Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-18 2009

IPCablecom 1.5 Part 18: CMS to CMS Signaling

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members, whether used domestically or internationally.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the Standards. Such adopting party assumes all risks associated with adoption of these Standards, and accepts full responsibility for any damage and/or claims arising from the adoption of such Standards.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this standard have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at http://www.scte.org.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2009
140 Philips Road
Exton, PA 19341

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

Contents

1 INTRODUCTION 1

1.1 SCOPE 1
1.2 SPECIFICATION LANGUAGE 2

2 REFERENCES 3

2.1 NORMATIVE REFERENCES 3
2.2 INFORMATIVE REFERENCES 4
2.3 REFERENCE ACQUISITION 5

3 TERMS AND DEFINITIONS 6

4 ABBREVIATIONS AND ACRONYMS 10

5 BACKGROUND AND MOTIVATION 12

5.1 REQUIREMENTS AND DESIGN PRINCIPLES 12
5.2 IPCABLECOM ARCHITECTURE 13
5.3 CMSS TRUST MODEL 15
5.4 CMS TO CMS ARCHITECTURAL MODEL 16
5.5 OVERVIEW OF CMS BEHAVIOR 18
5.6 BASIC TELEPHONY CALL FLOW 19
5.7 CMS-MGC BASIC TELEPHONY CALL FLOW 20

6 SIP PROFILE 23

6.1 INTRODUCTION 23
6.2 OVERVIEW OF SIP FUNCTIONALITY 23
6.3 TERMINOLOGY 23
6.4 OVERVIEW OF OPERATION 23
6.5 STRUCTURE OF THE PROTOCOL 23
6.6 DEFINITIONS 23
6.7 SIP MESSAGES 23
6.7.1 Requests 24
6.7.2 Responses 24
6.7.3 Header Fields 24
6.7.4 Bodies 24
6.7.5 Framing SIP Messages 24
6.8 GENERAL USER AGENT BEHAVIOR 24
6.8.1 UAC Behavior 24
6.8.2 UAS Behavior 25
6.8.3 Redirect Servers 26
6.9 CANCELING A REQUEST 26
6.10 REGISTRATIONS 26
6.11 QUERYING FOR CAPABILITIES 26
6.12 DIALOGS 26
6.13 INITIATING A SESSION 26
6.14 MODIFYING AN EXISTING SESSION 26
6.15 TERMINATING A SESSION 26
6.16 PROXY BEHAVIOR 26
6.17 TRANSACTIONS 27
6.18 TRANSPORT 27
6.19 COMMON MESSAGE COMPONENTS 27
6.19.1 SIP URI Component 27
6.20 HEADER FIELDS 27
6.20.1 Accept 28

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

6.20.2 Accept-Encoding *28*
6.20.3 Accept-Language *28*
6.20.4 Alert-Info *28*
6.20.5 Allow *28*
6.20.6 Authentication-Info *28*
6.20.7 Authorization *28*
6.20.8 Call-ID *28*
6.20.9 Call-Info *29*
6.20.10 Contact *29*
6.20.11 Content-Disposition *29*
6.20.12 Content-Encoding *29*
6.20.13 Content-Language *29*
6.20.14 Content-Length *29*
6.20.15 Content-Type *29*
6.20.16 CSeq *30*
6.20.17 Date *30*
6.20.18 Error-Info *30*
6.20.19 Expires *30*
6.20.20 From *30*
6.20.21 In-Reply-To *30*
6.20.22 Max-Forwards *30*
6.20.23 Min-Expires *30*
6.20.24 MIME-Version *30*
6.20.25 Organization *31*
6.20.26 Priority *31*
6.20.27 Proxy-Authenticate *31*
6.20.28 Proxy-Authorization *31*
6.20.29 Proxy-Require *31*
6.20.30 Record-Route *31*
6.20.31 Reply-To *31*
6.20.32 Require *31*
6.20.33 Retry-After *31*
6.20.34 Route *31*
6.20.35 Server *31*
6.20.36 FSubject *32*
6.20.37 Supported *32*
6.20.38 Timestamp *32*
6.20.39 To *32*
6.20.40 Unsupported *32*
6.20.41 User-Agent *32*
6.20.42 Via *32*
6.20.43 Warning *33*
6.20.44 WWW-Authenticate *33*
6.21 RESPONSE CODES 33
6.22 USAGE OF HTTP AUTHENTICATION 33
6.23 S/MIME 33
6.24 EXAMPLES 33
6.25 AUGMENTED BNF FOR THE SIP PROTOCOL 33
6.26 SECURITY CONSIDERATIONS: THREAT MODEL AND SECURITY USAGE RECOMMENDATIONS 33
6.27 TABLE OF TIMER VALUES 33

7 SIP EXTENSIONS 35

7.1 URIS FOR TELEPHONE CALLS 36
7.1.1 Routing Number, Number Portability, Carrier Identification Code, and Dial Around Indication Number *36*
7.1.2 Procedures at an Originating CMS *37*

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

7.1.3 Procedures at a Terminating CMS *37*
7.1.4 Procedures at Proxy *37*
7.2 RELIABILITY OF PROVISIONAL RESPONSES 37
7.3 SIP UPDATE METHOD 37
7.4 INTEGRATION OF RESOURCE MANAGEMENT AND SIP 37
7.4.1 Procedures at an Originating CMS *38*
7.4.2 Procedures at a Terminating CMS *38*
7.5 SIP-SPECIFIC EVENT NOTIFICATION 39
7.6 THE REFER METHOD 39
7.6.1 Procedures at an Originating CMS *39*
7.6.2 Procedures at a Terminating CMS *39*
7.7 SIP PROXY TO PROXY EXTENSIONS FOR SUPPORTING DCS 40
7.7.1 P-DCS-Trace-Party-ID *40*
7.7.2 P-DCS-LAES and P-DCS-REDIRECT *40*
7.7.3 P-DCS-Billing-Info *45*
7.7.4 P-DCS Option Tag *47*
7.8 THE SIP "REPLACES" HEADER 47
7.9 PRIVATE EXTENSIONS TO THE SIP PROTOCOL FOR ASSERTED IDENTITY WITHIN TRUSTED NETWORKS. 47
7.10 A MESSAGE SUMMARY AND MESSAGE WAITING INDICATION EVENT PACKAGE FOR THE SESSION INITIATION PROTOCOL (SIP) 48
7.11 GLOBALLY ROUTABLE USER AGENT URI (GRUU) 48
7.12 THE EARLY SESSION DISPOSITION TYPE FOR SIP 48
7.13 AN EXTENSION TO THE SESSION INITIATION PROTOCOL (SIP) FOR REQUEST HISTORY INFORMATION .. 49
7.14 REQUEST AUTHORIZATION THROUGH DIALOG IDENTIFICATION IN THE SESSION INITIATION PROTOCOL (SIP) 49
7.15 THE SESSION INITIATION PROTOCOL (SIP) JOIN HEADER 49
7.16 SUBSCRIBE TO DIALOG EVENT PACKAGE 49

8 CMS-CMS SIGNALING 50

8.1 CMS INTERFACES 50
8.1.1 Overview of CMS Behavior *52*
8.1.2 Overview of Tandem Proxy *57*
8.2 CMS RETRANSMISSION, RELIABILITY, AND RECOVERY STRATEGIES 57
8.3 CMS TO CMS ROUTING 57
8.3.1 Forming a SIP-URI from a tel-URI *58*
8.3.2 Routing a SIP(s) URI at Tandem CMSs *59*
8.3.3 Routing based on tel-URI *59*
8.4 CMS PROCEDURES 59
8.4.1 CMS Messages and Procedures for Basic Call Setup *59*
8.4.2 Emergency Call Procedures *91*
8.4.3 CMS Procedures for REFER *97*
8.4.4 CMS handling of Mid-Call Changes *102*
8.4.5 CMS handling of Call Teardown *110*
8.4.6 Sample Implementation of Call Transfer *111*
8.4.7 Sample Implementation of Ad-hoc Conference *117*
8.4.8 Automatic Recall and Callback *118*
8.4.9 Message Waiting Indicator *122*
8.4.10 SDP Interworking *124*
8.4.11 MGC Caller ID Procedures *128*
8.4.12 Procedures for Request History Information *130*
8.4.13 Operator Services *136*
8.4.14 Signaling Dialed Non-Geographic Numbers *138*

9 APPLICATION LAYER ANONYMIZER 139

9.1 SIGNALING CONTENT PRIVACY 140
9.2 IP ADDRESS PRIVACY 140

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

APPENDIX A TIMER SUMMARY **143**

APPENDIX B CMSS MESSAGE AND HEADER OVERVIEW **144**

APPENDIX C ENUM CLIENT REQUIREMENTS **148**

C.1 INTRODUCTION 148
C.1.1 General *148*
C.1.2 DNS Resolver Requirements *148*
C.1.3 Database Selector *148*
C.2 NAPTR 148
C.2.1 Service Field *148*
C.2.2 Case Insensitivity *149*
C.2.3 Regular Expression Delimiters *149*
C.2.4 Non-Terminal NAPTR Records *149*
C.2.5 Handling Multiple URIs *149*
C.2.6 EDNS0 Support *149*

LIST OF FIGURES

FIGURE 1. SYSTEM ARCHITECTURE – REALM 14
FIGURE 2. TRUSTED DOMAIN OF IPCABLECOM SERVICE PROVIDER 16
FIGURE 3. CMS SIGNALING MODEL 17
FIGURE 4. CMS – CMS SIGNALING BASIC CALL FLOW 20
FIGURE 5. CMS TO MGC SIGNALING 22
FIGURE 6. CMS TO CMS SIGNALING 51
FIGURE 7. OVERVIEW OF INTERDOMAIN TELEPHONY CALL FLOW 52
FIGURE 8. CALL FORWARDING SUPPORT 55
FIGURE 9. REFER SUPPORT 56
FIGURE 10. CMS MESSAGES FOR BASIC CALL SETUP 60
FIGURE 11. EMERGENCY CALL; NETWORK HOLD DISCONNECT PROCEDURES 92
FIGURE 12. EMERGENCY CALL; NETWORK HOLD RESUME PROCEDURES 93
FIGURE 13. EMERGENCY CALL; PSAP OPERATOR RINGBACK WHILE ON HOLD 94
FIGURE 14. EMERGENCY CALL; PSAP OPERATOR CALLBACK 95
FIGURE 15. END OF TRANSFERRED CALL 112
FIGURE 16. FAILURE CA– F1 – NO FREE CONFERENCE CIRCUITS 112
FIGURE 17. ESTABLISHING THE LEG FROM BRIDGE SERVER TO PARTY C 113
FIGURE 18. FAILURE CA– F2 – PARTY C BUSY 114
FIGURE 19. ON-HOOK INITIATES TRANSFER ACTION 115
FIGURE 20. RELOCATION OF PARTY B TO BRIDGE 116
FIGURE 21. TRANSFER COMPLETED, CMSI ENDS INVOLVEMENT IN CALL 117
FIGURE 22. END OF TRANSFERRED CALL 117
FIGURE 23. MULTIPLE FORWARDING SCENARIO 133
FIGURE 24. APPLICATION LAYER ANONYMIZER 139
FIGURE 25. ANONYMIZER FUNCTIONS 140
FIGURE 26. PRIVACY ISSUES 141

LIST OF TABLES

TABLE 1 - EGRESS PSTN GATEWAY ENCODING REQUIREMENTS 129
TABLE 2 - INGRESS PSTN GATEWAY ENCODING REQUIREMENTS 130
TABLE 3 - PARAMETERS AND HEADER FIELDS THAT ARE MODIFIED IN A CMSS COMPLIANT IMPLEMENTATION 133

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

1 INTRODUCTION

1.1 Scope

This specification describes the IPCablecom Call Management Server (CMS) to CMS Signaling protocol intended for use by a CMS to communicate with another CMS in order to support packet-based voice and other real-time multimedia applications. The protocol exchanges between a CMS and a Media Gateway Controller (MGC) are identical to those between CMSs, and so for purposes of this specification the MGC is considered identical to a CMS. CMSs currently support multimedia endpoints (within the IPCablecom infrastructure) that use the Network-based Call Signaling [24] (NCS) protocol and the PSTN Gateway Call Signaling Protocol [25] (TGCP) for communicating signaling information between the endpoint and the CMS. In the future, other protocols may be supported as well, and the CMS to CMS protocol is intended to be sufficiently general to accommodate such protocols without change.

The CMS to CMS protocol uses the Session Initiation Protocol 2.0 (SIP) specification with extensions and usage rules that support commonly available local and CLASS^{SM} services. This protocol is referred to as the Call Management Server Signaling (CMSS) protocol.

The CMSS protocol takes into account the need to manage access to network resources and account for resource usage. The usage rules defined in this specification specifically address the coordination between CMS Signaling and IPCablecom Dynamic Quality of Service (QoS) mechanisms for managing resources over the cable access network. In addition, this specification defines the protocols and messages needed between Call Management Servers for supporting these services.

This document specifies the protocols and procedures to use between CMSs belonging to a single service provider as well as between CMSs that belong to different service providers. In the case that the CMSs are owned by multiple service providers, it is assumed that the service providers have a mutual trust relationship.

Other IPCablecom documents describe interfaces between other system elements. These documents cover areas such as: Event Message recording for billing and other back office functions [23]; Dynamic Quality of Service [21]; Operations and Provisioning [61]; Electronic Surveillance [22]; and Security [26]. These other specifications indirectly place requirements on the signaling protocol to ensure that it transports the correct data needed to implement a complete system. This document includes syntax and protocols for implementing these requirements. Currently, the document does not address interworking with non-IPCablecom-compliant devices.

From time to time this document refers to the voice communications capabilities of an IPCablecom network in terms of "IP Telephony." The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this document is addressed to, or intended to affect, those issues. In particular, while this document uses standard terms such as "call," "call signaling," "telephony," etc., it should be recalled that while an IPCablecom network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, and that these differences may be significant for legal/regulatory purposes. Moreover, while reference is made here to "IP Telephony," it should be recognized that this term embraces a number of different technologies and network architecture, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this term.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

1.2 Specification Language

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example, another vendor may omit the same item.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

2 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

2.1 Normative References

[1] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January 1996.

