Dialogic® DSI SS7G41 Signaling Server
SIU Mode Release Notes

Document Reference: RN001LGD

Contents

Release 2.4.9

1 Overview

This release provides new features to support transparent operation of the ISUP Continuity Check procedures and to allow mapping of LIU alarms to a slave LIU port.

The release also includes changes and corrections as detailed below including a correction to dynamic Global Title configuration to prevent unexpected resource exhaustion when dynamically removing old and adding new Global Titles.

This release is fully backwards compatible with the previous release.

1.1 Applicability

This release is suitable for all users.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00118492

2 New Functionality

2.1 ISUP Continuity Check Transit

This release adds the ability to optionally configure an ISUP Circuit Group so that all Continuity Check messaging is passed transparently (rather than performing validation and running timers).

This functionality is activated by setting bit 23 (0x00800000) in the OPTIONS2 parameter of the ISUP_CFG_CCTGRP command.

2.2 LIU Alarm forwarding

This release provides the ability on the SS7LD signaling board to map PCM alarm conditions in both directions between a pair of LIUs. This is useful where voice circuits from the network are looped through the SIU and passed out to the secondary LIU to be sent to a media card hosted in a separate chassis. In the event of sync loss on the network facing LIU the SIU will generate AIS on the slave LIU.

The LIU_CONFIG configuration command has been extended to allow (for SS7LD boards) configuration of a slave LIU using a new configuration parameter, SLAVE, which identifies the slave PCM port and the setting of bit 0 of the OPTIONS parameter which indicates that LIU Alarm forwarding for the LIU has been configured. The master and slave LIU must exist on the same signaling board.

In order to configure the slave alarm mapping, set bit 0 of the OPTIONS field (eg OPTIONS=0x0001) and set SLAVE equal to the PORTID of the 'slave' port (that is the port that will generate AIS if an error is detected on this LIU).

To achieve bidirectional mapping of the alarms both LIUs must be configured with the other LIU as the slave (as shown in the example below).

```
LIU_CONFIG:PORTID=0,PCM=0-1,LIUTYPE=E1,LC=HDB3,OPTIONS=0x0001,SLAVE=1;
LIU_CONFIG:PORTID=1,PCM=0-2,LIUTYPE=E1,LC=HDB3,OPTIONS=0x0001,SLAVE=0;
```

3 Other Changes

3.1 MRF_CE – Concerned Entity Configuration

This release removes a restriction which previously prevented a concerned entity from being notified of status changes for both an Alias for a DPC as well as the DPC itself.

This release corrects operation of the Message Router Concerned Entity command in cases where the Concerned Entity is a User Part which is concerned about the status of a Local Point Code in a different Network Context.

3.2 Dynamic GTT Configuration

This release corrects an issue whereby when an SCCP_GTT was deleted the internal resource was not correctly freed up. This previously had the effect of progressively reducing the maximum available Global Title capacity until the unit was restarted.

3.3 MTP3 – MTP Restart in ANSI Networks

This release corrects operation of the MTP Restart procedure when configured for ANSI operation to ensure that the procedure terminates correctly. Previously under certain conditions periodic generation of TRW messages could occur.

3.4 MTP3 - Route Measurements

MTP3 Route measurements no longer include Signaling Network Management (SNM) or Signaling Link Test (SLT) messages. Previously received messages were counted.

3.5 M3UA – Reception of Badly Padded Frames

This release includes a change to M3UA operation to tolerate receipt of an M3UA message where the final parameter padding was not included in the overall message length.

3.6 M2PA – Remote Processor Outage

This release corrects an issue that could result in an M2PA link failing to recover correctly if failed whilst in the Remote Processor Outage state.

3.7 ISUP/BICC – Recovery from Auto Blocking

This release corrects a problem in ISUP which resulted in some Circuit Groups failing to recover correctly when reset by the user. The issue occurred when circuits were in the process of being auto blocked (due to failure of the ISUP host heartbeat) and a Circuit request was received from the user before auto-blocking had been established.

This release also increases (for high density configurations) the rate at which auto blocking is applied from 100 to 200 circuit groups per second.

3.8 Web Server (IPY00118492)

This release updates the internal web server used for browser access to a later release to address certain vulnerabilities.

3.9 Web Server SECURE Access

The WMSER policy option SECURE requires that HTTP digest authentication be used to access the system. SECURE has been extended such that access is additionally limited to HTTPS only transport and using only strong ciphers. When upgrading to this release a previously setting of SECURE will be modified to a value of AUTH which can be used for HTTP digest authentication and HTTP transport.

3.10 Web Server HTTPS SELF Certification

When generating a TLS certificate locally for HTTPS access, SHA256 is now used.

3.11 SSH Policy Extensions

This release adds a new SSH policy setting which restricts the use of SSH encryption algorithms to allow just the more secure algorithms. Operation is controlled using the SSHSER parameter of the Account Control Policy Set command ACPOS.

If SSHSER=INACTIVE then SSH is disabled. If SSH=ACTIVE then all encryption algorithms are supported. If SSHSER=SECURE then the Arcfour and cbc encryption algorithms are not supported for SSH.

3.12 HTTP Access

This release corrects an issue with policy enforcement to ensure that http access is correctly prevented when disabled. It also corrects an issue which previously could prevent certain user accounts having access to files in the syslog folder when using the browser interface.

3.13 Username Parameter Validation

This release corrects operation of parameter validation for the 'USER' parameter when creating a user account so that only alphanumeric characters are permitted (case insensitive [a-z], [0-9]). Existing accounts that have non alphanumeric characters are still maintained.

3.14 SS7LD Board – E1 Alarm Status

This release corrects an issue that could result in generation of incorrect E1 LIU status indications. As a result the board could, for example, indicate In Sync and AIS at the same time whilst the interface was good or indicate In Sync whilst actually receiving AIS. The condition was triggered by receipt of an AIS condition which cleared and was then reasserted quickly.

3.15 Telnet Operation

This release corrects an issue which prevented multiple users accessing Telnet from the same terminal server. It removes a race condition which could result in access to a Telnet port getting blocked until the unit is next restarted as a result of a user attempting to log on during startup. It also corrects an issue that could arise if two users attempted to log in to the same Telnet port at the same time

Dialogic
06-Oct-17
Revised 28-Dec-17

Release 2.4.3

1 Overview

This release is a maintenance release which includes support for multiple host modules in DTS mode as well as providing further changes and corrections as detailed below.

This is the first release since Release 2.4.1 and it is fully backwards compatible with that previous release.

1.1 Applicability

This release is suitable for all users.

2 Changes

2.1 DTS – Per-LSS User module_id's

When using DTS between SCCP and the Local Sub-System (ie. DTS Mode A), this release enhances operation of the SCCP_LSS command to allow Local Sub-Systems using DTS to make use of different USER_ID (module_id) values (rather than having to use the fixed DTC module_id).

This facilitates additional flexibility in designing systems with multiple hosts and multiple Local Sub-Systems (including the ability for traffic to bypass DTC as it passes up the stack). By default incoming SCCP traffic is shared across all available hosts, however use of the DTS_ROUTE command allows the user to create specific host assignments.

2.2 SCTP – Enhanced internal architecture

This release includes an updated SCTP implementation which has been enhanced to spread the processing load over multiple CPU cores to provide improved utilization of available CPU bandwidth.

The updates to SCTP also address a number of protocol issues and errors including correcting an issue that could result in SCTP locking up and causing a restart of the unit.

2.3 M3UA – Failure to Restore Link

This release corrects an issue within M3UA that potentially could result in a failure to correctly restore an Association following failure of an active link.

2.4 Diagnostics

This release introduces some additional diagnostic capabilities and measures to guard against excessively large system logs in the snapshot file.

Dialogic
13-Dec-16
Revised 14-Dec-16

Release 2.4.1

1 Overview

This is a maintenance release which includes changes and corrections as detailed below.

This is the first release since Release 2.3.9 and it is fully backwards compatible with that previous release.

1.1 Applicability

This release is suitable for all users.

2 Changes

2.1 MTP3 – STP Operation

This release includes important corrections to operation of MTP3 in STP configurations when using C-links. These changes ensure reliable generation of preventative TFP messages prior to routing over a link set and generation of TFA messages after stopping using a link set to reach the destination.

2.2 ISUP – ISP_MSG_MAINT_IND

When operating with 128 circuit groups, ISUP will no longer generate ISP_MSG_MAINT_IND (0x070a) messages.

2.3 ISUP – Application Heartbeat

The ISUP Application Heartbeat mechanism has been enhanced to require two failed attempts prior to declaring the host as failed. Each attempt allows 4 seconds for receipt of a response. When operating with more than 128 circuit groups, the period between successive heartbeats is reduced (to 7 seconds) and the rate at which Circuit Groups are automatically blocked is increased (to 100 groups per second). This ensures better detection and faster response in the case of high capacity systems.

2.4 M3UA – Error Indications

This release limits the maximum number of event reports from M3UA to one per DPC every 10 minutes when it is unable to send a message to a Destination because it is unavailable or unknown.

2.5 M3UA –Load sharing

M3UA now correctly load shares across multiple associations in the case that there are between 5 and 16 associations to a Remote Application Server or Signaling Gateway. Previously the maximum supported was 4 associations.

2.6 M3UA – SCON without congestion level

This release will accept an SCON message with no congestion level parameter and handle it as indicating congestion rather than no congestion.

2.7 Message Router – SSF Spare Values

This release corrects the coding of the ITU MTP3 Sub-Service field when interworking with other signaling variants (such as ANSI) so that spare bits are correctly set to zero.

2.8 Message Router - Performance

This release includes an optimization within Message Router Origin operation to improve performance in the case that the OGID values are not allocated from a contiguous block commencing at a low number.

2.9 MMI – Press return to continue

If after waiting 30 seconds for the user to respond to the "Press return to continue" on the MML interface the user has not entered anything the current command will be aborted and the text "EXECUTED" displayed.

2.10 Snapshot Generation

This release corrects an issue which prevented successful generation of a snapshot file as a result of exhaustion of internal file descriptors. The issue also caused reports of disk drive failure and Ethernet port failure.

Dialogic
21-Sep-16

Release 2.3.9

1 Overview

This is a maintenance release which includes a number of minor changes and corrections as detailed below.

This is the first generally available release since Release 2.3.2 and it is fully backwards compatible with that release.

1.1 Applicability

This release is suitable for all users.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00117001, IPY00117190, IPY00117249, IPY00117305, IPY00117310, IPY00117345, IPY00118008 and IPY00118009.

2 New Functionality

2.1 SCCP – GTT Capacity

This release increases the number of Global Title Translations supported per Network Context to 512.

3 Other Changes

3.1 Software Licensing (IPY00117310)

During restart, on detection of a new software license the unit will automatically perform a full hard restart so that the new license takes effect.

3.2 Disk Partition Full (IPY00118008)

This release corrects an issue that could, in the case of a large number of failed login attempts, result in one of the partitions on a hard disk filling to capacity. In turn this prevented correct creation of new user accounts with the result that new users were unable to gain SFTP access to the unit. This release corrects the issue by enforcing a limit on the maximum size of the offending log file.

3.3 Management Hosts (IPY00117190)

This release corrects an issue introduced in Release 2.2.3 where configuration of the optional second management host using the API_MSG_COMMAND message resulted in a restart of the system.

3.4 CNBOS Command - Board Configuration

This release checks the mandatory BRDTYPE parameter for the CNBOS command and rejects the command if the parameter is invalid or omitted.

3.5 Use of ITU-T links at 56kb/s

This release includes a correction to allow ITU-T SS7 links to optionally operate at 56kb/s. Previously only ANSI links supported 56kb/s operation.

