Dialogic® DSI Signaling Server SS7G3x SIU Mode Release Notes

Document Reference: RN001LFD
Publication Date: November 2012

Contents

Release 2.3.13

1 Overview

This release is a maintenance update which provides minor changes and corrections to existing operation.

This is the first Generally Available release since Release 2.3.10. It is fully backwards compatible with that release.

The changes and corrections are detailed below.

1.1 Applicability

This release is suitable for all users.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00100632, IPY00100906 and IPY00101319.

2 Changes

2.1 M3UA – STN_RSGLIST (IPY00100906)

Prior to this release the maximum number of entries for the STN_RSGLIST configuration command was 256. This has been increased to 512 allowing the Signaling Server to be configured with up to 256 SIGTRAN routes that are each able to route using 2 adjacent Signaling Gateways. The ability to dynamically add and remove entries is also supported.

2.2 SCCP – Generating UDTS or SST response using RSP pc_mask (IPY00100632).

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

2.3 ISUP – BICC Timer Configuration

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.

2.4 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.

2.5 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.

2.6 DTS – Support for 1024 Client Routing Requests (IPY00101319)

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
15-Oct-12
Revised 21-Nov-12

Release 2.3.10

1 Overview

This release enhanced MAP support by adding the MAP V3 service NotifySubscriberDataModified and additional parameters in the ProvideSubscriberLocation service. It also increases the number of Telnet MMI sessions from 2 to 4 and provides the ability to configure or disable the number of lines per page.

This release also includes updates and corrections as detailed below.

This release is fully backwards compatible with the previous release.

1.1 Applicability

This release is suitable for all users.

Dialogic® DSI Protocol Stacks MAP Programmer's Manual Issue 17 provides details of parameter coding for the new MAP services supported by this release.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00099749, IPY00100000 and IPY0010006.

2 New Functionality

2.1 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.

A new parameter, LINES, is now supported on the CNSYx MMI command. This parameter specifies the number of lines that Telnet MMI will display 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.

A new parameter, TLO, on the CNSYx MMI command allows a user to change the inactivity period before a Telnet MMI session automatically logs out. By default this timeout period is 30 minutes.

2.2 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.

2.3 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).

2.4 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.

3 Other Changes

3.1 MSLCP & STLCP Resource Leakage (IPY00099749 and IPY00100000)

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.

3.2 Per Network Context Default Route (IPY00100066)

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

3.3 System Snapshot

A new MMI command, MNSSI, has been introduced to take a snapshot of key system data, storing it in the syslog/snapshot.log file of siuftp account. Upon executing the command the signaling server will also combine all diagnostic data from the syslog subdirectory(excluding trace and binary files) and write them to a single file (syslog.zip) in root directory of the siuftp account. The creation of the syslog.zip is done as a background task so users should wait a few seconds to allow the task to complete before transferring the file of the system.

3.4 Diagnostic Traces

A defect was introduced in Release 2.2.1 where traced protocol messages no longer contained the internal system tick timestamp field associated with the message. This has been corrected. The event time stamp field, identified by a leading 'E' character, will now contain the system tick time the event occurred.

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
27-Apr-12
Revised 15-Aug-12

Release 2.3.9

1 Overview

This is the first generally available release since Release 2.2.2; it includes several new features and number of changes and corrections as detailed below.

This release provides for dynamic configuration of SIGTRAN protocols and adds support for multiple M3UA Network contexts allowing up to four local point codes. It also adds the ability to configure timer values for Sigtran M3UA, M2PA and SCTP protocol timers. It adds Default Routing for M3UA.

The release introduces the ability add a text label to identify each MTP route, link and link set and adds support for dual resilient SCCP-CO operation.

This release also includes several protocol updates and corrections to operation of the SIGTRAN protocols and the TCAP and MAP protocols.

This release is fully backwards compatible with the previous release.

1.1 Applicability

This release is suitable for all users.

It is essential for any users needing to dynamically end MTP Routes.

1.2 Resolved Customer Issues

The following customer issues are resolved in this release: IPY00092979, IPY00092981, IPY00093007, IPY00093621, IPY00094137, IPY00094372, IPY00097713, IPY00099008, IPY00099078, IPY00099105, IPY00099287.

2 New Functionality

2.1 MTP - Configuration Labels

The MTP configuration commands (MTP_LINKSET, MTP_ROUTE and MTP_LINK) now support an optional label parameter to simplify recognition of the entity when using the associated MMI commands CNLSP, CNCRP and CRSLP. The label is also returned in an SMNP query and reported in SNMP traps.

The label, which may contain up to 15 characters, is added by appending an additional parameter to the end of the command and prefixing it with the '$' character as follows.

```
MTP_ROUTE  1  2045  0  0x0008  0x0000  0  0  $Mumbai
```

2.2 SCCP-CL - Receiving Messages for any DPC

This release adds the ability for local sub-systems to receive Connectionless SCCP messages irrespective of the DPC contained within the message. This is achieved by a run-time configuration option associated with the Local Sub-System (LSS) which allows received messages for any DPC not explicitly configured to be sent to that LSS.

This functionality is enabled when configuring a LSS by setting bit 4 in the <lss_flags> field of the SCCP_SSR command.

2.3 SCCP-CO - Dual Resilient Operation

This release adds the ability, when operating in Connection Oriented mode, for the two SCCP instances within a dual resilient pair to co-operate to ensure that messages received from the network arrive at the correct SCCP instance.

This feature is automatically activated by the SIU when in a dual-resilient configuration using SCCP-CO.

2.4 M3UA - Default Routing

This release supports the ability to Route M3UA messages for which no explicit Route has been configured. When a message is passed to M3UA for Routing to the network M3UA searches its Routing Table for a Route matching the DPC in the message for transmission. If no match is found then an optionally configured Default Route may be used for Routing.

A Route may be designated as a default Route by setting bit 2 in the 'flags field of the STN_ROUTE command. Only one Default Route may be configured. The Default Route availability follows the same rules as other Routes.

If bit 0 of the STN_ROUTE flags is set then the Default Route will become available as soon as the network connections become available. In this case the DPC in the Route serves little purpose (though must still be unique in the Routing Table). A DPC of Zero could be used.

If bit 0 of the STN_ROUTE flags is not set then the Default Route will only become available when the DPC used in the configuration message becomes available. The Point Code of the Signaling Gateway through which the Route connects to the network may be used.

2.5 SIGTRAN - Dynamic Protocol Configuration

SIU Mode already supports the ability to dynamically add and remove TDM signaling configuration without impact to system operation. This release extends the functionality to support dynamic addition and removal of SIGTRAN objects.

Dynamic configuration works by loading an updated config.txt file and using the CNURI MMI command to load each new object instance in turn into the system.

Dynamic removal is similar except that the user removes the existing configuration from config.txt and uses the CNURE MMI command to remove each object from the system.

The CNURI and CNURE commands each require two parameters: MODE which identifies the config.txt command type and ID which identifies the object instance within that command type. The following table shows the new values for MODE and the meaning of the ID field in each case.

Config.txt command	**MODE setting**	**ID meaning**
STN_LINK.	SNLINK	SNLINK id.
STN_LAS	SNLAS	Local Application Server id.
STN_RAS	SNRAS	Remote Application Server id.
STN_RASLIST	SNRASL	M3UA RAS List id.
STN_ROUTE	SNRT	M3UA Route id.
STN_RSGLIST	SNRTL	M3UA Route List id.
STN_LBIND	SNBIND	M3UA bind id.

In addition, to allow the user to read back the current configuration settings, the following MMI commands are now supported:

CNSTP – Configuration SIGTRAN link Print

CNLAP – Configuration SIGTRAN Local Application Server Print

CNRAP – Configuration SIGTRAN Remote Application Server Print

CNRLP - Configuration SIGTRAN Remote Application Server List Print

CNGLP – Configuration SIGTRAN Gateway List Print

CNSRP – Configuration SIGTRAN Route Print

CNSBP - Configuration SIGTRAN Bind Print

A full definition of these commands is provided in an SS7G3x SIU Mode User Manual Supplement (document reference GA35LFD) available on request.

2.6 SIGTRAN Timer Configuration

Users can now modify timer values for SCTP, M2PA and M3UA using new config.txt commands SCTP_TIMER, M2PA_TIMER and M3UA_TIMER. A full definition of these commands is provided in section 4.

2.7 M3UA - Multiple Network Contexts

Operation has been enhanced to allow up to four separate M3UA Network Contexts each supporting a different local point code. Previously use of M3UA was restricted to a single Network Context.

M3UA Network Contexts are configured using the STN_NC command which has the following syntax:

STN_NC <nc> <ss7mode> <flags> <share>

With the exception of the new <share> parameter, the command is as specified in the SIU Mode User Manual. The <share> parameter allows the user to specify the percentage (in the range 1 .. 100) of the M3UA license capability that should be allocated to the specific Network Context. The total value of <share> for all Network contexts should not exceed 100.

Subsequent M3UA configuration commands as well as user part commands should reference the appropriate M3UA Network Context for M3UA.

The STLCP MMI command now lists one M3UA entry for each active Network Context and reports the 'share' of the overall M3UA license capability allocated to that NC.

The MSLCP MMI command now lists the Network context associated with each set of M3UA license capability measurements.

2.8 M3UA – 8bit SLS Rotation

The <options> field of the STN_NC command has been extended to support a new option which allows 8 Bit SLS rotation. Bit 0 should be set to 1 to activate SLS rotation. When SLS rotation is activated, <options> bit 1 is set to 1 to select 8 bit SLS rotation or set to zero for default SLS rotation based on MTP label format.

2.9 M3UA - Selective Tracing

M3UA operation has been enhanced to automatically generate a trace of any received message that results in generation of an M3U_MSG_M3U_EVENT (0x02ee) event indication. The trace is intended to assist with problem diagnosis and appears in the maintenance log (maint.log.txt).

2.10 DTS Per-client, LSS Heartbeats

This release introduces support for per-client heartbeats for each Local Sub-System (LSS) when using DTS. This allows systems to continue to operate effectively where one or more sub-systems on a client are unavailable by routing new dialogues only to available sub-systems.

When DTS heartbeats are enabled, the application is responsible for sending a UIS (User In Service) message to DTS for each LSS on a periodic basis as a heartbeat to keep alive the sub-system on that client. In the event that a valid UIS is not received for 30 seconds the sub-system will be marked as unavailable (on that client) to receive new incoming dialogues (although messages relating to existing dialogues will continue to be sent).

DTS heartbeat operation is activated by the user when starting up the client and will apply to all Local Sub-Systems operating on the client. In the DTS_CLIENT_REQ (0x776a) message with 'Request Type Octet' = DTS_CLIENT_STARTUP, the user needs to add a new two octet options field (offset=1, size =2 in the parameter area) and set bit 0 of the options to 1 to enable DTS heartbeat. Each client-based sub-system will not be brought into use until the first UIS message is received from the client.

It is recommended that the client sends a UIS message to DTS every 20 seconds.

3 Changes

3.1 Port Bonding

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.

3.2 FTP Passwords

Prior to this release if a '$' character was used as part of the FTP password that character was incorrectly stored within the system and a user would be unable to ftp into the server using the password that was set. This has been corrected.

3.3 SS7HDP – Long Messages

This release corrects an issue introduced in Release 2.2.2, which resulted in potential corruption of received MTP2 messages where the Signal Unit length between flags exceeded 253 octets.

3.4 Clock recovery from Unstructured E1/T1

This release corrects an issue when recovering clock from an Unstructured E1/T1 interface that prevented the recovered clock signal being used for other boards in the system.

3.5 SIU_REM_ADDR Command

Prior to this release if the SIU_REM_ADDR command was entered in a config.txt file without any parameters, a subsequent restart of the system would fail and the SIU would be unable to operate. Under such circumstances the system will now fully re-start and offer an alarm in the alarm interface indicating that the SIU_REM_ADDR command in the config.txt file is incorrectly formatted.

3.6 MMI - STCRP Route id > 999 (IPY00099078)

This release ensures that the STCRP command correctly displays the route id for all values. Previously values greater than 999 were not displayed at all.

3.7 MMI - MSSLP

Prior to this release the OOS duration reported for M2PA and MTP2 link statistics using he MSSLP MMI command was 10 times actual value in seconds. This has been corrected and the value in seconds is now reported.

