Dialogic

Dialogic® Converged Services Platform Release 8.4.1 Engineering Release 3

Changes from Previous Release

February 2008

Copyright and Legal Disclaimer

All contents of this document are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries. Reasonable effort is made to ensure the accuracy of the information contained in the document. However, due to ongoing product improvements and revisions, Dialogic Corporation and its subsidiaries do not warrant the accuracy of this information and cannot accept responsibility for errors or omissions that may be contained in this document.

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

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

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic Corporation or its subsidiaries may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic Corporation or its subsidiaries do not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic Corporation or its subsidiaries. More detailed information about such intellectual property is available from Dialogic Corporation's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. The software referred to in this document is provided under a Software License Agreement. Refer to the Software License Agreement for complete details governing the use of the software.

Dialogic Corporation encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.

Dialogic, Dialogic Pro, Brooktrout, Cantata, SnowShore, Eicon, Eicon Networks, Eiconcard, Diva, SIPcontrol, Diva ISDN, TruFax, Realblocs, Realcomm 100, NetAccess, Instant ISDN, TRXStream, Exnet, Exnet Connect, EXS, ExchangePlus VSE, Switchkit, N20, Powering The Service-Ready

Dialogic Product Line Warranty

Unless otherwise stated in an applicable product purchase agreement between the Customer and Dialogic, Dialogic warrants that during the Warranty Period, products will operate in substantial conformance with Dialogic's standard published documentation accompanying the product. If a product does not operate in accordance therewith during the Warranty Period, the Customer must promptly notify Dialogic. Dialogic, at its option, will either repair or replace the product without charge. The Customer has the right, as their exclusive remedy, to return the product for a refund of purchase price or license fee if Dialogic is unable to repair or replace it.

Warranty Period

In the event that you have no signed agreement setting out a warranty period, the Warranty Period shall be the standard warranty period set out on www.dialogic.com on the date of your purchase of the product.

The Warranty Period begins on the date of shipment of any products or software by Dialogic.

The Warranty Period for repaired, replaced or corrected products and software shall be coterminous to the Warranty Provided for the original products or software purchased.

To report warranty claims, Customer may contact Dialogic via email at techsupport@cantata.com or call (781) 433-9600.

Warranty Provisions

A. During the Warranty Period, Dialogic warrants to Customer only that:

(i) Products manufactured by Dialogic (including those manufactured for Dialogic by an original equipment manufacturer) will be free from defects in material and workmanship and will substantially conform to specifications for such products;

(ii) software developed by Dialogic will be free from defects which materially affect performance in accordance with the specifications for such software. With respect to products or software or partial assembly of products furnished by Dialogic but not manufactured by Dialogic, Dialogic hereby assigns to Customer, to the extent permitted, the warranties given to Dialogic by its vendors of such items.

B. If, under normal and proper use, a defect or non conformity appears in warranted products or software during the applicable Warranty Period and Customer promptly notifies Dialogic in writing during the applicable warranty period of such defect or non conformance, and follows Dialogic's instructions regarding return of such defective or non conforming Product or Software, then Dialogic will, at no charge to Customer, either:

(i) repair, replace or correct the same at its manufacturing or repair facility or

(ii) if Dialogic determines that it is unable or impractical to repair, replace or correct the product or software, provide a refund or credit not to exceed the original purchase price or license fee.

C. No product or software will be accepted for repair or replacement without the written authorization of and in accordance with instructions from Dialogic. Removal and reinstallation expenses as well as transportation expenses associated with returning such product or software to Dialogic shall be borne by Customer. Dialogic shall pay the costs of transportation of the repaired or replaced product or software to the destination designated in the original Order. If Dialogic determines that any returned product or software is not defective, Customer shall pay Dialogic's costs of handling, inspecting, testing and transportation. In repairing or replacing any product, part of product, or software medium under this warranty, Dialogic may use new, remanufactured, reconditioned, refurbished or functionally equivalent products, parts or software media. Replaced products or parts shall become Dialogic's property.

D. Dialogic makes no warranty with respect to defective conditions or non conformities resulting from any of the following: Customer's modifications, misuse, neglect, accident or abuse; improper wiring, repairing, splicing, alteration, installation, storage or maintenance performed in a manner not in accordance with Dialogic's or its vendor's specifications, or operating instructions; failure of Customer to apply Dialogic's previously applicable modifications or corrections; or items not manufactured by Dialogic or purchased by Dialogic pursuant to its procurement specifications. Dialogic makes no warranty with respect to products which have had their serial numbers removed or altered; with respect to expendable items, including, without limitation, fuses, light bulbs, motor brushes and the like; or with respect to defects related to Customer's data base errors. Improper packaging of product for repair will not be covered under this warranty agreement. No warranty is made that software will run uninterrupted or error free.

E. Warranty does not include:

a) Dialogic's assistance in diagnostic efforts;

b) access to Dialogic's Technical Support web sites, databases or tools;

c) product integration testing;

d) on-site assistance; or

e) product documentation updates.

These services are available either during or after warranty at Dialogic's published prices.

F. THE FOREGOING WARRANTIES ARE EXCLUSIVE & ARE GRANTED IN LIEU OF ALL OTHER EXPRESS & IMPLIED WARRANTIES (WHETHER WRITTEN, ORAL, STATUTORY OR OTHERWISE), INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND DIALOGIC'S SOLE OBLIGATION HEREUNDER, SHALL BE TO REPAIR, REPLACE, CREDIT OR REFUND AS SET FORTH ABOVE.

G. IN NO EVENT SHALL DIALOGIC, ITS DIRECTORS, OFFICERS, EMPLOYEES, AGENTS OR AFFILIATES, BE LIABLE FOR ANY COSTS OR DAMAGES ARISING DIRECTLY OR INDIRECTLY FROM YOUR USE OF ANY PRODUCT INCLUDING ANY INDIRECT,

INCIDENTAL, SPECIAL, EXEMPLARY, MULTIPLE, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLEGENCE), STRICT LIABILITY OR OTHER LEGAL THEORY, EVEN IF DIALOGIC, OR ANY OF ITS DIRECTORS, OFFICERS, EMPLOYEES, AGENTS OR AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY EVENT, DIALOGIC'S CUMULATIVE LIABILITY TO YOU FOR ANY AND ALL CLAIMS RELATING TO THE USE OF ANY PRODUCT SHALL NOT EXCEED THE TOTAL AMOUNT OF THE PURCHASE PRICE OR LICENSE FEES PAID TO DIALOGIC FOR SUCH PRODUCT.