[2] IETF RFC 2234, Augmented BNF for Syntax Specifications: ABNF, November 1997.

[3] IETF RFC4566, SDP: Session Description Protocol, July 2006.

[4] IETF RFC 2396, Uniform Resource Identifiers (URI): Generic Syntax, August 1998.

[5] IETF RFC 2397, The "data" URL Scheme, August 1998.

[6] IETF RFC 3261, SIP: Session Initiation Protocol, February 2002.

[7] IETF RFC 3262, Reliability of Provisional Responses in SIP, June 2002.

[8] IETF RFC 3263, Session Initiation Protocol (SIP): Locating SIP Servers, June 2002.

[9] IETF RFC 3265, SIP-Specific Event Notification, Roach A., June 2002.

[10] IETF RFC 3311, The SIP UPDATE Method, Rosenberg, J., September 2002.

[11] IETF RFC 3312, Integration of Resource Management and SIP for IP Telephony, October 2002.

[12] IETF RFC 3323, A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002.

[13] IETF RFC 3325, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, November 2002.

[14] IETF RFC 3420, Internet Media Types message/sip and message/sipfrag, November 2002.

[15] IETF RFC 768, User Datagram Protocol, August 1980.

[16] IETF RFC 5503, Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture, March 2009.

[17] IETF RFC 3515, The Session Initiation Protocol (SIP) Refer Method, April 2003.

[18] IETF RFC 3891, The Session Initiation Protocol (SIP) Replaces Header, September 2004.

[19] ITU-T Recommendation E.123, Notation for national and international telephone numbers, e-mail addresses and Web addresses, February 2001.

[20] ITU-T Recommendation E.164, The international public telecommunication numbering plan, May 1997.

[21] SCTE 165-4 2009, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.

[22] SCTE 165-13 2009 IPCablecom 1.5 Part 13: Electronic Surveillance Standard.

[23] SCTE 165-9 2009, IPCablecom 1.5 Part 9: Event Messages.

[24] SCTE 165-3 2009, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.

[25] SCTE 165-12 2009, IPCablecom 1.5 Part 12: PSTN Gateway Call Signaling Protocol Specification.

[26] SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.

[27] IETF RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), R. Mahy, August 2004.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

[28] IETF RFC 3966, The tel URI for Telephone Numbers, December, 2004.

[29] IETF RFC 4694, Number Portability Parameters for the "tel" URI, October 2006.

[30] IETF RFC 3761, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM), 2004.

[31] IETF RFC 3764, Enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record, 2004.

[32] IETF RFC 4415, IANA Registration for Enumservice Voice, 2006.

[33] IETF RFC 3402, Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm, 2002.

[34] IETF RFC 1034, DOMAIN NAMES - CONCEPTS AND FACILITIES, 1987.

[35] IETF RFC 2671, Extension Mechanisms for DNS (EDNS0), 1999.

[36] IETF Internet-Draft, Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP), draft-ietf-sip-gruu-15, October 2007, work in progress.

[37] IETF RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), June, 2002.

[38] IETF RFC 3455, Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP), January 2003.

[39] PacketCable IMS Delta Specification, PKT-SP-24.229-I05-090528, Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 Specification 3GPP TS 24.229, May 28, 2009, Cable Television Laboratories Inc.

[40] IETF RFC 3959, The Early Session Disposition Type for SIP, G. Camarillo, December, 2004.

[41] IETF RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, November, 2005.

[42] IETF RFC 4458, Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR), April 2006.

[43] IETF RFC 4538, Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP), June, 2006.

[44] IETF RFC 3911, The Session Initiation Protocol (SIP) Join Header, October, 2004.

[45] IETF RFC 5079, Rejecting Anonymous Requests in the Session Initiation Protocol (SIP), December 2007.

[46] IETF RFC 4235, An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP), November 2005.

[47] Telcordia GR-227, LSSGR: CLASS Feature: Automatic Recall (FSD 01-02-1260), April 2002, FR-64.

[48] Telcordia GR-529 LSSGR: Public Safety (FSDs 15-01-0000, 15-03-0000, 15-07-0000), Issue 1, June 2000.

[49] Telcordia GR-1277, LSSGR: Operator Services: Switching System Generic Requirements Using Integrated Services Digital Network User Part (ISUP), August 2001.

[50] Telcordia GR-2956, LSSGR: CCS SS7 Generic Requirements in Support of E9-1-1 Service, December 2002.

[51] IETF Internet-Draft, DAI Parameter for the "tel" URI, draft-yu-tel-dai-06.txt, January 2009, work in progress.

[52] IETF Internet-Draft, P-Charge-Info - A Private Header (P-Header) Extension to the Session Initiation Protocol (SIP), draft-york-sipping-p-charge-info-06, February 2009, work in progress.

[53] ATIS-1000113.2005, Signaling System No. 7 (SS7) -- Integrated Services Digital Network (ISDN) User Part.

2.2 Informative References

[54] IETF RFC 3398, ISUP to SIP Mapping, December, 2002.

[55] IETF RFC791, Transmission Control Protocol, Postal, J., September 1981.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

[56] SCTE 165-1 2009, IPCablecom 1.5 Part 1: Architecture Framework Technical Report.

[57] SCTE 165-17 2009, IPCablecom 1.5 Part 17: Audio Server Protocol.

[58] SCTE 165-2 2009, IPCablecom 1.5 Part 2: Audio/Video Codecs.

[59] PacketCable Basic Residential Feature Descriptions for PacketCable-Based VoIP Services, PKT-TR-VOIPBRF-R01-000608, June 8, 2000, Cable Television Laboratories, Inc.

[60] PacketCable Extended Residential Feature Descriptions for PacketCable-Based VoIP Services, PKT-TR-VOIPERF-R01-000831, August 31, 2000, Cable Television Laboratories, Inc.

[61] SCTE 165-5 2009, IPCablecom 1.5 Part 5: MTA Device Provisioning.

[62] PacketCable Architecture Framework Technical Report, PKT-TR-ARCH-FRM-V06-090528, May 28, 2009, Cable Television Laboratories, Inc.

[63] Telcordia GR-391, LSSGR: CLASS Feature: Calling Identity Delivery Blocking Features (FSD 01-02-1053), June 2000.

[64] Telcordia GR-246, Specification of Signalling System Number 7, December 2005.

[65] IETF RFC 2327, SDP: Session Description Protocol, April 1998.

[66] IETF RFC 3551, RTP Profile for Auditor and Video Conferences with Minimal Control, July 2003.

2.3 Reference Acquisition

- ATIS Document center: www.atis.org
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: http://www.cablelabs.com
- ITU-T Recommendations available at http://www.itu.int
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org/
  Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.
  The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
- Telcordia: http://www.telcordia.com/services/testing/lab_access/gr-listing.html

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

3 TERMS AND DEFINITIONS

IPCablecom specifications use the following terms:

Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g., bandwidth) for it on the DOCSIS network.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
Announcement Server	An announcement server plays informational announcements in IPCablecom network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user.
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data.
CNAM	Calling Name
Confidentiality	A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as Privacy.
Cryptanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext
Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate
Digital signature	A data value generated by a public key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum
Domain	An IPCablecom domain is made up of one or more IPCablecom zones that are operated and managed by a single administrative entity. An IPCablecom domain may also be referred to as an administrative domain.
Downstream	The direction from the head-end toward the subscriber location.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU
Errored Second	Any 1-sec interval containing at least one bit error.
Event Message	Message capturing a single portion of a connection
Exterior Border Proxy	A proxy involved in inter-domain communication. Exterior border proxies are used to communicate between different domains. Every non-isolated domain has interfaces with one or more other domains via one or more Exterior Border Proxies.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated"
Flow [IP Flow]	A unidirectional sequence of packets identified by ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow"). A unidirectional sequence of packets associated with a SID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Gateway	Devices bridging between the IPCablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway which sends and receives circuit switched network signaling tot he edge of the IPCablecom network.
Header	Protocol control information located at the beginning of a protocol data unit.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
Interior Border Proxy	A proxy involved in intra-domain communication. Interior border proxies are used between two realms in the same domain. This type of proxy is optional and not required for signaling.
IntraLATA	Within a Local Access Transport Area
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
LNP	Local Number Portability

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.
Network Management OSS	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.
Nonce	A random value used only once which is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
Off-Net Call	A communication connecting an IPCablecom subscriber out to a user on the PSTN
On-Net Call	A communication placed by one customer to another customer entirely on the IPCablecom Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
Realm	A realm is a set of one or more IPCablecom Zones managed as a single community of operation for the purposes of security administration and subdomain routing.
Root Private Key	The private signing key of the highest level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.
Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed by using encryption.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
Systems Management	Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.
Transit Delays	The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch which carries user media content and may carry voice signaling (MF, R2, etc.).
Tunnel Mode	An IPSEC (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPSEC ESP or AH transform are taken out.
Upstream	The direction from the subscriber location toward the head-end.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory
Zone	An IPCablecom zone consists of the set of MTAs in one or more DOCSIS HFC access networks that are managed by a single functional CMS.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations and acronyms.

ACR	Anonymous Call Reject
AVP	Audio Video Profile
BLV	Busy Line Verification
CA	Call Agent
CFB	Call Forwarding on Busy
CFNA	Call Forwarding No Answer
CFU	Call Forward Unconditional
CLASS	Custom Local Area Signaling Services
CMS	Call Management System
CMTS	Cable Modem Termination System
CODEC	Coder-DECoder
DCS	Distributed Call Signaling
DND	Do Not Disturb
DOCSIS®	Data-Over-Cable System Interface Specification
DP	DCS Proxy
EBP	Exterior Border Proxy
EI	Emergency Interrupt
EP	Endpoint
E.164	Telephone number standard of ITU
FQDN	Fully Qualified Domain Name
GAP	Generic Address Parameter
GC	Gate Controller
IBP	Interior Border Proxy
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	IP Security
ITU	International Telecommunication Union
LAES	Lawfully Authorized Electronic Surveillance
LNP	Local Number Portability
LRN	Local Routing Number
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MTA	Multimedia Terminal Adapter
NCS	Network Call Signaling
OCN	Original Called Number
OSPS	Operator Services Positioning System

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

OSS	Operations Support System
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request for Comments (IETF standard)
RGW	Residential Gateway
RKS	Record Keeping Server
RTP	Real-Time Transport Protocol
SCF	Selective Call Forwarding
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SS7	Signaling System #7
TCP	Transmission Control Protocol
TGCP	Trunk gateway control protocol
UAC	User agent – Client
UAS	User agent – Server
UDP	User Datagram Protocol
URI	Universal Resource Identifier
URL	Universal Resource Locator

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

5 BACKGROUND AND MOTIVATION

The design of the Call Management Server Signaling (CMSS) architecture recognizes the trend towards use of packet networks as the underlying framework for communications. These networks will provide a broad range of services, including traditional best-effort data service, as well as enhanced value-added services such as telephony and gaming. The Network based Call Signaling (NCS) and PSTN Gateway Call Signaling (TGCP) protocols are used to communicate between limited-function multimedia end-points, such as standard telephone sets and trunking gateways, and Call Management Servers (CMS). However, the NCS and TGCP protocols do not address the need for communication between multiple CMSs residing in one or more service providers' networks. This specification covers the signaling performed between CMSs. The initial real-time multimedia service that is supported by the NCS and TGCP function is that of interactive telephony. The NCS and TGCP protocols represent the same architecture and are largely similar. In the following, where a distinction is not important, they will sometimes be simply referred to as NCS.

It is recognized that packet based networks may also offer additional real-time multimedia services to endpoints that are IP capable. Also, improvements in silicon will reinforce the trend towards increased functionality and "intelligence" in endpoints. These intelligent endpoints will be addressed in a future specification to take advantage of the widespread availability of packet networks to enable a rich set of applications and services for users.

CMSs may have a need to interconnect with other entities and networks which in turn introduces at least two issues:

- Interoperability - The extensions specified in CMSS may not all be supported.
- Security - When information is sent to or received from an entity, that entity may not be trusted (e.g., a SIP endpoint or VoIP peer network) and special procedures may need to be invoked.

The current CMSS specification has been made flexible to accommodate the interoperability issue identified above. The security issue is resolved as follows; whenever signaling is sent to or received from a particular SIP entity, that entity is assumed to be trusted (see also Section 5.3).

A key element of the CMSS architecture is a recognition of the need for coordination between call signaling, which controls access to telephony specific services, and resource management, which controls access to network-layer resources. This coordination is designed to meet the user expectations and human factors associated with telephony. For example, in a telephony environment, the called party should not be alerted until the resources necessary to complete the call are available. If resources were not available when the called party picked up, the user would experience a call defect. In addition, PSTN users expect to be charged for service only after the called party answers the phone. As a result, it must be possible to track usage accounting in a way that allows customer billing to start once the called party picks up. Coordination between call signaling and resource management is also needed to prevent fraud. The coordination between call signaling and Dynamic QoS [21] protocols ensures that users are authenticated and authorized before receiving access to the enhanced QoS associated with the telephony service.

In the NCS and TGCP protocols, the functionality required of the multimedia endpoint is simple, and more of the functionality resides in the network in call management servers, where the state of a session is maintained. The CMS is responsible for establishing and managing session legs, and (indirectly) for requesting and obtaining network layer QoS for the session. The NCS and TGCP protocols specify the information and message exchanges between the multimedia endpoint and the CMS. When the session has to be routed through multiple CMSs, additional functionality is required in the protocol to communicate the information related to the session. This includes information provided by the endpoint to the network as well as information that may reside in the CMS or other entities within the network that relates to the session. Examples of such additional information that may reside in the network include billing and data that may otherwise be kept private from untrusted multimedia endpoints.