3.8 MMI - CNSTP

Previously the display SIGTRAN Link configuration MML command, CNSTP, displayed LIP2 (Local IP Port 2) twice in the output header. This has been corrected and command will now display LIP1 followed by LIP2 representing the configuration for the first and second local IP ports.

3.9 MMI - STEPP

An error was introduced in Release 2.2.0 where the status of the second Ethernet port was not displayed correctly by the STEPP MML command. This has been corrected.

3.10 MTP - Route Status and Configuration

The SS7 Route status and configuration output MMI commands STCRP and CNCRP have been enhanced to allow the user to request output for a specific individual route by including the optional ROUTE parameter on the command line.

3.11 MTP - Distribution of MTP Transfer Indications

Release 2.2.1 introduced the optional distribution of MTP3 Transfer Indications in a Round Robin manner across all available SIU Hosts by setting bit 0 in the options parameter of the SIU_HOSTS command.

This functionality has been enhanced so that a sequence number is inserted in the err_info field of the RX_IND message header thus allowing message sequencing to be coordinated across multiple hosts.

3.12 MTP - Dynamic Deletion of routes

Prior to this release when a user attempted to dynamically delete a MTP route a second MTP route was also deleted. Only the MTP route specified will now be removed.

3.13 ISUP - German National Variant (IPY00099287)

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. The parameter definitions are as follows:

Parameter Name	Protocol parameter value (Hex)	API parameter value (Hex)	Minimum Length	Maximum Length
NP.FF	0xff	0x1f8	4	4
NP.SSP	0xfc	0x1f9	1	2
NP.UKK	0xf5	0x1fa	1	3

3.14 SCCP - GTT for ITU 24 Bit point codes

This release corrects an issue that previously prevented Global Title configuration when using 24bit ITU-T format point codes.

3.15 SCCP - ANSI GTT Handling

Previously the Signaling Server incorrectly added an encoding scheme for ANSI GTTs when the GT_IND was set to "0010". This release will now only add it when GT_IND is set to "0001".

3.16 TCAP - Called Party Address

This release adds an option to force TCAP to always use the original Called Party Address throughout an outgoing dialogue rather than allowing it to be replaced by the address received in the first response received from the far end. To activate this feature, bit 11 of the <options> parameter in the TCAP_CONFIG or TCAP_NC_CONFIG commands should be set to 1.

3.17 TCAP - ASN.1 non-minimal length encodings

The TCAP specification Q.773 states that when ASN.1 encoding messages, length encodings should use as few as possible octets, e.g. encodings such as 0x8174 and 0x820074 should both be sent as 0x74. Previously TCAP would reject received network messages that did not conform to this rule. This restriction has been relaxed to accept messages that use ASN.1 non-minimal length encoding.

Outgoing messages are always encoded in accordance with the TCAP specification using the minimal length for ASN.1 lengths.

3.18 TCAP - Overlength outgoing messages

In the event that a message exceeds the maximum size for transmission to the network, TCAP will now discard the whole message and abort the dialogue. Previously in some situations just the dialogue portion was discarded resulting in a malformed message being sent to the network.

3.19 TCAP - Abort with User Abort Information

When sending an ITU-T TCAP Abort message containing the User-Abort-Information parameter, any additional dialogue portion is discarded to ensure valid formatting of the outgoing message.

3.20 MAP - Selective Tracing enabled by default

Selective Tracing within MAP, as documented within the MAP Programmer’s Manual, is now enabled by default for all events. If required, the MAP_MSG_S_SELTRACE_MASK can be used to modify which events are selectively traced.

3.21 MAP - GPRS Node Indicator parameter support

MAP services SendRoutingInfoForLCS and SubscriberLocationReport now support the GPRS Node Indicator parameter, MAPPN_gprs_node_ind (123).

3.22 MAP - Ellipsis parameter processing

Unrecognised parameters in received MAP messages are stored in the MAP Ellipsis parameter (MAPPN_ellipsis). This release corrects a problem (for some services including CHECK_IMEI) that previously caused only the first unrecognised parameter to be stored. A potential problem with ellipsis parameter formatting has also been corrected.

3.23 MAP - TC-REJECT component parameters passed to user

On receipt of a valid TCAP REJECT component from the network, MAP now uses two new parameters to pass additional TCAP component data to the MAP user for diagnostic purposes.

MAPPN_tcap_rej_problem_code (584) contains the Problem Code (0 to 7) of the REJECT component and MAPPN_tcap_rej_problem_type (585) contains the Problem Code tag that was used (0x80 to 0x83). The interpretation of the problem code value is dependent on the tag used.

Reception of a valid REJECT component will cause a MAP-NOTICE-IND dialog message or a MAP-SERVICE-CNF message (with error parameter) to sent to the MAP-User. In both cases the two new parameters will now be returned in the messages. For the MAP-NOTICE-IND message, the existing parameter MAPPN_invoke_id (14) will now also be returned with the new parameters to identify the component referenced by the REJECT (MAPPN_invoke_id is already returned by the MAP-SERVICE-CNF message).

3.24 MAP - ASN.1 indefinite length termination octets being returned in ellipsis data

When MAP encounters unrecognised data in received messages, it is returned to the MAP-User in the Ellipsis parameter. In the previous releases where the unrecognised data has been encoded using ASN.1 indefinite length encoding, it is possible for length termination octets ‘EOC’ (two 0x00 octets) to be returned at the end of the Ellipsis parameter data. This release corrects the fault. Ellipsis parameter data will not be incorrectly terminated by indefinite length encoding termination octets.

3.25 MAP - Begin Subscriber Activity with single address

For previous releases if the MAP-User specified only one of MAPPN_dest_ref (2) and MAPPN_orig_ref (4) parameters, sending of the BEGIN-SUBSCRIBER-ACTIVITY (BSA) service would be attempted and fail with MAPSWE_TX_FMT_ERR being reported. This has been corrected so that if only one of the parameters is present, it is ignored and the BSA component is not sent.

3.26 MAP - MAPPN_unk_sub_diag in MAP NOTE-MM-EVENT service

MAP now allows the optional parameter MAPPN_unk_sub_diag (61) to be used in the response for the MAP NOTE-MM-EVENT service when a User Error of 'Unknown Subscriber' is returned.

3.27 MAP - User and Provider Errors supported for all services

MAP now allows the error parameters MAPPN_user_err (21) and MAPPN_prov_err (22) in all MAP services that return a response to the MAP-User.

3.28 MAP – Additional error codes

MAP now supports the following additional user error codes:
MAPUE_unknown_MSC (3)
MAPUE_no_handover_number_available (25)
MAPUE_subsequent_handover_failure (26)
MAPUE_forwarding_failed (47)

3.29 MAP - Missing mandatory parameters in user response data

MAP now checks for missing mandatory parameters when the MAP-User enters response data. For previous releases it was only request data that was checked for missing mandatory parameters. The check now applies to both request and response primitive entry using the MAP_MSG_SRV_REQ message. Reporting of missing parameters is unchanged (from request checking): a MAPSWE_USER_MAND_MISSING error is reported in a MAP_MSG_ERROR_IND message and the number of the first mandatory parameter not found is given in the parameter data.

3.30 MAP – Segmented Result components

In the event that reassembly of partial response data fails (for TCAP segmentation using TC-RESULT-NL and TC-RESULT-L messages), instead of simply discarding the previously stored data, MAP will abort the affected InvokeID.

If abort occurs after a TC-RESULT-NL message, U-CANCEL is sent to TCAP, followed by MAP_CNF with a Provider error to the MAP-User and finally a U-REJECT to TCAP. Aborts that occur after a TC-RESULT-L message will just send the MAP_CNF message with Provider error. The Abort may be caused by parameter format checks or exhaustion of the buffer space. Exhaustion of the buffer space is also reported using MAPSWE_TC_RESULT_NL_TOO_BIG.

In addition this release modifies the processing of the SendParameters service so that response data received in multiple messages (one or more TC-RESULT-NL messages followed by a TC-RESULT-L) is correctly handled.

3.31 MAP – Invalid user-supplied Invoke id in response

If MAP receives an unknown Invoke ID in a response primitive in the MAP_MSG_SRV_REQ message, a software event report will now be generated. The event report uses the MAP_MSG_ERROR_IND message with error code MAPSWE_USER_INVOKE_ID_UNKNOWN (27) with the id field set to the UserDialogID and the first Diagnostic code set to the invalid InvokeID. MAP will also optionally generate a selective trace message with trace reason code MAPt_user_invoke_id_unknown (16).

3.32 IS-41 Unidirectional messages (IPY00099105)

This release adds support for the IS-41 Unidirectional message in situations where DTS is running above IS-41. Previously such messages were discarded.

3.33 INAP - INAP_FE command

Parsing of the config.txt command has been corrected to ensure the address entered is associated with a configured INAP local subsystem.

Prior to this release the INAP_FE command only allowed the configuration of functional entities for local subsystems. The INAP_FE command has been modified to support the configuration of functional entities for local and remote subsystems.

3.34 SCTP - Default Timers and Thresholds

The default SCTP timer values and congestion thresholds have been changed to the following more appropriate values:

Timer	Previous Default	New Default
RTO Minimum	500ms	200ms
RTO Maximum	2000ms	1400ms
RTO Initial	500ms	1000ms

Threshold	Previous Default	New Default
Congestion Abatement	600 messages	100 messages
Congestion Onset	800 messages	200 messages
Congestion Discard	1000 messages	400 messages

3.35 SCTP – Improved Robustness

This release contains enhancements to the SCTP implementation to remove a potential cause of association failure under heavy load due to incorrect handling of the receive window and also to prevent unnecessary transmit message discard as the transmit buffer reaches capacity.

3.36 SCTP - Event Indications

SCTP now generates event indications to the maintenance log whenever the state of an association or a path within an association changes. The messages (SCTP_MSG_STATUS_CHANGE, SCTP_MSG_NETWORK_STATUS & SCTP_MSG_CONG_STATUS) are identical in format to the messages documented within the *SCTP Programmer's Manual* which are issued to the SCTP user. The events are fully decoded within the maintenance log.

3.37 M2PA – Initial alarm state

This release also ensures that at startup the "SS7 link failure" alarm is correctly generated until the M2PA link successfully comes into service.

3.38 M2PA/M3UA - Throughput Licensing Alarms

This release corrects an issue which previously prevented generation of the the 'Traffic congest' and 'Traffic enforce' alarms when throughput for M3UA or M2PA reached the licensed throughput limit.

3.39 M3UA - Disable Loadsharing

This release allows the user to optionally disable loadsharing on a per Sigtran-route basis using the OPTIONS parameter of the STN_ROUTE command.

To unlock this capability (and preserve backwards compatibility), bit 15 of the OPTIONS parameter should now (always) be set to 1. Bit 1 of the OPTIONS field is then used to control whether load sharing is enabled or not. When bit 1 is set to 1 load sharing is activated and when bit 1 is set to 0 load sharing is disabled and traffic is routed over the first association whenever it is available and over the second association as a backup.

3.40 M3UA Traffic Mode

Prior to Release 2.2.2 the SIU automatically transmitted the Traffic Mode configured on the Local Application Server in an ASPAC message towards a Signaling Gateway. This was removed in Release 2.2.2. To preserve backwards compatibility this functionality has been re-introduced and the SIU will again transmit the traffic mode in this circumstance.

3.41 DTS – Mode B' operation

This release corrects an issue in DTS 'Mode B' operation where DTS is configured to run above TCAP user module(s). Prior to this release in this mode DTS could potentially send particular messages to an illegal module id. This has been corrected and the messages that DTS had previously sent to illegal destination are now handled as follows:

- DTS_CLIENT_CONF now sent back to source of DTS_CLIENT_REQ
- Default Routing key routes messages to the default local subsystem which is determined by the first SCCP_LSS configured in config.txt.

3.42 DTS - Use of Dialogue ID 0xffff

This release corrects an issue which previously prevented use of the value 0xffff as a dialogue_id when using DTS.

3.43 DTS - Client Rotation

This release corrects an issue which prevented correct selection of DTS clients in situations where the 'Sequence Number' set in the DTS_ROUTING_REQ message was not the same as the 'host_id' for the client.