3.6 SS7MD Link Congestion Count (IPY00118009)

This release contains corrections to the operation of two per-link measurements for the SS7MD board, the 'Congestion Count' and 'Tx Messages Discarded'.

3.7 STSLP Command - SS7 Link Status

This release corrects operation of the STSLP command to allow use of the LINK parameter to display status for a single link.

3.8 Message Router - Alias Point Code (IPY00117354)

Previously, if a Message Router concerned relationship was configured where the concerned entity was in a different Network Context from the Point Code it was concerned about an implicit route to an alias Point Code would be created in the Network Context of the concerned entity. Configuration of an SCCP RSP using this alias Point Code was rejected. This release corrects this issue and allows a SCCP RSP to route to an alias Point Code.

3.9 Message Router – Concerned Entity

This release corrects operation of Message Router Concerned Entity mapping in the case where the concerned domain is a User Part (ie CONC_DOMAIN=UPART) and the concerned entity is in a different network context to the affected entity (ie. CONC_NC != NC). Previously status indications were not passed to the user part in this case.

3.10 Message Router – Message Priority

This release corrects an issue that potentially resulted in message priority getting set to zero when a message passes through the Message Router Function.

3.11 Message Router - Destination DPC (IPY00117249)

This release corrects an issue introduced in Release 2.2.9 which prevented correct operation of the Message Router Destination DPC parameter when using 24 bit point codes.

3.12 Message Router - Measurements

This release corrects the 'period' reported in measurements for Message Router Origins, Routing Keys and Destinations. This applies both to the user interface and to periodic measurements files.

3.13 SCCP Load Share Table - Dynamic Addition

This release corrects an issue which prevented dynamic addition of an additional DPC to an SCCP Load Share Table.

3.14 SCCP – GTT using Translation Type 2

This release corrects operation when configuring SCCP Global Title Translation rules which use GT Translation Type 2. In previous releases, using an odd number of GTAI digits in the pattern or address (including any separators) would cause the Signaling Server to incorrectly pad the GTAI digits with an additional zero. This has been corrected.

3.15 SIGTRAN Route - Congestion Level

When viewing the status of a SIGTRAN route (using the browser interface or the STSRP command) the current congestion level is now displayed using the CONG_LEVEL parameter.

3.16 SIGTRAN Link Port Validation (IPY00117305)

This release provides enhanced checking of SIGTRAN link configuration parameters to prevent invalid configurations being accepted but subsequently failing to operate. Specifically all associations using the same local port value must use the same set of Local IP addresses.

3.17 SIGTRAN Link Measurements

This release corrects reporting of the 'Out of Service Duration' for M2PA links and allows SIGTRAN Link measurements on page 1 (SCTP) and page 2 (M3UA) to be individually reset on a per-page basis.

3.18 DTS Routing (IPY00117001)

This release corrects the operation on the 'Route on Billing ID' when using DTS in conjunction with host-based IS41.

3.19 ACPOS Command - Account Control Policy

This release corrects operation of the Account Control Policy Configuration command, ACPOS when the WMSER parameter is set to HTTPS.

3.20 License Commands

The licensing configuration and status commands have been improved. The CNLCP command now reports the actual licenses present on the system and their throughput, where applicable, in link equivalents. The STLCP command reports the actual capacity, in link equivalents, of the licensed transport layer capabilities.

3.21 Log files

Following a restart, logging to the mmi, maintenance, stats and alarms log files now appends to the existing file rather than starting a new file. This ensures better utilization of the available disk capacity.

3.22 IP Logging

This release corrects an issue that previously could result in PCAP logging to the syslog/iplog file stopping spontaneously.

Operation of IP has been enhanced so that it continues to operate during periods of system overload. Previously logging was disabled during periods of overload.

3.23 Snapshot Generation

Generation of snapshot files for diagnostic purposes now takes place in the background so that user access can continue whilst the snapshot is being created. During creation, the snapshot is called snapshot_notready.tmp, once read for use access it is renamed snapshot.tgz.

3.24 Security Enhancements

This release disables the ability for TLS encryption to be negotiated down to SSLv3 or lower to reduce the potential for 'POODLE' type 'man in the middle' security attacks.

When executing the ACPOS command this release checks for a certificate before accepting WMSER=HTTPS for configuration of 'HTTPS only' operation.

When using HTTPS certificate files it is no longer necessary to perform a restart. Instead the unit checks for a certificate file at the point the IPWSS command is used to set HTTPSCERT=FILE.

This release includes an update to the web server within the web management interface in order to guard against potential vulnerabilities.

Dialogic
04-Apr-16
Revised 15-Jun-16

Release 2.3.2

1 Overview

This release is a feature release which adds the ability to gather measurements on a periodic basis and store them in CSV format. Measurements are available for different layers of the protocol stack and are useful for traffic measurements and performance monitoring.

The release also supports new load balancing capabilities within the Message Router Functionality through the ability to configure SLS rotation and inversion on a per Custom Profile basis.

The release provides a fourfold increase in capacity for PCAP trace files allowing more information to be retained, includes enhancements to MAP operation and further changes and corrections as detailed below.

This is the first release since Release 2.2.9 and it is fully backwards compatible with that release.

1.1 Applicability

This release is applicable to all users.

The following user documentation describes fully the Periodic Measurement Collection capability:

Dialogic® DSI SS7G41 Performance Measurements Reference Manual Issue 2.

2 New Functionality

2.1 Periodic Measurement Collection

This release adds the ability to gather measurements on a periodic basis and store them in CSV format. Measurements are available for different layers of the protocol stack and are useful for traffic levels and performance monitoring.

Traffic measurements include, for example, the number of messages sent and received, the number of octets sent and received, the peak traffic rate and peak link utilization. Performance monitoring includes features such as error counts (to assist detection of transmission path issues), routing failure causes (to detect possible configuration issues) and a number of other parameters to assist with smooth operation of the network.

Measurements are collected on a per-entity basis (eg per-link, per-origin, per-network context) basis according to the type of measurement. The frequency of measurement collection can be selected on a per measurement type basis from the following values: 5 min, 10 min, 15 min, 30 min, 1 hour, 4 hours and 1 day.

Measurements are logged to a file called “stats.csv” in the syslog/stats subdirectory of the user account. The file will accumulate data until the file size reaches a maximum at which point a new file will be created and the original will be rotated into a file called “stats.n.csv” where n is a digit. A maximum of 10 files will be retained.

This release supports collection of the following measurement types:

LIU port,
SCTP link,
M2PA link,
M3UA per network context,
M3UA per network context peak traffic,
M3UA per-link,
M3UA per-link peak utilization,
MTP2 link,
MTP3 link set,
MTP3 per link peak utilization
SCCP per network context
Message Router Origin,
Message Router Destination,
Message Router Routing Key.

Control of the period for each measurement is provided using the System Administration > Server Management > Diagnostics > Stats Reports menu.

2.2 Message Router Load Balancing

This release adds the ability for a Message Router Custom Profile to provide configurable SLS rotation or inversion on a Origin, Destination or Routing Key basis to compensate for SLS imbalance on incoming traffic. The SLS parameter for the MRF_CP defines the algorithm as follows. SLS parameter values R0, R1, R2, R3 and R4 rotate the SLS 0, 1, 2, 3 or 4 bits respectively whilst values I0, I1, I2,I3 and I4 values invert the SLS as well as rotating it.

2.3 Increased PCAP Trace Capacity

This release provides a fourfold increase in the capacity of PCAP format trace logs in the syslog/trace subdirectory of the user account. The maximum file size has increased from 5MByte to 20Mbyte.

2.4 MSSCP Command – SCCP Measurements

A new command, MSSCP, has been introduced to report global SCCP measurements for each Network Context.

2.5 MSSTP Command – M3UA Measurements

The SIGTRAN link measurement command, MSSTP, has been extended to report M3UA peak utilization on page 3 of the command.

2.6 MAP – Additional Services

This release enhances support for the Provide Subscriber Information service in line with MAP specification 3GPP TS 29.002 V8.12.0 as well as introducing support for the proprietary MAP service – Update Device Configuration (UDC).

The coding and usage of these services is documented in the *MAP Programmer's Manual*.

3 Other Changes

3.1 SS7LD Clock Operation

This release corrects a clock recovery issue which in some circumstances resulted in the unit either attempting to recover clock from the wrong E1/T1 interface or entering holdover mode rather than switching to the next highest priority clock recovery source.

Operation of the SS7LD board is that when set to recover clocks it will always use the lowest numbered interface that contains a suitable signal. When using drop and insert to pass bearer circuits to a media processor, the user should take care to use the lowest number interfaces for network facing connections and the highest numbered interfaces for local (media) connections.

3.2 IP Logging

This release corrects operation of the IPLGI command by ensuring that the command is only accepted if the IPADDR parameter is set to an actual IP address value. Previously IP logging could be inadvertently disabled.

3.3 Alarms - Severity

The setting of the 'Alarm Severity' field in the alarm log has been corrected so that the original severity is retained even when the alarm has cleared. The 'Alarm State' should be used to determine which alarms are currently active.

3.4 Alarms – SCTP Path Failure

This release corrects an issue with the SCTP Path Failure alarm which sometimes prevented the alarm clearing when the path recovered.

3.5 MSSLP Command – Peak Utilization Monitor

The per link Peak Utilization Monitor on page 3 of the MSSLP command now reports Peak Rate to one decimal place and Peak Load to two decimal places in Erlangs for MTP2 links and Link Equivalents for M2PA links.

3.6 M2PA – Timer T2

This release corrects an issue which, in some cases, resulted in failure to start M2PA timer T2. This ensures that if the peer is not responding the link will periodically drop back to Out of Service and then reattempt alignment.

Dialogic
28-Nov-14

Release 2.2.9

1 Overview

This release is a significant feature release which provides as a Generally Available Release all the enhancements from Release 2.2.3 and a number of additional enhancements as described below.

It contains the ability to automatically restore the previous configuration files when reverting to the previous software release and supports the ability to rebalance Class 0 SCCP traffic to ensure even load distribution. It includes new SCTP configuration options, a number of MAP extensions and enhancements to Message Router Functionality.

This is the first Generally Available release since Release 1.3.9 and it is fully backwards compatible with that release. Users should read carefully the release notes for Release 2.2.3 and Release 2.2.9 prior to installing this release.

1.1 Applicability

This release is applicable to all users.

This release should be used in conjunction with DSMI MIB package V4.01 (or later). A new SNMP MIB (V4.03) is available which additionally includes definitions for the new alarms supported in this release.

The following user documentation updates are available for use in conjunction with this release:

Dialogic® DSI Signaling Servers – SS7G41 Operators Manual, Issue 11,
Dialogic® DSI Protocol Stacks – SCCP Programmer's Manual, Issue 11,
Dialogic® DSI Protocol Stacks – MAP Programmer's Manual, Issue 21.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00116444, IPY00116450, IPY00116703 and IPY00116844.

2 New Functionality

2.1 Software roll-back restores previous configuration

If it is necessary during a software update cycle to revert to the previous version of software then the MNRSI command should be used with RESTART=PREVIOUS. This causes the previous release of software to be automatically reinstalled. From this release it will also automatically restore the previous configuration files (config.txt, config.CF3 & SWS.CF3) that were saved internally at the time of the software upgrade (providing the operating mode (SIU or SWS) is not changed during the roll back).

This feature simplifies the process of reverting to an earlier software release where the configuration file formats were not completely compatible (such as reverting to a pre Release 2.0.0 version). Users are still advised to make their own configuration backup prior to performing a software upgrade but the new feature makes it less likely that it will need to be used.

NOTE: If a software release (old or new) is manually loaded and the unit restarted without using the RESTART=PREVIOUS then the restoration procedure will not revert to previous configuration files.