H. CUSTOMER AND DIALOGIC HEREBY WAIVE THEIR RIGHT TO TRIAL BY JURY TO THE FULLEST EXTENT PERMITTED BY LAW IN CONNECTION WITH ALL CLAIMS ARISING OUT OF OR RELATED TO THIS WARRANTY, THE PRODUCTS COVERED HEREBY OR THE PERFORMANCE OF ANY PARTY HEREUNDER.

I. THIS WARRANTY SHALL BE CONSTRUED UNDER AND GOVERNED BY THE LAWS OF THE COMMONWEALTH OF MASSACHUSETTS WITHOUT GIVING EFFECT TO ANY CHOICE OR CONFLICT OF LAW PROVISION OR RULE (WHETHER OF THE COMMONWEALTH OF MASSACHUSETTS OR ANY OTHER JURISDICTION) THAT WOULD CAUSE THE APPLICATION OF THE LAWS OF ANY JURISDICTION OTHER THAN THE COMMONWEALTH OF MASSACHUSETTS. CUSTOMER SPECIFICALLY AND IRREVOCABLY CONSENTS TO THE PERSONAL AND SUBJECT MATTER JURISDICTION AND VENUE OF THE FEDERAL AND STATE COURTS OF THE COMMONWEALTH OF MASSACHUSETTS AND SUCH COURTS SHALL HAVE EXCLUSIVE JURISDICTION WITH RESPECT TO ALL MATTERS CONCERNING THIS WARRANTY OR THE ENFORCEMENT OF ANY OF THE FOREGOING.

J. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

About this Publication

Purpose

This publication provides guidelines for using the Dialogic® CSP.

Safety Labels

The following Safety labels may appear in this information product to alert customers to avoidable hazards. The following are in the order of priority:

DANGER

Danger indicates the presence of a hazard that will cause death or severe personal injury if the hazard is not avoided.

WARNING

Warning indicates the presence of a hazard that can cause death or severe personal injury if the hazard is not avoided.

CAUTION

Caution indicates the presence of a hazard that will or can cause minor personal injury or property damage if the hazard is not avoided. Caution can also indicate the possibility of data loss, loss of service, or that an application will fail.

Conventions used

This information product uses the text conventions explained below. In addition, hexadecimal numbers are preceded by a zero and small “x.” For example, the decimal number 15 is represented in hexadecimal as 0x0F.

Convention	Description
. . .	A horizontal ellipsis in an API message indicates fields of variable length.
:	A vertical ellipsis in an API message indicates that a block of information is repeated or is variable.
n	The letter *n* is a generic placeholder for a number.
`Sans serif mono space`	Indicates a command name, option, input, output, non-GUI error, and system messages.
`Sans serif monospace italic`	Indicates a parameter name in an input message. Example: `move *.dot a: c:` *`-s`* The *`-s`* is the parameter.
Serif italic	Indicates the name of a book, chapter, path, file, or API message. Example: *`UserDirectory/Config.exe`*
Boldface	Indicates keyboard keys, key combinations, and command buttons Example: **Ctrl+Alt+Del**
Sans serif boldface	Identifies text that is part of a graphical user interface (GUI). Example: Go to the **Configuration** menu and select **Card**->**Span Configuration**

Contents

Copyright and Legal Disclaimer i-1
Dialogic Product Line Warranty i-3

1 Changes from Previous Releases

Licensing 1-2

Changes in Release 8.4.1 Controlled Introduction

Voice over IP (VoIP) Enhancements 1-4
SS7 Enhancements 1-13
DSP Enhancements 1-15
General Platform Enhancement 1-17

Changes in Release 8.4.1 Engineering Release 2

DSP Enhancements 1-24
CCS Enhancements 1-25
VoIP Enhancements 1-26

Changes in Release 8.4.1 Engineering Release 3

VoIP Enhancements 1-32
Digital Signaling Processing Enhancements 1-34

1 Changes from Previous Releases

Overview

Purpose This chapter summarizes the changes in the following releases:

- *Changes in Release 8.4.1 Controlled Introduction (1-3)*
- *Changes in Release 8.4.1 Engineering Release 2 (1-23)*
- *Changes in Release 8.4.1 Engineering Release 3 (1-31)*

Important! Be sure to read the next section on Licensing before installing Release 8.4.1 software.

Licensing

Release 8.4.1 does not have any new licensing requirements.

Important! DSP Series 2 card and the DSP Series 2 Plus card have the same licensing.

Changes in Release 8.4.1 Controlled Introduction

Voice over IP (VoIP) Enhancements

FR219 - PRACK Support

The CSP supports four provisional responses:

- 100 Trying
- 180 Ringing
- 182 Queued Message
- 183 Session Progress

You can enable the CSP to support the Provisional Response ACK (PRACK) method to send non 100 provisional responses more reliably over User Datagram Protocol (UDP). This feature is disabled by default.

Important Points Regarding this Feature

The following are the details of this feature:

- The Offer/Answer model for PRACK (section 5 of RFC 3262) is not supported.
- The Support/Require mode for PRACK is at the stack level and not on a call-by-call basis.
- The CSP now supports the Provisional Response method to send non 100 provisional over User Datagram Protocol (UDP)
- There is not indication about the presence/absence of “100rel” tag in the “Supported/Require” header to the host in the RFS, PPL EI for 180Ringing or PPL EI for 183 Session progress for the following respectively:
  - Received INVITE
  - 180 Ringing
  - 183 Session Progress
- The RFC 3262 states the following: “The UAS sending the response reliably should send provisional responses once every two and a half minutes.” The SIP stack supports this standard for the 182 Queued message.

FR351 - Support for SIP INFO Message

Prior to this feature the CSP SIP stack could not generate an INFO message nor could it report an inbound INFO message.

With this feature, the SIP stack can generate the INFO message by the host and report the receipt of an INFO message to the host.

The INFO message will also supports the Subject header with read and write access.

The INFO method carries the session related control information that is generated during a session. ISUP and ISDN signaling messages used to control telephony call services are examples of session control information.

By default, inbound SIP INFO messages are not reported to the host.