3.44 RSI - Link failure and recovery

This release corrects an issue which could potentially result in a failed RSI link being unable to automatically recover without restarting the unit. It also corrects a problem which could result in the RSI interface (used between SIU and hosts or for the inter-SIU link) stalling at very high traffic rates and causing the SIU to go into overload.

3.45 MMI Logging

This release masks the parameter area in the MMI log file for any unrecognized parameters to prevent inadvertent display of passwords following a miss-typed parameter name.

3.46 PCAP Logging

This release corrects a problem when logging MTP message traces in PCAP format which sometimes resulted in the global header being omitted from the file. This happened when the last message logged to the previous file caused the file size to exactly equal the file size limit.

3.47 Use of Ctrl-X to cancel listing (IPY00097713)

When MMI outputs multiple pages of data for a MMI print command the output pauses to allow users time to view the data. MMI allows users to press the return button to move onto the next page or to enter Ctrl-X to abort the MMI command. This release expands the prompt to include details of the option to abort the listing as follows: "Press return to continue or Ctrl-X to cancel".

3.48 Unrecognised Module_ID

Messages received by the server with an unknown destination module_id are now processed and logged to the maintenance log.

4 Commands

4.1 SCTP_TIMER

Synopsis

The SCTP_TIMER command provides the ability to configure the SCTP protocol timers from the configuration file.

Syntax

```
SCTP_TIMER [<nc_id>] <reserved> <timer_id > <value>
```

Example

```
SCTP_TIMER 0 Rmax 1600
```

```
SCTP_TIMER NC1 0 RMIN 200
```

Example

<nc_id>

SS7 Network Context. This parameter uniquely identifies the SS7 network that the SCTP timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

<reserved>

Reserved for future use and must be set to zero.

<timer_id>

A text identifier for the timer to be configured. It should be set to one of the following:

RMIN, RMAX, RINIT, CK, HBT, T1I, T2I, SACKD

<value>

The timer value in milliseconds.

Any timers not explicitly configured continue will be set to the default values shown in the following table:

Mnemonic	Default	Granularity	SCTP Timeout
Rmin	200ms	1ms	Minimum RTO
Rmax	1400ms	1ms	Maximum RTO
Rinit	1000ms	1ms	Initial RTO
Ck	30000ms	1ms	Cookie lifetime
Hbt	1000ms	1ms	Time between heartbeats
T1i	3000ms	1ms	Starting timeout of an INIT chunk
T2i	3000ms	1ms	Starting timeout of a SHUTDOWN chunk
Sackd	10ms	1ms	SACK delayed Ack

4.2 M2PA_TIMER

Synopsis

The M2PA_TIMER command provides the ability to configure the M2PA protocol timers from the configuration file.

Syntax

```
M2PA_TIMER [<nc_id>] <reserved> <timer_id > <value>
```

Example

```
M2PA_TIMER 0 T1 200
```

```
M2PA_TIMER NC1 0 T7 15
```

Parameters

<nc_id>

SS7 Network Context. This parameter uniquely identifies the SS7 network that the M2PA timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

<reserved>

Reserved for future use and must be set to zero.

<timer_id>

A text identifier for the timer to be configured. It should be set to one of the following:

T1, T2, T3, T4N, T4E, T6, or T7

<value>

The timer value in multiples of tenths of a second (100 ms).

Any timers not explicitly configured continue will be set to the default values shown in the following table:

Mnemonic	Default	Granularity	M2PA Timeout
T1	40s	1s	'Alignment Ready' timer value
T2	10s	1s	'Not Aligned' timer value
T3	2s	1s	'Aligned' timer value
T4N	7s	1s	'Normal Proving' timer value
T4E	500ms	100ms	'Emergency Proving' timer value
T6	3s	1s	'Remote Congestion' timer value
T7	1s	100ms	'Excessive Delay Of Acknowledgement' timer value

4.3 M3UA_TIMER

Synopsis

The M3UA_TIMER command provides the ability to configure the M3UA protocol timers from the configuration file.

Syntax

```
M3UA_TIMER [<nc_id>] <reserved> <timer_id > <value>
```

Example

```
M3UA_TIMER NC1 0 TACK 30
```

```
M3UA_TIMER NC1 0 Tbeat 310
```

Parameters

<nc_id>

SS7 Network Context. This parameter uniquely identifies the SS7 network that the M3UA timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.

<reserved>

Reserved for future use and must be set to zero.

<timer_id>

A text identifier for the timer to be configured. It should be set to one of the following:

Tack, Tr, Tdaud, Tbeat.

<value>

The timer value in multiples of tenths of a second (100 ms).

Any timers not explicitly configured continue will be set to the values shown in the following table:

Mnemonic	Default	Granularity	M2PA Timeout
Tack	2s	100ms	Peer response timeout
Tr	1s	100ms	Recovery timer for inactive ASPs
Tdaud	30s	1s	DAUD generation timer
Tbeat	30s	1s	M3UA heartbeat timer

Dialogic
03-Feb-12
Revised 09-Apr-12

Release 2.2.2

1 Overview

This maintenance software release corrects a defect in SCTP operation which could result in a system reset under high load conditions. The release also corrects operation of M2PA throughput licensing and the display of Global Title configuration.

This release is backwards-compatible with the previous version.

1.1 Applicability

This release contains an important correction to SIGTRAN SCTP operation. All SIGTRAN users are advised to upgrade to this release at a convenient opportunity.

1.2 Resolved Customer Issues

The following customer issue is resolved in this release: IPY00092503.

2 Changes

2.1 SCTP – Recovery from Congestion

This release corrects operation under high loads within SCTP which could result in the unit failing to come out of congestion. This could lead to the unit performing an automatic restart or in some cases requiring a manual restart to recover.

2.2 M2PA – Throughput Licensing

Prior to this release M2PA License management did not correctly manage and report using the MSLCP MMI command traffic received by the Signaling Server. The software has been modified to properly manage received M2PA data.

2.3 Global Title Translation

Release 2.2.1 introduced a problem which resulted in the Global Title MMI commands CNGPP and CNGAP displaying invalid configuration data. This has been corrected.

Dialogic
10-Dec-10

Release 2.2.1

1 Overview

This release is a feature release introducing several new features and a number of corrections. It is the first release since V2.17 and it replaces Release 2.2.0 which was only used for trial. The release includes several security enhancements and introduces the concept of 'strong' passwords. It supports per-association configuration of SIGTRAN Local IP Addresses, the ability to create PCAP format trace logs and other features as detailed below.

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

- The format of the version has changed from Vx.yy to "Release x.y.z" to align more closely with other Dialogic® Products.
- This release supports operation in "SIU-Mode" only. The "SGW-Mode" software is now a separate software distribution and the release numbers and release dates are no longer interlocked.
- The filename of this distribution is **ss7g30-siu.tgz.** When upgrading software from an earlier release for the first time it is necessary to rename the file to **sgw.tgz** prior to loading it onto the unit.
- All new passwords must now meet the 'strong' password requirements as detailed in section 2.1 below.
- Passwords are now set using a new command (CNUAS – Configuration User Account Set) rather than the CNSYS command which was previously used. Refer to section 2.1 below for full details.

An updated Dialogic® DSI Signaling Servers SIU Mode User Manual (Issue 10) is available and provides further detail of the new functionality.

Users should familiarize themselves with the full content of the release notes for this version prior to deployment.

1.1 Applicability

This release enhances security as well as introducing several enhancements and corrections as detailed below. All users are advised to upgrade to this release at a convenient opportunity.

1.2 Resolved Customer Issues

Updates to resolve the following customer issues are included in this release: IPY00091013, IPY00091121 and IPY00092069.

2 New Functionality

2.1 Security enhancements with strong passwords

This release enhances IP security, strengthening the system against SYN attacks and, to prevent hijacking of routing path, allowing redirects from gateways known to the routing table.

The release also introduces the concept of 'strong' passwords which means that whenever a password is set is must conform to strict new rules.

Passwords must be set using the new CNUAS command (detailed in issue 10 of the SIU Mode User Manual). The CNSYS command no longer supports setting passwords.

Prior to this release a single system password was supported which could optionally be used to specify the password to be used for FTP access. This release separates these two uses of password into explicit 'User Accounts' called 'admin' and 'siuftp' which are configured using the CNUAS command:

The 'admin' user account is used to gain access to the MMI interface.

The 'siuftp' user account is used to gain access by sftp/ftp into the siuftp account for file transfer and for ssh access for secure telnet.

All new passwords must obey the following criteria:

- Passwords must be between 8 and 15 characters in length.
- Passwords must contain at least one upper case character, one lower case character, one digit and one special character (~ $ % ^ @ #)
- The password must not be the same as any of the previous 8 passwords.

Note: Passwords set prior to this release will continue to operate. The strong password rules will only apply to the setting of new passwords.

When a user enters a password incorrectly 3 times the session will log off and the MMI port will be unavailable for 30 seconds. When logging in MMI will now display the time of the last successful login and failed attempts to login to will be reported to the MMI log.

2.2 Per-association config of Local IP Address

This release supports per-association configuration of up to two local IP addresses for each SIGTRAN link. Two new parameters <lip1> and <lip2> have been added to the STN_LINK command. See issue 10 of the SIU Mode User Manual for syntax and revised description of the command.

<lip1> is the first local IP address for the association and must be non-zero. If a local IP address is configured on one STN_LINK then all subsequent STN_LINK commands must have at least one local IP address configured.

<lip2> is the second local IP address for the association. It should be set to 0 if not required and must not be the same as <lip1>.

Note: Prior to this release configuration of local SIGTRAN IP address was performed at a system level using the IPEPx MMI command which activated SCTP on a particular Ethernet port. The use of the SCTP parameter on the IPEPx MMI command has been deprecated. The system will ignore the setting of this parameter if per-association hosts are specified. The parameter itself will continue to be supported to ensure the software remains backwardly compatible with configurations that did not specify per-association local IP addresses.

The parameter names in the example config.txt file have been renamed in line with the latest STN_LINK command syntax.

2.3 Distribution of MTP3 Transfer Indications

This release offers optional distribution of MTP3 Transfer Indications in a Round Robin manner across all available SIU Hosts. To support this feature the SIU_HOSTS configuration command has been modified to accept a new options parameter as follows:

SIU_HOSTS <num_hosts> <backup_mode> { **<options>** }

To activate the feature, bit 0 of the 32 bit <options> field should be set to 1. For normal operation bit 0 should be set to zero. All other bits are reserved for future use and should be set to zero.

2.4 PCAP format trace logs

The release adds the ability to log MTP3 and M3UA traces to PCAP format log files. In a similar manner to text log files the system supports multiple size-constrained log files named trace.pcap, trace.pcap.1, trace.pcap.2 etc. storing them in the syslog subdirectory of the siuftp account.

A new parameter, **TRACEFMT**, has been introduced on the CNSYx MMI command. This parameter is used to specify the format of the log files written to locally on the unit. Logs written to the host remain as TEXT only format.

TRACEFMT can take the following values: TEXT (default), PCAP or DUAL (where PCAP and TEXT log files will be created).

PCAP logging requires that the appropriate M3UA/MTP tracing options are set on the CNTMx command to log MTP transfer requests and indications.

2.5 RSI traffic measurements

This release supports two new MMI commands to report traffic measurements for each SIU host (MSHLP) and to the partner SIU (MSRLP). Refer to SIU User Manual Issue 10 for a full definition of these commands.

2.6 Manual test for Alarms and Alarm LEDs

Two new MMI commands have been introduced to allow users to test the system alarm mechanism. ALTEI (Alarm Test Initiate) allows the activation of MINOR, MAJOR and CRITICAL test alarms and on the SS7G32 activates the appropriate LED on the front panel. ALTEE (Alarm Test End) clears the test alarm. Refer to SIU User Manual Issue 10 for a full definition of the ALTEI and ALTEE MMI commands.

2.7 Viewing board and SIGTRAN configuration

Two new commands have been introduced to allow users to view the configuration of boards (CNBOP) and SIGTRAN Links (CNSTP) using MMI without needing to refer to the config.txt file. Refer to SIU User Manual Issue 10 for a full definition of these commands.

2.8 Routes per Remote Signaling Gateway

The maximum number of SIGTRAN routes per Remote Signaling gateway has been increased from 32 to 255.