2.1 SCCP – Rebalance of Class 0 Traffic

This release introduces the ability for Connectionless Class 0 SCCP traffic to be evenly balanced towards a Remote Signaling Point through regeneration of the SLS in a cyclic manner.

The option can be selected on a per-RSP basis by setting bit 6 in the rsp_flags field of the SCCP_SSR command when configuring the Remote Signaling Point.

2.2 SCCP - Multiple Global Title Translation Tables

This release introduces the concept of multiple Global Title Translation Tables which allows the MAP user to select a different SCCP routing plan on a per dialogue basis.

Selection of the Translation Table is performed using a new integer parameter RIID (Routing Indicator Identifier) which takes a value between 1 and 65535 and acts as a token to identify the table. Refer to the *MAP Programmer's Manual* for further details.

The RIID parameter is optional and can be used when configuring the GT Translation (in the SCCP_GTT config.txt command), and when configuring a Remote Signaling Point (in the SCCP_RSP command).

2.3 MAP – Update MAP LCS Services

This release updates the MAP Subscriber Location Report and Send Routing Info for LCS services to MAP TS 29.002 v12.3.0 to allow more data to be sent and received.

2.4 MAP – Options to Control Default TCAP QoS

This release adds two new global MAP options to control the default value for the Quality of Service (QoS) parameter sent to TCAP (when QoS is not explicitly specified by the MAP user). These options are supported in the OPTIONS parameter of the MAP_CONFIG command as follows:

Bit 8, when set, causes the 'Return on Error' field to be set by default.

Bit 9, when set, causes Sequence Control to be disabled by default (selecting Class 0 operation).

2.5 SCTP – Per-association options

The following new per-association options are supported in the OPTIONS parameter of the STN_LINK command:

Bit 8, when set, disables use of the Nagle algorithm to ensure that outgoing packets are transmitted without delay.

Bit 9, when set, disables path MTU discovery and selects a fixed MTU value of 1438.

Bit 10, when set, designates the path associated with the first remote IP address (RIP1) as the primary SCTP path that if available will always be used.

2.6 Message Router - Dynamic Configuration of Origins

This release adds two new commands, MROGI and MROGE, which (subject to certain prerequisites) permit dynamic addition and removal of Message Router Origins.

To add a new Origin, first add a new MRF_OG command to config.txt then execute the MROGI command. To remove an Origin, first remove the MRF_OG command from config.txt then execute the MROGE command.

To dynamically add Origins, there must already be at least one active origin that uses the same NC / DOMAIN / SI combination. Likewise it is not possible to dynamically remove the last Origin using a specific NC / DOMAIN / SI combination.

2.7 Message Router – Alternative Destinations

The Message Router Function allows messages for a given destination to be routed based on the availability of one or more DPCs associated with the destination. The MRF_DE command supports a new DPC parameter. If present the status of the configured DPC will be checked and the table row will only be selected if the DPC is available. If available this DPC will be copied into the routing label of the message.

3 Other Changes

3.1 Alarms

A new alarm, "SS7 link cong", is reported when an SS7 link is in congestion.

A new alarm, "SCTP path fail", is reported for a SIGTRAN link when one or more paths within an active SIGTRAN association have failed.

The release includes a correction to avoid incorrectly reporting “File Sys Warning” alarms.

Parse errors are now reported on Page 2 of the active alarm list.

3.2 Dual Operation

This release corrects an issue that previously could result in a failure of two units operating in a dual configuration to correctly exchange remote accessibility data.

3.3 SS7LD Board – MTP2 T6 Timer Operation

MTP2 on the SS7LD Signaling Board has been corrected such that it no longer starts the T6 timer upon reception of SIB when the link is in service and the retransmission buffer is empty.

3.4 Message Router – Concerned Entities

This release enhances the operation of Message Router, Concerned Entity notifications to prevent multiple identical notifications being issued at the same time and to remove unnecessary delay when communicating status changes to multiple entities.

This release also removed a restriction that previously allowed only one Concerned Entity to be concerned about a specific DPC in a different Network Context.

3.5 LIU Control

This release provides the ability for test purposes to dynamically control Line Interface Unit operation on E1/T1 interface ports. The Maintenance PCM Set (MNPCS) MMI command allows the setting of diagnostic loopbacks, generation of AIS and generation of PRBS data on the interface. The command syntax is:

```
MNPCS:PORTID=[,AISGEN=][,LOOPMD=][,PRBSGEN=];
```

Current settings for the AISGEN, LOOPMD and PRBSGEN are displayed on the PCM Status (STPCP) command. Modifications to the default values for the parameters are not preserved over a system restart.

3.6 MSSLP Command - SIGTRAN Link Measurements

This release corrects the measurement period reported on page 2 of the MSSLP command following change of system time.

3.7 STSTP Command – SIGTRAN Link Status

Page 2 of the SIGTRAN Link Status command (STSTP) has been enhanced to include the status of implicitly configured paths (configured within the SCTP INIT or INIT ACK). It also reports additional per-path attributes.

3.8 SCCP - Dynamic Global Title Configuration

This release corrects the operation of dynamic Global Title Configuration to preserve the sequence in which entries in the table are used irrespective of the sequence in which they are added. The entry with the lowest GTPID value is always used first.

3.9 MAP – Update Location Data (IPY00116450)

This release corrects handling of the Update Location service to ensure that any unexpected or unsupported parameters data from a received message are passed to the user in the MAPPN_ellipsis parameter.

3.10 MAP – Reporting of User Error codes (IPY00116444)

This release corrects the reported User Error Code values when TCAP Reject components are received with Invoke problem codes of 'Initiating Release' or 'Resource Limitation'. The respective codes MAPUE_initiating_release (38) and MAPUE_resource_limitation (37) are now used.

3.11 MAP – Authentication Data Ellipsis revised

Coding of the responses for SEND-AUTHENTICATION-INFO-ACK and SEND-IDENTIFICATION-ACK has been corrected. A new parameter MAPPN_auth_set_list_ellipsis (737) is used for AuthenticationSetList table data and the MAPPN_ellipsis parameter is used for top-level response results tables for both services.

The MAPPN_send_auth_info_resp_ellipsis parameter is now obsolete and code (652) is no longer used. Applications that use MAPPN_ellipsis and/or MAPPN_send_auth_info_resp_ellipsis with these service responses should be reviewed and re-compiled with the new header file. Full details are contained in *MAP Programmer's Manual*.

3.12 MAP – Authentication Data received in multiple messages

This release ensures that MAP correctly handles response authentication data, even when received in multiple TCAP messages using TCAP segmentation (TC-RESULT-NL messages followed by a TC-RESULT-L). This affects the MAP-SEND-AUTHENTICATION-INFO and MAP-SEND-IDENTIFICATION services.

3.13 MAP – SLR 'cellIdOrSai' Table Coding

To improve compatibility with other switches (eg Huawei MSC), this release accepts received SUBSCRIBER-LOCATION-REPORT (SLR) messages where the 'cellIdOrSai' table is coded either with an ASN.1 Primary tag or a Constructed tag. For outgoing SLR messages the Constructed tag is always used.

3.14 MAP – Diameter Identity Parameters

The maximum size of Diameter Identity parameters has been increased to 255 octets as specified by MAP TS 29.002 v12.3.0.

3.15 SCTP – Primary Address Down (IPY00116703)

This release corrects an issue where an association to a multi-homed peer, failed to establish if the peer responded to the INIT from a different address than the INIT had been sent to even if that address had previously been configured as a valid peer address.

3.16 SCTP – Maximum Retransmissions

The maximum number of times a HEARTBEAT message is lost before the network address marked failed and the maximum number of times a data chunk will be retransmitted before the association is aborted have both been changed from a default value of 2 to a default value of 3.

3.17 SCTP - Reverse Path IP Filter

By default, reverse path filtering is enabled. This ensures that packets received from a remote source IP address are only accepted when the packet is received on the interface that would be used to send packets to that IP address. The purpose of reverse path filtering is to prevent receipt of spoofed IP packets. In some situations, (eg asynchronous routing) it may be necessary to disable this filtering for correct multi-path operation.

Reverse Path Filtering can be disabled by setting RPFILTER=0 in the ACPOS command (System Policy Management). By default RPFILTER is set to 1.

3.18 SCTP - Secure Mode

This release corrects the operation of "Secure Mode" for an SCTP association when operating in multi-homing mode.

3.19 M2PA – Timer Granularity and Default Values

M2PA now supports 100ms granularity for all per-link timers and default timer values have been changed to align with ITU-T Q.703 recommendations as follows: T1 45s, T2 30s, T3 1.2s, T4n 8.2s, T4e 0.5s, T6 5.5s and T7 1.7s.

This release also corrects an issue where, in certain circumstances, M2PA timers T3 and T4 were started simultaneously which could result in links prematurely exiting the proving state.

3.20 DTS – Host Status Requests Cause Restart (IPY00116844)

This release corrects an issue introduced in Release 2.2.3 where multiple calls to the DTS Host Status MMI command STDHP eventually lead to the system spontaneously restarting.

Dialogic
03-Oct-14
Revised 23-Oct-14

Release 2.2.3

1 Overview

This release is a significant feature release which adds support for IPv6, adds the ability to provide Mobile Number Portability in conjunction with the Dialogic® ControlSwitch™ System and provides a number of OA&M enhancements.

IPv6 is supported for the configuration of SIGTRAN protocol software as well as SIU host links (RSI), NTP, SNMP, IP Gateways and firewalls. IPv6 access to the unit is permitted using Browser, Telnet, FTP, SFTP and SNMP.

Mobile Number Portability (MNP) is supported in conjunction with the Dialogic Directory Services Engine (DSE) which contains the MNP database.

This release supports enhanced syntax for config.txt commands. The new syntax allows parameters to be entered in any order and allows optional parameters to be omitted. Each parameter is entered in terms of parameter name and parameter value

The release also includes major enhancements to the Alarm List including addition of new fields, addition of an Alarm Log (which list historic alarms) and the additional logging of alarms to a text file for offline analysis.

This release includes major new SNMP enhancements including the ability to view the active alarm list using SNMP and provision for SNMP notifications on changes of state of alarms. In addition, this release addresses an important syntax issue with respect to the SNMP MIB.

This release is fully backwards compatible with Release 1.3.9, however there are some important differences as follows which should be read and understood prior to commencing installation:

- This release should be used in conjunction with SNMP MIB V4.xx, which owing to the correction of a syntax error in the MIB is not fully backwards compatible with the previous MIB. A mechanism is provided to allow users to select the previous mode of operation as a short term option to ease migration. See below for details of the changes and how to retain compatibility if required.
- IP configuration is maintained when upgrading to this release however downgrading to an earlier (pre 2.0.3) release will result in the reset of the system IP configuration to its default values. It is therefore important to take a backup of the config.txt and config.CF3 files prior to upgrading to this release.
- The IP configuration commands for local IP address configuration have changed. Instead of using IPEPP/IPEPS to configure local IP addresses the commands IPNIC/IPNIP/IPNII/IPNIE should be used.
- For local IP Address configuration, IP Gateway and IP firewall configuration rather than using a separate SUBNET mask the IP address and netmask should expressed in CIDR notation where the IP address and netmask are separated by the '/' character and netmask is a integer identifying the number of leading (i.e. significant) bits in the mask.
- IP firewall configuration is maintained when upgrading to this release however downgrading to an earlier (pre 2.0.3) release will result in the IP firewall configuration reverting to the values it held prior to system upgrade.

Users should familiarize themselves with the full content of these release notes prior to commencing deployment.

1.1 Applicability

Users are encouraged to use Release 2.2.9 which supersedes this release and is now Generally Available to all users.