This feature is supported by call agent and non-call agent calls.

FR554 - Outbound SIP Call with Call Agent Mode

Dynamic Switching Media Streams

Call Agent Mode (CAM) in the CSP provides dynamic switching of media streams on or off the CSP RTP channels with a minimal amount of SIP messages.

Inbound Calls

Prior to this feature, the CSP supported bearer on/off switching of Call Agent Mode for inbound calls only. The CSP can connect the inbound leg of a SIP call to a TDM network or to a DSP media service.

This functionality allows the caller to be connected to an operator in a PSTN network. It also allows the application of DSP services such as playing announcements to the calling (inbound) leg.

Bearer switching is based on a coupling and decoupling mechanism. Coupling associates a physical timeslot with a virtual timeslot to enable bearer-switched service. Decoupling dissociates a physical timeslot from a virtual timeslot to enable bearer-free switched service.

The bearer switching takes place whenever required with minimal interaction from the host.

Outbound Calls - New

With this feature, the CSP has the bearer on/off switching capability for outbound call legs too.

This capability is needed when the media services in the CSP (like DSP-2 card) or media transit path (like external TDM IVR or operator) is required for the called party.

A directory assistance operator is located behind a TDM switch. The initial conversation between the operator and called party is bearer-switched through the CSP. Later, the operator drops out of the call flow while connecting the calling party and the called party bypassing the bearer path from the CSP.

FR620 - Via Heading Reporting

This feature reports to the host the IP address and Port Number of the top most Via header field of the inbound SIP sessions. The information in the Via header could be of the last gateway or router to handle the call.

- The host can route the outbound SIP session based on the reported Via headers.
- The Via head is reported for the session-establishing the INVITE. It is not reported for session-modifying INVITEs (Re-INVITES).
- Only hostnames with length up to 80 bytes are reported. If an INVITE message with hostname length greater than 80 bytes is obtained then the SIP Header Field TLV (0x299C) itself will not be reported. But the other TLVs, SIP Header Field Container and SIP Header Field will be reported.
- If port number is absent or if it is NULL then the SIP Port Number TLV will not be reported.
- If port number is equal to or greater than 2147483647 then it will be reported as 7f ff ff ff.

This feature is configurable and is turned off by default.

FR626 - SIP Offer Answer for Delayed Media in Call Agent Mode

This feature enables the SIP Offer/Answer model for delayed media in Call Agent mode.

Prior to this feature, the CSP supported the Offer/Answer model for normal call scenarios as follows:

- The User Agent Client (UAC) made an offer in the initial INVITE message.
- The User Agent Server (UAS) generates the Answer in the 200 OK message.

In a delayed-media scenario, the roles of the UAS and UAC reverses from the normal scenario above. The UAS generates the first offer and the UAC generates the answer. The CSP now can accept and generate delayed media calls in bearer free mode.

FR627 - SIP Population of Status in Outbound NOTIFY Message

The SIP stack allows the CSP to send multiple NOTIFY messages.

The NOTIFY message follows a REFER message. If the reference is pending, then the host sends a PPL Event Request for NOTIFY with response class 1xx.

Similarly, the host sends response class 2xx if the reference was successful and 5xx or 6xx in the cases where the reference failed.

If the first PPL Event Request for the NOTIFY message has a 1xx response status, then the CSP checks for more PPL Event Request for NOTIFY messages from the host.

The CSP accepts and processes PPL Event Request for the NOTIFY message until it gets a PPL Event Request for the NOTIFY message with a final response status (2xx-6xx). Any subsequent PPL Event Request for the NOTIFY message after that will be nacked. The host can send any number of PPL Event Requests for the NOTIFY message with a 1xx response status before sending a final response.

FR666 - Refer-To Header Parameter Access

REFER is a SIP method defined by RFC 3261. The REFER method indicates that the recipient (identified by the Request -URI) should contact a third party using the contact information provided in the request.

The Refer-To is a request header field (request header) as defined by RFC 3515. It appears only in a REFER request. It provides a URL to reference.

The SIP stack in the CSP has the capability for inbound and outbound refer requests.

In addition to the Refer-To Parameters, the username, host name, and passwords are reported in a *PPL Event Indication* message for a Consultative REFER.

Prior to this feature, the SIP stack already supported the reporting of the username, host name, and passwords for a Blind REFER.

FR667 - PPL Event Request for RE-INVITE Message

This feature allows the CSP to support the RE-INVITE message for a Call Agent Mode call in bearer-free mode using a new PPL Event Request (0x0024). This PPL Event Request generates a Re-INVITE regardless of the call direction: incoming or outgoing.

FR669 - PPL Event Request for RE-INVITE

This feature allows the CSP to support the RE-INVITE message for a Call Agent Mode call in bearer-free mode using PPL Event Request (0x0024). This PPL Event Request generates a Re-INVITE regardless of the call direction: incoming or outgoing.

This PPL Event Request will work only if the call is in bearer-free mode or else it will NACK with a value 0x130C (Call is not in bearer-free mode.)

FR671 - SIP Subject Header in REFER

The Subject Header field is now an optional header in the REFER message. This feature allows read and write access for the Subject Header field in the REFER message.

Read access is allows the host to receive the content of the Subject Header field, if it is present in the inbound REFER message. You can configure whether or not to report the Subject Header field.

Write access allows the host to fill into the Subject Header field of the outbound REFER message. This functionality is available for Call Agent and non-Call Agent calls.

FR735 - SIP Display Name Parameter in From Header

This feature allows access to display name parameter in the From Header field in SIP methods. The display name in the From Header field will be reported to the Host for incoming request method and can be configured for specific value for an outgoing request method.

FR736 - Refer to Phone Number

This feature allows the CSP to support telephone number in an outbound REFER method.

REFER is a SIP method as defined by RFC 3261 that indicates that the recipient (identified by the Request-URI) should contact a third party using the contact information provided in the request. Refer-To is a request header field with in the REFER method as defined by RFC 3515.

Prior to this feature, the CSP supports only the SIP URL in the Refer-To header. The host had to provide the username and host name in the PPL Event Request method to generate the REFER. By default CSP fills in the port number, in case the host has not supplied it. There was no provision for the host to use a telephone number in Refer-To header.

With this feature, the CSP supports telephone number in an outbound REFER method.

> **Important!** The telephone number supplied by the host is not validated by CSP.