2.9 IS41 - Transparent Component Handling

The ability to send and receive transparent IS41 component parameters (IS41PN_transp_component) that exceed 255 octets in length has been added by the introduction of a new IS41 code shift parameter. Further details of this mode of operation are available on request.

3 Other Changes

3.1 Software Distribution Format

Prior to this release a single software distribution supported both ‘SIU-Mode’ and ‘SGW-Mode’ operation. These two modes will now have separate software distributions.

The new filename of the SIU distribution is ss7g30-siu.tgz. When upgrading from an earlier release users should rename the file sgw.tgz prior to installation. Subsequent upgrades will accept files of either name.

It is possible to install SIU-Mode and SGW-Mode software on a server at the same time although only one mode can be operational at any time. Users can determine what software is present on the system by looking at page 2 of the CNSWP command.

If a system is running in SIU mode and a SGW software distribution is installed or if a user attempts to switch to SGW mode and there is not a SGW mode distribution present on the system the software will boot into TEST mode to allow users to correct the software or configuration.

3.2 Operating period for Trial Mode

It is now possible to run the unit in trial mode without requiring an SIU License. When operating in trial mode (without software licenses) the period of operation is now 1 hour instead of 10 hours. Users with a need to trial the product for longer than one hour should approach their account team with a business justification and request a 30 day trial license.

3.3 System log consolidation

Prior to this release a number of separate diagnostic logs were saved in the syslog subdirectory of the siuftp account. The information from these logs is now consolidated into two log files: startup.log and shutdown.log.

3.4 SPCI 'Switch Error' alarm

A new alarm event has been added to identify units that are using SPCI boards with the on-board BOOT switch set incorrectly. The alarm event is "Switch error" and the ID field indicates the board position. If this alarm occurs it indicates that the switch setting is incorrect. The unit should be opened (in accordance with the user documentation) and the BOOT switch set to position 8.

3.5 CNSYP command divided into two pages

To increase clarity the command CNSYP has been modified so that parameters that are rarely changed are displayed on a second page of output.

3.6 CNLSP display of <flags> field

The flags field in the CNLSP command was incorrectly displayed with bits 0 & 1 both set. These bits are reserved and should not be set by the user. The command has been modified to display the correct value.

3.7 Configuration of GTT using 24 bit Point Codes

This release corrects a problem when configuring 24 bit Point Codes using the SCCP_GTT_ADDRESS command which sometimes discarded the most significant byte of a 24-bit point code in the PC parameter.

3.8 SNMP Changes

Several minor changes and corrections have been made to SNMP operation as follows:

Generation of the index field in the NOTIFICATION-MIB has been corrected. The field is defined as type UNSIGNED32 but previous releases incorrectly transmitted the field as type INTEGER.

NOTIFICATIONs now include an additional field indicating the 'id' value of the object to which the notification relates.

Previously Remote Application Server (RAS) state was always considered 'UP' state. This release reports the actual state.

A problem where the loss of an SS7 linkset was reported but the subsequent recovery was not reported has been corrected.

A problem which sometimes caused an SNMP GET on an SNMP LIU to fail leading to an eventual system restart has been corrected.

To benefit fully from these enhancements users should upgrade the associated MIBs used by their SNMP manager to V2.00 or later of the DSMI SNMP MIB package. Whilst structurally the V2.00 MIBs are backwards compatible, the variable names used in the MIBs have been changed so tools and scripts that rely on specific variable names should be modified to match the new values.

3.9 No System Resources

Prior to this release some internal failure conditions (eg. board failure) could result in certain MMI commands (eg. MSMLP) locking out subsequent MMI commands and reporting 'NO SYSTEM RESOURCES'. This has been corrected.

3.10 Message Tracing

A fault introduced in V2.17 software where the combination of the activation of message tracing and the use of the CNSYS MMI command could result in the system going into overload and subsequently restarting has been corrected.

3.11 TCAP status (STTDP and STTRP)

Previously the commands STTDP and STTRP only operated correctly when TCAP had been configured explicitly using the TCAP_CONFIG command but did not operate when TCAP had been implicitly configured using the SCCP_SSR command. This has been corrected.

3.12 Updated SS7MD firmware

This release includes updated firmware for the SS7MD board to prevent the possibility of the board shutting down unexpectedly.

3.13 IS41 - Ellipsis parameter Handling

For previous releases there was a fault when processing network messages from TCAP. Invalid received parameter data could be returned to the IS41-User when there was more than one unknown parameter tag in the received data. Unknown parameters are accumulated into the IS41PN_ellipsis parameter and returned to the user in raw tag, length, data format. This is now corrected.

Dialogic
14-Oct-10

Release Notes for V2.17

1 Overview

This is the first software release since V2.15. This release is a maintenance release which enhances the capabilities of the SIU in respect to IP security and auditing as well as introducing corrections to SCCP, TCAP, MAP, ISUP and SIGTRAN operation.

To allow for audit of user MMI sessions, all user dialogues are logged to a rolling log file to permit subsequent review of the command history. The release also improves security on FTP and Secure FTP by removing read access to files and directories outside the siuftp account.

This release is backwards compatible with the previous release however users using Secure FTP to access the system should take note that the landing directory is now different from the previous release so users will need to change to the 'siuftp' subdirectory before proceeding as normal.

1.1 Applicability

This release enhances security as well as introducing several corrections as detailed below. Users are advised to upgrade to this release at a convenient opportunity.

1.2 Resolved Customer Issues

Updates to resolve the following customer issues are included in this release: IPY00081954, IPY00082268, IPY00082308, IPY00082378, IPY00090633, IPY00090696.

2 New Functionality

2.1 MMI Logging

To allow for audit of user MMI sessions, all user dialogues are logged to a rolling log file to permit subsequent review of the command history. The text format log files include all MMI commands, responses and events.

Log files are created in the 'syslog' sub-directory of the siuftp account. The most recent file is called mmi.log and older files are called mmi.log.1, mmi.log.2 and so on up until mmi.log.9. The capacity of each file is limited to prevent disk overflow.

Each entry in the file includes the date and time of the event. For security the text value of the PASSWORD and CONFIRM parameters are replaced by the string "******".

3 Other Changes

3.1 FTP Security

This release enhances IP security by removing the ability for 'anonymous' FTP access and restricting the visibility of the built-in file system.

Note: Secure FTP users will by default land in the parent directory of siuftp and will need to change to the siuftp directory before commencing operation. Most Secure FTP clients provide an option to configure the default initial directory. If available users may choose to use this instead of manually changing to the siuftp subdirectory.

3.2 Configuration Changes

Under certain circumstances previous releases did not always save configuration data following execution of the IPGWI, IPEPS or CNSNS commands. As a result, if the unit was restarted immediately after execution of one of these commands and prior to execution of any other commands that changed configuration then the configuration changes would be lost. This has been corrected.

3.3 Detection of missing license

On detection of a missing software license, the SIU will now complete startup and report in the MMI ALLIP command that the relevant configuration line cannot be executed due to a missing license. Previously the boot sequence could fail resulting in no MMI prompt.

3.4 SIGTRAN Routing Contexts

This release supports full 32 bit bit SIGTRAN Routing Contexts for the STN_LAS and STN_RAS configuration commands. Previously only 16 bit values were supported.

Prior to this release the SIU was unable to interwork with a Signaling Gateway which did not use a Routing Context. This has been corrected and the SIU will interwork with a Signaling Gateway without a Routing Context, provided bit 0 of the flags parameter associated with the STN_LAS command is set, indicating that the configured routing context should be ignored and no routing context will be transmitted.

3.5 M3UA – Single RC to multiple SG

Prior to this release when a single Local Application Server (LAS) was configured together with two or more Signaling Gateways (SGs) the routing context (RC) of the LAS was only transmitted to the first SG. This prevented multiple SGs working with the same RC. The SIU will now send the RC to each SG.

3.6 ISUP – CGSC Reset Request

ISUP software has been modified to ensure that, irrespective of the internal call control state, a Circuit Group Supervision request from management to Reset the group will force the circuit to IDLE.

3.7 SCCP – GTT Configuration

In previous versions, when configuring an ITU Global Title Translation with the Global Title Indicator set to "0100", on occasions bit 8 of Octet 3 of the Global Title was incorrectly set to '1'. This bit will now always be set to '0'.

3.8 TCAP - Send TC-NULL message if unexpected component

In previous releases the reception of a network message with an erroneous component with the same invoke id as an earlier result or error component was not handled correctly. The erroneous component was discarded but in the associated TCP_MSG_DLG_IND message the TCPPN_CPT_PRESENT parameter (components present) was set to 1. This would leave TC-User modules such as MAP, INAP or IS41 expecting a subsequent component indication from TCAP which would not be sent.

This release corrects the behavior by sending a TC-NULL component primitive indication in a TCP_MSG_CPT_IND message sent to the TC-User in place of the discarded component. The message consists of the TCPPT_TC_NULL primitive type octet and a single TCPPN_LAST_CPT parameter set to 1.

3.9 MAP - Message generation after MAP-NOTICE-IND and/or TC-U-REJECT

For previous releases, MAP did not correctly handle some situations that required MAP-NOTICE-IND messages to be sent to the user and/or U-REJECT to be sent to TCAP and the dialog was left in an inappropriate state. MAP should either close the dialog and send a MAP-CLOSE-IND message or move to a next state and send the user a MAP-DELIMITER-IND message. This release ensures that it is correctly handled.

In order to prevent unexpected behaviour in some MAP applications this change can be disabled by setting Bit 7 of the MAP_CONFIG options parameter to 1. It should only be set to this value when the messages now being generated cause problems for the MAP application. Otherwise the flag should be set to it default value of 0.

Dialogic
05-Mar-10

Release Notes for V2.15

1 Overview

This release is a maintenance release which includes enhancements to MAP allowing the received Quality of Service (QoS) parameter received from TCAP to be passed to the MAP-User. It also includes various corrections as detailed below.

This release is backwards compatible with the previous release.

1.1 Applicability

There is no critical reason to upgrade to this release, however users are encouraged to do so as convenient.

1.2 Resolved Customer Issues

Updates to resolve the following customer issues are included in this release.

IPY00081613, IPY00081639 IPY00081707, IPY00081833.

2 New Functionality

2.1 QoS Transparency

MAP on the SIU can now optionally be configured to include any QoS information received from TCAP in the corresponding indication to the MAP-User. This is controlled at run-time using bit 6 in the <options> field of the MAP_CONFIG command in config.txt

When the option is enabled, whenever QoS data is received from TCAP it will be passed to the MAP_User in the next Dialogue Indication message, as detailed in the table below:

Parameter	MAP Primitive						
	OPEN–IND	CLOSE–IND	DELIMITER-IND	U-ABORT-IND	P-ABORT-IND	OPEN-CNF	NOTICE–IND
Destination address	M			O		O	
Destination reference	O						
Originating address	O			O		O	
Originating reference	O						
Result						M	
Refuse reason						O*	
Release method							
User reason				M			
Provider reason					M	O	
Diagnostic information				O			
Application context name	M					O	
Source					M		
Problem diagnostic							M
Quality of Service†	O	O		O	O	O	
Ellipsis	O						
Release confirm		O					
Report cause							O
NC	O						

* May only be used with MAP V2 and V3 dialogues.

† QoS returned only if MAPF_QOS_TRANSPARENT option is set.

3 Other Changes

3.1 SIU DUAL Operation

This release corrects an issue whereby in the event that ISUP circuit groups were transferred from one SIU to the other SIU in quick succession some groups failed to transfer correctly.

3.2 STIPP

This release corrects an issue whereby entry of an invalid STIPP command without the mandatory IPADDR parameter could cause unpredictable operation and potentially re-boot. The command will now be rejected with a MISSING PARAMETER indication.

3.3 RSBOI

Operation of the RSBOI command has been corrected to ensure that signaling links are correctly re-activated following the reset. Previously, it was sometimes necessary to manually deactivate and re-activate the links following a reset to achieve correct operation.

3.4 STSSP

Previously, if a concerned subsystem resource was configured in the SCCP_CONC_SSR with an id of 0 the STSSP MMI command would display an erroneous subsystem resource with an id of 2048. This has been corrected and the STSSP command will now display only valid subsystem resources when a concerned sub-system resource with an id of 0 is configured.