This release should be used in conjunction with DSMI MIB package V4.01 (or later). Please note that due to a correction of syntax errors within the MIB this MIB is not fully backwards compatible with the previous release however an option is provided to allow the SS7G41 to operate in accordance with the old MIB to ease migration. Please note the section on SNMP MIB Compatibility below.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00115900, IPY00115902, IPY00115903, IPY00115914, IPY00116128, IPY00116129 and IPY00116136.

2 New Functionality

2.1 SNMP MIB Compatibility

The SNMP DSMI Notification MIB has been restructured to remove syntax errors encountered with certain SNMP managers. This release should be used in conjunction with V4.01 or later of the DSMI MIB package.

Due to the nature of the changes to the Notification and Alarm MIBs the notifications transmitted by the system are not compatible with SNMP manager using MIB packages earlier than V4.00. To provide for continued backwards compatibility with earlier MIB packaged a new parameter, MIB, has been introduced on the CNSNS command. By default this parameter is set to a value of V4 however if a SNMP manager wishes to continue to use MIB packages earlier than V4 the MIB parameter can be set to PRE_V4.

2.2 Enhanced config.txt Command Syntax

This release rolls out enhanced format config.txt command syntax for the majority of the currently supported commands (whilst maintaining backwards compatibility so that existing config.txt files continue to function as normal).

The new syntax allows parameters to be entered in any order and allows optional parameters to be omitted. Each parameter is entered in terms of parameter name and parameter value as follows:

```
<command>:<parameter1>=<value1>,<parameter2>=<value2>;
```

For example:

```
MTP_LINKSET:LINKSET=0,OPC=321,APC=320,LABEL=Paris;
```

Many commands support an optional user-provided text ‘LABEL’ parameter to improve readability. This label parameter is used in both user output and SNMP where applicable.

Full details of command syntax (and which commands support the new format) are contained in *SS7G41 Operator’s Manual, Issue 9*.

2.3 IPv6 Support and IPv4 Changes

This release adds IPv6 support and in doing so makes some changes to the commands previously used for IPv4 configuration. IPv6 is supported for the configuration of SIGTRAN protocol software as well as SIU host links (RSI), NTP, SNMP, IP Gateways and firewalls. IPv6 access to the unit is permitted using Browser, Telnet, FTP, SFTP and SNMP.

For both IPv4 and IPv6, static IP addresses are now specified in CIDR notation containing IP address followed by the '/' separator followed by the subnet mask (which is an integer identifying the number of leading (i.e. significant) bits in the mask).

To accommodate IPv6 configuration the old commands IPEPS/IPEPP have been replaced (for IPv4 and IPv6) by the new commands IPNIC and IPNIP for configuring IP Network Interfaces. The STEPP/MSEPP commands have been replaced by STNIP and MSNIP which display status and measurements for the network interfaces.

The IPGWx commands have been modified to support IPv6. As both IPv4 and IPv6 networks can have a default gateway the 'Default' identification should be assigned to the IPNW parameter rather than the IPGW id parameter. When configuring non default gateways the IP Network and Network Mask are both configured using the IPNW in CIDR notation.

A new config.txt command IP_TOKEN allows the user to create a token associated with a numerical IPv6 (or IPv4) address. This token can then be used throughout config.txt when configuring IP addresses without the need to retype the full IP address each time.

2.4 SCCP_GTT Command

This release adds the ability to have separate Global Title Translation (GTT) tables for incoming and outgoing messages. This is achieved by the addition of a new optional parameter (GTTSRC) to the config.txt command SCCP_GTT. When GTTSRC=LOCAL the command only applies for messages generated by a local sub-system (ie. outgoing messages). When GTTSRC=REMOTE the command only applies to messages passed up to SCCP from the network (ie. incoming messages). If GTTSRC=ANY (or the parameter is omitted) the command applies to all messages.

A new optional parameter (BAK_DUAL) has been added to the SCCP_GTT command that when set to Y causes any SCCP messages that matches the GTT pattern, but cannot be routed due to network failure, to be passed to SCCP on the partner unit so that it can reattempt routing.

A new optional parameter (OPTIONS) which is reserved for future use has been added to the SCCP_GTT command.

2.5 Mobile Number Portability Option

This release supports a purchasable run-time option which in conjunction with Message Router functionality allows the SS7G41 to work in conjunction with the Dialogic Directory Services Engine (DSE) which is an element of the Dialogic® ControlSwitch™ System for the realization of Mobile Number Portability. Further information on this feature is available on request.

2.6 IP Port Bonding

IP Port bonding has been enhanced to support more than 2 ports in a single bond. Previously a Port Bond was created using the IPEPS MMI command and setting the IP address of a particular IP port to be the 'standby port' of another IP Port. The mechanism has changed and a BOND is considered a distinct Network Interface that Ethernet Port Network Interfaces can be attached to. To configure a Port Bond a BOND Network Interface should first be added using the IPNII command. Individual Ethernet Port Network Interfaces can then be added to the bond using the IPNIC command. The bond will use the MAC address of the lowest numbered Ethernet Port.

2.7 IP Firewall

Operation of the IP Firewall has been enhanced to support more sophisticated IP rules. In addition to being able to limit traffic for a particular service based on a source network/address the command now supports specification of a destination network/address. The parameters NETWORK and MASK have been replaced with IPSRC and IPDEST where IP Network Addresses and associated network masks should be entered in CIDR notation.

Previously the IPEPx command could be used to limit access to the Web management interface for particular Ethernet ports. This functionality has been removed. If required the IP firewall should instead be used to limit access from particular IP addresses.

2.8 IP Ping and Route Tracing

The STIPP command has been enhanced to support the ability to trace the route to an IP Address providing indications of the best, worst and average ping times to the destination and each way point.

2.9 New and changed config.txt Commands

The new command SIU_DUAL replaces the old command SIU_REM_ADDR.

The ability to specify the Network Context (NC) in the commands MTP_CONFIG, SCCP_CONFIG and STN_CONFIG means that the commands MTP_NC_CONFIG, SCCP_NC_CONFIG and STN_NC_CONFIG are no longer required.

The SCCP_RSS command (whilst still available for backwards compatibility) has been replaced by three new commands SCCP_LSS, SCCP_RSP and SCCP_RSS to configure SCCP Local Sub-System, SCCP Remote Signaling Point and SCCP Remote Sub-System resources respectively.

2.10 New MML Commands

New MML commands allow the user to read the current configured values for MTP and SIGTRAN protocol timers. The commands CNM2P, CNM3P, CNQSP, CNG2P, CNG3P and CNGSP are documented in the *SS7G41 Operator's Manual*.

2.11 Browser Interface

Several small changes and enhancements have been made to the browser interface to improve ease of use. Changes include a new color scheme, addition of status information at the top of each page, the ability to connect to the partner unit and some layout changes affecting SCCP and TCAP configurations.

Presentation of large amounts of data now uses tables and allows the user to select the data rather than needing to scroll through the whole table. The number of line displayed per view is user configurable and data tables can be sorted (by clicking the head of the column) or filtered (by clicking on the required data component value).

2.12 Alarm Log Enhancements

This release includes a number of enhancements to the operation of the Alarm Log mechanism which result in format changes to the ALLIP (Alarm List) command and the alarms.log CSV text file and the addition of the date and time of alarm occurrence.

A new command, ALLOP, provides alarm log history. The command is similar to the ALLIP command except that it reports the previous 1000 alarm events (occurrence or clearing of alarms).

Alarm events are also archived to the text file 'alarm.log' in the syslog/alarms sub-directory of the ftp account.

The following alarm log fields have been added or modified:

NODE – A new user configurable field providing a short-form identity of the unit. This is displayed on the browser interface, on the MMI interface at login and included on a per alarm event basis in the SNMP ALARM MIB and the CSV format alarms.log file. The field is up to 9 alphanumeric characters and is set using the CNSYS command.

SEQUENCE – Sequential reference number of an entry in the alarm log since the last restart.

CODE – Numeric identifier of the alarm code. Each alarm condition has a unique CODE value.

STATE – Current state of the alarm which can be Active, Acknowledged (the alarm is still active but has been acknowledged by an operator) or Cleared. The user can acknowledge an alarm using the browser interface or using the new ALLIS command specifying the SEQUENCE parameter.

SEVERITY – Perceived severity of the active alarm (previously called CLA).

TITLE – Descriptive title for the alarm code. The text for some alarm types has changed slightly from the previous release to align with the values reported for SNMP events.

TYPE – Classification of the alarm into an alarm type from the following list: communicationsAlarm (2), qualityOfServiceAlarm (3), processingErrorAlarm (4), equipmentAlarm (5) and environmentalAlarm (6). This field replaces the previous Category (CAT) field so the STSYP command no longer lists the count of alarms in the following categories: System, PCM and Protocol.

CAUSE – Probable cause for the alarm code based on the principles of ITU Recommendations M.3100, X.733, and X.736 and GSM 12.10 (ETS 300 618). The values used are defined in the DSMI-TC MIB (V3.00).

DIAG1, DIAG2 – Additional diagnostic information provided on the occurrence of an alarm. The meaning of these fields varies based on the alarm code.

The new command ALCDP lists for each CODE the assigned SEVERITY, TYPE and CAUSE.

The STSYP and STSWP commands now report the count of "Warning" alarms in addition to the existing counts of "Critical", "Major" and "Minor" alarms.

2.13 SNMP Alarm MIB

This release adds support for a new SNMP MIB which allows the current active alarm log to be read using SNMP and permits generation of SNMP notifications whenever the state of an alarm changes (i.e. on Occurrence, Acknowledgement or Clearing of the alarm condition). The new DSMI-ALARM.mib is part of the DSMI MIB (D3028_6_2MIB) V4.xx MIB set.

Generation of SNMP notifications is controlled by a new parameter (DSMIEVENT) of the CNSNS (Configuration SNMP Set) command. The following values are supported:

OBJECT – Report SNMP notifications based on changes of state related to the individual object MIBs only. (This is the default and is equivalent to pre Release 2.2.0 operation)

ALARM – Report SNMP notifications based on changes of state related to the ALARM object MIB only.

ALL – Report SNMP notifications based on changes of state related both to individual object MIBs and to the new ALARM MIB.

NONE – Do not report any SNMP notifications.

2.14 Message Router Enhancements

To align with other commands, Message Route configuration commands used in config.txt have changed format from MRxxI to MRF_xx. For example MROGI becomes MRF_OG. The old format commands are still supported for backwards compatibility.

The ability to discriminate incoming traffic by OPC has been added to the Message Router Origin command (MRF_OG).

The ability to send traffic to the partner SIU has been added to the Message Router Destination command (MRF_DE) by using DOMAIN=PARTNER.

In scenarios where traffic from the network cannot be transmitted to an Application Server (AS) due to SCCP determining that the Point Code of the AS is unavailable, the message is sent by SCCP to SCCP on the partner unit to allow routing over an alternative Application Server connection.

2.15 MTP3 – Increased Link Set Capacity

The number of supported MTP link sets has increased from 64 to 120.

2.16 MTP3 – Peak Utilization Monitor

This release adds a Peak Utilization Monitor which captures the peak traffic utilization over a 10 second period on a per-link basis for all MTP3 signaling links. It allows the user to read back the peak utilization over the previous 5 minute interval, the previous 1 hour interval and the previous 24 hour interval.

The monitor tracks peak utilization in Message Signal Units per second transmitted or received over a 10 second measurement interval and link utilization as a percentage based on number of octets transmitted and received in a 10 second measurement interval.

The Peak Usage Monitor is accessed using the existing MSSLP MMI command by setting PAGE=3. For full details refer to the SS7G41 Operator's Manual.

