* is a unique index. Each ISUP NSAP section defines a lower-level interface of the ISUP layer, such as a single connection to MTP.

The following table lists the configurable parameters in an ISUP NSAP configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Parameter name	Default	Range	Usage
Variant (Required if DefaultVariant is not specified)	None	ANSI88 ANSI92 ANSI95 ANSIBICC ETSIV2 ETSIV3 ITU ITUBICC ITUBLUE ITUWHITE ITU97 JNTT JTTC Q767	<p>Protocol variant employed for this MTP interface. The value of this field must match the MTP protocol variant defined in the MTP NSAP definition section.</p> <p>The matching occurs as follows:</p> <ul style="list-style-type: none"> • ITUWHITE/BLUE/97/BICC, ETSIV2/V3, and Q767 ISUP variants match the ITU MTP variant. • ANSI88/92/95/BICC variants match the ANSI MTP variant. • JNTT and JTTC ISUP variants match directly with the identical MTP variant. <p>If the Variant parameter is not present, the DefaultVariant parameter from the ISUP general parameters section is used. Either the Variant or the DefaultVariant parameter must be present.</p>
Ssf	National	National International Reserved Spare	Value used in the sub-service field (SSF) of the service information octet in outgoing ISUP messages on this MTP interface.

SSP parameters (<SspConfig>)

The SSP parameter section of the *SS7_config_default.xml* file begins with the following XML tag:

```
<SspConfig>
```

It contains SSP general parameters, which define and control the general operation of the Signaling Server.

The SSP general configuration section appears as a subsection within the <SspConfig> section. Its XML tag is <GenConfig>.

The following table lists the configurable parameters in the SSP general configuration section and their default values. Parameters in bold must be present in the *ss7_config_default.xml* file.

Parameter name	Default	Range	Usage
Server1	SS701	A valid hostname or alias.	Hostname or alias of the first Signaling Server. This name and the name of the second Signaling Server are used internally by the server processes for coordination. Do not change these names unless the names SS701 or SS702 (or both) cause a conflict in the IP network, for example, if multiple pairs of Signaling Servers are deployed in the same IP network.
Server2	SS702	A valid hostname or alias.	Hostname or alias of the second Signaling Server.

10 Glossary

A

ADTCP: An audio driver that provides a TCP interface to MIOSIP for rendering SSML fragments.

AMR: Adaptive multi-rate; an audio data compression scheme optimized for speech coding. This scheme was adopted by 3GPP and is used in video services.

ASR: Automatic speech recognition; ASR resources, called ASR engines in the MRCP framework, typically enable users of information systems to speak entries rather than punching numbers on a keypad. See also MRCP.

Authorization and Usage Indication interface: XML-over-HTTP mechanism that authorizes call sessions and gathers information for call detail reports.

B

blind transfer: A call transfer in which the originating caller is not announced and is connected directly to destination. In a blind transfer the Vision™ Server redirects the caller to the callee without remaining in the connection and does not monitor the outcome.

bridge transfer: A blind transfer in which the Vision™ Server redirects the caller to the callee and remains as a listener.

C

Call Server: Component of the Vision™ Server that manages call control and routing capabilities.

CallPlacer interface: XML-over-HTTP mechanism for initiating outbound sessions or calls for VoiceXML applications.

CCXML: Call Control Extensible Markup Language; a W3C Working Draft standard language for providing telephony call control support for dialog systems, gateways, and conferencing services.

CCXML application definition file: A file that maps individual CCXML applications to number ranges that trigger the execution of those applications.

clock: A periodic reference signal used for synchronization on a transmission facility, such as a telephony bus. See also clock master, clock slave, clock fallback.

clock master: A board that drives the clock signal for a system of boards connected by a bus cable. See also clock slave.

clock slave: A board that derives its clock signal from a bus cable; the clock signal is driven by the bus clock master. See also clock master.

consultation transfer: A call transfer in which the Vision™ Server initiates a transfer between two parties, but does not stay attached to the call once it is

successfully established. The caller remains connected to the Vision™ Server if the transfer fails.

D

DTMF: Dual tone multi frequency; an inband signaling system that uses two simultaneous voiceband tones for dialing. Also called touchtone. Some times DMTF is used to generally describe any telephony keypad press, even if tones are not generated.

G

G.711: An ITU PCM encoder/decoder specification for mu-law and A-law encoding.

H

H.100 bus: A TDM telephony bus standard for integrating hardware from various PC board vendors. The H.100 specification defines a ribbon cable bus that transports telephony voice data and signaling data across PCI boards. The H.100 bus is an interoperable superset of the H-MVIP and MVIP-90 telephony buses.

H.223: A protocol used to multiplex control and audio and video media on and off of a single DS0 within a trunk.

H.263: An ITU video compression standard. H.263 supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions.

H.264: An ITU and ISO video compression standard that compresses video into lower bandwidth compared to H.263 and MPEG-4. H.264 is also called MPEG-4 Part 10.