3.5 Alarm LEDs

This release corrects a problem where the MAJOR alarm LED failed to illuminate.

3.6 BICC - Application Heartbeat

Prior to this release, when the ISUP heartbeat timer expired ISUP would send a hardware-blocking message to the remote signaling point for each affected circuit group. As BICC does not support hardware-blocking the functionality has been modified such that on heartbeat timer expiry for BICC circuit groups will send a circuit group reset message followed by maintenance-blocking message.

3.7 ISUP - Circuit Group Management Reset

Operation of Circuit Group Supervision Management Reset requests has been enhanced to ensure that circuits are fully returned to the idle state irrespective of the operational state of the application.

Previously the circuit was not returned to the idle state until a valid RLC had been received from the application for any circuits that had been carrying active calls prior to the reset. Under normal operating conditions this was fine however it could lead to issues in situations where the reason for the management reset was that the application had crashed or had been restarted. Under such conditions the application would not have generated the RLC. The new mode of operation will ensure that in this scenario the restarted application can immediately start receiving calls.

3.8 ISUP – ANSI 8-bit SLS support

This release introduces optional support 8-bit SLS values for use in US networks. Selection of 8 bit SLS values is activated by setting bit 22 of the <options2> parameter in the ISUP_CFG_CCTGRP command in config.txt.

When ISUP has been configured for 24 bit point codes and bit 22 of the <options2> parameter has been set ISUP will set the SLS to the 8 least significant bits of the CIC otherwise it will set the SLS to 5 bits.

Dialogic
10-Dec-09

Release Notes for V2.14

1 Overview

This software release introduces support for the MAP GetPassword and RegisterPassword services under MAP V1 and corrects the formatting of the response message sent to TCAP from MAP for some services. This release also optionally supports the reporting of MTP3 Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the local point code to a management module on the host.

This release is backwards-compatible with previous versions.

1.1 Applicability

All users wishing to benefit from the increased capabilities introduced should consider upgrading to this release.

2 New Functionality

2.1 MAP

The MAP services GET-PASSWORD and REGISTER-PASSWORD, previously available under MAP V2, are now also available for use under MAP V1. The parameter area content tables for the services are now as follows:

GET-PASSWORD		
Parameter	**Class**	**Context**
Primitive type octet	M	V1, V2
Timeout (default = 30 seconds)	O	V1, V2
Invoke ID	M	V1, V2
Linked ID	O	V1, V2
Guidance Info	M	V1, V2
Ellipsis	O	V2

GET-PASSWORD-ACK		
Parameter	**Class**	**Context**
Primitive type octet	M	V1, V2
Invoke ID	M	V1, V2
Current Password	M	V1, V2
Ellipsis	O	V2

REGISTER-PASSWORD		
Parameter	**Class**	**Context**
Primitive type octet	M	V1, V2
Timeout (default = 600 seconds)	O	V1, V2
Invoke ID	M	V1, V2
SS Code	M	V1, V2
Ellipsis	O	V2

REGISTER-PASSWORD-ACK		
Parameter	**Class**	**Context**
Primitive type octet	M	V1, V2
Invoke ID	M	V1, V2
Where user error is not included:		
New Password	M	V1, V2
Ellipsis	O	V2
Where user error is included:		
User error	M	V1, V2
Registration Failure Cause	O	V1, V2
Network Resource	O	V1, V2
Per Call Basis	C[1]	V1
Notification To Held Retrieved Party	C[1]	V1
User to User Service Indicator	C[1]	V1
Maximum Conferees Number	C[1]	V1
Hunt Group Access Selection Order	C[1]	V1
Call barring cause	O	V2
Ellipsis	O	V2

1. One or none of these parameters may be included when User Error is SS_Subscribion_Violation.

2.2 Signaling Network Management Messages

The MTP_CONFIG command has been extended to support the setting of bit 17 in the options field. This bit controls how received Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the local point code are processed and supports the following values.

- 0 – Normal operation; messages are discarded.
- 1 – Messages are sent to fixed module_id 0x0a on the host.

3 Other Changes

3.1 MAP - Correction to TCAP formatting of Response messages

For previous releases the TCAP formatting of the response messages for some services could be incorrect. This fault affected response messages where only an Invoke ID parameter was defined (no other parameters). This caused an invalidly formatted response message to be sent to TCAP. The following services were affected:

- AuthenticationFailureReport
- SetReportingState
- StatusReport
- Register-CC-Entry
- SendEndSignalling
- PrepareHandover
- SendAuthInfo (for MAP V3)

The fault has been corrected for this release and the response messages are correctly formatted when sent to TCAP.

Dialogic
16-Oct-09

Release Notes for V2.13

4 Overview

This is the first generally available software release since V2.00, it includes a number of major enhancements as well as some corrections as detailed below.

The ability to support termination and monitoring of ATM signaling links has been added can be achieved on the 2U product, (SS7G32) by fitting a new board type, the Dialogic® SS7MD Network Interface Board.

The SIU has been enhanced to distribute traffic from MAP, INAP and IS41 modules on the SIU to applications on multiple hosts

This release also increases the number of SIU hosts supported to 128, allows the simultaneous configuration and operation of MAP, INAP and TCAP, extends the services and parameters supported by MAP and enhances the configuration options for SCCP, M3UA and M2PA.

This release addresses a number of defects, including important corrections for M3UA and Global Title configuration, and provides some further changes to improve maintainability.

This release is fully backwards compatible with the previous release.

4.1 Applicability

All users wishing to benefit from the increased capabilities or corrections introduced should consider upgrading to this release.

4.2 Resolved Customer Issues

Updates to resolve the following customer issues are included in this release.

IPY00080729, IPY00081131.

5 New Functionality

5.1 Support for ATM Signaling Links

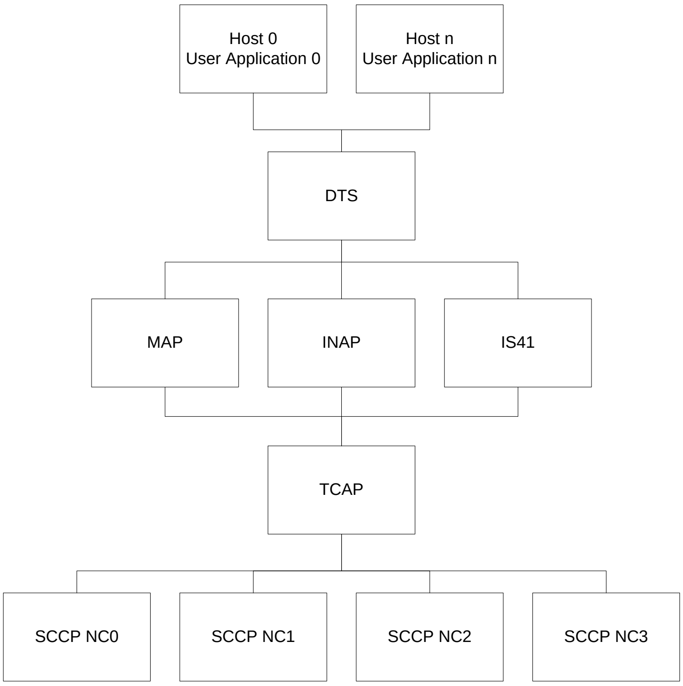
This release is capable of offering termination and monitoring of ATM signaling links. This functionality is available on the SS7G32 (but not on the SS7G31) and requires a new type of signaling board to be fitted in the field. The new board type is designated the Dialogic® SS7MD Network Interface Board. This board supports up to 124 Low Speed SS7 links or 4 High Speed Links which can be either ATM or Q.703 Annex A.

For details regarding the fitting of SS7MDL4 Signaling Boards and their configuration for TDM and ATM Signaling and Monitoring refer to the Dialogic® DSI Signaling Servers User Manual Supplement for ATM Operation.

When using two SS7MD boards, the maximum link density for the SS7G32 is increased to 248 low speed or 8 high speed signaling links.

5.2 User Part DTS Support

The Distributed Transaction Server module (DTS) has been enhanced to distribute traffic from MAP, INAP and IS41 modules on the SIU to applications on multiple hosts.



To support the use of DTS above MAP, INAP and IS41, the SCCP_SSR Configure Local SCCP Sub-Systems command has been extended to allow the specification of new <protocol> parameter values. In addition to the SCCP, TCAP, MAP, IS41, INAP or DTS values, the command will also accept the new values DTS-MAP, DTS-INAP and DTS-IS41. Different local subsystems maybe specify different DTS variants; however the DTS-protocol and the non-DTS-protocol cannot be specified simultaneously.

When using DTS-MAP, DTS-INAP or DTS-IS41 the user must first send a DTS_CLIENT_REQ *Client Start-up Request* message to inform DTS of the client state. After which, protocol traffic can be sent and received directly through DTS. The user application should specify the Module ID of DTS (0x30) instead of the protocol Module ID (e.g. 0x15 for MAP).

DTS ensures that subsequent components of a dialog are always returned to the host which last processed that dialog, enabling any host to take over an in-progress dialog exchange. When dialogs originate from more than one Host/Application, care should be taken to ensure that the same dialogs IDs are not unintentionally used by the other Hosts/Applications.

DTC is not required for message passing when DTS operates above MAP/INAP/IS41; however the DTS module will still send status indications to the Application.

5.3 Simultaneous MAP/INAP/IS41 Operation

Prior to this release it was only possible to run one of MAP, IS41 or INAP on the SIU at a time. This release allows one two or three of these protocols to be run simultaneously. To achieve this, the Outgoing Dialog ID ranges are automatically divided equally between the configured protocols. The Application should be configured to use matching ranges. The base dialog IDs will be allocated in sequence, starting with MAP, then INAP and IS41.

- The base dialog ID for the first protocol will always be zero.
- The base dialog ID for the second protocol will be the total number of TCAP dialogs divided by the number of configured protocols (1 to 3).
- The base dialog ID for the third protocol will be 2x the total number of TCAP dialogs divided by the number of configured protocols (1 to 3).

The table below shows the distribution of dialog IDs and base dialog IDs, assuming that the maximum numbers of supported TCAP dialogs (32768) are configured.

	Outgoing dialogs			Base outgoing dialog ID		
	MAP	INAP	IS41	MAP	INAP	IS41
MAP	32768			0		
INAP		32768			0	
IS41			32768			0
MAP & INAP	16384	16384		0	16384	
MAP & IS41	16384		16384	0		0
INAP & IS41		16384	16384		0	16384
MAP, INAP & IS41	10922	10922	10922	0	10922	21844

5.4 MAP Services

This release implements six new MAP services – Reset, SetReportingState, StatusReport, RemoteUserFree, RegisterCC and EraseCC. The new services are defined as per the 3GPP TS 29.002 v8.2.0 specification. The release also enables the Interrogate-SS service for use with the MAP V1 application context, expands the Subscriber Information that can be requested by some services and adds some parameters to the UpdateLocation service. Details of the primitives and parameters associated with these services are provided in issue 12 of the MAP Programmer’s Manual.

5.5 IS41 Services

This release introduces IS41 support for the ServiceRequest operation as defined in the 3GPP2 X.S0010-A v1.0 standard. The service is also compatible with the 3GPP2 MAP standards X.S0004-540-E v2.0 and X.S0004-550-E v2.0. Further details of the primitives and parameters associated with this service are available on request.

5.6 128 Hosts

The number of SIU hosts supported has been increased from 64 to 128.

5.7 M3UA Optional Routing Contexts

SIU configuration has been enhanced such that it is no longer mandatory to associate a routing context with a local or Remotes Application Server.

When bit 0 of the flags parameter associated with the STN_LAS command is set the configured routing context will be ignored and no routing context will be transmitted.

When bit 0 of the flags parameter associated with the STN_RAS command is set the configured routing context will be ignored and a routing context will not be required from a received remote application server in an activate message.

5.8 GTT Configuration

Additional MMI commands have been introduced to display SCCP Global Title configuration. These commands will display GTT Translations (**CNGTP**), GTT addresses (**CNGAP**) and GTT patterns (**CNGPP**).

Additionally, two aspects of Global Title Translation configuration have been corrected.

In previous versions the SIU would reject configurations which contained the "?" or "+" characters. These characters are used when specifying SCCP_GTT_PATTERN <gtai_pattern> parameter.