2.17 SCCP - GTT Load Share Table Measurements

A new measurements command MSLTP has been added which allows the user to read measurements associated with GTT load share tables.

2.18 INAP – User control of TCAP Idle Timeout

This release allows the INAP user to optionally control the TCAP Idle Timeout on a per dialogue basis.

A new parameter (INAPPN_dlg_idle_timeout 0x20) is defined for use in the INAP_MSG_DLG_REQ message when the primitive type is INAP-OPEN-REQ (1), INAP-OPEN-RSP (0x81) or INAP-DELIMIT-REQ (3).

The parameter is a 1 or 2 octet value which contains the timeout value in seconds. When the two octet version of the parameter is used the first octet is the most significant value.

3 Other Changes

3.1 SIU Host Configuration

The mechanism for configuring the minimum number of SIU Hosts has changed. The value should now be set using the MIN_HOSTS parameter in the config.txt command SIU_HOSTS. If the number of active hosts falls below this value then all network facing MTP and M3UA links are automatically deactivated.

Note: Users of Message Router or Signaling Gateway Functionality should typically set MIN_HOSTS to zero otherwise network facing links will remain deactivated.

3.2 Snapshot and Diagnostic Files

This release includes minor changes to the structure and filenames used within the browser based Files menu to improve clarity as follows:

The filename of the snapshot file (which is stored in the 'User' folder) is now snapshot.tgz (rather than syslog.tgz). This is the file that should be provided for the diagnosis of technical support issues.

The content of diagnostic files startup.log, shutdown.log and diag.log contained within the snapshot.tgz file has been enhanced.

The previous 'Snapshot' folder is now called diag to remove ambiguity and the 'Licenses' and 'Server' folders have been removed.

A default config.txt is now available in the 'Configuration' folder and is called 'default_config.txt'. This should be used as the starting point when creating a new config.txt. It contains the syntax for each command.

3.3 Diagnostic Core Files

In the event that an internal process crashes and the system is restarted (either automatically or by user action) a new diagnostic core dump is created. This file (core.tgz) is created in the syslog subdirectory of the ftp account and can be used by Dialogic to investigate the cause of the failure.

3.4 Restart Error

Reporting of the "Restart Error" alarm has been changed so that instead of multiple "Restart Alarm" events being generated the unit will now generate a single "Parse Error" alarm. Further information on the cause of the error is now available on page 2 of the active alarm list.

When the unit fails to start up correctly (indicated by "Config fail" or "Parse errors" alarms) the unit will actively prevent dynamic configuration changes. The user must correct the configuration issues and restart the unit.

3.5 MNRSI Command (IPY00115903)

This release corrects an issue with the operation of the MNRSI command which previously failed to execute correctly if a second user was logged on and executed a command shortly after MNRSI was executed.

3.6 MSSYP Command (IPY00115914)

This release allows the overload count (NOVLD) to be optionally reset by using RESET=Y when executing the MSSYP command.

3.7 MSSLP Command

This release corrects operation of the MSSLP command to prevent it causing a restart. Previously an internal race condition could occasionally result in the unit restarting, especially when operating under extreme overload conditions.

3.8 MSSTP Command (IPY00115902)

This release corrects the value of the measurement period for the MSSTP command which previously was a smaller value than it should be. In addition the TBUSY and TCONG parameters on page 2 of the MSSLP command have been corrected to display duration in seconds (rather than tenths of a second).

3.9 SS7MD Board Operation

This release corrects an issue introduced in Release 1.3.6 that resulted in possible failures of the link to come back in service if it was manually deactivated and then activated.

3.10 MTP3 - Dual Operation with Discrimination Disabled

This release corrects the processing of messages received on the partner link set when point code discrimination is disabled to ensure that messages are sent to the network (rather than the user) whenever an MTP_ROUTE to the DPC is defined.

3.11 SCCP – Event Report Limiting

To avoid excessive reporting of identical SCCP Maintenance Events (SCP_MSG_MAINT_IND) and Software Events (SCP_MSG_ERROR_IND), the unit now issues a maximum of 10 event indications for any given event type over any one minute interval. Further events during the interval are suppressed.

3.12 MAP –User parameters > 255 octets

This release supports larger parameter lengths for two parameters (MAPPN_siginfo 2560 octets and MAPPN_ellipsis 500 octets) which exceed the previous 255 octet limit. In order to use parameters over 255 octets in length the MAP User must use the MAP Code Shift mechanism. Further information is available on request.

3.13 MAP – Merged Components

When Not Last (NL) components are received by the MAP module, the parameters are decoded and saved until the final Last component (L) is received. Then the saved parameters are combined with the latest parameters. For this release a maximum parameter length test is performed after merging. If the resultant parameter length exceeds the maximum allowed for the parameter, a service provider error is reported to the MAP-User and, if Not Last, a reject sent to the network.

3.14 M3UA/M2PA License Allocation (IPY00116128)

This release corrects the allocation of licensed capacity when using the TDMSHARE parameter to share allocation between TDM interfaces and either M3UA or network facing M2PA. Previously due to a rounding error the licensed capacity was artificially reduced.

3.15 SNMP Trap Events on Startup (IPY00116136)

This release prevents suppression of SNMP trap events during the startup sequence to ensure that the SNMP manager is notified of the creation of all objects during the initialization sequence.

3.16 SNMP V3 Configuration (IPY00115900)

The use of the ENGINE parameter for the CNSMI command has changed and is now optional. If not specified then the default engine ID for the system will be used. ENGINE can be displayed using the CNSNP command.

When configuring an SNMP V3 User Account, the CNUSI command now supports the PRIV (Privacy Protocol) and PRIVPASS (Privacy Password) parameters which previously could only be entered using the CNUSC command.

3.17 API_MSG_COMMAND (IPY00116129)

This release corrects the operation of the API_MSG_COMMAND message in the case that command=4 to request MTP2 link status. Previously an undefined value was returned.

3.18 Alarms

A new alarm, “SS7 linkset lost”, indicates failure of a Link Set.

A new alarm, "NTP sync fail" is generated when NTP is configured but the unit has been unable to establish contact with the NTP server.

This release corrects an issue that previously resulted in incorrect reporting of alarms for BPOS=0, PCM=0 when the PORTID was not set to zero.

3.19 Ability to trace SMNP messaging

This release expands the PCAP diagnostic logging function to allow logging of UDP messages as used for SNMP. To achieve this, LGTYPE=UDP should be set using the IPLGI command. This option also allows filtering based on individual UDP port numbers using LGDATA parameter.

3.20 IP Logging

When operating in SIU mode the IPLGI command ensures that the parameter LGTYPE is not set to WSAPI as this value is only valid in SWS mode. Previously when set to this value the IP logging mechanism was prevented from operating.

Dialogic
17-Jun-14
Revised 23-Oct-14

Release 1.3.9

1 Overview

This is a maintenance release which contains corrections to operation of SS7LD and SS7MD boards and the SCTP protocol.

The release is fully backwards compatible with the previous release.

This is the first full release since Release 1.3.6 and it is fully backwards compatible with that release.

1.1 Applicability

This release is suitable for all users.

2 Changes

2.1 SS7LD Board – Memory Leak

This release corrects a problem which occurred in systems using the SS7LD board whereby a progressive memory leak within the board driver resulted in the unit restarting. The time between restarts is non-deterministic but some users have experienced a restart within 1 to 2 months of operation.

2.2 SS7MD Board – LIU Status

This release corrects the generation of LIU status reporting to ensure that state transitions are not missed. When operating in T1 mode there was previously a timing issue that could result in loss of status indications and a LIU status mismatch.

This release corrects an issue with the SS7MD board that under extreme load could result in links failing and being unable to recover.

2.3 SCTP - Potential Restart

This release corrects operation within SCTP which could occasionally result in a restart following receipt of an INIT on an unconfigured port.

Dialogic
19-May-13
Revised 29-Jul-14

Release 1.3.6

1 Overview

This is a feature release which increases the maximum available number of TCAP dialogs for users interfacing directly to TCAP from 64k to 1million (2^{20}), it increases the licensed throughput capacity from 256 link equivalents to 512 link equivalents and adds new MAP protocol capabilities.

The release also allows DTS host routing to be configured using the config.txt file on the SIU (removing the need for application functionality), provides a new routing mode for use with IS-41 signaling which forces all messages with the same BillingId to be routed (under normal routing conditions) to the same host.

The release also adds support for dynamic configuration of SCCP Global Titles, adds a new Message Router hunt algorithm and provides further changes and corrections as detailed below.

This is the first GA release since 1.2.10 and it is fully backwards compatible with that release. Users that make use of the new increased TCAP dialogue capacity should avoid downgrading to 1.2.x software.

1.1 Applicability

This release is suitable for all users.

The following user documentation updates are available for use in conjunction with this release:
Dialogic® DSI Signaling Servers – SS7G41 Operators Manual, Issue 6,
Dialogic® DSI Software Environment Programmer's Manual, Issue 15,
Dialogic® DSI Protocol Stacks – SCCP Programmer's Manual, Issue 10,
Dialogic® DSI Protocol Stacks – TCAP Programmer's Manual, Issue 13,
Dialogic® DSI SIGTRAN Stack – M3UA Programmer's Manual, Issue 9,
Dialogic® DSI Protocol Stacks – DTS User Guide, Issue 10.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00102639, IPY00102686, IPY00102722, IPY00102727, IPY00102728 and IPY00102788.

2 New Functionality

2.1 Increased TCAP Dialogue Capacity

For users accessing the SIU at the TCAP level the SIU can now be configured to support up to 1M (1,048,576 or 2^{20}) dialogs. The maximum number of invokes allowed by the TCAP module has also be increased to the same value.

To use this increased capacity (which requires more than 16 bits to uniquely refer to a dialog) it is necessary to use a new extended addressing scheme which makes use of the existing 'id' field in the message header and a new Name-Length-Data parameter (TCPPN_DID) in the parameter area of the message. This parameter must be the first parameter in the parameter area of the message. The parameter must contain 4 octets of data representing the full 32-bit Dialog Id.

The TCPPN_DID parameter (value=23) is required in the following messages: TCP_MSG_CPT_REQ, TCP_MSG_DLG_REQ, TCP_MSG_CPT_IND and TCP_MSG_DLG_IND. It is used between a TCAP user and TCAP on the SIU.

In addition the 'id' field in the message header must be set to the significant 16 bits of the Dialog Id.

To support an extended dialog range for TCAP the <options> field on the TCP_MSG_CONFIG has been extended to 32 bits and a new bit, bit 16, should be set to use the extended addressing scheme. When the bit is set TCAP may be configured with a dialogic range of up to 1M dialogs using the TCP_MSG_CONFIG and TCAP_CFG_DGRP configuration command.

2.2 512 Link Equivalent Throughput

This release adds the ability to license the unit for capacities of up to 512 link equivalents (compared with the previous maximum of 256 link equivalents).

To use this increased capacity users should purchase multiple licenses to make up the desired throughput capacity. For example, a 256 SIU link license and a 128 SIU link license would permit a total throughput capability of 384 link equivalents.

2.3 MAP - EPS-AuthenticationSetList data

Support for EPS-AuthenticationSetList data as used by the SendAuthenticationInfo service has been added to the response in accordance with the MAP specification 3GPP TS 29 002 version 9.4.0 (Release 9). Two additional parameters have been added to the request for the same service: numberOfRequestedAdditional-Vectors and additionalVectorsAreForEPS. The parameters for both changes are only required for MAP-V3 Application Contexts as defined in the specification.