5.1 Requirements and Design Principles

This section briefly describes the application requirements that led to the set of CMSS design principles.

The need to support primary line telephony service requires enhanced bearer channel and signaling performance, including:

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

- *Low delay* – end-to-end packet delay must be sufficiently small that it does not interfere with normal multimedia sessions. The ITU recommends no greater than 300 ms roundtrip delay for a telephony service.
- *Low packet loss* – packet loss must be sufficiently small that it does not perceptibly impede session quality or, in the case of telephony, performance of fax and voice band modems.
- *Short post-dial delay* – the delay between dialing the last digit and receiving positive confirmation from the network must be sufficiently short to ensure that users do not perceive a difference from post-dial delays typically experienced in the circuit switched network; in particular, the delay must not be so long that the user is led to believe that the network has failed.
- *Short post-pickup delay* – the delay between a user picking up a ringing phone or acknowledging a multimedia session and the voice or media path being cut through must be sufficiently short to ensure that the initial talk-spurt, e.g., "hello", is not clipped.

A number of key design principles that arise from the requirements and philosophy above are identified:

1. It is essential to provide network-layer Quality of Service while allowing the service provider to derive revenues from the use of such service.
2. The CMSS architecture must allow for communication between CMSs in the network. At a high level, one may regard a CMS as performing complex signaling tasks on behalf of an endpoint. When the network includes multiple CMSs, CMSS should provide the call signaling function between the CMSs on an individual call basis. Within such a context, the CMSS architecture must allow the network to support limited-function multimedia endpoints, while allowing additional functions to be performed by the CMSs (including the maintaining call state in the CMSs).
3. The CMSS architecture must enable interoperability with SIP entities that do not support all of the extensions specified by CMSS. CMSS compliant implementations will use the extensions and procedures defined in this document. However, when communicating with non-CMSS compliant implementations, CMSS compliant implementations will only use the extensions supported by both implementations. Furthermore, CMSs may be configured to require peer support for certain extensions, and fail calls with peers that do not support those extensions.
4. The architecture must ensure that the network is protected from fraud and theft of service. The service provider must be able to authenticate users requesting service and to ensure that only those authorized to receive a particular service are able to obtain it. Furthermore, the service provider must be able to track the usage of such services in order to support billing.
5. The architecture must enable the service provider to add value by supporting the functions of a trusted intermediary. In the case of telephony, this includes protecting the Privacy of calling and called party information, and ensuring the accuracy of the information that is provided in messages from the network.
6. The architecture must be implementable, cost-effectively, at very large scale.

5.2 IPCablecom Architecture

The CMS to CMS Signaling (CMSS) Architecture follows the principles outlined above to support a robust multimedia service. Figure 1 introduces the key components in the architecture.

Multimedia Terminal Adapters (MTAs) may either be embedded into the Cable Modem (CM) or they may be stand-alone. The cable access network interfaces to an IP backbone through a CMTS that is the first trusted element within the provider's network. The CMTS performs network resource management, acts as a policy enforcement point, and as a source of event messages that can be used for billing.

The CMS establishes and receives sessions on behalf of an endpoint by using the NCS protocol to communicate with the MTA. The CMS uses the protocol specified here to communicate with other CMSs. In addition, it may also perform the function of a Gate Controller (GC), which is responsible for authorizing the enhanced Quality of Service for the media stream. The CMS acts as a source of event messages that can be used for billing.

Media Service Nodes represent network-based components that operate on media flows to support the service. Media service nodes perform audio bridging, play announcements, provide interactive voice response services, etc.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

The protocol exchanges between a CMS and a Media Service Nodes are identical to those between CMSs, and so for purposes of this specification a Media Service Node is considered identical to a CMS. Media Service Nodes may be decomposed into a controller and a player, in which case CMSS signaling is performed with the controller.

PSTN gateways interface to the Public Switched Telephone Network. The PSTN gateway may be decomposed into a Media Gateway Controller (MGC), a signaling gateway (SG), and a Media Gateway (MG). The TGCP protocol is used between the MGC and the MG. The protocol exchanges between a CMS and an MGC are identical to those between CMSs, and so for purposes of this specification, the MGC is considered identical to a CMS.

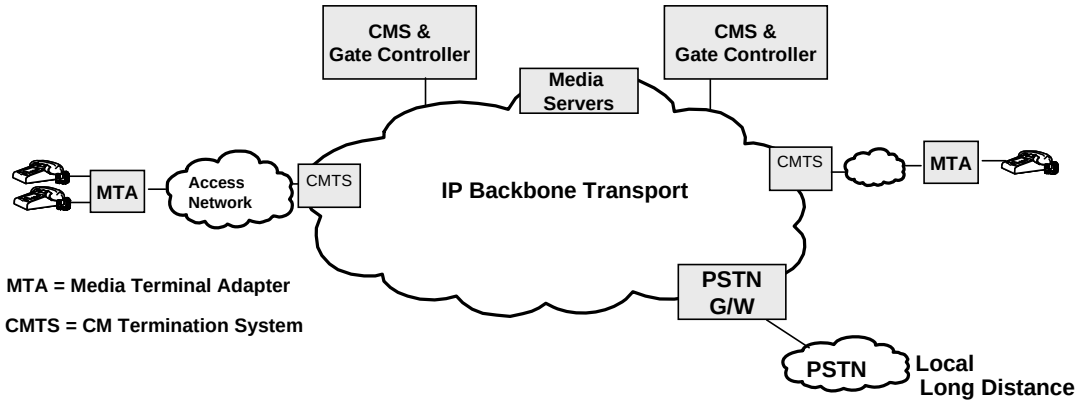

Figure 1. System Architecture – REALM

Access to network resources must be controlled by the service provider. The CMTS receives resource management requests from endpoints, and is responsible for ensuring that packets are provided the QoS they are authorized to receive (either through packet marking, or through routing and queuing the packets as a specific QoS-assured flow). The CMTS requires authorization from a Gate Controller (on a session by session basis for the multimedia service) before providing access to enhanced QoS for an end-to-end IP flow. Thus, the CMTS is able to ensure that enhanced QoS is provided only for end-to-end flows that have been authorized and for which usage accounting is being performed. Since the CMTS knows about the resource usage associated with individual IP flows, it generates the usage events that allow a user to be charged for service [23].

DQOS1.5 [21] introduces the concept of a "gate" in the CMTS. Conceptually, gates manage access to enhanced quality of service. The gate is a packet classifier and policer that ensures that only those IP flows that have been authorized by the CMS are granted access to enhanced QoS in the access and backbone networks. Gates are "admitted" selectively for a flow. For a multimedia service, gates are opened and controlled for individual sessions. Admitting a gate involves an admission control check that is performed when a resource reservation or commit request is received from the endpoint, and it may involve resource reservation in the backbone network if necessary. The packet filter in the gate allows a flow of packets to receive enhanced QoS for a session from a specific IP source address and port number to a specific IP destination address and port number.

CMSs implement a set of service-specific control functions required to support the telephony service:

- Authentication and authorization: Since services are only provided to authorized subscribers, CMSs authenticate signaling messages and authorize requests for service on a session-by-session basis.
- Name/number translation and call routing: CMSs translate dialed numbers or names to a next-hop IP address based on call routing logic.
- Service-specific admission control: CMSs can implement a broad range of admission control policies for the telephony service. For example, CMSs may provide precedence to particular calls, e.g., emergency calls initiated by dialing a special number such as 911. Admission control may also be used to implement overload control mechanisms, e.g., to restrict the number of calls to a particular location or to restrict the frequency of call setup to avoid signaling overload.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

- Signaling and service feature support: CMSs maintain and track all signaling activities to ensure compliance and to manage subscriber features. For example, in the case of telephony, 3-way calling, caller ID, etc.

A CMS is responsible for a set of endpoints and the associated CMTSs. While endpoints are not trusted, there is a trust relationship between the CMTS and its associated CMSs, since the Gate Controllers in the CMSs play a role as a policy server that controls when the CMTS can provide enhanced QoS service. There is also a trust relationship among CMSs. Details of the security model and mechanisms are specified in [26].

CMSS supports inter-working with the circuit switched telephone network through PSTN gateways. A PSTN gateway may be realized as a combination of a Media Gateway Controller (MGC), Media Gateway (MG), and a Signaling Gateway (SG). A media gateway acts as the IP peer of an endpoint for media packets, converting between the data format used over the IP network and the format required for transmission over the PSTN, e.g., PCMU. The signaling gateway acts as the IP peer of a PSTN endpoint for call signaling, providing signaling inter-working between the IPCablecom network and conventional telephony signaling protocols such as ISUP/SS7. The MGC uses the PSTN Gateway Call Signaling Protocol (TGCP) to control the operation of the media gateway.

Additionally CMSS supports inter-working with other IPCablecom architectures, in particular IPCablecom 2.0. IPCablecom 2.0 adds support for SIP-based endpoints, and a SIP-based service platform that may be used to support a variety of services, please see [62] for further details on the IPCablecom 2.0 architecture and associated network elements. The CMSS interface support direct inter-working with IPCablecom 2.0 Call Session Control Functions (CSCFs) network elements for the majority of session related procedures. There are however a few instances where direct inter-working via CMSS is not possible. As such, specific procedures are documented to cover these special cases. In particular special inter-working procedures are provided for electronic surveillance, accounting and SDP. The procedures for electronic surveillance can be found in Section 7.7.2.5, the procedures for accounting can be found in Section 7.7.3.4, and the procedures for SDP can be found in Section 8.4.10.

There are additional system elements that may be involved in providing the multimedia service [56]. For example, in the case of telephony service, the CMS may interface with other servers that implement the authorization or translation functions. Similarly, announcements, voicemail, and three-way calling may be supported using media service nodes in the network. Management of security interfaces between system elements is explained in [26].

This specification provides generic capabilities that can be used to implement additional features. Features that have an intra/inter-domain (CMS-CMS) impact are considered and specifically addressed below.

5.3 CMSS Trust Model

CMSS defines a trust boundary around the various systems and servers that are within a single domain. These trusted systems include the Internal and External Border Proxies[1], CMSs, CMTSs of the cable access network, and various servers such as bridge servers, voicemail servers, announcement servers, etc. Outside of the trust boundary are the customer premises equipment, i.e., the MTAs, the Public Switched Telephone Network (PSTN)[2], and various media service nodes operated by third-party service providers. At the boundary of the trusted domain are CMTSs/Edge Routers at the transport level and EBP/CMSs at the signaling level. The EBP interfaces to other IPCablecom domains. Although these other IPCablecom domains are outside the trust boundary, CMSS still trusts call signaling sent to and received from these other IPCablecom domains.

[1] More generally referred to as tandem proxies or simply proxies.

[2] but not the PSTN GW.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

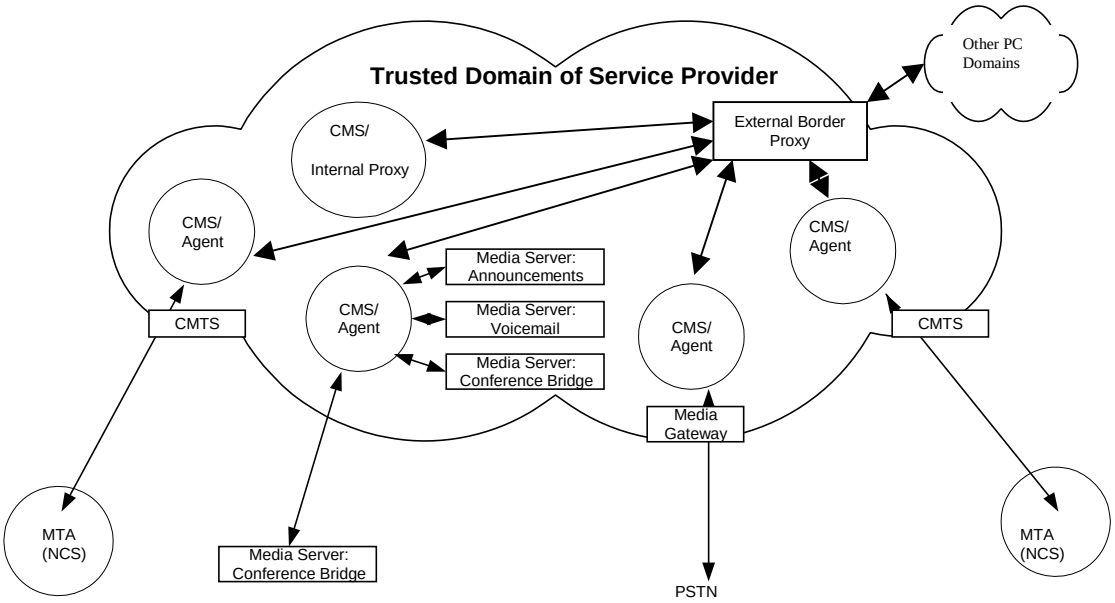

Figure 2. Trusted Domain of IPCablecom Service Provider

5.4 CMS to CMS Architectural Model

The Call Management Server (CMS) is an architectural entity that performs those services necessary to enable endpoints to establish IP multimedia sessions. The CMS is a complex of server functions that support session signaling, number translation, and feature support. In addition to processing signaling messages, the CMS provides functions for service and feature authorization, call routing, and service-specific admission control. As a trusted decision point, the CMS may also coordinate with Gate Controllers (which act as Policy Decision Points from a resource management point of view) to control when resource reservations are authorized for particular users and media flows.

This specification describes the messages required to support IP Telephony between entities that support one or more of the role indicated in the following table:

Role	Distinguishing function
Call Agent (CA) or CMS as defined above.	Support of endpoints implementing Network-Based Call Signaling (NCS) [24].
Media Gateway Controller (MGC)	Interworking with the PSTN. Use of PSTN Gateway Call Signaling (TGCP) [25] to control trunks.
Announcement Servers, Bridge Servers, or VoiceMail Servers	Provide various media services.
Tandem server within a domain, or a gateway server between service provider domains.	Routing functions only.