In previous releases the number of Global Title Address Information digits was artificially limited due to a buffer overflow condition.

5.9 GTT Load Share handling of Class 0 messages

Global Title Load Share Tables are supported on the SIU when configured via the SCCP message-based interface.

Global Title Load Share Tables use the User SCPPN_SEQ_CTRL parameter (or received SLS value) to determine the Load Share Table entry (point code) to use. The SCPPN_SEQ_CTRL parameter is only present for Class 1 messages so the module has been enhanced so that for non-Class 1 messages, the Load Share Tables use the message's SLS value. The SLS value for these messages is an incrementing value, updated each time a (non-Class 1) message is sent.

Operation using Class 1 messages is not affected by this change.

Note: It is recommended that Class 1 messages are used for Global Title Load Share Tables in order to preserve message sequence throughout a network whenever a dialogue may have more than one message sent in the same direction.

5.10 SCCP User in Service Indication

Prior to this release SCCP automatically sent a "user in service" indication at startup for all configured local subsystems. SCCP configuration has been enhanced to allow the user to disable automatic generation of "user in service" and allow applications to indicate when they are in service using a SCP_MSG_SCMG_REQ message.

The SCCP_CONFIG and SCCP_NC_CONFIG commands support a new parameter, <auto_uis>, on a per Network Context basis:

```
SCCP_CONFIG <local_spc> <ssf> <options> <auto_uis>

SCCP_NC_CONFIG <nc_id> <local_spc> <ssf> <options> <auto_uis>
```

The parameter supports the following values.

0. Do not automatically send "user in service" messages; local subsystems must send them.
1. Automatically sends a "user in service" message for all configured local subsystems

The parameter will default to 1 if not entered.

5.11 SCCP Sub-System Resource initialization state

SCCP configuration has been enhanced to allow users to specify the default presumed availability state at startup for remote signaling points and remote subsystems. Prior to this release both the RSP and RSS were assumed by SCCP to be available at startup.

When bit 3 of the <rsp_flags> in the SCCP_SSR RSP command is not set the the RSP is assumed at startup to be available. When the bit is set the RSP is assumed to be not available.

When bit 3 of the <rss_flags> in the SCCP_SSR RSS command is not set the the RSS is assumed at startup to be available. When the bit is set the RSS initial startup state will be derived from the state of the underlying RSP.

Note: Prior this release the SIU ignored values set by the <rss_flags> parameter when configuring remote subsystems (RSS) using the SCCP_SSR configuration command. As a consequence users were unable to specify that the SIU should assume that a remote subsystem is immediately available when it received an indication that the remote signaling point code had become available. This has been corrected and the SIU will now assume that the remote subsystem is available when the remote point code indicates it is available and the flag is set.

5.12 SCCP User generation of SCCP UDTS/XUDTS

In most situations where a UDTS/XUDTS message is required to be sent, it is automatically generated by SCCP on the SIU. In some situations it may be desirable for a received UDTS/XUDTS to be passed up to the user in a Notice indication and for this to be used to generate an onward UDTS/XUDTS to a further node. In order for a user to do this the SCCP module now supports generation of UDTS and XUDTS messages on demand. Further details on the user generation of SCCP UDTS/XUDTS messages are available on request.

5.13 ISUP Processing of CUG indicator

Bit 21 of the <options2> parameter in the **ISP_CFG_CCTGRP** command has been introduced to, when set, allow the reception of the CPG message in the forward direction.

6 Other Changes

6.1 Performance Optimization

A number of software enhancements have been implemented to enhance performance by exploiting the more fully the capability of the Multi-Core processors used within the SIU.

6.2 MTP2 Timer Defaults

The default values used for HSL MTP2 timers have been modified to ensure that they are suitable for use high speed operation.

MTP2 Timer	HSL
T1	300 s
T2	30 s
T3	1.2 s
T4N	30 s
T4E	500 ms
T5	100 ms
T6	5.5 s
T7	1.5 s

6.3 Default Management Host

The parameter DMHOST on the CNSYS command was introduced in V2.00 to allow users to specify a default management host other than host 0. On restart however the SIU reverted to host 0 as the default management host. This problem has been corrected and on restart the SIU will use the management hosts configured by DMHOST as the default management host.

6.4 Point Code Status

On startup, by default, the SIU MTP resilient layer assumes that the status of a Point Code is out of service. User parts or applications above may instead be configured to assume on startup that the Point Code is in service. Prior to this release if the SIU MTP resilient layer received an out of service indication for a Point Code it believed to be already out of service it discarded the receive status. Potentially therefore a user part could be left in an in service state even though the state is known by the SIU MTP resilient layer to be out of service. The SIU MTP resilient layer has been enhanced to generate the correct point code status whenever it receives an update from the network or its partner SIU even when it does not actually change state itself.

6.5 Parse Errors

Previously, when the system detected configuration for a feature or capability which had not been licensed the system reported parse error alarm ‘unacceptable command’ in the alarm list (ALLIP) output. This operation has been changed and the system now reports "Feature not licensed or inactive" in this circumstance.

Prior to this release if a line in config.txt file contained an illegal character or over length line the system would discard all subsequent lines in the config.txt file and additionally not provide an indication to the user that a problem had occurred. This operation has been changed and the system will now parse all lines in the config.txt and report “config.txt line discarded” for each failed line.

6.6 Dynamic MTP Link Addition / Removal

The ability to dynamically add and remove MTP links was introduced in V2.00 however a problem existed where the removal of a link did not result in the reduction in the count of license resources associated with the link. As a consequence the addition of subsequent links could result in the SIU rejecting the configuration incorrectly as exceeding the license limits. This has been corrected and license resources are now properly decremented when dynamically removing MTP links.

6.7 M3UA Configuration

Previously, a SIU operating in DUAL mode would only allow the configuration of a single Local Application Server within a Network Context. As each Remote Application Server on a SIU requires a 1:1 relationship with a Local Application Server an SIU in DUAL mode could only be configured to communicate with a single Remote Application Server. The check has been modified to allow multiple Local Application Servers within a Network Context provided that they share the same Originating Point Code

Prior to this release a SIU incorrectly formatted/interpreted M3UA messages transmitted/received with 24 bit or 16 bit point codes. This has been corrected and M3UA on the SIU now fully supports ANSI 24 bit and ITU 14, 16 and 24 bit point codes.

M3UA configuration on the SIU has also been modified to allow M3UA to be configured in Network Contexts other than Network Context 0. M3UA configuration remains limited to a single Network Context at a time.

Previously, options configured by the user on STN_ROUTE command were ignored with bit 1 (Route will load share between all Signaling Gateways in the route) internally being set by the SIU software. This behavior has been modified such that users will now be able to set bit 0 (Route is assumed to be available) of the options field. Bit 1 will continue to be set by the SIU software.

6.8 SS7HDP Diagnostics

Additional diagnostic information captured has been introduced so that in the unlikely event of a signaling processor failure on an SS7HDP board details of the cause will be logged to the built-in maintenance log file maint.log which is located in the syslog subdirectory of the siuftp account.

6.9 HSL on framed T1 interfaces

Prior to this release when an MTP HSL link was configured as T1_FRAMED the individual timeslots operated at 56 kbit/s rather than respecting the settings of the per-link flags. The software has been modified to respect the flags settings allowing correct operation for both 56kbit/s and 64kbit/s timeslots.

6.10 SCTP Associations

SCTP configuration has been modified to allow users to specify the SIUs IP address as the remote IP address when configuring M2PA SIGTRAN links. Users may find this useful in Lab scenarios when they wish to test applications above a single SIU running M2PA in a 'loop back' mode without the need for a network connection to another system. Looping back the SIGTRAN links will require the configuration two M2PA Sigtran links where the IP address is the IP address of the SIU and the hport of the first link is the pport of the second link and the hport of the second link is the pport of the first.

6.11 MAP RequestedInfo Parameter

For previous releases, when the MAPPN_req_info parameter was coded with more than one bit set, only a single bit was ever sent in the output message. This affected the ATI and PSI services. For this release, the parameter is correctly encoded into the output message when more than one bit is sent. Note: that on this release the number of valid bits for encoding for this parameter has increased.

6.12 MAP ATI service

Previous releases allowed some parameters to be sent but they would be discarded if received. The parameters affected were MAPPN_selectedlsa_id, MAPPN_msc_num, MAPPN_geodetic_info, MAPPN_currenr_loc_retrieved and MAPPN_sai_present in the ATI, PSI and SRI v3 services. These parameters can now be received correctly for the services.

6.13 MAP MAPPN_cell_id parameter

Previous code releases allowed the MAPPN_cell_id parameter have lengths between 5 and 7 octets. This is invalid according to TS29.002, the CellGlobalOrServiceAreaIdFixedLength variable should have a fixed length of 7 octets. This release forces the parameter to have a length of 7 octets.

6.14 MAP MAPPN_requestedequipinfo

The minimum size of this parameter has been altered from 2 to 1. This is in accordance with MAP spec 29.002. The maximum size remains at 8 for backwards compatibility

6.15 MAP Correction to reception of SendAuthInfo

For previous releases, Send-Authentication-Info v3 messages with no parameters where rejected by MAP when received from TCAP. This release corrects this behaviour; Send-Authentication-Info messages with no parameters are now accepted.

Note: that the IMSI and NumberOfRequestedVectors parameters for this service are normally Mandatory according to the specifications, however if the message is repeated the specifications state that the parameters can be excluded, thus a Send-Authentication-Info message with no parameters is valid.

6.16 TCAP User Part Configuration outside NC0

Prior to this release if a user wish to configure a TCAP user part (MAP, INAP, IS41) in the SIU using the SCCP_SSR command in a network context other than NC0 they were also required to provide a 'dummy' entry in NC0 for the protocol to operate correctly. This restriction has been removed.

6.17 DTS Configuration

To allow operation with more than 16 TCAP hosts a new command DTS_CONFIG has been added. The DTS_CONFIG command provides the ability to control the parameters of the DTS module.

The syntax of the command is:

DTS_CONFIG <max_instance> <reserved>

<max_instance> is the maximum number of TCAP hosts which will receive traffic from DTS.

<reserved> is reserved for future use and must be set to zero.

Dialogic
28-Sep-09
11-Nov-09 (Revised)

Release Notes for V2.00

1 Overview

This is the first software release since V1.02 and includes a number of enhancements and corrections as detailed below.

The SIU has been enhanced to realize a high-performance protocol monitor supporting up to 3 SS7HDP boards and transmitting data to multiple SIU hosts configurable on a per Monitor link basis.

This software also extends dynamic configuration on the SIU by allowing users to dynamically add or remove PCMs, MTP routes, SS7 signaling links, SS7 linksets and monitoring links. This enhancement allows users to introduce or modify particular signaling elements within a signaling server without impact to existing operation.

Support is introduced for built-in real-time logging to disk of events and errors on the SIU as well as selective logging to disk of diagnostic traces.

This release includes additional enhancements relating to increased SSR resources, SSR status reporting, large message support, management host configuration as well as extending the MAP and TCAP capabilities on the SIU .

Also included in this release are fixes relating to PCM alarm port mapping as well as a number of other management and protocol fixes.

These release notes should be read in conjunction with issue 8 of the Dialogic® DSI Signaling Servers SIU Mode User Manual

This release is backwards-compatible with previous versions.

1.1 Applicability

Users wishing to benefit from the increased capabilities or corrections introduced should consider upgrading to this release.

2 New Functionality

2.1 Monitoring

Utilizing the monitoring capabilities of the SS7HDP card the SIU has been enhanced to realize a high-performance protocol monitor supporting up to 3 signaling boards, each monitoring a licensable number of links. Data from the monitored links can be transmitted to applications operating on multiple SIU hosts that may be selected on a per Monitor link basis.

When used in a passive monitoring mode, the SS7HD board treats the signaling timeslot as an HDLC channel. When operating in monitoring mode, the 3rd and successive identical frames may be filtered. It is possible to configure both monitoring and terminated SS7 links on the same signaling card.

Monitor links may be configured using the new **MONITOR_LINK** configuration command with status and measurements being viewed using new **STMLP** and **MSMLP** commands.