2.4 MAP - UpdateGPRSLocation, CancelLocation and PurgeMS to MAP Release 8

The implementation of the following MAP services has been extended to support all the parameters detailed in MAP Release 8 as detailed in 3GPP TS 29.002 v8.18.0:

MAP-UPDATE-GPRS-LOCATION
MAP-CANCEL-LOCATION
MAP-PURGE-MS

2.5 SIU Based DTS Route Configuration

Prior to this release, applications on each DTS host were required to send DTS routing requests to DTS when it detected startup or restart of the SIU. This release optionally allows the DTS routing requests to be configured on the SIU removing the burden from the host application.

To support configuration of DTS Routes a new config.txt configuration command is supported, DTS_ROUTE. The syntax of this command is:

DTS_ROUTE:[NC=NC0],DRID=,HOSTID=[,SSN=][,CLSEQ=0][,OPTIONS=0][,LABEL=];

The current configuration can be displayed using the new MMI command CNDRP which has the following syntax:

CNDRP:[DRID=,][NC=,][HOSTID=,];

A new MMI command, MSDHP, has been introduced to report per DTS host measurements. The syntax of this command is:

MSDHP:[RESET=];

2.6 DTS - Route on IS41 Billing ID

This release adds the ability to route message to DTS hosts based upon the IS41 BillingID parameter. This enables multiple dialogs that form part of the same call to be routed to the same SIU host.

When enabled, IS41 messages will be routed by Billing ID provided that the message is a TC-Query and the component part contains an INVOKE with a TCAP private operation of ORREQ, ANLYZD, CCDIR, OANSWER, ODISCONNECT, TANSWER or TDISCONNECT.

Messages that do not match these criteria are routed according to the existing DTS rules. Once the host has been selected, subsequent messages forming part of the same dialog will be sent to the same host by the existing DTS method of using the transaction id.

The feature is enabled by setting bit 0 in the DTS_CONFIG <options> within config.txt. The command syntax is:

DTS_CONFIG <num_hosts> <options>

2.7 Message Router - Destination Selection

When acting as a message router the existing routing key HUNT=BALANCE has been extended to permit routing to destinations in the NETWORK domain. When using HUNT=BALANCE the CIC range should be specified, by default the Base CIC is 0 and the CIC range is 4096. To include more than 4096 CICs (eg for BICC), it is necessary to use multiple routing keys.

A new HUNT type of SHARE1 has been introduced. When HUNT=SHARE1, destination rows in the destination table will be load shared based on the SLS value in the message.

2.8 Dynamic GTT Configuration

This release provides the ability to dynamically add and remove Global Titles without impact to other components in the system.

In the same manner as other dynamic configuration commands, new GTT addresses are loaded from an updated config.txt file using the CNGAI MMI command, GTT patterns are loaded using the CNGPI MMI command and the GTT itself is loaded and applied using the CNGTI MMI command. GTTs can also be removed by first deleting them from the config.txt file and unloading them from the system by executing a CNGTE to remove the translation followed by CNGPE to remove the pattern and CNGAE to remove an address.

3 Other Changes

3.1 IPEPS Command - Subnet Mask (IPY00102639)

This release includes validation of the SUBNET parameter to ensure that only bit masks with contiguous bits may be specified. Previously invalid entries were accepted but failed to operate correctly.

3.2 MNSSI Command - Snapshot Creation

Operation of the MNSSI command which creates a diagnostic snapshot of the server has been enhanced to capture additional information relating to the file system and the base server.

3.3 MSCLP Command (IPY00102686)

This release corrects a problem that previously resulted in failure to display M3UA license measurements when both MTP3 and M3UA are operating in the same network context.

3.4 STDHP Command –Format Enhanced

The format of the STDHP MMI command has been enhanced. The command has a new single page format and includes the DRID (DTS Routing Request ID) parameter for SIU configured Routing requests. The output shows how messages for a particular LSS (NC and SSN) will be routed based on existing routing requests and the hosts to which routing will be performed, based on the currently active hosts.

3.5 STSLP Command – MTP2 Status

This release corrects the MTP2 status displayed for SS7MD boards following link deactivation. Previously it reported 'Initial Alignment' rather than 'Out Of Service'.

3.6 Message Router – Dual Operation

This release corrects a configuration issue which could be encountered when operating in dual mode if a Remote Application Server has the same DPC as the local point code of the SS7G41.

3.7 Message Router - Point Code Status (IPY00102788)

This release corrects an initialization issue that previously resulted in Message Router Concerned Entities receiving indications that Destination Point Codes (DPC) were active when in fact they were not active. The issue corrected itself as soon as the DPC became active for the first time.

3.8 Message Router – SCCP Routing

In the event that an Application Server is inaccessible from the local SIU instead of discarding the message SCCP will now pass the message to SCCP on the partner unit to allow it to attempt to route the message.

3.9 ISUP – Clearing Cause on Reset (IPY00102727)

This release modifies ISUP behaviour so that on reception of a circuit reset or group circuit reset from the network ISUP will now use clearing cause value 41 (temporary failure) in the release indication to the user (rather than 31 (normal unspecified) as previously used).

3.10 BICC – Auto-Blocking (IPY00102728)

This release corrects operation of the BICC protocol so that ISUP correctly re-asserts blocking following receipt of a single circuit reset from the network on a locally blocked circuit by issuing a CGB message. Previously blocking was not re-asserted in this case.

3.11 MAP - Multiple Network Contexts (IPY00102722)

This release corrects a fault when operating with Network Contexts other than NC=0 when a MAP user sends MAP-OPEN-REQ followed by a MAP-DELIMITER-REQ message without any Service Requests (MAP_MSG_SRV_REQ)).

3.12 MAP - Formatting of Abort sent to TCAP

This release correctly formats the UABORT send from MAP to TCAP upon receipt of an invalid or unknown DialogID in a message from TCAP.

3.13 MAP – Discarded 'NotLast' Components

This release corrects an issue that previously could cause parameters received in a 'NotLast' Result response message from TCAP to be discarded. This fault only occurred when the response was received in two or more parts and parameter data was decoded for a 'NotLast' component and no parameter data was decoded for the 'Last' component.

3.14 M3UA - Network Appearance

This release introduces the option to ignore the M3UA Network appearance (NA) in received messages. This option is configured by setting bit 5 of the STN_LINK options.

3.15 M3UA - Auditing of Congested Destinations

Previously when connecting to a Signaling Gateway, enabling the Destination Audit (DAUD) option enables auditing of both unavailable and congested destinations. This behavior has been modified so that congested destinations are only audited in ANSI Network Contexts.

3.16 M3UA - Network Context Configuration

The STN_NC command requires that the <share> parameter be set when multiple Network contexts are specified to ensure that the throughput is correctly shared between different Network Contexts. Prior to this release this rule was not fully enforced and it was possible to configure M3UA network contexts without a share parameter that resulted in an incorrect distribution of the License between the Network Contexts. This has been corrected to ensure that <share> must always be set on the STN_NC command.

3.17 DTS Client and Routing Request Logging

The Signaling Server will now report DTS_ROUTING_REQ and DTS_CLIENT_REQ messages to the management host and maintenance log file.

3.18 Memory and File Sys Warning Alarms

The alarms "Memory failure" and "File sys err" have been renamed "Memory warning" and "File sys warning" to reflect the less critical nature of the condition. In the event that either of these warnings are indicated the user should invoke a full system restart at the next suitable maintenance window using the command MNRSI:RESTART=HARD;

3.19 SNMP – Memory Warning

SNMP operation has been modified such that if a memory warning alarm is detected during startup an SNMP trap will be sent to the SNMP manager.

3.20 IP Firewall Configuration

This release corrects an issue which previously could result in loss of IP firewall configuration following a restart.

Dialogic
11-Sep-13
Revised 27-Feb-15

Release 1.2.10

1 Overview

This is a maintenance release containing a number of changes and corrections as detailed below.

It corrects an important issue relating to M3UA route availability (see 3.8 below) which was introduced in Release 1.2.0. Consequently any users of Release 1.2.0 and later are advised to upgrade to this release.

The release also introduces the ability to configure the TCAP idle dialogue timeout from within config.txt.

This is the first Generally Available release since 1.2.5 and it is fully backwards compatible with that release.

1.1 Applicability

This release is suitable for all users.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00102249, IPY00102349 and IPY00102543.

2 New Functionality

2.1 TCAP Idle Dialogue Timeout

This release allows the timeout value for the TCAP Idle Dialogue Timeout to be configured in the config.txt file using a new TCAP_TIMER command which has the following syntax where the <reserved> field should be set to zero and the <value> is the timeout value in seconds.

TCAP_TIMER <reserved> TDLG_IDLE_TOUT <value>

3 Other Changes

3.1 CNCGP Command - Extended options

This release corrects the extended options field (the most significant 16 bits of the 32 bit OPTIONS parameter) in the Circuit Group configuration display. Previously this was not displayed for inactive circuit groups.

3.2 MNSSI Command – Additional Diagnostics

This release enhances operation of the diagnostic snapshot creation command MNSSI in order to provide additional system parameters relating to hard drive and Ethernet port status.

3.3 MRRKP Command - Routing Key Print

This release corrects the value displayed for Custom Profile (CP) in the Message Router Routing Key configuration.

3.4 STSTP Command - SIGTRAN Status

This release improves operation of the STSTP when PAGE=2 to ensure appropriate reporting of path status for associations that are not in the active state.

3.5 SS7MD – Increased buffer allocation

This release increases internal buffer resources for the SS7MD board to prevent failure of SS7 links when operating with high throughput applications with high numbers of SS7 links.

3.6 ISUP - OPC Validation

The release removes the ISUP Circuit Group configuration requirement that the OPC must have already been used as a local point code for an SS7 link set or SIGTRAN Local Application Server.

3.7 TCAP – Dialog Idle Timer

This release corrects a fault with the TCAP Dialogue Idle Timeout which previously resulted in timeouts greater than 6,553 seconds expiring early.

3.8 M3UA – Route availability (IPY00102249)

This release corrects a problem (introduced in Release 1.2.0) that results in M3UA sometimes failing to detect remote point code availability when a route becomes available. The fault occurs when a DAVA from the network is preceded by a SCON message indicating a congestion status of zero. As a result SCCP and Message Router deployments might have failed to detect point code recovery.

3.9 config.txt - STN_LINK Local IP Address

The release adds a validation check for the STN_LINK command to prevent attempts to configure a local IP address which has not previously been configured as a system IP address.

3.10 config.txt - MRCEI Command

This release improved the error reporting in the event that the configured ALIAS already exists. The error code ‘already used’ will be displayed.

3.11 config.txt - STN_ROUTE for Message Router

This release provides a correction to Message Router Functionality in cases where the NETWORK domain contains destinations that are accessible via routes define using the STN_ROUTE command. This ensures that messages from the AS domain can correctly be routed to the NETWORK domain.

3.12 Message Router - Tracing

This release adds support for tracing messages received from an Application Server and for messages sent from the Message Router to a User Part. Previously tracing of these events was either not supported or not supported in PCAP format.

3.13 Message Router – Concerned Entity (IPY00102349)

This release corrects an issue encountered at startup when using Message Router Functionality in conjunction with a local User Part (e.g. SCCP) as a Concerned Entity whereby initial availability of the destination is not notified to the User Part.

3.14 Maintenance Logs

Additional events generated from MTP3, TCAP, M2PA and SCTP are now logged and or decoded in the maintenance log and sent to the management host. These messages include the following: MTP_MSG_LINK_CONG, TCPEV_DLG_TIM_TIMEOUT, TCPEV_EXCESSIVE_DLG_ABORTS, M2P_MSG_EVENT_IND and SCTP_MSG_EVENT_IND.