FR893 - Send and Receive SIP Signals Using the Same Port

Prior to this feature, the CSP received inbound SIP signals on a specific User Datagram Protocol (UDP) port - by default it was port 5060. The receiving port could be changed at run time.

All outbound SIP signals were sent out on a UDP port allocated by the CSP when you configured SIP. This port number could be any valid (and unused) port number above 1023. The port used for outbound SIP signaling from the CSP remained constant until SIP was deconfigured.

With this feature, the CSP now sends and receives SIP signals using the same port as configured by the host. By default, the CSP uses port 5060 for all SIP traffic.

FR894 - Access To Contact Header

Contact Header

For an endpoint to endpoint call, one endpoint receives an INVITE message (in this case the CSP) and returns a 200OK response. The endpoint that sent the INVITE message uses the Contact information from the 200OK response to send the ACK message to the CSP and subsequent messages such as BYE.

Likewise, the endpoint that receives the INVITE (in this case the CSP) uses the Contact header to send future requests such as BYE. Final responses to INVITE message have to be routed back the same path.

Read and Write Access

This feature allows the host read and write access to the following fields in the contact header in the 200OK response for an INVITE message:

- Contact Display Name
- Contact Username

- Contact Parameters

Note that the host portion cannot be changed because if it is changed, the remote endpoint would not be able to route future requests to the CSP correctly.

FR895 - Report and Control of P-Asserted and P-Access Network Info Headers

The CSP SIP stack can report the “Remote-Party-ID” and the “RPID Privacy” headers if present in the SIP INVITE message.

Now with this feature, the SIP stack can read and write the “Privacy” header as follows:

- Privacy (Defined in RFC 3323)

and the following private headers (P-Headers):

- P-Asserted-Identity (Defined in RFC 3325)
- P-Preferred-Identity (Defined in RFC 3325)
- P-Access-Network-Info (Defined in RFC 3455)

By default, the SIP stack does not report these P-headers. You have to enable this functionality.

The SIP stack does not modify any other SIP headers for privacy related to this feature.

FR928 - SIP 182 Queued Message

One usage of the 182 Queued message is as follows: the called party is temporarily unavailable but the server decides to queue the call rather than reject it.

When the called party becomes available, it returns the appropriate final status response.

The reason phrase might give further details about the status of the call for example, “5 calls queued; expected waiting time is 15 minutes.”

The server might issue several 182 (Queued) responses to update the caller about the status of the queued call.

With this feature, the SIP stack is enhanced to allow the host to:

- generate the 182 Queued message
- report the receipt of the 182 Queued message to the host

This feature is supported in Call Agent and Non-Call Agent calls.

FR991 - Session Description Protocol (SDP) Pass-Through for Call Agent Mode

SDP Signaling Endpoint

The Call Agent Mode (CAM) turns the CSP into a centralized SIP call controller that allows direct flow between the external end-points.

In CAM, the CSP acts as a SIP Back-to-Back User Agent and is not only a full-fledged SIP signaling end-point (User Agent) but also a Session Description Protocol (SDP) signaling endpoint. The CSP originates and terminates SIP and SDP signaling and establishes independent signaling sessions with external endpoints.

In order to facilitate direct media flow between the external endpoints, the CSP interworks essential inbound SDP parameters into NPDI TLVs to carry this information to the host application. The reverse process occurs for outbound SDP parameters.

Any Non-Audio Media Supported

Prior to this release, the SDP processing in the CSP could handle only audio media sessions. With this release, the SIP stack is extended to provide more transparency when media capabilities are negotiated between endpoints.

This transparency comes by tunneling an essential portion of raw SDP text between the external endpoints. This approach is flexible because it allows any non-audio media session (not just T.38 fax) to get setup across the CSP. In addition, the endpoint's media capabilities can evolve without affecting the CSP.

FR874 - H.323 Digit Collection

The H.323 Digit Collection feature will enable you to collect Dual Tone Multi-Frequency (DTMF) digits using the H.323 protocol in the CSP. DTMF digits can be received and sent by the H323 protocol and can be sent in-band or out-of-band. When this feature is implemented in the CSP, the DTMF digits, routed to Layer 4 Dialing Plan (L4 DP) using the IP network, are either in signaling or in Real Time Protocol (RTP) format. These digits will be decoded for the customer as part of their dialing plan.

Currently, the DTMF digits are internally propagated and bypassed directly to the PSTN side using the *DSP Service Request* message. The customer is unable to initiate the collecting of digits.

Instead of bypassing the direct propagation of digits to the PSTN side, two new configuration bytes provide enhanced digit routing in order to support digit collection. These configuration bytes support both signal and alphanumeric type applications.

SS7 Enhancements

FR839 - SS7 Raw Data to Host

The SS7 Raw Data to Host feature allows the customer a way of tracking all Message Signaling Units (MSUs) and Link Status Signaling Units (LSSUs) transmitted to the network and received from the network.

This feature allows the SS7 Series 3 and SS7 PQ cards to send PPL event indications containing LSSUs and MSUs (received from the network as well as sent to the network) to the host. The *PPL Configure* (0x00D7) message is used to enable and disable (default) the feature.

This feature is started by setting (enabling) configuration bytes 0x10 in the following PPL components:

- Enabling the PPL event indications containing the raw LSSUs for transmission/reception to and from the network is done by enabling the configuration bytes 0x10 in the MTP2 LSC and MTP2 IAC PPL components.
- Enabling the PPL event indications containing the raw MSUs for transmission/reception to and from the network is done by enabling the configuration bytes 0x10 in MTP3 HMDT and HMRT PPL components.

When the feature is enabled all the supported LSSUs and MSUs are reported to the host in the PPL event indication.

FR902 - ANSI ISUP Segmentation Configuration

This feature provides the ISUP CPC configuration byte ANSI ISUP Segmentation 0xD4 that allows you to select the forward indicator E bit in the Initial Address Message (IAM) for ANSI segmentation or as a spare.

ANSI ISUP specification T1.113 - 1995 defines the E bit of the forward indicator in Initial Address Message (IAM) as the IAM Segmentation Indicator. If the E bit is set in the IAM, the receiving exchange will start timer T36 and wait for the Information (INF) message. During this time, the Address Complete Message (ACM) will not be sent back even when requested by the host call control.