A typical monitoring application requires that the monitoring E1/T1 must be configured as 'high-impedance' to avoid corruption of the signal on the line. High-impedance can be configured on the **LIU_CONFIG** command by setting the liu_type parameter to **6** for 'E1 high impedance' or **7** for 'T1 high impedance'.

Refer to the "Specification" section of the SIU user manual for details on the licensing of monitoring links and the "Configuration Guidelines" section for further information on the configuration and operation of monitoring on the SIU.

2.2 Dynamic Configuration

The SIU currently supports the ability to dynamically add MTP routes, Circuit Groups and SSRs as well as change circuit group configuration and remove circuit groups using the **CNURx** set of MMI commands.

This functionality is extended to support the dynamic additional and removal of MTP linksets, MTP routes, MTP links, LIUs and Monitor links allowing users to extend or modify their system configuration without the need for a system restart and without impact on existing configuration elements.

In support of this extension to dynamic configuration additional MMI commands have been introduced to display the current configuration of LIUs (**CNPCP**), MTP Linksets (**CNLSP**), MTP Links (**CNSLP**) and Monitor Links (**CNMLP**).

In the event of an incorrect entry in the config.txt file the CNURx commands have been extended to provide additional output to aid the user in indentifying the cause of a parse error.

Refer to the "Management Interface" section of the SIU user manual for full definitions of the commands and their use and the "Configuration Guidelines" section for further information on the operation of dynamic configuration within the SIU.

2.3 Message Logging

The SIU has been enhanced to provide built-in real-time logging to disk of events and errors as well as the selective logging to disk of diagnostic traces.

Logging to disk of events and errors by default allows a user to capture any management information at the point a failure occurs. Selective logging to disk of traces completes the capture of all the information that may be required to investigate particular issues.

Although activation of trace logging has a performance impact on a system, users who do not require the full performance capabilities of the SIU may choose to permanently activate selective tracing thus ensuring the full capture of any significant information required for problem analysis.

To activate selective tracing the user should first configure where they wish the trace messages to be logged using the **CNSYx** command **TRACELOG** parameter and then configure and activate the relevant trace mask using **CNTMx** commands. **TRACELOG**, by default, will be set to log trace messages to local **FILE**. The user can however modify **TRACELOG** configuration to either transmit the messages to the management module on the management **HOST** (as occurred on previous software versions) or to **DUAL** to log locally as well as transmit to the management host.

Events and errors will be logged to files of the name 'maint.log' in the syslog sub-directory of the siuftp account. These files will be limited to be a maximum size of 5MB with support being provided for up to 10 files. When the maint.log file reaches the 5MB limit, or the system is restarted, it will be renamed maint.log.1 and a new maint.log file will be created. If there is an existing maint.log.1 file that will be renamed maint.log.2. Other log files will consequently be renamed in a similar manner with the oldest file maint.log.9 being removed.

When configured, trace messages will be logged to files of the name 'trace.log' in the syslog sub-directory of the siuftp account. In the same manner as maintenance logs these files will be limited to be a maximum 5MB with support being provided for up to 10 files.

A new parameter, **RESET**, is supported on the **MNRSI** command. When set all log files in syslog will be removed from the server during restart. e.g.

```
MNRSI:RESET=Y;
```

Refer to the "Management Interface" section of the SIU user manual for further information on configuration and the "Diagnostics" section for further information regarding Diagnostics within the SIU.

2.4 SSR Status Reporting

A new command, STSSP, has been introduced to report the status of a SSR using MMI. Refer to the "Management Interface" section of the SIU user manual for further information.

2.5 SCCP Increased Sub System Resource support

The number of sub-systems resources, (SSR), has been increased from 256 per Network Context to 512 per Network Context.

2.6 Management Host Configuration

On startup a SIU host is selected by the server to be its primary management host. Prior to this release the host selected was always host 0. While users were able to modify which host was the primary manager by sending in an API_MSG_COMMAND message on subsequent restart the primary management host reverted back to host 0. A new parameter, **DMHOST**, has been introduced on the **CNSYx** MMI command to allow the user to configure which management host they wish to be the default primary management host. When set this host will immediately become the primary manage host and on restart the configured value will be preserved and this host will again be selected.

2.7 BICC/M3UA Long message support

M3UA and BICC have been enhanced to accept and output longer SIF length messages. This is necessary to support configurations which require a SIF length longer than the normal 272 octet limit.

A parameter**, <max_sif>**, has been introduced on the **ISUP_CONFIG** configuration command. While for normal ISUP operation max_sif should be set to 272 the parameter can be set to values of up to 4200 octets. The max_sif size is network dependant and for BICC operation a smaller value would normally be more appropriate value, e.g. 544 octets.

2.8 TCAP Dialog Ranges

The configuration of TCAP dialogue ranges has been enhanced by removing the restriction that had previously required the most significant bit to be set for incoming user dialogues. TCAP no longer inspects whether the most significant bit is set in the 'base_icdlg_id' parameter in the TCAP Configuration command (TCAP_CONFIG) and that all values for the configured outgoing range are less than 0x8000. This allows the full available dialogue range (0x0000 to 0xffff) to be allocated in any way between incoming and outgoing dialogues ranges.

The configured incoming and outgoing dialogue ranges can now start anywhere and be any size, except for the following restrictions:

- The incoming and outgoing ranges cannot overlap each other.
- Neither configured range should exceed the maximum possible dialogue number (0xffff).
- The incoming and outgoing range bases (base_ogdlg_id & base_icdlg_id) cannot be equal.
- The number of dialogues for both incoming and outgoing ranges cannot be set to zero, however it is possible to configure one of the ranges to have zero dialogues.
- The total number of dialogues for both incoming and outgoing ranges cannot exceed the maximum number of dialogues allowed by the module (normally 0xffff).

If any of the above conditions are not met the TCAP_CONFIG configuration will be rejected.

2.9 MAP AnyTimeModification service

This release adds support for a new MAP service AnyTimeModification. The new service is defined by the 3GPP TS 29.002 v8.2.0 specification. Details of the primitives and parameters associated with this service are provided in issue 12 of the MAP Programmer's Manual.

.

2.10 MAP Dialogue Status message

A new Message, **MAP_MSG_R_DLG_STATUS,** has been introduced to allow the user to query the MAP module to determine the current status of a dialogue. The application should send the message with the version number and all other fields in the parameter area set to zero.

The application sending the message should request that a confirmation message is returned by the MAP module after the message has been processed. This is achieved by setting the rsp_req field in the message header. This will cause a confirmation message of the same format to be returned. The status field in this message is zero on success or an error code otherwise.

MESSAGE HEADER	
FIELD NAME	**MEANING**
type	**MAP_MSG_R_DLG_STATUS** (0x67ef)
id	Dialogue id
src	Management module id
dst	**MAP_TASK_ID**
rsp_req	Sending layer's bit must be set
hclass	0
status	0
err_info	0
len	50

PARAMETER AREA		
OFFSET	**SIZE**	**NAME**
0	1	version - must be set to zero
1	1	Dialogue state (see table below)
2	2	tcap_dlg_id
4	1	dest_address length
5	18	dest_address
23	1	orig_address length
24	18	orig_address
42	2	num_invokes - number of active invokes in a dialogue
44	2	Network Context
46	1	Application Context Name
47	1	Application Version
48	2	reserved – must be set to zero

Dialogue State

Dialogue State Values	
Value	**Description**
0	Idle.
1	Waiting for initial data.
2	Waiting for user requests.
3	Dialogue initiated.
4	Dialogue pending.
5	Dialogue accepted.
6	Dialogue established.
7	First process components state.
8	Wait for component.
9	Waiting for components and have already received an open response state.
10	Dialogue terminating.
11	Components received during AC negotiation.

2.11 MAP Send-Authentication Mandatory Parameters for V3

According to the specifications, it is possible to resend this operation without parameters. This was not possible with mandatory parameters MAPPN_imsi and MAPPN_nb_req_vect. These parameters have now been made optional.

2.12 MAP_MSG_NC_CONFIG Tracing

Tracing has now been enabled for the MAP Network Context Configuration message MAP_MSG_NC_CONFIG. Users can enable tracing of this message by activating tracing of MAP using the CNTMS command and setting bit 7 of the MMASK parameter.

2.13 M3UA ANSI_24 routing label with 8-bit SLS

M3UA previously only supported 5-bit SLS values when using the ANSI_24 routing label. The SIU now also supports ANSI_24 routing label with 8-bit SLS. No specific configuration changes are required.

2.14 M3UA SLS bit rotation

SLS bit rotation is a method of load sharing in networks. It is disabled by default. It can be enabled by setting bit 0 in the flags field of the STN_NC configuration command.

2.15 Route-Server availability

This release includes functionality to allow M3UA to configure routes via specific servers that are considered available as soon as the Signalling Gateway is available without waiting for the reception of a DAVA.

This functionality is enabled on a per-Route/Server combination using bit 0 of a new **<flags>** parameter on the **STN_RSGLIST** command.

When set M3UA will consider the route via the specified server to be available without performing a destination audit.

Refer to the "Configuration" section of the SIU user manual for a full revised definition of the STN_RSGLIST command.

3 Other Changes

3.1 PCM LIU Alarm forwarding

The SIU is capable of receiving alarms on a network facing LIU and mapping them through to a secondary 'slave' LIU. A problem has been corrected and alarms are correctly mapped through to the secondary alarm port.

3.2 STDHP

Prior to this release the **STDHP** command incorrectly reported the status for SSNs in Network Contexts other than NC0. The command now correctly reflects the status of hosts according to the routing configured for DTS. Refer to the "Management Interface" section of the SIU user manual for a revised definition on the **STHDP** command.

3.3 SIU Configuration

The SIU will now explicitly reject **MTP_LINK** configuration commands where either the stream has not been previously configured or the timeslot has been previously assigned to another **MTP_LINK**.

Prior to this release the SIU would not allow the user to configure MTP links where the signaling timeslot was on a different board from the blink. This has been corrected.

3.4 ISUP – Processing of CUG indicator

Bit 20 of the <options2> parameter in the **ISP_CFG_CCTGRP** command enables automatic release of the incoming call if the CUG indicator from the Optional Forward Call indicators indicated 'closed user group call, outgoing call access not allowed'. It was identified that this also automatically released incoming calls when the CUG indicator indicated 'outgoing access allowed'. This behavior has now been corrected.

3.5 ISUP – Duplicated parameter in the IAM

In previous releases when transmitted the Called IN Number parameter was duplicated in the IAM message sent to the user application. The duplication has been removed.

3.6 ISUP – Handling of REL and RLC from the user

Under certain conditions ISUP could send a REL followed by a RLC message to the network. This has been corrected.

3.7 MTP Route Modification & Loadsharing

When a Route is modified, the logic used to establish which linksets are loadshared over is different to when links are first configured. If linksets with more than eight links are used and only 4 sls bits are available then only the first linkset is used.

Prior to this release the distribution of traffic over linksets had the potential to unexpectedly change due to overload resulting in message loss.

3.8 MTP Default Route Failure

Prior to this release, when a Transfer Request was sent using a default MTP route processing of the message could potentially fail and result in a restart of the Signaling Server. This is now resolved.

3.9 MAP Software Event during AC negotiation.

When a dialogue is received by MAP but the application context is not supported, the dialogue is aborted and, if possible, an alternative application context name is included in the U-ABORT. If a component follows the BEGIN, there will be no dialogue in existence when the component is received by MAP (since the dialogue has been aborted) so a Software Event (invalid dialogue ID) will be reported. MAP will now no longer report this Software Event.

3.10 MAP Send Routing Info Correction

In the previous releases the ASN.1 table used for Send-Routing-Info for v1/v2 was incorrectly encoded in regards the MAPPN_net_sig_info parameter. This has been corrected. The encoding of the v3 was already correct is not affected.

3.11 MAP Check IMEI v3 correction

A change has been made to the MAPPN_requestedequipinfo parameter to allow the permitted size to range between 2 and 8 octets. (Previously the permitted length of this parameter was fixed at 1 octet).

3.12 MAPPN_fwd_to_num and MAPPN_no_reply_condition_time parameter enhancements

The parameter MAPPN_fwd_to_num has been expanded to allow use of AddressString parameters with a range of 1 to 20 octets as specified by TS 29.002. Previously the parameter allowed only ISDNString parameters with a range of 1 to 9 octets.