The list of roles may be expanded in the future. Although trust levels vary between providers, the document assumes CMSs within a REALM and across multiple domains trust each other. MTAs, however, are untrusted NCS endpoints. Note: where multiple roles are combined within a single node, the interface between them is hidden and untestable.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

All of the various types of endpoint management systems currently fall into one of two different categories of CMSs. A CMS[3] is a trusted entity that establishes calls on behalf of an untrusted endpoint, e.g., an MTA, in the customer premise. The role of the CMS is to verify the signaling messages from the untrusted source, and provide various network services, such as translation, authentication and accounting. The second category is the Proxy. Proxies are classified into two types: proxies used within a domain, and proxies used between domains. The Interior Border Proxy (IBP) is a proxy that can be used for inter-realm (intra-domain) signaling and the Exterior Border Proxy (EBP) is required for inter-domain signaling. Where a distinction between the different types of proxy is either unimportant or is evident from the text, they will be simply referred to as proxies or tandem proxies.

A CMS is a SIP User Agent (UA). If the CMS controls NCS endpoints, the CMS furthermore contains a Gate Controller (GC) with a hidden and untestable interface between the UA and the GC as shown in Figure 3.

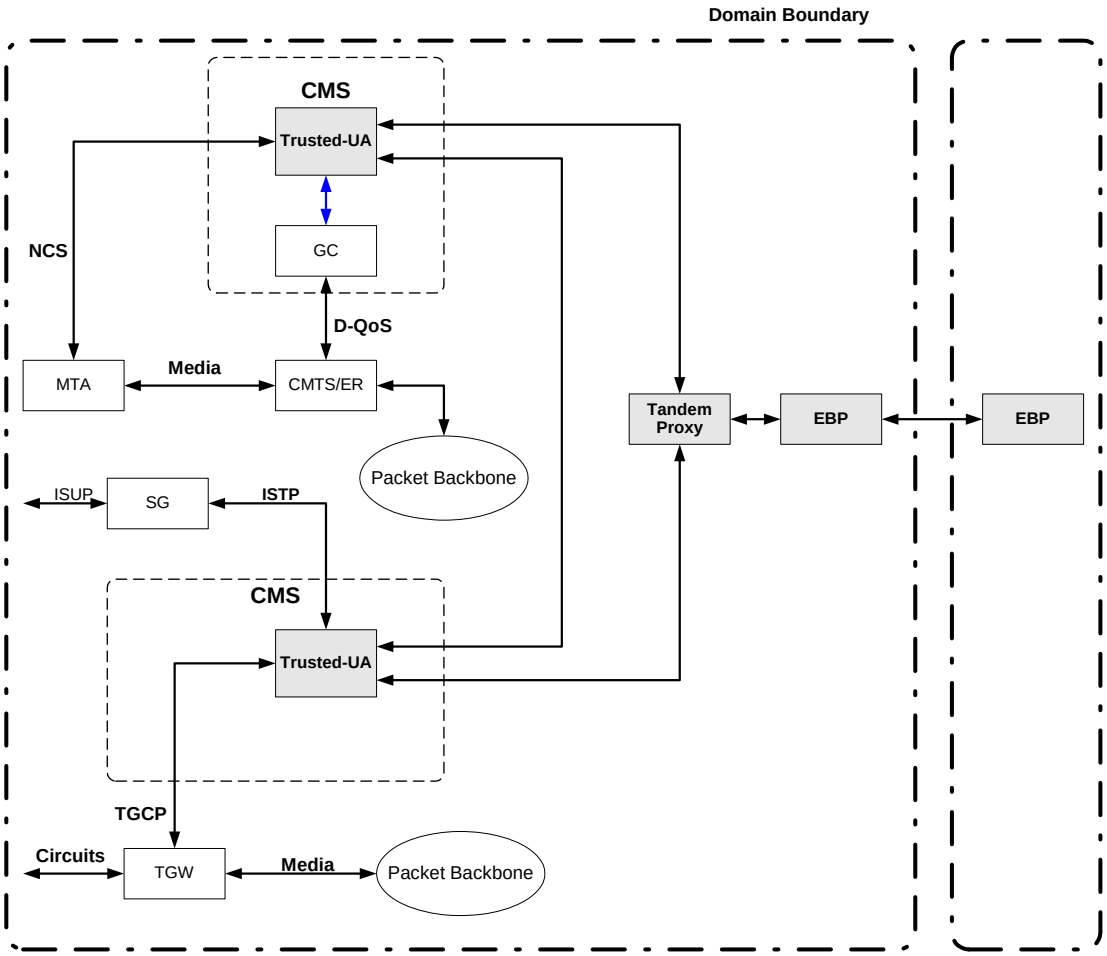

Figure 3. CMS Signaling Model

A CMS establishes connections either on its own behalf or on behalf of a non-SIP endpoint. Examples of the former are voicemail and conference bridge servers; in these cases the CMS is a trusted network entity that establishes connections on its own behalf. Examples of the latter are the Call Agent (CA) described in NCS [24], the Media-Gateway-Controller (MGC) described in [25], and the Announcement Controller (ANC) described in [57]; in all of these cases there is centralized call control, protocol messages, e.g., NCS, are exchanged between the CMS and the endpoint device, and the endpoint device does not participate in the SIP signaling exchanges directly.

[3] CMS/MGC and other types of centralized control CMSs fall within this category as well.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

The term CMS in this specification refers to either of the above categories. Where only one category is being described, the term proxy[4] or CMS will be used as a representative for the category being described.

Unless otherwise stated in this document, a CMS MUST follow the requirements given for SIP user agents in [6] and a proxy MUST follow the requirements given for SIP proxies and redirect servers in [6].

Tandem proxies act as call routers and security association aggregation points. They may also provide additional functions such as signaling transformation gateways, signaling firewalls, etc. Depending on its role, a tandem proxy may remain in the call-signaling path for the duration of the call. More detailed tandem proxy information can be found in Section 8.1.2.

5.5 Overview of CMS Behavior

IPCablecom defines the Call Management Server (CMS) as a complex of server functions which support call signaling, number translation, call routing, feature support and admission control. Within the CMS complex, the IPCablecom architecture allocates many of these responsibilities to the Proxy/CA/MGC and the Gate Controller (GC) function. In addition to processing session-signaling messages, a CMS provides functions for service and feature authorization, name/number translation, session routing, and service-specific admission control. As a trusted decision point, the CMS may also coordinate with Gate Controllers (which act as Policy Decision Points from a resource management point of view) to control when resource reservations are authorized for particular users. While the CMS is responsible for session control functions associated with proxying signaling requests, the Gate Controller is responsible for the policy decision regarding whether a requested QoS level should be admitted. Upon receipt of signaling information, a CMS instructs the Gate Controller to authorize a QoS level in advance of any resource reservation signaling (see [21] for more details).

The CMS associated with the endpoint originating a call is referred to as the originating CMS and is denoted by CMS_O. The CMS associated with the terminating endpoint is referred to as the terminating CMS and is denoted by CMS_T. The Gate Controllers (GC_O, GC_T) are the trusted policy decision points for controlling when and which resources are allowed to be reserved by endpoints; they coordinate with the CMTSs ($CMTS_O$, $CMTS_T$) through DQoS signaling. The CMTSs are the policy enforcement points, and ensure that the media path is provided the QoS it is authorized to receive.

The IPCablecom CMS-CMS architecture extends the use of the basic INVITE/200-OK/ACK SIP transaction. A provisional response, the 183-Session-Progress, and its acknowledgement, the PRACK/200-OK, are used with the initial INVITE to exchange capabilities and establish session state in the network prior to alerting the user. Following this exchange, the endpoints engage in resource reservations to obtain the resources they will need for the media streams. If the resource reservations are successful, the originating CMS performs an UPDATE/200-OK exchange. At this point the initial INVITE continues with a 180-Ringing or 183-Session-Progress, then a PRACK/200-OK followed by the final 200-OK response and ACK to the initial INVITE. In all cases, all provisional and final responses to an INVITE message traverse the path taken by the original INVITE through one or more CMSs and proxies; other messages, however, pass end-to-end directly between the originating CMS and the terminating CMS.

In support of billing functions, the originating CMS (CMS_O) includes information containing the account number of the caller and the Billing-Correlation-ID in the INVITE message that it sends.

Operator services such as Busy Line Verification (INVITE(BLV)) and Emergency Interrupt (INVITE(EI)) are initiated from a Media-Gateway-Controller type of CMS and sent to the number being verified/interrupted.

In call sequences associated with three-way calling, inter-domain call transfer, and inter-domain call forwarding, the CMS performs redirection. One possibility is that the CMS simply passes revised SDP to the other CMS, causing a redirection of media flow without changing the call topology. Alternatively, the CMS makes use of the REFER method to redirect the entire call. The REFER causes the receiver to initiate a new call using the information provided.

[4] This may be further refined, e.g., into IBP and EBP. The term tandem proxy may also be used instead of just proxy.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

5.6 Basic Telephony Call Flow

Figure 4 presents a high-level overview of an example basic call that uses the CMSS protocol between the CMSs through a proxy while the end-points (MTAs) are using the NCS protocol.

In this example[5], when the MTA goes off-hook and the user dials a telephone number, the originating MTA (MTA_O) collects the dialed digits and exchanges initial NCS messages with the originating CMS (CMS_O) to notify it of the dialed digits and create a (media) connection. As a result of creating the connection, MTA_O returns a session description using the Session Description Protocol (SDP), which will subsequently be passed to CMS_T. When CMS_O wishes to ensure that adequate resources are available in the network before users who wish to communicate are alerted, it includes additional information in the SDP. This additional information is a QoS "Pre-Condition" that needs to be satisfied before the terminating user is alerted. CMS_O verifies that MTA_O is a valid subscriber of the telephony service and determines that this subscriber is authorized to place this call. CMS_O then translates the dialed number into the address of a terminating CMS (CMS_T) and sends the (1) INVITE message to it containing the SDP with the added pre-conditions.

It is assumed that the originating and terminating CMSs trust each other. CMS_O includes additional information, such as billing data containing the telephone number of the caller, in the INVITE message that it sends to CMS_T via the proxy. CMS_T then translates the dialed number into the address of the terminating MTA (MTA_T) and exchanges NCS signaling with MTA_T to create a (media) connection for the terminating endpoint. As part of the task of creating the connection, MTA_T selects the encoding and bandwidth requirements for the media streams and returns to CMS_T a session description containing a subset of the capabilities that were present in the NCS Create Connection request that are acceptable to MTA_T. CMS_T sends a GATE-SET message to the terminating CMTS ($CMTS_T$); this GATE-SET message conveys policy instructions allowing $CMTS_T$ to create a gate for the IP flow associated with this phone call subsequent to the admission control that is performed following a resource reservation request. CMS_T may send information in the GATE-SET message to notify $CMTS_T$ of billing-related information such as the IP address of the terminating RKS, the Billing Correlation ID (see [23] for details (BCID) of the terminating event message stream, etc. (see [21] for further detail). CMS_T then sends the (2) 183- Session-Progress response back to CMS_O via the proxy. Included in the 183-Session-Progress response is the SDP from MTA_T, with an indication added by CMS_T that the terminating side agrees to meet the preconditions specified in the INVITE before alerting the user. CMS_O then sends a GATE-SET message to the originating CMTS ($CMTS_O$) to indicate that it can admit a gate for the IP flow associated with the phone call. CMS_O then sends an NCS ModifyConnection request to MTA_O, enabling MTA_O to start reserving resources.

The initial INVITE request and the 183-Session-Progress response contain a SIP Contact header to indicate the contact address of the remote CMS to be used for subsequent end-to-end SIP signaling exchanges as well as the BCID and the Financial Entity ID (FEID) of the CMS sending the message. CMS_O acknowledges the 183-Session-Progress directly to CMS_T using the (3) Provisional Reliable Ack (PRACK) message. The contact address is in the form of a Globally Routable User-Agent URI (GRUU). The terminating CMS_T acknowledges the PRACK message with the (4) 200-OK message. At this point, resource reservation has not yet completed, and thus the preconditions have not yet been met. CMS_T now issues a modify connection command to MTA_T instructing it to reserve network resources.

Once MTA_O has successfully completed its resource reservation thereby meeting its precondition, it sends an NCS signaling message to CMS_O which in turn sends the (5) UPDATE message directly to CMS_T. CMS_T acknowledges the UPDATE with the (6) 200-OK. When MTA_T has reserved its resources it exchanges NCS signaling with CMS_T. At this point in time, all preconditions have been met, and CMS_T can exchange NCS signaling with MTA_T instructing it to alert the user (ring the destination telephone). CMS_T then sends the (7) 180-Ringing message to CMS_O via the proxy indicating that the terminating phone is ringing, and that the calling party should be given a ringback call progress tone. CMS_O exchanges NCS signaling with MTA_O instructing it to provide ringback, and CMS_O sends another (8) Provisional ACK (PRACK) directly to CMS_T to acknowledge receipt of the (7) 180-Ringing message.

The terminating CMS_T acknowledges the PRACK with a (9) 200-OK. When the called party answers, by going off-hook, MTA_T exchanges NCS signaling with CMS_T to notify the off-hook and enable a full duplex connection. CMS_T also sends a (10) 200-OK final response to the (1) INVITE to CMS_O via the proxy. CMS_O acknowledges the

[5] Call flows throughout this document are examples only; IPCablecom does not mandate particular call flows.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

200-OK directly with the (11) ACK and exchanges NCS signaling with MTA_O instructing it to stop local ringback and enable a full duplex connection. At this point the resources that were previously reserved are committed, and the call is "cut through."

Either party can terminate the call. When CMS_O receives an on-hook notification from MTA_O, CMS_O sends a (12) BYE message directly to CMS_T, which is acknowledged with (13) 200-OK. Each CMS exchanges NCS signaling with its MTA to delete the connection and release the resources reserved.