However, the ANSI ISUP specification T1.113 - 2000 defines the E bit of the forward indicator as a spare. In this case, ISUP implementation may run into the problem when receiving an IAM with the forward indicator E bit set, and call control requests such as Connect AB, PPL Event Requests of ACM from the host call control are received before

timer T36 expires. These messages will be positively acknowledged, but the ACM will not be sent to the network. Eventually, the call fails when timer T7 expires from the transmission end.

The ISUP CPC PPL Component (0x0012) provides ANSI ISUP Segmentation (0xD4) configuration byte to define whether the forward indicator E bit in the IAM should be interpreted as a segmentation indicator. When this configuration byte is set, timer T36 will be started for the INF message, and Call Control request for the ACM will not be processed if received before timer T36 expires. If this configuration byte is not set, the forward indicator E bit is considered as a spare, and the ACM can be sent out immediately, and there is no waiting period for the INF message.

FR903 - SS7 CIC Group Query

This host initiated feature enables the customer to determine what CIC groups are configured in order to perform detailed queries, for each CIC group, without any prior knowledge of the existing configuration.

The feature supports the *SS7 CIC Query* (0x0067) message to display CIC group information. This host initiated message, with the following parameters, is used to query all of the CIC groups for a stack.

- SS7 Stack (0x08) AIB with SS7 Stack ID
- Destination Point Code (DPC) (0xFFFFFFFF) used to query all CIC groups for the stack. The resultant CIC group information can be used to query a particular CIC group.

The AIB in the response message is used to differentiate between the following queries:

- For existing CIC group queries: to query information on a particular CIC group, use the SS7 CIC AIB (0x14).
- For CIC group queries: to query information on all of the configured CIC groups, use SS7 Stack AIB (0x08)

DSP Enhancements

FR 478 DSP Series 2 Plus Card

This feature introduces the new DSP Series 2 Plus card and Multi-Function Media I/O Plus card that will replace the existing DSP Series 2 card and Multi-Function Media I/O card. This document describes any differences between these CSP cards and includes any new hardware and software functionality.

The DSP Series 2 Plus card is functionally equivalent to the DSP Series 2 card and is also backwards compatible with the DSP Series 2 card. Both cards can be used in the same CSP chassis.

FR 704 - DSP Series 2 to CSP Matrix Series 3 Card Over Ethernet

Important! This feature is not supported by the DSP Series 2 Plus card.

Currently in the CSP, the communication between the DSP Series 2 and the CSP Matrix Series 3 Card use the mid-plane HDLC bus. Communication over the HDLC bus slows the maximum number of messages that can be transmitted to be less than 100 per second, not allowing the user to achieve high call rates that require DSP services.

Using Ethernet communication for messaging between the DSP Series 2 and CSP Matrix Series 3 Card allows increased performance by providing more message transactions per second.

This feature supports a new RCOMM state machine on the DSP Series 2 card that monitors the status of the link between this card and CSP Matrix 2000 card. Communication over the HDLC bus will continue to be supported. Licensing of this feature is not required.

FR752 - Vocabulary Index File (VIF) Size Limit Increase

Prior to this feature, the size of Vocabulary Index File (VIF) was limited to 1 MB on the DSP Series 2 card. This feature doubles the VIF size limit to 2 MB. This increase in VIF size allows the DSP Series 2 card to handle more announcements, an important capability when adding multiple language support for global customers.

A VIF supports up to 40,000 lines without noticeable pre-start delay. If a VIF has greater than 40,000 lines, it may take approximately one second before the file starts to play.

FR853 - Supervisor Conference

This feature provides support for a new conferee type for unified conferences on both the DSP Series 2 and DSP Series 2 Plus cards This feature will handle a typical call center scenario that involves a caller, operator and supervisor.

The caller will be connected to a conference in an input-only mode. The operator and the supervisor will be connected to a conference in two-way mode. The caller and the operator will be connected using a one-way connect message to enable the caller to hear to the operator.

- The operator can talk and hear both the caller and supervisor
- The supervisor can hear the caller, but the caller cannot hear the supervisor.

FR 911 - Pulse Dialing Detector

This feature describes the addition of a pulse dialing detector on to the DSP Series 2 card of the CSP.

Both DTMF and Dial Pulse detection are supported. Dial Pulse detection is co-resident with the DTMF detector and supports all of the features associated with the DTMF signal detection, such as record/playback cancellation on detection. The DTMF and Dial Pulse detectors will have the same densities as the DTMF detector alone (192 bits per stream).

It is common in some areas to have legacy switches and telephones that only support pulse (rotary) dialing. By incorporating a pulse dialing detector, the CSP will enable the customer to develop applications which accept user input from callers who do not have DTMF-capable telephones.

FR 960 - Receiving FSK

Currently, the CSP supports sending Frequency Shift Keying (FSK) data containing On-hook Caller ID in the *Outseize Control* (0x002C) message and Off-hook Caller ID in the *Resource Connect* (0x0127) message. It also supports sending and receiving FSK data containing SMS DLL messages that comply with ETSI and CTSI (China Telecom) call flows.

The Receiving FSK feature uses the *Resource Connect* (0x0127) and *Resource Information Notify* (0x0141) messages that allow the host to receive FSK data from an off-hook channel.

General Platform Enhancement

FR412/FR731 - CSP Card Updates and ROMs

The CSP card updates, as listed below, are customer initiated by manually setting the DIP switch positions on the cards listed below.

- Ethernet Link, Force 100 Mbps/Full Duplex
- No Static IP Address
- Software Loading Using Second Ethernet Port

Refer to the API changes, in the Converged Services Platform API Reference, for detailed information on the DIP switch settings in the Hardware Information field in the *Card Status Report 0x00A6* message.

Ethernet Link, Force 100 Mbps/Full Duplex

These feature enables the cards listed below to be able to force the Ethernet links to a 100 Mbps/full duplex mode instead of the default auto-negotiate mode. In certain cases, the auto-negotiation fails to achieve the highest possible rate when customers routers are in force full 100 configurations.

FR731

- *CSP Matrix 2000 Card*
- *IP Signaling Series 3 Card*
- *SS7 Series 3 Card*
- *ISDN Series 3 Card*
- *DSP Series 2 Card*

FR412

- *IP Network Series 2 Card*

Important! If you use the Ethernet Link, Force100 Mbps/Full Duplex mode with a hub/switch/router that is not in a forced full 100 Mbps configuration, the results can vary and a link connection may not be possible.