3.15 Timestamps following restart

This release ensures that when using Network Time Protocol (NTP) the timestamp maintained by the built-in hardware clock is updated to the NTP time. This ensures that any timestamps in the diagnostic 'messages' file generated immediately following a restart (which would be derived from the hardware clock) are correct.

3.16 NTP Operation (IPY00102543)

The release corrects an issue which resulted in a spontaneous unit restart when NTP was active but had failed to achieve NTP synchronization as a result of the time difference between the two servers exceeding a set threshold (1000 seconds). The restart would occur after approximately 9 hours of operation.

Now if unable to obtain synchronization, the unit will show the NTP status as inactive and will stop attempting to synchronize. To recover from this condition the user should manually reactivate NTP.

Dialogic
31-May-13

Release 1.2.5

1 Overview

This is a maintenance release which contains a critical change to allow SS7G41 units fitted with latest versions of the SS7LD board to function correctly. Previous software releases will not operate correctly with the latest revisions of the SS7LD board.

The release also includes a correction relating to throughput licensing when acting as a SIGTRAN gateway and a correction to the validation checks when configuring MTP linksets.

This is the first release since 1.2.3 and it is fully backwards compatible with that release.

1.1 Applicability

This release is applicable to all users. It is essential for correct operation of any SS7G41 units containing SS7LD boards with **serial number RC920000** or later. The serial number of the board can be read using the STBOP MMI command.

2 Changes

2.1 SS7LD Boards from Serial Number RC920000

Due to a new hardware device on later revisions of the SS7LD signaling board, any SS7G41 units fitted with SS7LD boards with Serial Number RC920000 and greater will not operate correctly with software prior to this release.

When fitting new SS7LD boards in the field, users should seek to upgrade to this software release prior to fitting the new board.

Prior to downgrading to an earlier software release in the field, users should use the STBOP command to confirm that the unit does not contain any SS7LD boards with a Serial Number of RC920000 or greater.

The impact of using an incompatible software release is that the SS7 signaling links will fail to come into service.

2.2 M3UA Licensing

This release corrects the usage of the SIU and SWS licenses to ensure the correct allocation of license capability for M3UA when the Signaling Server is acting as a Signaling Gateway towards a M3UA application server.

2.3 Multiple Network Contexts

This release corrects an important issue affecting users of multiple network contexts in dual operation which previously in some cases prevented configuration of multiple Originating Point Codes (OPC). The issue occurred only when NC0 is in use and prevented configuration of other Network Contexts.

Dialogic
07-Mar-13

Release 1.2.3

1 Overview

This release is a feature release which includes two significant new features: Sigtran Gateway Capability and Message Router Functionality. Together these combine to offer flexible extensions to existing SIU functionality and allow the SS7G41 to be used in an autonomous mode without necessarily requiring an SIU host or user application.

The release also increases the number of M3UA routes supported to 4096 and includes other changes and corrections as detailed below.

This is the first Generally Available release since Release 1.1.1, it is fully backwards compatible with that release.

1.1 Applicability

This release is applicable for all users.

The following additional User Documentation describes in detail the new Sigtran Gateway Capability and Message Router Functionality:

Dialogic® DSI SS7G41 Signaling Server – Introduction to Message Router Functionality (GA017LGD).

2 New Functionality

2.1 Sigtran Gateway Capability

This release adds the ability for the Signaling Server to operate as an M3UA Sigtran Gateway. The SS7G41 adds support for the Sigtran Nodal Inter-working Function (NIF) allowing it to appear as a Signaling Gateway and connect using M3UA to Application Servers. Operating as a Sigtran Gateway the SS7G41 can then provide connectivity to TDM networks or to downstream nodes using Sigtran M3UA or M2PA.

When operating as a Sigtran Gateway the SS7G41 can be used as a replacement for SS7G2x and SS7G3x Signaling Servers operating in SGW mode. Users should note that there are differences in the way in which the products are configured (the SS7G41 uses a text based configuration file (config.txt) for all protocol configuration commands whereas the SS7G2x/SS7G3x products in SGW mode previously used interactive configuration commands) but the same underlying functionality is available. In addition there are new capabilities offered by the Message Routing Functionality which allow the user to route messages based on parameters in the MTP routing label.

2.2 Message Router Functionality

This release includes new Message Routing Functionality. The Message Router provides the ability to flexibly route messages between the Network Domain (MTP or M3UA), User Parts and Sigtran Application Servers using M3UA. The routing is based on the MTP routing label and allows messages from a specific Origin to use individual Routing Keys to selectively match routing label parameters and determine which Destination to be sent towards. The Message Router can be configured to act as a Sigtran Signaling Gateway or simple Signaling transfer Point (STP). The Signaling server can also behave as an SCCP Router by configuring the Message Router to send traffic through the local SCCP for Global Title Translation.

In addition to routing messages, the Message Router allows for the maintenance and mapping of point code status across the Signaling Server. The Message Router is able to respond to Signaling Route Set Test and Sigtran Destination Audit messages and generate the appropriate Route Status messages (eg Transfer Allowed/Transfer Prohibited and Sigtran Destination Available/Unavailable) to adjacent for Point Codes. To preserve operating flexibility, the user must explicitly configure the identity of nodes that are concerned about the status of other nodes within the network. This is achieved using the concept of Concerned Entities.

Measurements of traffic passing through each state of the Message Router are automatically captured and accessible to the user. Message tracing can optionally be enabled for diagnostic purposes to log to rotating file all messages as they pass through the Message Router. In addition any messages that are unable to be routed (either due to an inaccessible destination or invalid routing configuration) are automatically logged as selective traces to the trace log.

2.3 Deactivating Network Links on Loss of all Hosts

Normal SIU operation in the event that all host links have failed is to deactivate any network facing links. This release extends the functionality by allowing SIGTRAN M3UA links to be nominated on a link by link basis to be considered as a 'host' link.

M3UA links can be nominated as 'host' links by setting bit 15 in the <options> field of the STN_LINK command. If any SIGTRAN links have been configured as 'host' M3UA links and all these links are down then all MTP and any non 'host' M3UA links will be deactivated until at least one 'host' M3UA link returns to service.

2.4 M3UA – Support for 4096 Routes

This release increases the maximum number of M3UA routes from 256 to 4096.

3 Other Changes

3.1 MNSSI command

The MNSSI takes a snapshot of key system data, storing it in a single file (syslog.tgz) in the root directory of the ftpuser account. This release adds the ability to include trace files in the snapshot file which is achieved by setting the parameter TRACE=Y when executing the MNSSI command.

3.2 CNHSS command - Tracing to Management Host

This release corrects the operation of the CNHSS command when used to change the default management host (DMHOST) to ensure that any message tracing will change immediately to the new DMHOST rather than waiting until the next restart.

3.3 STCGP command – Circuit Group Status

This release corrects an anomaly with the STCGP command when displaying the status of ISUP circuit groups that previously caused circuits in Wait for ACM or Wait for RLC states to be considered in maintenance.

3.4 STN_LINK command - M3UA Network Appearance

To assist detection of incorrect configuration data, in the event that an STN_LINK command sets NA to a non-zero value but does not set the option bit 3 to indicate that NA is in use, the command will now be rejected.

3.5 Event Logging

The following maintenance events are now logged to the maintenance log and to the management host: MTP2 events (MGT_MSG_SS7_EVENT), M3UA errors (M3U_MSG_M3U_ERROR) and M3UA events (M3U_MSG_M3U_EVENT).

3.6 ISUP – Measurements

The SS7G41 maintains a number of ISUP Circuit Group measurements accessible using the MSCGP command. These measurements include a count of the number of calls answered and a measure of accumulated call duration from the point of answer. By default the point of a call being 'answered' is determined by generation or reception of either an Answer message or a Connect message.

This release introduces a new run-time configuration option (bit 15 of the <options> field in the ISUP_CONFIG command) which modifies the behavior of the measurements so that the point at which the call is 'answered' is deemed to be upon generation or reception of the Address Complete message. This is more useful for certain types of application which use the time between Address Complete and Answer to play tones or announcements.

3.7 ISUP – IAM after RESET

This release includes a change to ensure correct operation when a locally originated circuit group reset is immediately followed by an outgoing IAM (before the Group Reset Acknowledgement is received). Previously it was possible that the circuit required a second circuit group reset request to recover from this unusual event.

3.8 M3UA – Trace for received Transfer Requests

A new M3UA trace event (bit 16) has been added to the input mask for M3UA to enable receipt of outgoing Transfer Requests from user parts to be traced.

3.9 M3UA – 8-bit SLS values with 5-bit rotation

This release corrects the operation of SLS rotation to ensure that when operating with 8-bit SLS values and 5-bit SLS rotation the most significant bits of the SLS are preserved rather than being set to zero.

3.10 DTS – Support for 1024 Client Routing Requests

This release increases the maximum number of permitted DTS Routing Requests from 256 to 1024 to allow for clients that use multiple routing requests. The total number of DTS Routing Requests received by DTS must not exceed 1024. Each DTS client/SSN/NC combination uses one DTS Routing Request.

Dialogic
02-Nov-12
30-Nov-12 (Revised)

Release 1.1.1

1 Overview

This release is a feature release which enhances SCCP support and allows SS7LD boards to be used in 'drop and insert' mode. It also includes changes and corrections as detailed below.

SCCP Global Title Load Share Tables provide the ability for a Global Title Translation to result in a list of Destination Point Codes to increase system resilience in the event of a DPC failure.

'Drop and Insert' functionality allows a combined media and signaling E1/T1 to be terminated on the SS7G41 with the signaling processed by the SS7G41 and the media passed on through another E1/T1 interface to the media processor.

This release is fully backwards compatible with the previous release.

1.1 Applicability

This release is applicable for users who require the newly introduced capabilities or corrections.

1.2 Resolved Customer Issues

The following customer issue has been resolved in this release: IPY00100565.

2 New Functionality

2.1 Global Title Load Share Tables

Global Title Load Share Tables support the distribution of messages for a configured Global Title translation rule across a number of Destination point codes. A load share table holds a number of Point Codes across which messages will be distributed.

A new configuration command**, SCCP_LOAD_SHARE_TABLE,** allow users to establish a Load Share Table and select run-time options.

A second command, **SCCP_LOAD_SHARE_DPC** should be used to associate a destination point code with the Load Share Table. The command should be used multiple times, each time adding a single point code to the Load Share Table.

A Load share table can be associated with a GTT by configuring it as the point code in the **SCCP_GTT_ADDRESS** command.

A new command, **CNLTP**, displays current Load Share Tables and the command **CNLDP**, shows the assignment of Destination Point Codes to a Load Share Table.

The command syntax is specified in the *SS7G41 Operator's Manual*.

2.2 Drop and Insert

'Drop and Insert' functionality allows a combined media and signaling E1/T1 to be terminated on the SS7G41 with the signaling processed by the SS7G41 and the media passed on through another E1/T1 interface to the media processor.

To support 'Drop and Insert' a new configuration command**, STREAM_XCON**, has been introduced to control the cross connect switch on the signaling boards, enabling the cross- connection of timeslots between the two PCM ports on each signaling.

The command syntax is specified in the *SS7G41 Operator's Manual*.

3 Other Changes

3.1 NTP Initialization

This release enhances the NTP startup sequence to more quickly adjust to the current time.

3.2 SS7MD Monitoring Timestamps

When monitoring with timestamps is configured for SS7MD the output produced includes a timestamp indicating the real time that the message was received. This release adds a new per-board option to ensure that timestamps are always later than the previous reported timestamp. In situations where for whatever reason time is adjusted backwards the timestamps will increase at the minimal amount until the current time is again greater than the previous reported timestamp.

To select this option bit 19 of <options> parameter in the SS7_BOARD command should be set to 1.