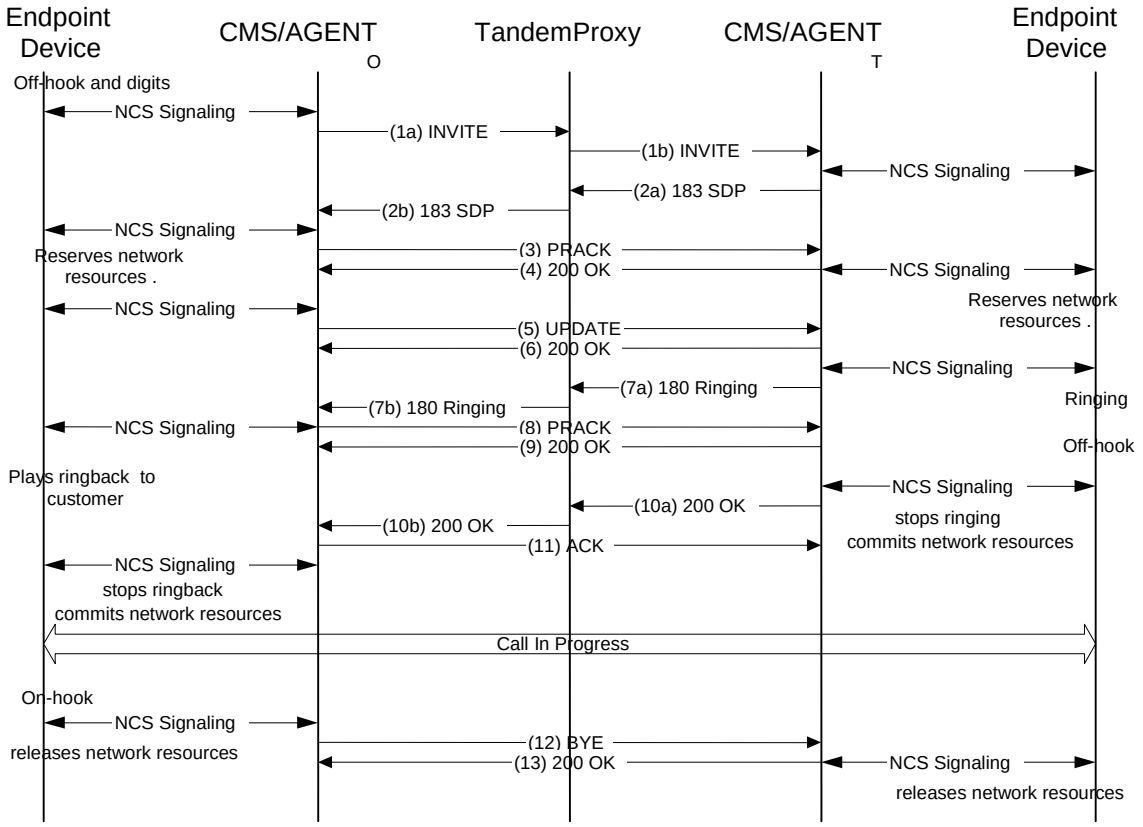

Figure 4. CMS – CMS Signaling Basic Call Flow

5.7 CMS-MGC Basic Telephony Call Flow

This section presents a high level overview of a basic call that uses the CMSS protocol between a CMS and an MGC to make an on-net to off-net call. The procedure shown follows the SIP to ISUP mapping recommendations provided in [54]. Note that CMSS in general is intended to be compatible with the interworking recommendations provided in [54].

The following procedure may be used to make a basic on-net to off-net call using CMSS as the protocol between a CMS and a MGC.

1. The subscriber goes off hook.
2. The MTA exchanges NCS signaling message with the CMS to notify the CMS that the subscriber went off hook.
3. The CMS instructs the MTA to start sending dial tone to the user by exchanging NCS signaling messages with the MTA.
4. The subscriber dials a valid telephone number.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

5. The MTA collects the dialed digits and exchanges NCS messages with the CMS to notify the CMS of the dialed digits.
6. The CMS exchanges NCS messages with the MTA to create a (media) connection. As a result of creating the connection, the MTA returns a session description using the Session Description Protocol (SDP).
7. The CMS sends the MGC a (1) INVITE message containing the SDP.
8. The MGC exchanges TGCP signaling messages with the MG to create a (media) connection. During this exchange, session description information is also exchanged.
9. The MGC then sends a (2) 183-Session-Progress response back to the CMS with the SDP from the MG.
10. The CMS exchanges DQoS messages with the CMTS and NCS messages with the MTA so that the MTA will start reserving resources.
11. The CMS acknowledges the 183-Session-Progress using the (3) Provisional Reliable Ack (PRACK) message.
12. The MGC acknowledges the PRACK message with a (4) 200-OK message.
13. Once the MTA has successfully completed its resource reservation, the MTA exchanges NCS signaling messages with the CMS.
14. The CMS sends the (5) UPDATE message to the MGC.
15. The MGC sends an IAM message to the SG.
16. The MGC acknowledges the UPDATE message with a (6) 200-OK.
17. The MGC receives an ACM message from the SG.
18. If the ACM indicates, that the called party is being alerted, the MGC sends a (7) 180-Ringing message to the CMS. If the ACM instead indicated progress or in-band information available, the MGC would have sent a 183-Session-Progress instead (see [54] for details). In this latter case, the MGC would also exchange TGCP signaling with the MG instructing the MG to send packets to the MTA so that in-band media provided by the PSTN can be heard by the subscriber.
19. The CMS exchanges NCS signaling with the MTA instructing it to play ringback to the subscriber.
20. The CMS sends another (8) Provisional ACK (PRACK) to the MGC to acknowledge the receipt of the 18x message.
21. The MGC acknowledges the PRACK with a (9) 200-OK.
22. The MGC receives an ANM message from the SG.
23. The MGC exchanges TGCP signaling with the MG instructing it to enable a full duplex connection.
24. The MGC sends a (10) 200-OK final response to the initial INVITE from the CMS.
25. The CMS exchanges NCS signaling with the MTA instructing it to enable a full duplex connection.
26. The CMS acknowledges the 200-OK with an (11) ACK message, the call is "cut through".
27. The subscriber goes on hook.
28. The MTA exchanges NCS signaling with the CMS to notify the CMS of the on hook condition.
29. The CMS exchanges NCS signaling with the MTA instructing it to delete the connection and release resources.
30. The CMS sends the MGC a (12) BYE message.
31. The MGC sends the CMS a (13) 200-OK to acknowledge the BYE message.
32. The MGC sends a REL message to the SG.
33. The SG sends a RLC message to the MGC.
34. The MGC exchanges TGCP messages with the MG instructing the MG to delete the connection.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

Figure 5 shows a basic on-net to off-net call flow using CMSS as the protocol between the CMS and the MGC.

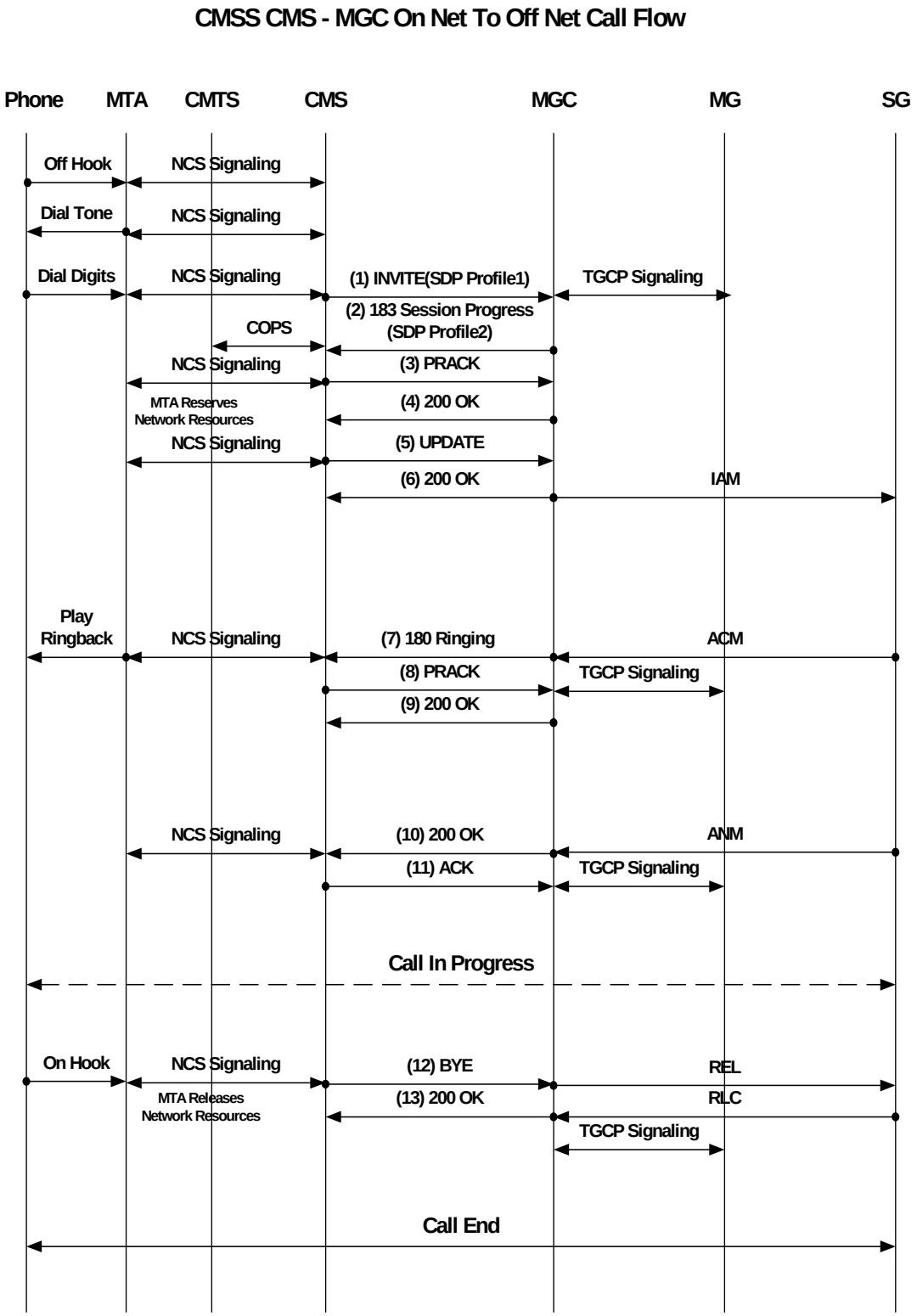

Figure 5. CMS to MGC Signaling

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

6 SIP PROFILE

This section defines a SIP [6] profile for usage in CMSS compliant systems. This section is structured to mirror the SIP document and its section numbering. The subsections of this section are numbered such that the second digit tracks the SIP section numbers of the SIP specification [6], and section titles at all header levels track the section titles of the SIP specification [6].

This section and Section 7 define the nearly complete set of enhancements and restrictions to a standard SIP implementation based on [6]. However, not all details of the required behavior can be captured in these sections. Later sections provide details needed for certification and interoperability testing, which are generally not present in [6]. Sections 6 through 9 are considered normative.

6.1 Introduction

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 1.

Since there are no requirements in SIP/2.0 [6] Section 1, CMSS implementations are automatically compliant with it.

6.2 Overview of SIP Functionality

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 2.

Since there are no requirements in SIP/2.0 [6] Section 2, CMSS implementations are automatically compliant with it.

6.3 Terminology

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 3.

Since there are no requirements in SIP/2.0 [6] Section 3, CMSS implementations are automatically compliant with it.

6.4 Overview of Operation

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 4.

Since there are no requirements in SIP/2.0 [6] Section 4, CMSS implementations are automatically compliant with it.

6.5 Structure of the Protocol

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 5.

Since there are no requirements in SIP/2.0 [6] Section 5, CMSS implementations are automatically compliant with it.

6.6 Definitions

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 6.

The reader should note that the term "client" in this section covers both UAs and proxies.

Since there are no requirements in SIP/2.0 [6] Section 6, CMSS implementations are automatically compliant with it.

6.7 SIP Messages

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7, except as noted below.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

6.7.1 Requests

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7.1, except as defined in this section.

The INVITE, ACK, CANCEL, BYE, and OPTIONS methods MUST be supported. The REGISTER method MAY be supported.

The SIP URI as defined in [6] and tel URI as defined in Section 7.1 MUST be supported in the Request-URI.

When generating an initial INVITE for a basic telephone call, the Request-URI SHOULD identify the called party using a tel URI or by using the telephone-subscriber syntax (i.e., "user=phone") in a SIP URI. Refer to Section 8.3 for details on forming the associated Request-URI.

6.7.2 Responses

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7.2.

6.7.3 Header Fields

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7.3 and its subsections.

Furthermore, CMSS compliant applications MUST be able to both generate and accept short and long form header field names as defined in [6] Section 7.3.3.

6.7.4 Bodies

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7.4 and its subsections except as defined in this section.

6.7.4.1 Message Body Types

CMSS compliant applications MUST support the message body type "application/sdp".

The message body type "application/sdp" MUST be supported with the INVITE, UPDATE, and PRACK methods as well as any non-failure response to these methods. Furthermore, the message body type "application/sdp" MUST be supported in success responses to OPTIONS requests, and 488 responses to INVITE requests.

Refer to Appendix B for a complete list of supported values.

6.7.4.2 Message Body Length

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7.4.2.

6.7.5 Framing SIP Messages

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 7.5.

6.8 General User Agent Behavior

Behavior of CMSS User Agents (UA) MUST be in accordance with Section 8 of this document and with [6] except as noted in this section.

Note that the behavior defined in this section applies only to requests and responses outside of a dialog. Behavior within a dialog is defined in 6.12.

6.8.1 UAC Behavior

Support for the REGISTER method is OPTIONAL, however, if supported, it MUST be as specified in [6] Section 8.1.