The parameter MAPPN_no_reply_condition_time has been expanded to allow use of Ext-NoReplyConditionTime parameters (1 to 100) as well as original NoReplyConditionTime parametes (5 to 30).

3.13 DTS - SCCP Notice Indications

DTS in previous releases incorrectly treated SCCP Notice indications as SCCP Unitdata indications leading to incorrect transaction information being used. This could result in some messages being returned to the wrong host. This release corrects the handling to ensure these Notice indications go the correct host.

Dialogic
13-Jan-09
16-Jul-09 (Revised)

Release Notes for V1.02

1 Overview

This release includes new functionality aimed at call control deployments where the voice circuits are received from the network and passed through the SIU to an external media processing board. It provides the ability for PCM alarms received from the network to be passed on to the remote media board.

The release also includes enhanced support in for German ISUP parameters and includes other changes as detailed below.

This release is backwards-compatible with previous release.

2 New Functionality

2.1 PCM LIU Alarm forwarding

The ability to map PCM alarm condition from a network facing LIU across to a secondary (or slave) LIU has been added. This is useful in situations 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 automatically generate AIS on the slave LIU.

The LIU_CONFIG configuration command has been extended to allow configuration of a slave LIU. The full command syntax is as follows:

```
LIU_CONFIG <port_id> <pcm> <liu_type> <line_code> <frame_format>
           <crc_mode> <syncpri> <build_out> <slave_port_id>
           <flags>
```

The meaning of the three fields in bold text are as follows:

<build_out> - For SS7HD boards this specifies the range of "build out" settings for a T1 interface as documented in the SIU User Manual. For SPCI4 boards the field is reserved and must be set to zero.

<slave_port_id> - Logically identifies the slave PCM port in the SIU range. The port_id should be unique within the system, in the range 0 to 11 and be a port that has already been defined in a preceding LIU_CONFIG command.

<flags> - A 16-bit value used to configure run-time configuration options. Bit 0 is used as detailed in the following table:

Table 1. Run time options

Bit	Parameter
0	No slave port. Value in <slave_port_id> parameter position will be ignored.

1	<slave_port_id> contains ID of an LIU to be considered a slave to the LIU being defined by the statement.

2.2 ISUP – Auto reject CUG calls

A new per-circuit group option, bit 20, has been added to the <options2> parameter in the ISP_CFG_CCTGRP command.

If enabled incoming calls will be released with release cause #29 (0x1d) when the Closed User Group Call indicator from the Optional Forward Call indicators indicates 'closed user group call, outgoing call access not allowed'.

2.3 ISUP – Enhanced support for German ISUP

The release extends support for German ISUP parameters. When the German ISUP variant (3) is selected for a circuit group, the following additional parameters are supported in the IAM message between the network and user application:

Table 2. ITU Parameters

Code	**Parameter**
0x6e	Call diversion treatment indicators
0x70	Call offering treatment indicators
0x6f	Called IN number
0x72	Conference treatment indicators
0x4b	CCSS
0x7a	CCNR
0x73	Display information

The following German ISUP specific parameters are also supported:

Table 3. German specific ISUP parameters

Parameter Name	Parameter Value				Mandatory /Optional Parameter	Length		Message used
	German ISUP		API					
	Hex	Dec	Hex	Dec		Min	Max	
NP.FF	0xff	255	0x1f8	504	Optional	1	1	IAM
NP.SSP	0xf5	245	0x1f9	505	Optional	1	2	IAM
NP.UKK	0xfc	252	0x1fa	506	Optional	1	3	IAM

2.4 SS7HD board failure fault codes.

This release provides additional diagnostic information in the event of a board failure. This functionality is supported only for SS7HD boards.

Should a board failure occur, a fault code is displayed in the output of the ALLIP command. The same fault code is also sent to the management host in the status field of a MGT_MSG_EVENT_IND message.

Table 4. SS7HD board failure fault codes

Fault Code	Description
0xd0	Board hardware failure
0xd1	Board HBI error
0xd2	Board messaging failure
0xd3	Board Signalling Processor failure
0xd4	Board CPU exception
0xd5	Board POST failure
0xd6	Board watchdog timeout

3 Other Changes

3.1 ISUP – Handling of RLC from user application

If it is determined that an incoming call must be released, for example because the user to user service requests are not supported in the IAM, and the user application returns a RLC message in response to the release from ISUP, the RLC message is not conveyed to the network, but is replaced with a REL message containing an appropriate cause value. In previous releases the RLC from the user was conveyed to the network.

3.2 ISUP - Formatting of the INR message

A new per-circuit group option, bit 19, has been added to the <options2> parameter in the ISP_CFG_CCTGRP command.

The default behaviour of ISUP is to add an End of Optional Parameters octet to the end of messages (that may contain optional parameters) when no optional parameters are present. Setting bit 19 will cause ITU INR messages containing no optional parameters to be transmitted to the network without the End of Optional Parameters octet. This option only applies to ITU INR messages and should only be enabled for ISUP variants where no optional parameters are permitted in the message.

3.3 MTP3 – Timer default values

Default values for the following MTP3 timers have been modified to fall within ITU/ANSI recommended ranges as detailed:

Table 5. MTP3 – Timer default values

MTP3 Timer	Previous Default Value	New Default Value
ITU T14	3 seconds	2.5 seconds
ITU T15	3 seconds	2.5 seconds
ANSI T20	270 seconds	105 seconds
ANSI T21	270 seconds	105 seconds

3.4 TCAP - Zero sized Dialogue Group ranges

Previous releases could fail configuration if the value of <nog_dialogues> parameter or <nic_dialogues> parameter in TCAP_CFG_DGRP statement was set to zero. TCAP in this release now permits Dialog Group(s) to be defined with either <nog_dialogues> or <nic_dialogues> having a zero value.

3.5 TCAP - Active dialogue count in STTRP output

In previous releases the Status Transaction Print command, STTRP, did not account for active incoming dialogues allocated to dialogue groups in the displayed ICD field. This has been addressed such that the ICD field displays the total number of active incoming dialogues including those allocated to dialogue groups.

Dialogic
05-Nov-08

Release Notes for V1.01

4 Overview

This maintenance software release removes the need for a M2PA license when configuring M2PA SIU interlinks and allows users of the SS7SBG30M2PAJ link license to configure up to the maximum number of M2PA network facing links. This release also includes a number of updates to improve the security of the system.

This release is backwards-compatible with previous versions.

5 Changed Functionality

5.1 M2PA

Prior to this release M2PA Inter-SIU links required a M2PA license to operate. M2PA Inter-SIU links can now be used without an M2PA license. Using M2PA Inter-SIU links now does not affect the number of licenced links available for network-facing M2PA Links.

A correction to the STSLP command has been made to allow the reporting of status for M2PA Inter SIU links.

Previously the SS7SBG30M2PAJ license only supported the configuration of 128 M2PA links. This error has been addressed and the license will now support the configuration of up to 256 M2PA links.

5.2 Security Updates

A number of additions have been made to improve the security related to common TCP/IP attacks and also to protect the operating system from keyboard access.

Dialogic
12-Sep-08

Release Notes for V1.00

1 Overview

This is the first full release of software for the Dialogic® DSI SS7G31 and SS7G32 Signaling Servers. The DSI SS7G31 is a 1U form factor Signaling Server supporting a single SS7 signaling board and the DSI SS7G32 is a 2U form factor Signaling Server supporting up to three SS7 signaling boards. The SS7G32 is a form fit and function replacement for the existing SS7G2x range of signaling servers with a number of additional capabilities as detailed below whilst the SS7G31 offers the same functionality in a smaller form factor.

The SS7G31 and SS7G32 both support SIU (Signaling Interface Unit) and SGW (Sigtran Signaling Gateway) operating modes. Users should refer to the full documentation set for the product range which comprises:

- Dialogic® DSI Signaling Servers SIU Mode User Manual
- Dialogic® DSI Signaling Servers SGW Mode User Manual
- Dialogic® DSI SS7G31 and SS7G32 Signaling Servers Hardware Manual
- Dialogic® DSI Signaling Servers – SNMP User Manual

These release notes relate to the SIU Mode of operation. They highlight the key differences between the existing SS7G2x product (running V5.11 software) and the SS7G3x software.

2 Key Differences between SS7G2x and SS7G3x

2.1 RAID

Each SS7G31 and SS7G32 is supplied complete with dual Hard Disk Disk drives operating in a RAID configuration. This allows operation to be maintained even in the event of a disk failure. The SS7G32 allows faulty disks to be swapped without impact on operation whilst the SS7G31 requires the unit to be powered down to replace a faulty disk drive. Full operation of RAID is detailed in the User Manual.

2.2 Capacity

The maximum capacity of the SS7G32 is 192 SS7 MTP2 Low Speed Links (LSL) and up to 6 High Speed Links (HSL) or 256 M2PA links. The actual capacity depends on the number of SS7 boards, the board type and the software license fitted.

The maximum number of MTP routes supported is 4096.

The maximum M3UA capacity is 256 M3UA links, 256 Remote Application Servers and 256 M3UA Routes The actual capacity depends on the software license fitted.

2.3 Licensing

The SS7G3x uses a different licensing model to the SS7G2x. The MTP3, ISUP, SCCP and SNMP licensing capability is combined into four different SIU mode licenses offering different levels of capacity. Consequently it is not necessary to purchase separate SCCP, ISUP or SNMP licenses.

Additional licenses are required for M3UA and M2PA when operating in SIU Mode. The M3UA and M2PA licenses offer different densities and throughput capacity.

TCAP, MAP, INAP and IS41 protocols are licenced in the same manner (although with a new license) to the SS7G2x.

For a full list of licenses supported by the SS7G3x for SIU operation as well as detailed descriptions of their capabilities see the User Manual.

2.4 TEST Mode

The SS7G3x ships without software licenses installed. To facilitate loading of software licenses, the unit powers up in a new TEST mode. TEST mode's principal purpose is to provide sufficient software functionality to allow the addition of either an SIU Mode license or an SGW Mode license as well as any other protocol licenses required. Once the licenses have been copied onto the unit (following the procedure defined in the User Manual) the unit should be restarted using the following command:

```
MNRSI:RESTART=SOFT,SYSTYPE=SIU;
```

TEST mode may also be used to validate basic operation of the Signaling Server hardware prior to deployment. TEST mode will allow the activation of up to 12 SS7 links following the configuration procedures described in the User Manual. TEST mode is not intended for operational use and will not run protocols above MTP.

2.5 Ethernet Configuration

The SS7G31 supports 4 Gigabit Ethernet Ports whilst the SS7G32 supports up to Six Gigabit Ethernet Ports ports.

To allow for the increase in the Ethernet capabilities of the SS7G32 the configuration of local IP addresses have been migrated from the CNSYx command to the IPEPx command where an IP address can be configured on a per-Ethernet port basis.

In a similar manner to the CNSYx command a user can use the IPEPx command to configure up to 2 bonded active/standby Ethernet Ports pairs for resilience on the SS7G31 and up to 3 bonded pairs on the SS7G32.

Activation of SCTP on a particular Ethernet port is now configurable using the SCTP parameter on the IPEPx command. Up to 2 Ethernet Ports may be configured for SCTP use.

Configuration of the default gateway has been migrated to the IPGWx command so that all IP gateways can be managed from within the same command. The default IP gateway can be specified using the IPGWx command by setting the IPGW to DEFAULT and GATEWAY to the default gateway's IP address.

2.6 Configuration and License Backup

The ability to backup licenses and configuration for the SS7G2x was provided using the built-in CD-ROM drive. The SS7G3x products do not have a CD-ROM drive but have a USB port allowing backup of licences and configuration data to an industry standard USB pen drive.

2.7 Diagnostic Software

This release includes support for the generation of an additional diagnostic log file, restart_disk.log. The restart_disk.log text file along with the existing diagnostic files restart_gct.log, restart_top.log, restart_ip.log and restart_sensor.log can be recovered from the syslog directory using FTP as detailed below:

```
ftp 123.123.123.123
user siuftp
password siuftp (or the ftppwd as set by the CNSYS command)
cd syslog
ascii
get restart_gct.log
get restart_top.log
get restart_sensor.log
get restart_ip.log
get restart_disk.log
bye
```

Dialogic
12-Aug-08