To set the Ethernet Link, Force100 Mbps/Full Duplex mode on any of the above cards, refer to the DIP switch settings in the Converged Services Platform Hardware Product Descriptions.

No Static IP Address

This feature allows the cards listed below to enable the No Static IP Address mode instead of using the default Static IP mode.

- *CSP Matrix 2000 Card*
- *IP Signaling Series 3 Card*

In the No static IP Address mode, RARP or BOOTP must retrieve an IP address for the CSP Matrix 2000 card or IP Signaling Series 3 card. This feature is enabled by setting DIP switch S1 (SW1/IP Signaling) position 8 on either card to OFF to enable the following functionality:

- If RARP or BOOTP can not obtain an IP address, the static IP address will not be used.

This allows the CSP Matrix 2000 or IP Signaling Series 3 cards to reset and try RARP or BOOTP again to obtain the correct IP address, rather than use the static IP address that is stored in RAM.

When DIP switch S1 (SW1/IP Signaling) position 8 is set to ON (default) the following functionality is enabled:

- If RARP or BOOTP can not obtain an IP address, the static IP address will be used.

To set the No Static IP Address mode on any of the above cards, refer to the DIP switch settings later in this chapter.

Software Loading Using Second Ethernet Port

This feature allows the card listed below to use the second Ethernet port if the first port (default) cannot obtain the software load.

- *CSP Matrix 2000 Card*

If you want to include the second Ethernet port in obtaining an IP address, set DIP switch S1, position 7, to OFF prior to booting up. To use this feature, refer to the sequence of events described below:

- The CSP Matrix 2000 card tries to retrieve an IP address from the I/O card default Ethernet port ETH1 to obtain the software load.
- If this attempt is unsuccessful, the CSP Matrix 2000 card then tries to obtain the software load through Ethernet port ETH2.
- If still unsuccessful, the CSP Matrix 2000 card uses the stored static IP address for ETH1 to obtain the software load.

Important! To enable the static IP address, ensure DIP switch S1, position 8 is set to ON.

To set the Software Loading Using the Second Ethernet mode on the above card, refer to the DIP switch settings later in this chapter.

ROM Upgrades

Important! The cards listed below with model numbers require ROM upgrades to support the Ethernet Link, Force100 Mbps/Full Duplex mode. ROM upgrades must be factory-installed.

CSP Card	Model Number	ROM Revision Number
CSP Matrix 2000 Card	CSP - BDL - 1310 CSP - BDL - 1314 CSP - BDL - 1331 EXS - CPU - 1301 EXS - CPU - 1351	03.04:02 03.04:02 03.04:02 03.04:02 03.04:02
IP Signaling Series 3 Card	MGC - SCS - 1002	03.04:02

FR704 - Ethernet Link Redundancy for DSP Series 2 Card

On the CSP platform, the DSP Series 2 card functionality has been updated to support the *IP Address Configure* (0x00E7) message in order to enable Ethernet Link Redundancy.

Refer to the API and TLV information below, for changes in the *Alarm* (0x00B9) message. Also refer to the modified Ethernet Link Redundancy (0x09) and Active Ethernet Port (0x0A) TLVs.

To enable this feature, *IP Address Configure* message includes the following TLVs:

- Ethernet Link Redundancy (0x09) TLV to enable and disable Ethernet Link Redundancy
- Activate Ethernet Port (0x0A) TLV to select the active port with the values being 1 (NET1/upper port), 2 (NET2/middle port), or 3 (NET3/lower port).

While the DSP Series 2 card is in Ethernet Link Redundancy mode, all three external ports NET1, NET2 and NET3, located on the Multi-Function Media I/O card, can be used.

Important! Only one port can be the active redundant port.

Important! By default, Ethernet Link Redundancy will be disabled to provide complete backwards compatibility.

Host Support

To support Ethernet Link Redundancy, the host can do the following:

- Enable/disable Ethernet port redundancy using the Ethernet Link Redundancy (0x09) TLV within the *IP Address Configure* (0x00E7) message.
- Force an Ethernet Link Switchover using the Activate Ethernet Port TLV (0x0A) within the *IP Address Configure* (0x00E7) message.
- Query the Ethernet Mode and Active Link via *IP Address Query* (0x00E6) message.

Alarms

When a Link is detected as being down on the Active port, the DSP Series 2 card automatically detects the condition and switches over to an available Standby port without host intervention. The switchover response time is less than two seconds, so that NFS file read and write functions are not impacted.

- The DSP Series 2 card generates the following alarms when relating to the status of the ports. Refer to the *Alarm* (0x00B9) message, 0x02 Card Alarms. When resolved, these alarms are cleared by sending the *Alarm Clear* (0x00C1) message.
- An Ethernet Link Failure (Major, 0x22) alarm when the link is detected as being down on any of the three Ethernet ports.
- An Ethernet Link-Up (Informative, 0x39) alarm, when the link is detected as being up on any of the three Ethernet ports.

  Important! The Ethernet Link-Up (0x39) alarm is not cleared, and is sent only when an Ethernet port link has been detected for the first time.

- An Ethernet Port Switchover (Informative, 0x4F) alarm is sent if the active Ethernet port configuration changes while in Redundant Port mode. This alarm can not be cleared.

The Ethernet mode and Active port configured via *IP Address Configure* (0x00E7) message is retained after a soft reset.

FR886 - CSP Messages Longer Than 512 Bytes

The maximum recommended NPDI size is as follows:

- 780 for the *Route Control* message (including the NPDI ICB size)
- 820 bytes for the other messages below (including the NPDI ICB size)

- *Outseize Control* message
- *PPL Event Indication* message
- *PPL Event Request* message
- *Connect with Data* message
- *Request for Service with Data* message
- *Channel Released with Data* message

Changes in Release 8.4.1 Engineering Release 2

DSP Enhancements

FR1010 - Configurable Barge-In for Play Files

This feature allows a single call session to have multiple announcements that can perform differently when subscribers press digits. This functionality increases the flexibility for application development.

This feature does not apply to conferences or child conferences.

FR1200 - Disable Idle Channel Recording

This feature allows you to prevent recording idle channels. It is configurable on a per channel basis and is disabled by default. That is, recording idle channels is allowed by default.