When a request is forked, multiple responses may be received, each of which results in the creation of an early dialog. Furthermore, each response may contain an answer and each early dialog may involve early media. Support for multiple simultaneous media streams for a single call, however is OPTIONAL for an MTA. In particular, MTAs may not be able to receive media from multiple different sources simultaneously, e.g., due to resource constraints, or

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

when security services are used on the media stream. Furthermore, having multiple different sources sending media to the MTA at the same time has QoS implications that are outside the scope of this document.

As a result of this, whenever a given request results in multiple early dialogs with multiple simultaneous media streams, the UAC SHOULD NOT enable early media on more than one of these dialogs. The details of how that is achieved are left to the implementation, however below are two options:

- The UAC may provide the MTA with the answer SDP from one of the early dialogs. The MTA in turn will only process media received in accordance with that SDP.

- When answer SDPs are received on the early dialogs, the UAC may issue new offers on all but one of these to suppress early media. Note that this will also suppress final media until a new offer/answer exchange has been performed.

Note that when media stream security is not being used, and the answer SDP is not provided until the final answer, the UAC cannot prevent the MTA from receiving multiple early media streams.

Once a final dialog has been established, media SHOULD be allowed on that dialog only.

6.8.1.1 Generating the Request

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 8.1.1, except as noted below.

Request-URI in the request contains the address of the callee. This will normally be a telephone-number, but it may also be a general SIP URI[6]. The From and To fields in the request might contain random strings that protect the Privacy of the session originator.

Refer to Section 6.20 for further details of various header field values to be used.

By default, CMSS compliant implementations MUST NOT require support for any particular extension. However, a given deployment MAY be configured to require one or more extensions to be supported. A default CMSS implementation will thus not use the Require or Proxy-Require header fields in requests outside of a dialog. Instead, a list of supported extensions will be included in the SIP Supported header in requests outside of a dialog. Once a dialog has been established (whether early or final), one or more of the supported extensions can then be required.

The above defines the default CMSS implementation, however a particular deployment MAY require that one or more extensions are supported. The set of extensions that are required to be used in a particular deployment can be configured on the CMSS. When one or more of such extensions have been configured as required, requests outside of dialogs will include the relevant option tags in the Require and/or Proxy-Require header fields. It should be noted that signaling with endpoints as well as proxies that do not support a required extension will result in failures.

The IETF allows option tags to be defined for their purpose only in standards-track RFCs. In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

6.8.1.2 Processing Responses

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 8.1.3 except as noted in this section.

When receiving a 401 (Unauthorized) or 407 (Proxy Authentication Required) response, the SIP authorization procedure SHOULD only be followed if the UAC has credentials for the realm in question.

When receiving a 420 (Bad Extension) response, the SIP retry procedures SHOULD NOT be followed in the case where the deployment has been configured to require support of any of the extensions listed in the Unsupported header. In all other cases, the SIP retry procedures SHOULD be followed.

6.8.2 UAS Behavior

The CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 8.2 and its subsections.

[6] This can, for example, be used when forwarding to a an Interactive Voice Response (IVR) system.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

6.8.3 Redirect Servers

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 8.3.

6.9 Canceling a Request

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 9 and its subsections.

6.10 Registrations

Proxies MUST, and UACs MAY, support the SIP REGISTER method in accordance with [6] Section 10. Support for registrars is OPTIONAL; however if supported, it MUST be as specified in [6] Section 10.

6.11 Querying for Capabilities

CMSS compliant applications MUST be in accordance with SIP/2.0 [6], Section 11.

6.12 Dialogs

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 12 and its subsections.

6.13 Initiating a Session

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 13 and its subsections, except as noted in this section.

CMSS compliant implementations SHOULD include a message body of type "application/sdp" with the initial INVITE.

When an initial INVITE is received with an offer SDP, an answer SDP SHOULD be included in the first non-failure response to the INVITE. Note that if the response is not sent reliably, then the same answer SDP must be sent in the final response.

6.14 Modifying an Existing Session

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 14 and its subsections, except as noted in this section.

When a CMSS compliant implementation sends a re-INVITE, it SHOULD include a message body of type "application/sdp" with a new offer. Furthermore, CMSS compliant implementations MUST support the procedures for modifying an existing session described in Section 8.4.4.

6.15 Terminating a Session

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 15 and its subsections.

6.16 Proxy Behavior

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 16 and its subsections, except as noted in this section.

Support for multiple simultaneous media streams for a single call is OPTIONAL for an MTA. Since parallel forking may result in multiple simultaneous media streams for a single call, systems that interact with CMSS compliant implementations should avoid using parallel forking and early media at the same time.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

6.17 Transactions

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 17 and its subsections except as noted in this section.

Behavior of CMSS servers (proxies) MUST be in accordance with Section 8 of this document, which takes precedence over [6] Section 17 in case of any conflicts.

6.18 Transport

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 18 and its subsections.

6.19 Common Message Components

6.19.1 SIP URI Component

The definition of a SIP URI is as given in [6] Section 19.1.1 and extended in Section 7.1.1 in this document.

6.20 Header Fields

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 20 and its subsections, except as defined in this section.

In addition to the extensions listed in Section 7, the following SIP headers MUST be supported by CMSS compliant applications.

1. Accept
2. Accept-Encoding
3. Accept-Language
4. Allow
5. Call-ID
6. Contact
7. Content-Disposition
8. Content-Encoding
9. Content-Length
10. Content-Type
11. CSeq
12. From
13. Max-Forwards
14. MIME-Version
15. Proxy-Require
16. Record-Route
17. Require
18. Route
19. Supported
20. Timestamp
21. To

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

22. Unsupported

23. Via

Other SIP headers MAY be supported by CMSS compliant applications. CMSS compliant applications SHOULD ignore unsupported optional headers.

Listed below is each SIP header defined in [6], and the requirements for supporting each in CMSS are identified.

6.20.1 Accept

The Accept header MUST be supported as specified in [6] Section 20.1.

6.20.2 Accept-Encoding

The Accept-Encoding header MUST be supported as specified in [6] Section 20.2, except as noted below.

The Accept-Encoding header MAY be used by CMSS compliant implementations. The "identity" encoding value MUST be supported; other encodings MAY be supported.

6.20.3 Accept-Language

The Accept-Language header MUST be supported as specified in [6] Section 20.3, except as noted below.

CMSS compliant implementations SHOULD include the "Accept-Language" header in requests or responses as defined in [6]. The value "en" for English MUST be supported, other values MAY be supported based on configuration data.

6.20.4 Alert-Info

The Alert-Info header MUST be supported for emergency calls (see Section 8.4.2) ; otherwise, it MAY be supported. When included, it MUST be as specified in [6] Section 20.4.

It is noted that there are security risks associated with acting on the Alert-Info header as described in [6] Section 20.4.

6.20.5 Allow

The Allow header field MUST be supported as specified in [6] Section 20.5. CMSS compliant implementations MUST include the "Allow" header in the initial INVITE and the 200-OK response to the initial INVITE. When an Allow header is not received, the set of supported methods is unknown.

Refer to Appendix B for a list of supported methods.

6.20.6 Authentication-Info

Support for the Authentication-Info is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.6.

See also Section 6.22.

6.20.7 Authorization

Support for the Authorization header field is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.7.

See also Section 6.22.

6.20.8 Call-ID

The Call-ID header MUST be supported as specified in [6] Section 20.8, except as noted below.

CMSS restricts contents of the Call-ID header in order to support user Privacy.

When Privacy is requested by the session originator, the Call-ID MUST NOT contain the "@" sign and hence consists of a single "word" as defined in [6] Section 25.1. The "word" MUST be a random identifier, and MUST be unique across all possible UAs with probability of greater than 0.999999. A suggested implementation is a text encoding (which does not contain an "@") of a cryptographic hash of phone number, time, a random number, and a

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

quantity provisioned or manufactured to be unique across UAs of otherwise identical manufacture. The last quantity is suggested to help prevent UAs of an otherwise identical manufacture from producing identical "random" Call-IDs when presented with identical stimuli.

6.20.9 Call-Info

The Call-Info header MUST be supported as specified in [6] Section 20.9 except as noted below.

The Call-Info header "purpose" parameter value of "answer_if_not_busy" MUST be supported; other encodings MAY be supported.

It is noted that there are security risks associated with acting on the Call-Info header as described in [6] Section 20.9.

6.20.10 Contact

The Contact header MUST be supported as specified in [6] Section 20.10, except as noted below.

CMSS compliant applications MUST populate the Contact header field in an INVITE request, and in a 2xx response to an INVITE request, with a SIP URI. The contact address MUST be in the form of a Globally Routable User-Agent URI (GRUU) [36] as specified in 7.11.

When the user is requesting Privacy, the Contact header field SHOULD NOT contain any domain names; the IP address form SHOULD be used instead. It should be noted that, in systems with multiple network interfaces, use of the (single) IP address form can reduce the overall system reliability. If multiple interfaces exist and reliability is a concern, it is considered a reasonable trade-off to refrain from using the IP address form. When providing a GRUU on behalf of a user that is requesting Privacy the CMSS compliant application MUST provide a GRUU that does not reveal the identity of the user (i.e., a GRUU that has the properties of a temporary GRUU as defined in draft-ietf-sip-gruu [36]).

CMSS compliant applications MUST populate the Contact header field in a 3xx response to an INVITE request with a valid SIP or tel-URI. If the new destination is a telephone number, it SHOULD contain a tel URI with the number of the new destination as described in Section 7.1. Support for any other type of URI is OPTIONAL.

6.20.11 Content-Disposition

The Content-Disposition header MUST be supported as specified in [6] Section 20.11, except as noted below.

The Content-Disposition header MAY be used by CMSS compliant implementations. The value "session" MUST be supported; other values MAY be supported.

Note that the default value for message bodies of type "application/sdp" is "session", whereas the default value for all other message body types (e.g., "message/sipfrag") is "render". If the default value is not desired, then the Content-Disposition header MUST be included.

6.20.12 Content-Encoding

The Content-Encoding header MUST be supported as specified in [6] Section 20.12, except as noted below.

The Content-Encoding header MAY be used by CMSS compliant implementations. The "identity" encoding value MUST be supported; other encodings MAY be supported.

6.20.13 Content-Language

Support for the Content-Language header is OPTIONAL, however if supported, it MUST be as specified in [6] Section 20.13.

6.20.14 Content-Length

The Content-Length header MUST be supported as specified in [6] Section 20.14.

It should be noted, that when stream-based protocols (such as TCP) are being used, a Content-Length header field must always be included, even if set to zero.

6.20.15 Content-Type

The "Content-Type" header MUST be supported as specified in [6] Section 20.15.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

Refer to Appendix B for a list of supported values.

6.20.16 CSeq

The CSeq header MUST be supported as specified in [6] Section 20.16.

6.20.17 Date

Support for the Date header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.17.

6.20.18 Error-Info

Support for the Error-Info header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.18.

It is noted that there are security risks associated with acting on the Error-Info header as described in [6] Section 20.18.

6.20.19 Expires

Support for the Expires header in the non-REGISTER methods and responses defined in [6] is OPTIONAL[7]; however, if supported, it MUST be as specified in [6] Section 20.19.

6.20.20 From

The From header MUST be supported as specified in [6] Section 20.20, except as noted below.

In support of user Privacy, CMSS restricts the allowed contents of the SIP "From" header.

When the session originator requests Privacy, compliant applications MUST generate a From header according to the following rules :

- The display-name MUST be "Anonymous".
- The addr-spec MUST contain the identifier "anonymous" for userinfo.
- The addr-spec MUST contain the non-identifying hostname "anonymous.invalid".

6.20.21 In-Reply-To

Support for the In-Reply-To header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.21.

Note that use of this header is subject to security considerations as described in [6] Section 20.21.

6.20.22 Max-Forwards

The Max-Forwards header MUST be supported as specified in [6] Section 20.22, except as noted below.

When a CMSS compliant implementation of a back-to-back User Agent (B2BUA) forwards a request, it SHOULD use a Max-Forwards value equal to the incoming Max-Forwards value minus one.

6.20.23 Min-Expires

Support for the Min-Expires header is OPTIONAL (since support for the REGISTER method is optional); however, if supported, it MUST be as specified in [6] Section 20.23.

6.20.24 MIME-Version

The MIME-Version header MUST be supported as specified in [6] Section 20.24, except as noted below.

The MIME-Version header MAY be used by CMSS compliant implementations. The version "1.0" value MUST be supported; other values MAY be supported.

[7] Note that, per Section 7.5, support for the Expires header is required for the SUBSCRIBE method.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

6.20.25 Organization

Support for the Organization header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.25.

6.20.26 Priority

The Priority header MUST be supported for emergency calls (see Section 8.4.2); otherwise, it MAY be supported. When included, it MUST be as specified in [6] Section 20.26.

There are security ramifications for entities that act on this header.

6.20.27 Proxy-Authenticate

Support for the Proxy-Authenticate header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.27.

See also Section 6.22.

6.20.28 Proxy-Authorization

Support for the Proxy-Authorization header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.28.

See also Section 6.22.

6.20.29 Proxy-Require

The Proxy-Require header MUST be supported as specified in [6] Section 20.29, except as noted below.

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

Refer to Appendix B for a list of supported values.

Refer to Section 6.8.1.1 for considerations around the use of required proxy extensions.

6.20.30 Record-Route

The Record-Route header MUST be supported as specified in [6] Section 20.30.

6.20.31 Reply-To

Support for the Reply-To header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.31.

6.20.32 Require

The "Require" header MUST be supported as specified in [6] Section 20.32, except as noted below.

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

Refer to Appendix B for a list of supported values.

Refer to Section 6.8.1.1 for considerations around the use of UserAgent extensions.

6.20.33 Retry-After

Support for the Retry-After header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.33.

6.20.34 Route

The Route header MUST be supported as specified in [6] Section 20.34.

6.20.35 Server

Support for the Server header is OPTIONAL; however, if supported, it MUST be as specified [6] Section 20.35.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

6.20.36 FSubject

Support for the Subject header is OPTIONAL, however, if supported, it MUST be as specified [6] Section 20.36.