3.3 ISUP – BICC Timer Configuration (IPY00100565)

Previously when a BICC variant circuit group was configured, ISUP incorrectly overwrote any user-configured timer values in the associated timer table. This has been corrected so that user-configured timer values are preserved.

3.4 ISUP - Circuit group supervision message type handling

On receipt of a Circuit Group (Un)Blocking message or acknowledgement containing a invalid 'Circuit Group Supervision Message Type Indicator' field, ISUP will now generate a Confusion Message with 'cause' set to 110.

3.5 SCCP – Generating UDTS or SST response using RSP pc_mask

This release corrects operation when generating UDTS or an SST response towards a point code where the configured RSP (Remote Signaling Point) is identified by a pc_mask (rather than an explicit match of the point code. This ensures that the National Indicator is appropriately set from the configured RSP data.

Dialogic
25-Jun-12
17-Jun-14 (Revised)

Release 1.1.0

1 Overview

This release is a feature release which enhances the MMI capability and adds additional MAP services. It is the first release since 1.0.5.

The release supports up to four Telnet MMI sessions and up to eight browser based MMI sessions. It adds additional parameters to control the format of MMI output.

The release also adds the ability to configure multiple M3UA originating point codes (OPC) in each network context which is useful in some applications.

This release is fully backwards compatible with the previous release.

1.1 Applicability

This release is applicable to all users.

2 New Functionality

2.1 Browser based MMI

This release allows up to eight independent browser based MMI sessions.

The browser based MMI now supports equivalents to the existing MMI commands STTDP, STIPP and STDEP. To identify how to access browser commands, the '?' query can be used on the Telnet command line interface to produce help output for an MMI command. This help output will now also identify the associated browser page where the equivalent function can be accessed. In addition the browser interface identifies the command line MML command/parameter that performs the equivalent function.

2.2 Telnet MMI.

Prior to this release the signaling server allowed telnet access on two ports, 8100 and 8101.This release extends telnet access so that users can telnet into two further ports 8102 and 8103.

The CNSYx command supports a new parameter, LINES, which specifies the number of lines that will be displayed before prompting a user to "Press return to continue or Ctrl-X to cancel". When LINES is set to 0 this paging mechanism is disabled.

The CNSYx command supports a new parameter, TLO, to change the inactivity period (in minutes) before a Telnet MMI session automatically logs out. By default this timeout period is 30 minutes.

A new MMI command, STUAP, has been introduced which displays which users are currently logged on.

The per-port MMPTx commands are no longer available.

2.3 MAP - NotifySubscriberDataModified service

Support for the MAP NotifySubscriberDataModified service has been added in accordance with the MAP specification 3GPP TS 29 002 version 10.3.0 (Release 10). The service is MAP-V3 only as defined in the specification.

2.4 MAP - ProvideSubscriberLocation service

Support for the MAP ProvideSubscriberLocation service has been extended to include additional parameters. The implementation is now compatible with the MAP specification 3GPP TS 29 002 version 10.3.0 (Release 10).

2.5 MAP - 'Additional Roaming Not Allowed Cause'

New MAP V3 services error parameters have been added in support of the ProvideSubscriberLocation service. Additionally the new error parameter 'Additional Roaming Not Allowed Cause' is now supported. These new error parameters are enabled for use by all MAP-V3 services supported by the MAP implementation that use the applicable error codes.

2.6 M3UA - Multiple Local Point Codes

Configuration of Local Application Servers has been enhanced to allow Local Application Servers to be configured within the same Network Context with differing Originating Point Codes. M3UA will also support multiple local point codes which operating in dual resilient mode while partnered with another Signaling Server.

SCCP continues to support a single local point code per Network Context.

3 Other Changes

3.1 STTDP command - TCAP Dialog Status

The STTDP command now omits any dialogues that are in the IDLE state resulting in a more compact display.

3.2 CNPCP command - PCM Status – Board Position

This release corrects the board position displayed by the CNPCP command (which previously was one greater than it should have been).

3.3 MTP2 - HSL Links

This release corrects an issue which previously could result in restricted HSL link throughput when operating over high latency links.

3.4 ISUP - 8 Bit SLS Rotation

This release corrects generation of 8 bit SLS values when using bit 22 of the <options2> field for Circuit Group Configuration.

3.5 MAP - Ellipsis parameter in Dialog messages

When the MAP user specifies MAPPN_dest_ref and MAPPN_orig_ref parameters together with MAP-V1 application context parameter in a MAP-OPEN-REQ message, the MAP module automatically sends a Begin Subscriber Activity (BSA) component to TCAP. Previously if the user also included the MAPPN_ellipsis parameter in the message the MAP binary could terminate. This issue has been corrected.

Dialogic
30-May-12

Release 1.0.5

1 Overview

This is a maintenance release which includes several important corrections as detailed below. All users are advised to upgrade to this release which is the first generally available release since 1.0.2.

This release is fully backwards compatible with the previous release.

1.1 Applicability

All users are advised to upgrade to this release.

Additionally SNMP users are advised to upgrade to SNMP MIB package V2.02 or later.

The following user documentation updates are available for use in conjunction with this release:
Dialogic® DSI Signaling Servers – SS7G41 Hardware Manual, Issue 2,
Dialogic® DSI Signaling Servers – SS7G41 Operators Manual, Issue 3,
Dialogic® DSI Signaling Servers – SS7G41 SIU Developers Manual, Issue 3,
Dialogic® DSI Signaling Servers – SNMP User Manual, Issue 3.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00099654 and IPY00099685.

2 New Functionality

2.1 Message Based Link Set Selection

This release provides the ability to select (on a message by message basis) which outgoing link set is used for MTP-TRANSFER-REQ messages. This is different to normal MTP3 operation where selection of an outgoing route is based on the Destination Point Code (DPC) contained within the message. This functionality is targeted at a specific customer requirement. Further details are available on request.

3 Other Changes

3.1 Ethernet Port Bonding (IPY00099654)

This release corrects an issue which arose when using Ethernet port bonding to bond Ethernet port 1 with Ethernet port 0. Under these conditions if the unit was restarted it would revert to a condition where it needed to be manually reconfigured into SIU mode.

The release also simplifies the status for bonded Ethernet ports by the STEPP MMI command. Instead of reporting ACTIVE/STANDBY/DOWN the status is now either UP or DOWN.

3.2 Serial Number Display

The CNSYP MMI command has been enhanced to display the serial number of the unit using the UNIT_SERIAL parameter.

3.3 Disk Drive Control

This releases corrects operation of the internal Hard disk Controller to ensure reliable support for hot swapping of hard drives. In such cases it is essential to follow the disk replacement procedures described in the operators manual.

3.4 License Sharing

This release corrects the usage of the TDMSHARE parameter on the CNSYS MMI command so that when multiple throughput-based protocols are used, the allocation of license capability for M2PA and M3UA is correctly allocated between the protocols based on the user command.

3.5 Diagnostic Snapshot

The MNSSI command takes a snapshot of key system data, storing it in the syslog/snapshot subdirectory of ftpuser account. This release causes all snapshot data (excluding trace and binary files) to be written to a single file (syslog.zip) root directory of the ftpuser account.

3.6 SNMP Licensed Capability

The Licensed Capabilities reported over SNMP have been corrected. Users are advised to update the SNMP MIB to V2.02 or later which includes revised descriptions of the Licensed Capabilities values.

3.7 Startup Sequence

A problem during the boot sequence which could cause the system to hang waiting for user input has been corrected.

This release corrects a problem that could occasionally prevent units containing SS7LD boards from starting up correctly.

3.8 Alarms and Event Reports

A new alarm, "No active host", has been introduced to indicate communication with all configured SIU hosts has failed.

A new alarm, "CMOS Bat Low", has been added to indicate event that the CMOS back-up battery back-up has become discharged.

A new alarm, "File sys err" has been added in the case that a file system check (at startup) detects possible errors. In the event that this alarm occurs users should restart their system to attempt auto correction.

From startup M2PA links are now shown as failed until they come in service.

MTP2, M2PA and M3UA links no longer generate alarms when they have been manually deactivated.

License events from M2PA and M3UA, including license throughput congestion, will be reported to the management host and maintenance log using the MGT_MSG_LIC_EVENT message.

3.9 STCRP - SS7 Route Status

The SS7 Route status MMI command STCRP has been enhanced to allow a user to request the status of an individual route by specifying the optional C7RT parameter on the command.

3.10 MSLCP & STLCP Resource Leakage

This release corrects a resource leakage issue encountered using the MSLCP and STLCP commands where an internal message was not released. If the commands were executed a large number of times this could result in internal congestion and ultimately a system restart.

3.11 Per-Network Context Default Route

Previously only one default MTP or M3UA route could be specified on a Signaling Server. This has been changed so one default route (MTP or M3UA) can be specified per Network Context.

3.12 SS7MD – Sync Alarm (IPY00099685)

This release corrects an issue with the PCM Sync alarm when using CRC4 Multiframe Operation on the SS7MD board which previously resulted in failure for the alarm to clear despite the PCM signal being valid.

3.13 PCM – Bit Errors and Code Violations

Two additional PCM Measurements are now reported; BITERR is the count of bit errors detected by the framer and CV is the count of line code violations.

3.14 INAP_FE command

The INAP_FE command now supports the configuration of functional entities for both local and remote subsystems.

3.15 ISUP - German National Variant

This release corrects the coding of three optional German ISUP parameters used in the Initial Address Message (IAM). Previously the NP.FF was defined with wrong length and the NP.SSP and NP.UKK parameters were assigned the wrong parameter value.

3.16 SCCP – Disable UDTS Generation

An option has been introduced to allow automatic generation of UDTS messages by SCCP to be disabled. Further details are available on request.

3.17 M2PA - Dynamic Configuration

Previously issues existed where a user was unable to deactivate an SS7 M2PA link, dynamically add a TDM with the same blink as an existing M2PA link (which identifies the SIGTRAN link id for M2PA) as well as not being able to re-add a previously removed SS7 M2PA link. These have been corrected.

3.18 M3UA – Default Trace Mask

To improve usability the MMI command CNTMS has been modified to offer default values for the input and output trace masks that allow tracing RX_IND and TX_REQ messages without needing to explicitly set the trace masks.

Dialogic
27-Apr-12

Release 1.0.2

1 Introduction

This is the first full release of SIU Mode software for the Dialogic® DSI SS7G41 Signaling Server. The SS7G41 is a functional replacement for the existing SS7G31 and SS7G32 signaling servers. It delivers high density (up to 248 Low Speed Links or 8 High Speed Links) in a low profile 1U form factor and supports one or two signaling boards that are either high or low density.

In addition to being a functional replacement for the SS7G3x products, the SS7G41 delivers a number of enhancements including a browser based management interface, enhanced security, individual user accounts, and a simplified license model.

The SS7G41 support SIU (Signaling Interface Unit) and SWS (Signaling Web Server) operating modes. The full documentation set for the product range which comprises:

- Dialogic® DSI SS7G41 Hardware Manual.
- Dialogic® DSI SS7G41 Operators Manual.
- Dialogic® DSI SS7G41 SIU Developers Manual.
- Dialogic® DSI SS7G41 SWS Developers Manual.
- Dialogic® DSI SS7G41 SIU Migration Guide.

Users of the SS7G3x product range should refer to the SS7G41 SIU Migration Guide which highlights some of the key differences between the two products and will assist users migrating from those Servers.

NOTICE

This Release should NOT be loaded onto pre-production SS7G41 units (as used for the field trial). Pre-production units are identified by a Serial Number of the format S/N LGD00xxx.

Users of Pre-production units should contact their Dialogic Support centre for further instructions

Dialogic
21-Oct-11