Race conditions can occur between a request to record a channel and a channel releasing. These conditions can cause the CSP to record an idle channel.

CCS Enhancements

FR1000 - ISDN Over Ethernet

Prior to this feature, the communication between the ISDN Series 3 card and the CSP Matrix 2000 card uses the mid-plane HDLC bus. Communication over the HDLC bus slows the maximum number of messages that can be transmitted to be less than 100 per second, not allowing the user to achieve high call rates that require ISDN services.

Using Ethernet communication for messaging between a ISDN Series 3 card and CSP Matrix 2000 card allows increased performance by providing more message transactions per second.

This feature supports a new RCOMM state machine on the ISDN Series 3 card that monitors the status of the link between this card and CSP Matrix 2000 card. Communication over the HDLC bus will continue to be supported. Licensing of this feature is not required.

FR1146 - State Syncing on PPL Event Request for ANM

Prior to this feature, when the PPL Event Request for ANM is sent either to L3P CIC component of ANSI/ITU or to L3P BT IUP component the L4CH SM is not in the answered state. To put the L4CH SM in answered state, you needed to use a custom PPL.

This feature puts the L4CH SM in an answered state when the PPL Event Request for ANM is sent to either of the following:

- L3P CIC component of ANSI or ITU
- L3P BT IUP component for BT IUP

VoIP Enhancements

FR1041 - IP Network Interface Series 2 Card: Ethernet Link Status, Duplex Type and Speed

This feature allows the host to query the following on the IP Network Interface Series 2 card at any time:

- the Ethernet Link status
- speed and duplex type of the NET1, NET2 and NET3 ports located on the Multi-Function Media I/O card

When restarting the host application or initiating a new host application, the Ethernet port status needs to be known. Based on that status, appropriate actions could be taken like taking all the channels OOS in that card. whenever the Ethernet link goes down, an *Alarm* message is sent to the host. When the Ethernet link comes back up, an *Alarm Clear* message is sent.

This feature will add a functionality to query the individual Ethernet link status, speed and duplex type for the IPN Series 2 card using the *Card Query* message (0x0083). These shall be reported in the *Card Query* response. They will also be reported in the Card status report (0x00A6) whenever the card comes in service after a reset.

The *Card Status Query* message response is obtained from the switch when the host sends a *Card Status Query* message.

The *Card Status Query* message is obtained when the IPN Series 2 card comes into service after reset.

FR1023 - IP Network Series 2 NLP Control Support

The IP Network Series 2 card NLP Control Support feature allows the enabling or disabling of the Non-Linear Processor (NLP) sub-component within the IP Network Series 2 card Echo Cancellation control. This feature is supported by adding new bitmap values to the RTP Echo Cancellation (0x0103) TLV. This TLV remains backward compatible to allow enabling and disabling of the existing echo cancellation function.

This feature is not supported by the VDAC-ONE card.

FR895 - Report and Control of P-Asserted and P-Access Network Info Headers

The CSP SIP stack can report the “Remote-Party-ID” and the “RPID Privacy” headers if present in the SIP INVITE message.

Now with this feature, the SIP stack can read and write the “Privacy” header as follows:

- Privacy (Defined in RFC 3323)

and the following private headers (P-Headers):

- P-Asserted-Identity (Defined in RFC 3325)
- P-Preferred-Identity (Defined in RFC 3325)
- P-Access-Network-Info (Defined in RFC 3455)

By default, the SIP stack does not report these P-headers. You have to enable this functionality. The SIP stack does not modify any other SIP headers for privacy related to this feature.

FR893 - Send and Receive SIP Signals Using the Same Port

Prior to this feature, the CSP received inbound SIP signals on a specific User Datagram Protocol (UDP) port - by default it was port 5060. The receiving port could be changed at run time.

All outbound SIP signals were sent out on a UDP port allocated by the CSP when you configured SIP. This port number could be any valid (and unused) port number above 1023. The port used for outbound SIP signaling from the CSP remained constant until SIP was deconfigured.

FR330 - SIP Support for MIME

Prior to this feature, the CSP Session Initiation Protocol (SIP) did not support Multipurpose Internet Mail Extensions (MIME) in outgoing messages. This feature allows a user to send proprietary MIME or standard MIME such as ISUP in outgoing messages. MIME data in incoming messages will be reported to the host.

FR882 - SIP Notify Subscription State

This features adds support for Subscription-State headers in REFER-NOTIFY requests in Call Agent Mode (CAM) and non-CAM configurations.

The benefits of this feature include:

- Host control on REFER-NOTIFY Subscription-State header.
- Host control on the duration of REFER-NOTIFY subscription (“expires” parameter).
- Host control on the retry-after time interval, which would be used to inform the remote UA when the REFER request could be retried in case the previous REFER failed.
- Customizable reason code in the Subscription-State header of REFER-NOTIFY that terminates the subscription.

FR883 - SIP Notifications of Options

The SIP stack can now report the receipt of SIP OPTIONS to the host.

The SIP method, OPTIONS, allows a User Agent (UA) to query another UA or a proxy regarding its capabilities. This feature allows a client to discover information about the supported methods, extension content types with or without a dialog being established.

When the CSP receives an OPTIONS message, it is reported to the host as a PPL Event Indication including the Request URI in the message.

FR884 - SIP Referred By Mechanism

This feature supports the insecure refer technique using the Referred-By mechanism. This mechanism supports Call Agent Mode (CAM) and non-CAM configurations. The Referred-By header is disabled by default.

There are applications of the REFER where it is desirable to provide the refer target with the information about the referrer. The refer target can use this information when deciding whether to admit the referenced request. This feature provides the refer target with the SIP URI of the referrer.

FR688 - Report REFER Request URI in PPL Event Indication

The REFER message implements a call transfer service.

A user agent (referrer) uses the REFER message to request another user agent (referee) that it is in session-establish state with, to contact a third user agent (refer target).

The Refer target is identified by a SIP URI in the Refer-To header field in the REFER message.

You can enable this feature to get the Request-URI, in the Request-Line of the REFER message, reported to the host.

> **Example:** With a SIP-to-ISDN call, if any ISDN related information like UUI, UUI encoding, or presentation indicator is present as a parameter in the Request-URI, this feature allows the host to get this data.