6.20.37 Supported

The "Supported" header MUST be supported as specified in [6] Section 20.37, except as noted below.

In addition to the standards-track RFCs' option tags, option tags from non-IETF documents MAY also be used, as long as they are defined in this document.

Refer to Appendix B for a list of supported values.

Refer to Section 6.8.1.1 for considerations around the use of UserAgent extensions.

6.20.38 Timestamp

The Timestamp header MUST be supported as specified in [6] Section 20.38, except as noted below.

CMSS compliant implementations MAY send the Timestamp header in requests; if received, this header MUST be processed as described in [6] Section 20.38.

6.20.39 To

The To header MUST be supported as specified in [6] Section 20.39, except as noted below.

In support of user Privacy, CMSS restricts the allowable contents of the SIP "To" header. The "To" header may indicate the dialed digits in a tel-URI (see Section 7.1). This information is of end-to-end significance, and might reveal information about the caller's location, e.g., local, long-distance, PBX, or international.

When the call originator requests Privacy, CMSS compliant applications MUST generate a "To" header according to the following rules:

- The display-name MUST be absent.
- If a global telephone number is used (as defined in [28]), then the userinfo part of the addr-spec MUST contain a full E.164 number, including the country code.
- If a local telephone number is used (as defined in [28])), then the userinfo part of the addr-spec must contain a phone-context. When possible, the phone-context should be a country code.

When the call originator does not request privacy, CMSS compliant applications SHOULD generate a "To" header according to the following rules:

- If a global telephone number is used (as defined in [28]), then the userinfo part of the addr-spec must contain a full E.164 number, including the country code.
- If a local telephone number is used (as defined in [28]), then the userinfo part of the addr-spec must contain a phone-context. When possible, the phone-context should be a country code.

6.20.40 Unsupported

The Unsupported header MUST be supported as specified in [6].

6.20.41 User-Agent

Support for the User-Agent header is OPTIONAL; however, if supported, it MUST be as specified [6] Section 20.41.

6.20.42 Via

The Via header MUST be supported as specified in [6] Section 20.42, except as noted below.

When the user is requesting Privacy, the Via header field SHOULD NOT contain any domain names; the IP address form SHOULD be used instead. Support for IP address Privacy is described in more detail in Section 8.4.1.1.3. It should be noted that, in systems with multiple network interfaces, use of the (single) IP address form can reduce the overall system reliability. If multiple interfaces exist and reliability is a concern, it is considered a reasonable trade-off to refrain from using the IP address form.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

A border proxy (EBP) which is passing a request outside of the trusted domain of the service provider MAY encrypt all "Via" headers except the topmost header (i.e., the "Via" header of the terminating proxy) to a non-recognizable string. The proxy MAY include the encrypted string in the Via header, or it may cache the encrypted "Via" headers and include a local token string in the Via header.

6.20.43 Warning

Support for the Warning header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.43.

6.20.44 WWW-Authenticate

Support for the WWW-Authenticate header is OPTIONAL; however, if supported, it MUST be as specified in [6] Section 20.44.

See also Section 6.22.

6.21 Response Codes

CMSS compliant applications MUST be in accordance with SIP/2.0 [6] Section 21 and its subsections, except as specified below.

CMSS compliant applications SHOULD NOT issue a 401 or a 407 response; however, they MUST process any such received responses in accordance with Section 6.8.1.2.

CMSS compliant implementations MUST be in accordance with reference [45] in their ability to process any 433 Anonymity Disallowed final response that is received.

6.22 Usage of HTTP Authentication

Support of HTTP Authentication is OPTIONAL; however, if used, it MUST be as specified in [26] and [6] Section 22. Where these documents conflict, [26] takes precedence.

See also Section 6.21.

6.23 S/MIME

Support of S/MIME is OPTIONAL; however, if used, it MUST be as specified in [26] and [6] Section 23. Where these documents conflict, [26] takes precedence.

6.24 Examples

The examples provided in [6] Section 24 do not apply to CMSS compliant implementations. For equivalent examples, refer to Section 8 in this document.

6.25 Augmented BNF for the SIP Protocol

CMSS compliant applications MUST comply with SIP/2.0 [6] Section 25.

6.26 Security Considerations: Threat Model and Security Usage Recommendations

CMSS complaint applications MUST comply with the IPCablecom Security specification [26].

Support for the SIP Security Considerations specified in [6] Section 26 is considered OPTIONAL, unless they conflict with the IPCablecom Security specification [26], in which case they MUST NOT be used.

6.27 Table of Timer Values

CMSS compliant applications MUST comply with SIP/2.0 [6] Appendix A.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

CMSS compliant applications MUST also support the timer values defined in Appendix A according to the procedures specified in 8.4.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

7 SIP EXTENSIONS

SIP [6] has a flexible mechanism for adding extensions and new fields to the protocol for support of additional capabilities. This section defines a set of SIP extensions that enables IPCablecom CMSS-compliant systems to provide a robust multimedia service platform supporting basic telephony, CLASS, and custom calling features, while at the same time allowing the supported services to evolve to a multimedia environment. Many of the extensions have been documented in RFCs, to which this document provides cross-references.

This section describes procedures applicable to both NCS and SIP based endpoints; however, it should be noted that SIP based MTAs are out of scope of IPCablecom 1.5 and are described and listed in this section for reference purposes only. The term SIP User Agent (UA) in this section refers to an originator/terminator of SIP requests. The combination of a UA with its SIP Proxy is in many ways equivalent to a CMS; likewise a CMS may be decomposed into a UA and a SIP Proxy (with a hidden and untestable interface between them) as shown in Figure 3.

This section follows the naming convention of SIP [6] of User Agents, Clients, Servers, and Proxies. User Agent Clients initiate requests and in particular initiate sessions (i.e., they are call originators), and User Agent Servers respond to requests and in particular accept session requests (i.e., they are call terminators). A User Agent performs either role as required within the context of the call. The description of each extension in this section gives the specific procedures for CMSs and Proxies.

This specification extends SIP in several ways, which are summarized here. A CMSS compliant implementation MUST support all of these:

- CMSS supports a resource reservation scheme in which network resources are reserved prior to alerting the user. This is done through specification of preconditions that must be met prior to continuing the session establishment. Confirmation that the preconditions are met is indicated by an additional end-to-end message exchange (UPDATE/200-OK), which is nested within the normal INVITE/200-OK/ACK message exchange. This extension allows network resources to be reserved prior to alerting the user and also allows network resources to be committed after the user has accepted the invitation, i.e., answered the call. This extension is described further in [11].
- CMSS supports Privacy extensions to SIP. These extensions enable users to make connections without identifying themselves or revealing location information. When Privacy is not requested by the originator, calling number delivery and calling name delivery is provided to the destination (i.e., Caller-ID service) in a reliable manner. Entity identity is also provided to support regulatory features such as Customer Originated Trace, enabling a destination party to report a harassing session even if the originator requested anonymity. This extension is further described in [12] and [13].
- CMSS supports the DCS proxy-to-proxy extensions to SIP that allow proxies to pass additional information between them to perform service-provider functions such as accounting, authorization, billing, coordination of resources, electronic surveillance, etc. This extension is further described in [16].
- CMSS supports the ability to send a reliable provisional response to a SIP request, ensuring the delivery of the provisional response to the initiating UA, with retransmissions as needed. This extension is further described in [7].
- CMSS supports the ability to send a request to another user agent to instruct that other user agent to initiate a new INVITE. Three extensions are defined for this, as described in [17], [9] and [18].
- CMSS supports the ability to send a request to another user agent to update that user agent with parameters of the session that do not impact the state of the session (e.g., media parameters). This extension is further described in [10].

The remainder of this section defines further extensions to SIP required by a CMSS compliant application.

This section, and Section 8, define the nearly complete set of enhancements and requirements to a standard SIP implementation based on [6]. However, not all details of the required behavior can be captured in these sections. Later sections provide details needed for certification and interoperability testing. Sections 6 through 9 of this document are normative.

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

7.1 URIs for Telephone Calls

CMSS compliant implementations MUST support URIs for telephone calls as specified in RFC3966 [28], except as noted in this section.

7.1.1 Routing Number, Number Portability, Carrier Identification Code, and Dial Around Indication Number

CMSS compliant implementations MUST support extensions to the tel URI that relate to number portability and freephone service, as specified in RFC 4694 [29], except as noted in this section.

CMSS compliant implementations MUST support extensions to the tel URI that relate to the subscriber's presubscribed or dialed Carrier ID Code (CIC), as specified in [29] and draft-yu-tel-dai [51], except as noted in this section.

CMSS compliant implementations MUST support extensions to the tel URI to define a dial-around-indicator to indicate how the CIC was derived, as specified in [51] with the exceptions noted in this section.

These extensions are defined as optional in the tel URI sense. RFC3966 [28] specifies that an implementation MAY ignore optional parameters. However, CMSS compliant implementations MUST support the extensions as specified in [29] and [51], and hence they MUST NOT be ignored when received.

Unless stated otherwise in this document, the set of requirements within [51] that apply to a CMSS compliant implementation depend on the role of the CMS as follows:

- a CMS that plays the role of a Call Agent serving NCS endpoints MUST follow the requirements for "Network Node A" specified in [51],
- a CMS that plays the role of a proxy MUST follow the requirements for "Network Node B" specified in [51],
- an MGC MUST follow the requirements for the "GSTN GW" as specified in [51].

CMSS compliant implementations will use the [51] CIC feature to identify not only freephone carriers but also customers' pre-subscribed or dialed carrier access codes as follows:

- If the number dialed is a freephone number and a CIC parameter is included in the response to the freephone database query, then the CIC MUST identify the carrier serving that freephone number, irrespective of the customers presubscribed or dialed carrier.
- If the number dialed is a not a freephone number and carrier-based routing is to be done for the call, then the CIC MUST identity the pre-subscribed carrier for the caller, unless the caller dialed a carrier access code, in which case the CIC for that carrier MUST be used. Also, if the number dialed is not a freephone number and carrier-based routing is to be done for the call, then the dial-around-indicator parameter MUST be included. The dial-around-indicator parameter SHOULD NOT be included in any other case. When the dial-around-indicator parameter is included, it MUST be set to one of the following values:
    - "presub" - the CIC contains the caller's presubscribed carrier
    - "presub-da" - the CIC contains the caller's dialed carrier-identification-code; the caller has a presubscribed carrier
    - "presub-daUnkwn" - the CIC may contain either a caller dialed carrier-identification-code or the caller's presubscribed carrier
    - "da" - the CIC contains the caller's dialed carrier-identification-code; the caller does not have a presubscribed carrier
    - "CIC-chrgPty" - the CIC is the preferred carrier of the charged party
    - "altCIC-chrgPty" - the CIC is the alternate carrier of the charged party
    - "verbal-clgPty" - the CIC was delivered verbally by the calling party
    - "verbal-chrgPty" - the CIC was delivered verbally by the charged party
    - "emergency" - this is an emergency call

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

- "operator" - the carrier was selected by a network operator

7.1.2 Procedures at an Originating CMS

If the Request-URI of an initial INVITE requires routing via an equal access carrier in the PSTN and is either a tel-URI or a Sip URI with user=phone, a carrier-id-code parameter MUST be included in the telephone-subscriber part with a value corresponding to the identity of the carrier preferred by the party paying for the call. Note that, for freephone numbers, this will be the carrier serving the freephone number. If CMS_O provides support for the caller to select a preferred carrier on a per-call basis, the carrier-id-code parameter MUST be included in the telephone-subscriber part and set to the carrier-id-code that the caller has dialed, unless the number dialed is a freephone number. The carrier-id-code MAY furthermore be included in the Refer-To URI of a REFER request, when the party performing the refer is the party paying for the call.

A Tel or SIP(s) URI containing "npdi" in the telephone-subscriber part MUST NOT appear other than in an initial INVITE Request-URI or the Refer-To URI of a REFER request sent to a proxy or CMST.

An originating CMS that performs the local-number-portability lookup and passes the REFER or initial INVITE request to a proxy or a terminating CMS MUST generate a Request-URI containing a SIP(s) or Tel URI with the "npdi" parameter in the telephone-subscriber part.

An originating CMS that performs the local-number-portability lookup and passes the REFER or initial INVITE request to a proxy or a terminating CMS MUST include the "rn" parameter indicating the returned value if the local-number-portability lookup returned a value different from the dialed number.

7.1.3 Procedures at a Terminating CMS

No specific procedures are defined.

7.1.4 Procedures at Proxy

A Tel or SIP(s) URI containing a "npdi" in the telephone-subscriber part MUST NOT appear other than in an initial INVITE Request-URI or the URI of a Refer-To header in a REFER request sent to another proxy or CMS_T.

A proxy that performs the local-number-portability lookup and passes the REFER or initial INVITE request to another proxy or CMS_T MUST, in each of these cases, generate a SIP(s) or Tel URI containing "npdi". A proxy that performs the local-number-portability lookup and passes the REFER or initial INVITE request to another proxy or CMS_T MUST include the "rn" parameter indicating the returned value if the local-number-portability lookup returned a value.

7.2 Reliability of Provisional Responses

CMSS compliant implementations MUST support the extensions defined in [7], except as noted in this section.

CMSS compliant implementations MUST by default include a Supported header containing the value "100rel" in the initial INVITE request. Alternatively, if a CMS is configured to require use of reliable provisional responses, the initial INVITE request MUST include a Require header containing the value "100rel".

When a CMSS compliant implementation receives an INVITE request with a Supported header that contains the value "100rel", the CMS MUST send all non-100 provisional response reliably as defined in [7].

7.3 SIP UPDATE Method

CMSS compliant implementations MUST support the extensions defined in [10] except as noted in this section.

CMSs MUST include the method "UPDATE" in the Allow header field in the relevant requests and responses as described in Section 6.

7.4 Integration of Resource Management and SIP

CMSS compliant implementations MUST support the extensions defined in [11] except as noted in the subsections below. In particular, CMSS compliant implementations MUST support segmented QoS preconditions. CMSS

Documents
Document Sharing Hub

Full document details: SCTE 165-18 2009

compliant implementations MAY support end-to-end QoS preconditions, although the procedures are not specified here.