I

INAP: Intelligent Network Application Part; an SS7 protocol that facilitates building platform-independent, transport-independent, and vendor-independent applications. Such applications include service switching points (SSPs), internet protocol (IP) applications, service control points (SCPs), enhanced services platforms, service circuit nodes, and other custom applications.

ISDN: Integrated services digital network; a standard for providing voice and data telephone service with all digital transmission and message-based signaling.

ISUP: ISDN user part; the SS7 protocol layer that allows for the establishment, supervision, and clearing of circuit-switched connections between two SS7 signaling points, such as central office switches. Despite its name, the ISUP layer is not unique to interconnecting. It is used to manage all types of circuit-switched connections.

ITU: International Telecommunications Union; an international standards body for telecommunications.

IVR: Interactive voice response; a telephony application in which callers interact with programs using recorded or synthesized voice prompts, DTMF digits, or speech recognition to query or deliver information.

M

Media Resource Function: Component of the Dialogic® Vision™ VX Integrated Media Platform that provides media processing including record, playback, and interfaces to speech recognition resources. The Media Resource Function is implemented by MIOSIP.

MIB: Management information base; an SNMP collection of objects that represent a managed node. Physically, a list of variables. Logically, a table with rows of variables.

MIOSIP: Implements the Media Resource Function of the Dialogic® Vision™ VX Integrated Media Platform. MIOSIP provides SIP call control, media processing over RTP, DTMF generation and recognition, and an MRCP client to automatic speech recognition (ASR) resources.

MPEG-4: An ISO/IEC standard for compressing multimedia data (video, audio, and speech).

MRCP: Media Resource Control Protocol; an application protocol for implementing automatic speech recognition (ASR) and text-to-speech services (TTS). MRCP provides a distributed system of ASR and TTS engines connected over an IP network.

MTP: Message transfer part; the SS7 protocol layers responsible for the reliable, in-sequence delivery of packets between two SS7 signaling points. The MTP functions include message routing, signaling link management, signaling route management, and congestion control.

MVIP-95: Device driver specification for H-MVIP, H.100, and H.110 telephony buses.

N

NETANN: Basic Network Media Services with SIP; an interface that enables applications in a SIP network to locate and invoke basic services on a media server. These services include network announcements, user interaction, and conferencing services. Also called RFC 4240.

O

OSP: Open Settlement Protocol; a European Telecommunications Standards Institute (ETSI) protocol used to exchange authorization, accounting, and usage information for IP telephony.

P

PSTN: Public switched telephone network; a public telephone network.

R

route: A connection path. On the PSTN network, a route is a logical collection of trunks. On the IP network, a route is a destination URL.

RTP: Real time transport protocol; a layer added to the internet protocol (IP) that addressed problems caused when real-time interactive exchanges (such as

audio data) are conducted over lines designed to carry packet-switched (connectionless) data.

S

- SCCP:** Signaling connection control part; an SS7 protocol that provides both connection-oriented and connectionless data transfer over an SS7 network. It extends the service provided by the SS7 MTP layers by adding extended addressing capabilities and multiple classes of service. The SCCP addressing capabilities allow a message to be addressed to an individual application or database within a signaling point. See also SS7.
- SDP:** Session description protocol, a protocol that defines a text-based format for describing streaming media sessions and multicast transmissions.
- Signaling Server:** An optional component of the Vision™ Server that provides redundant and scalable ISUP signaling.
- SIP:** Session initiation protocol. An IP signaling and telephony control protocol used mainly for voice over IP calls and multimedia communications. SIP relies on the session description protocol (SDP) for session description and the Real Time Transport Protocol (RTP) for actual transport.
- SRGS:** Speech Recognition Grammar Specification (SRGS); a syntax for representing the grammars used in speech recognition.
- SS7:** Signaling system 7; an out-of-band signaling system that provides fast call setup using circuit-switched connections and transaction capabilities for remote database interactions.
- SSML:** Speech Synthesis Markup Language; a proposed standard for enabling access to the internet using speech. SSML provides a standard way to control various aspects of speech (such as pronunciation, volume, pitch, and rate) over a variety of platforms.
- SSML Processor:** Component of the Dialogic® Vision™ VX Integrated Media Platform that processes SSML requests for audio and text-to-speech.

T

- T.38 fax:** A standard for real-time fax over IP that makes it possible for fax machines from different vendors to talk to each other over IP networks. The T.38 standard defines how to conduct group 3 facsimile transmission between terminals in which a portion of the transmission path between terminals includes (besides the PSTN or ISDN) an IP network such as the internet.
- TCAP:** Transaction capabilities application part; an SS7 protocol that provides applications with transaction support over the SS7 network. It enables the exchange of non-circuit related data, such as database queries and responses and remote feature invocation requests between SS7 signaling points. The TCAP layer relies on both the MTP and SCCP layers for message addressing and delivery.
- TDM:** Time division multiplexing; a technique for transmitting a number of separate data, voice, or video signals simultaneously over one communications medium by quickly interleaving a piece of each signal one after another.

telecom configuration file: File that provides information about the resources that interface with the Call Server and about other elements, such as the number of routes and the circuit selection.

trunk: The physical interface between the telephone network and the Vision™ Server. In telephone networks, a trunk is a shared connection between two switches. It differs from a line in that it is not dedicated to one subscriber or extension. T1 and E1 trunks carry 24 and 31 circuits, respectively.