FR674 - Connect One-Way for Music on Hold

The Connect One-Way for Music on Hold feature allows customers to connect to SIP channels in order to support listen-only music for calls put on hold. This feature supports backwards compatibility.

FR0088 - SIP Signaling Support for T.38 Fax Media Sessions (for Non-Call Agent Mode)

The Session Initiation Protocol (SIP) is a signaling protocol used for establishing sessions in an IP network. A session can be a simple two-way telephone call or a collaborative multi-media conference session. SIP uses Session Description Protocol (SDP) to convey and negotiate media session information.

Prior to this feature, the CSP signaling stack establishes only audio media sessions. This feature enhances the SIP and SDP stacks to allow the existing CSP media resources to originate and terminate T.38 fax media sessions. The CSP can now:

- Signal T.38 fax parameters using the network
- Control of local DSP resources to start a T.38 fax session

The CSP SIP signaling state machine can initiate a switchover from audio to T.38 fax or Pass-Through image sessions.

- A session starts with audio capabilities, and upon fax tone detection, the T.38 fax capabilities are negotiated.
- Upon successful negotiation, the session continues with the fax capabilities. The media termination hosts exchange T.38 Internet fax packets.

FR1047 - Disabling the SIP Domain Name System (DNS) Server

Prior to this feature, you enabled and disabled the Domain Name System (DNS) Server at the card level. The DNS task and a UDP socket, used to contact the DNS Server, is created when the Matrix Controller card boots up. Disabling the DNS Server disables the DNS functionality in the Matrix Controller card.

Important! By default, the DNS Server is not configured (disabled).

Once the DNS Server is configured in the CSP SIP stack, there was no provision to disable the DNS Server lookup.

This feature allows the host application to disable the DNS Server lookup at any time. Disabling the DNS Server stops the CSP from sending outbound SIP calls requesting a DNS Server lookup.

FR1166 - SIP Remote Party ID and RPID Privacy for Outbound Calls

Important! This feature contains information for the SIP Remote Party ID and RPID Privacy for both inbound and outbound calls.

The SIP Remote Party ID and SIP RPID Privacy header fields allow certain telephony services as well as some regulatory and public safety requirements.

These services include the following:

- calling identity delivery
- calling identity delivery blocking

- tracing originator of call

Baseline SIP supports each of these services independently, but cannot support all combinations. For example, a caller that wants to maintain privacy and consequently provides unintelligible information in the SIP From header field will not be identifiable by intermediaries. However, since SIP does not allow the contents of the From header field to be modified by intermediaries, the intermediaries that do not directly perform cannot perform certain services.

FR1188 - SIP Tunneling

SIP tunneling is a mechanism that transports any kind of data using SIP signaling messages.

The CSP SIP stack now supports tunneling with the host playing an important role.

The SIP stack acts as a “black box” and the host determines what data to tunnel and what format to transport.

FR1250 - SIP Access To Parameters in To Header

This feature gives the host read and write access to the parameter field of the “To” header of the initial INVITE request. The SIP stack reports to the host the parameters (if present) in the “To” header of the INVITE within the Request for Service with Data or PPL Event Indication for subsequent data. This reporting is disabled by default.

Changes in Release 8.4.1 Engineering Release 3

VoIP Enhancements

FR989 - IP Network Interface Series 3 Card

The IP Network Interface Series 3 line card (hereafter referred to as the IPN-3 card) is the third generation IP Network card in the CSP product line. The following were the first two versions:

- VDAC-ONE card
- IP Network Interface Series 2 (hereafter referred to as the IPN-2 card)

Backward Compatible

Functionally, the IPN-3 card is very similar to the IPN-2 card. Beside some minor differences to a few OAM messages, the IPN-3 interfaces (internally and externally) are backward compatible with the IPN-2 card.

New VoIP Module

The IPN-3 has a new VoIP Module using the Mindspeed Picasso DSP Chips.

New Physical Network Architecture

On the IPN-2 card there are three Ethernet ports configured as a Link Aggregation Group (LAG) allowing a 300 Mbps pipes. The IPN-3 card provides six Ethernet ports:

- two dedicated to a segregated control network
- four dedicated to a public network

Only two ports need to be trunked because the maximum bandwidth needed does not exceed 200 Mbps (about two DS3 worth of G.711).

FR1338 - Support SIP Max Forward in INVITE Message

This feature allows the CSP to insert the Max-Forwards header in outbound requests from the CSP SIP stack.

The Max-Forwards header is optional and is disabled by default. The host can also configure the Max-Forwards value.

FR641 Host-Based SIP Stack

In addition to the existing embedded SIP stack, this ER introduces a SIP stack from Radvision. The stack resides on the host as a standalone stack and is not integrated in SwitchKit.

This implementation gives the developers a direct access to SIP fields and SIP headers, and eliminates the dependency on SwitchKit APIs. Instead, developers will use the Radvision API's.

Refer to the Radvision documentation on the Dialogic support site below.

http://excelsupport.cantata.com/memberarea/pubsets/Radvision/radvision.asp

Digital Signaling Processing Enhancements

DSP2 Plus Card

The Dialogic® Digital Signal Processing Series 2 Plus (DSP2 Plus) card and its associated Dialogic® Multi-Function Media I/O Plus card are the latest cards in the Digital Signaling Processing Card family.

The DSP Series 2 Plus card can perform a single function or a combination of the following functions:

- Conferencing
- Echo Cancellation
- File Playback/Record
- Frequency Shift Keying (FSK)
- Media Streaming over RTP
- Positive Voice Detection/Answering Machine Detection (PVD/AMD)
- Signal Energy Detection
- Tone Generation and Detection
- T.30 Fax

FR1302 - Ability to Increase Gain on Incoming Calls

This feature allows the developer to increase the gain (db level) of an incoming call, and to adjust it to a desired level. Low level incoming calls can cause wrong detection and failure in the functionality of the application. The ability to increase the gain on incoming calls can be very helpful and can prevent problems by adjusting the incoming level to the appropriate level.

This feature introduces two new ICBs (0x26 and 0x0026) which are included in the *API Reference*.

FR1169 - Report Actual NFS Server ID When Using VIF Bypass

The Vocabulary Index File (VIF) Bypass function allows playing a file directly from an onboard cache, and bypasses the VIF lookup function for determining the file location. This feature retrieves the actual NFS server ID, where the file is stored, and reports it to the application.