7.4.1 Procedures at an Originating CMS

CMSS compliant implementations MUST support use of segmented QoS preconditions as defined in the following subsections, however if a given deployment does not want to use QoS preconditions, the session originator (CMS_O) MUST NOT include any QoS precondition attributes in the SDP, and the procedures below do not apply. When QoS preconditions are supported and can be used, one of the following three procedures MUST be followed.

7.4.1.1 Default Operation Using QoS Preconditions Strength "Optional"

Unless configured otherwise, the session originator (CMS_O) MUST include a Supported header containing the value "precondition". For each media flow in the SDP sent with the INVITE, the precondition-type MUST be "qos", and the status-type MUST be segmented, i.e., there needs to be separate attributes for the local and the remote segment as described in [11]. The strength-tag in the desired-status attributes MUST be "none" and the direction-tag in the local and remote desired-status attributes MUST be "sendrecv".

When CMS_O receives an answer SDP, CMS_O MUST see if the answer SDP contains any QoS preconditions: if it does, then session establishment MUST continue in accordance with the QoS preconditions. Otherwise, session establishment is already progressing and CMS_O MUST simply continue with local QoS operations independent of session progress.

7.4.1.2 QoS Preconditions Strength "None"

If a given deployment has no preference about the use of QoS preconditions, the session originator (CMS_O) SHOULD include a Supported header containing the value "precondition". For each QoS precondition it includes in the SDP, the precondition-type MUST then be "qos", and the status-type MUST be segmented, i.e., there needs to be separate attributes for the local and the remote segment as described in [11]. The strength-tag in the desired-status attributes MUST be "none",and the direction-tag in the local and remote desired-status attributes MUST be "sendrecv".

When CMS_O receives an answer SDP, CMS_O MUST see if the answer SDP contains any QoS preconditions; if it does, then session establishment MUST continue in accordance with the QoS preconditions. Otherwise, session establishment is already progressing and CMS_O MUST simply continue with local QoS operations independent of session progress.

7.4.1.3 QoS Preconditions Strength "Mandatory"

If a given deployment requires use of QoS preconditions, the session originator (CMS_O) MUST include a Require header containing the value "precondition". For each media flow in the SDP sent with the INVITE, the precondition-type MUST be "qos", and the status-type MUST be segmented, i.e., there needs to be separate attributes for the local and the remote segment as described in [11]. The strength-tag in the desired-status attributes MUST be "mandatory", and the direction-tag in the local and remote desired-status attributes MUST be "sendrecv".

7.4.2 Procedures at a Terminating CMS

When an INVITE is received without any QoS preconditions, the procedures in this section do not apply; instead normal SIP processing of the call occurs. When an INVITE with QoS preconditions is received, three sets of procedures are defined in the following subsections.

7.4.2.1 QoS Preconditions Strength "None" or "Optional"

Unless configured otherwise, on receipt of an INVITE request containing "optional" or "none" QoS preconditions using a segmented status-type, a terminating CMS (CMS_T) MUST generate a 183-Session-Progress response with an SDP containing mandatory preconditions. For each media flow with QoS precondition in the answer SDP, the precondition-type MUST be "qos" and the status-type MUST be segmented, i.e., there needs to be separate attributes for the local and the remote segment as described in [11]. The strength-tag in the desired-status attributes MUST be "mandatory" (i.e., CMS_T must upgrade the strength to "mandatory" in the answer), and the direction-tag in the local and remote desired-status attributes MUST be "sendrecv".

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

Unless configured otherwise, CMS_T MUST NOT proceed with the session until resources have been reserved in both the local and remote segments. If the desired status of the originating segment (remote from CMS_T's point of view) QoS precondition does not match its current status, then CMS_T MUST request a confirmation of the originating segment QoS reservation from CMS_O by adding an "a=conf:" attribute where the precondition-type MUST be "qos", the status-type MUST be "remote", and the direction-tag MUST be "sendrecv".

CMS_T MUST wait for the UPDATE message from the originator containing the success/failure indication of each precondition as determined by the originator. If that confirmation indicates a failure for a mandatory precondition, CMS_T MUST send a 580-Precondition-Failure response with the outcome of the preconditions to CMS_O.

Once the preconditions are met, CMS_T alerts the user, and the SIP transaction completes normally.

7.4.2.2 QoS Preconditions Strength "Mandatory"

On receipt of an INVITE request containing mandatory QoS preconditions using a segmented status-type, a terminating CMS (CMS_T) MUST generate a 183-Session-Progress response with an SDP. For each media flow with QoS precondition in the answer SDP sent, the precondition-type MUST be "qos", and the status-type MUST be segmented, i.e., there needs to be separate attributes for the local and the remote segment as described in [11]. The strength-tag in the desired-status attributes MUST be "mandatory", and the direction-tag in the local and remote desired-status attributes MUST be "sendrecv".

Unless configured otherwise, CMS_T MUST NOT proceed with the session until resources have been reserved in both the local and remote segments. If the desired status of the originating segment (remote from CMS_T's point of view) QoS precondition does not match its current status, then CMS_T MUST request a confirmation of the originating segment QoS reservation from CMS_O by adding an "a=conf:". attribute where precondition-type MUST be "qos", the status-type MUST be remote, and the direction-tag MUST be "sendrecv".

7.5 SIP-Specific Event Notification

CMSS compliant implementations MUST support the extensions defined in [9].

7.6 The REFER Method

CMSS compliant implementations MUST support the extensions defined in [17] except as noted in this section. Note that this method makes use of the Notify mechanism defined in 7.5.

In CMSS, the use of the REFER method is specified both within an existing dialog and outside of a dialog as a dialog creating request.

7.6.1 Procedures at an Originating CMS

The CMS originating a REFER MUST include additional header parameters in the Refer-To header for a nested P-DCS-Billing-Info header, and SHOULD include the additional header parameters for nested P-DCS-Laes, and P-DCS-Redirect headers, as specified in Section 7.7. **NOTE**: Please refer to section 7.7.2. for additional guidance regarding the usage of P-DCS-Laes and P-DCS-Redirect headers.

The Accept header MUST be present in a REFER request and the value MUST include "message/sipfrag".

An originating CMS MAY initiate the REFER request as part of an existing INVITE established dialog or outside of the dialog as a dialog creating request. If the REFER is sent outside of a dialog then the CMS MUST include a Target-Dialog header in the REFER that identifies the associated INVITE established dialog.

7.6.2 Procedures at a Terminating CMS

If the action requested by the REFER is a SIP INVITE, then the NOTIFY sent when it completes MUST include the call-leg identification for the newly established session (i.e., the From, To, and Call-ID headers).

The uri-parameters in a SIP or tel URI in a Refer-To header MUST be present in the generated INVITE request as described in sections 6.19 and 7.7. Further, any nested headers (using the '?' syntax defined in RFC 3261 [6]) present in the Refer-To header MUST be present in the INVITE request.

If the REFER is received outside of an existing dialog then CMS_T MUST verify that the REFER contains a Target-Dialog header as defined in 7.14. If the header is absent then CMS_T MUST reject the REFER with a 400-Bad-

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

Request final response. If the Target-Dialog header is present, then CMS_T MUST associate the dialog in the target header with an existing SIP dialog. If the dialog identified by the Target-Dialog does not match an existing SIP dialog at CMS_T then CMS_T MUST reject the REFER with a 481-Transaction-Not-Found final response. If the dialog identified by the Target-Dialog header does match an existing dialog, then CMS_T MUST associate the REFER with that dialog. Furthermore, if the Refer-To header in the REFER does not contain a nested P-DCS-Billing-Info header, then CMS_T MUST use the BCID from the dialog identified in the Target-Dialog header as the BCID for the new dialog that is created as a result of the REFER. Refer to section 7.14 for further details on the Target-Dialog mechanism.

7.7 SIP Proxy to Proxy Extensions for Supporting DCS

CMSS compliant implementations MUST support the extensions defined in [16] except as defined in this section.

7.7.1 P-DCS-Trace-Party-ID

Support for the P-DCS-TRACE-PARTY-ID header is not required.

7.7.2 P-DCS-LAES and P-DCS-REDIRECT

For the purposes of this specification, the 4th paragraph in Section 8 of [16] is intended to require that CMSS compliant devices fully implement the P-DCS-LAES and P-DCS-REDIRECT headers as defined in [16] (with the exceptions noted in this specification), and also implement a mechanism that allows the service provider to turn this feature on or off as required by applicable legislation. For example, an operator may be required to include these headers as specified in [16] for calls within the operator's own network, while excluding the headers for calls that terminate on another operator's network.

7.7.2.1 P-DCS-LAES Header

The P-DCS-LAES-Header is used to pass the responsibility for performing electronic surveillance on a call from one CMS to another. For example, if a call terminates to a line that is marked for surveillance, and the line also has call-forwarding activated, then the terminating CMS can include the P-DCS-LAES header in the forwarded INVITE request or 302-Redirect response to inform the forwarded-to CMS that it should perform the surveillance function.

The P-DCS-LAES header contains information to support surveillance of both call-data and call-content. The call-data information, which consists of the BCID assigned to the call-data event stream and the address of the Delivery Function (DF) to receive the call-data events, is always present. The call-content information, which consists of the CCCID assigned to the call-content stream, plus the address of the DF to receive call-content, is optional.

The P-DCS-LAES header syntax is as defined in [16].

The Laes-bcid field MUST always be present. The Laes-cccid field MUST be present when the Laes-content field is present. The Laes-key field MUST NOT be included.

7.7.2.2 Surveillance Procedures at Originating CMS

An originating CMS (CMS_O) is required to perform electronic surveillance functions for an originating call if the originating line has an outstanding lawfully authorized electronic surveillance order. An originating CMS may also choose to perform electronic surveillance functions on behalf of a terminating CMS for certain-call forwarding and call-transfer scenarios. The following subsections detail the responsibilities of the originating CMS for these various surveillance scenarios.

7.7.2.2.1 CMS_O Receives REFER Request or Redirect Response

When CMS_O receives a 3XX Redirect response containing a P-DCS-Laes header in response to an INVITE, or receives a REFER request containing a P-DCS-Laes header in the Refer-To header for an active dialog, then it MUST copy the received P-DCS-Laes header into the subsequent INVITE that is generated as a result of the REFER or Redirect. This will enable the new terminating CMS to perform the surveillance on behalf of the CMS that generated the Redirect response or REFER request message.

The following subsections describe the CMS_O behavior when the P-DCS-Leas header cannot be forwarded to the new terminating CMS for some reason.

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009

7.7.2.2.1.1 Redirected Call Ends Early

If CMS_O receives a REFER request or 3XX Redirect response message as described above, but the call ends before the subsequent INVITE is sent (say the call is abandoned), then CMS_O MUST send a SurveillanceStop message to its local DF containing the following information:

- The local BCID already assigned to the call (note, this is a required field in the event message header),
- The remote BCID assigned by CMS_T and received in the P-DCS-Laes header,
- The call-data IP address and port of the remote DF of CMS_T received in the P-DCS-Laes header,
- An indicator specifying that both call-data and call-content surveillance are to be stopped,
- An indicator specifying that the local surveillance session (if active) and remote surveillance session are to be stopped.

This will tell the remote DF (i.e., the DF of CMS_T) that the call has ended, and not to expect further surveillance information.

7.7.2.2.1.2 P-DCS-LAES Header Cannot Be Included in Subsequent INVITE

If CMS_O is unable to include the P-DCS-Laes header in the subsequent INVITE for some reason (see Section 7.7.2), then CMS_O may choose either to perform the required surveillance function or to stop the remote surveillance session.

7.7.2.2.1.2.1 CMS_O Chooses To Perform Requested Surveillance

If CMS_O chooses to perform the requested call-data surveillance function, it MUST send a SignalingStart message to its local DF containing the following information:

- The local BCID already assigned to the call (note, this is a required field in the event message header),
- The remote BCID assigned by CMST and received in the P-DCS-Laes header,
- The call-data IP address and port of the remote DF of CMST received in the P-DCS-Laes header.

This will bind the local BCID to the remote surveillance session, and thus enable the local DF to relay subsequent call-data events for this call to the remote DF and BCID of the terminating CMS. Note that if CMS_O is already monitoring the call (e.g., due to an outstanding lawfully authorized surveillance order on the originating subscriber) when it receives a P-DCS-Laes header, then it MUST send a second SignalingStart message to its local DF, containing the appropriate parameters as specified above. This means that the DF must be able to receive two SignalingStart messages for the same call. The second SignalingStart should be used by the local DF only to establish the local-to-remote binding for relay of call-data and possibly call-content to the remote DF.

If the P-DCS-Laes header received in the 3XX Redirect response or REFER request also indicates that call content surveillance is to be performed (in addition to call data), then CMS_O MUST allocate a local CCCID for the call and request the CMTS of the originating line (or MG of the originating trunk if the originator is off-net) to provide a copy of the call content to the local DF. (Note, if the originating line or trunk is already being surveilled, then CMS_O simply uses the already allocated CCCID). In addition to the call-data information specified above, CMS_O MUST include the following data in the SignalingStart message to the local DF:

- The local CCCID assigned to the call,
- The remote CCCID assigned by CMST and received in the P-DCS-Laes header,
- The call-content IP address and port of the remote DF of CMST received in the P-DCS-Laes header.

This will enable the local DF to relay subsequent call-content packets received from the originating CMTS or MG for this call to the remote DF and CCCID of the terminating CMS.

When the call ends, CMS_O MUST send a SurveillanceStop message to its local DF containing the local BCID and indicating that both local and remote call-data and call-content surveillance are to be stopped. This will terminate the surveillance session in the remote DF for both call-data and call-content (if applicable), clear the local-to-remote binding information in the local DF, and stop the local surveillance session (if active).

Documents
Document Sharing Hub
Full document details: SCTE 165-18 2009