TTS: Text-to-speech; a system that converts written language to speech.

V

Vision™ Console: Web-based configuration tool that configures the Vision™ Server.

VoiceXML: Voice Extensible Markup Language; a language that enables users to interact with the internet through voice recognition technology.

VoiceXML application configuration file: A file that maps individual VoiceXML applications to number ranges that trigger the execution of those applications.

VoiceXML Interpreter: Component of the Dialogic® Vision™ VX Integrated Media Platform that interprets VoiceXML dialogs.

VoiceXML Subsystem: Component of the Dialogic® Vision™ VX Integrated Media Platform that provides media processing for VoiceXML applications. The VoiceXML Subsystem consists of the VoiceXML Interpreter, SSML Processor, and Media Resource Function.

Index

A

active server 29, 30
association 67

B

backup server 30
block circuit command (ss7cli) 55
block group command (ss7cli) 55

C

circuit 38
 blocking 38
 commands 56
 obtaining status information for 41
 resetting 40
 status circuit (ss7cli) 68
 troubleshooting 51
 unblocking 38
circuit group 38
 blocking 39
 commands 55
 resetting 41
 unblocking 39
command line interface 28, 29, 30, 32,
 38, 43, 53, 54
configuration files 24, 87
configuring 15
 sample configuration files 24
 the physical interface 21
 the SS7 network 23
 Vision Signaling Server 17, 18, 19

D

disable link command (ss7cli) 55

E

enable link command (ss7cli) 55

H

halt board command (ss7cli) 57

I

Inhibit link command 55
ISUP 114
 circuit group parameters 117
 configuring 23
 general parameters 114
 NSAP parameters 120
 tracing 82
 USAP parameters 119

L

link 32
 commands 55
 disabling 32
 enabling 32
 inhibiting 33
 obtaining statistical information for
 35
 obtaining status information for 34
 stats link (ss7cli) 60
 status link (ss7cli) 47, 70
 troubleshooting 49
 uninhibiting 33

linkset 32

 commands 55
 obtaining statistical information for
 36
 obtaining status information for 34
 status linkset 72

load board command (ss7cli) 57

log file 47

M

M3UA 102

- M3UA SAP 74
- managing 27
 - circuit groups 38
 - circuits 38
 - links 32
 - linksets 32
- MTP 90
 - configuring 23
 - general parameters 90
 - link parameters 93
 - linkset parameters 99
 - managing links and linksets 32
 - NSAP parameters 92
 - route parameters 100
 - tracing 84
- N**
- NSAP 75
- O**
- obtaining information 28, 43
- P**
- packet 44, 84
- physical interface 21
- ports 22
- process
 - starting 37
 - stopping 37
- PSP 63
- R**
- reset circuit command (ss7cli) 55
- reset group command (ss7cli) 55
- restarting processes 37
- route 53
 - obtaining information about 43
 - stats route command (ss7cli) 64
 - status route command (ss7cli) 76
- S**
- SCTP 111
- SCTP SAP 79
 - server 53
 - commands 57
 - determining which server is active 29
 - obtaining information about 28
 - switching 30
 - taking out of service 31
- SIGTRAN 18
- SNMP interface 29, 30, 31, 32, 38, 43
- SS7 command line interface 53
- SS7 configuration file 87
 - parameters 87
 - samples 24
 - using for server configuration 15, 23
- SS7 network 23, 47, 49
- SS7 standards 13
- ss7_config_default.xml 24, 87
- ss7cli 53, 54
- ss7trace 44
- SSP parameters 122
- stats link command (ss7cli) 47, 55, 60
- stats m3ua command (ss7cli) 62
- stats psp command (ss7cli) 63
- stats route command (ss7cli) 56, 64
- stats sctp command (ss7cli) 65
- stats sctsap command (ss7cli) 66
- stats tsap command (ss7cli) 81
- status assoc command (ss7cli) 67
- status circuit command (ss7cli) 55, 68
- status link command (ss7cli) 55, 70
- status linkset command (ss7cli) 55, 72
- status m3ua command (ss7cli) 73
- status nsap command (ss7cli) 75
- status route command (ss7cli) 56, 76
- status sctsap command (ss7cli) 79
- status server command (ss7cli) 57, 80
- stopping or restarting processes 37
- switch command (ss7cli) 57

switching servers 30

T

trace isup command (ss7cli) 57, 82

trace m3ua command (ss7cli) 83

trace mtp command (ss7cli) 57, 84

trace sctp command (ss7cli) 85

tracing 44, 82, 84

troubleshooting 47, 49

trunk 22, 47

U

unblock circuit command (ss7cli) 55

unblock group command (ss7cli) 55

uninhibit link (ss7cli) 55