

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-09 2019

IPCablecom 1.5 Part 9: Event Messages

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices 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•ISBE 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•ISBE members.

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

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE 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 document 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•ISBE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2019
140 Philips Road
Exton, PA 19341

Note: DOCSIS® and PacketCable™ are registered trademarks of Cable Television Laboratories, Inc., and used in this document with permission.

Table of Contents

1	INTRODUCTION	9
1.1	IPCABLECOM EVENT MESSAGES	9
1.2	IPCABLECOM REFERENCE ARCHITECTURE	10
1.3	IPCABLECOM, VOICE-OVER-IP OVER CABLE	10
1.4	DOCUMENT SCOPE	11
1.5	DOCUMENT OVERVIEW.....	12
1.6	REQUIREMENTS AND CONVENTIONS	12
2	REFERENCES	13
2.1	NORMATIVE REFERENCES	13
2.2	INFORMATIVE REFERENCES	13
3	TERMS AND DEFINITIONS	15
4	ABBREVIATIONS AND ACRONYMS	19
5	BACKGROUND	26
5.1	TRADITIONAL TELEPHONY BILLING FORMATS.....	26
5.2	MOTIVATION FOR EVENT BASED BILLING.....	26
5.3	ORIGINATING/TERMINATING CALL MODEL TO SUPPORT CUSTOMER BILLING AND SETTLEMENTS	26
5.4	REAL-TIME BILLING	27
5.5	REAL-TIME AND BATCH EVENT MESSAGE DELIVERY	27
5.6	TERMINOLOGY AND CONCEPTS	27
5.6.1	<i>Service</i>	28
5.6.2	<i>IPCablecom Transaction</i>	28
5.6.3	<i>Call</i>	29
5.6.4	<i>Event Message</i>	29
5.6.5	<i>Attribute</i>	29
5.7	SUPPORTING DOCUMENTATION.....	29
6	IPCABLECOM OBJECTIVES	30
6.1	IPCABLECOM 1.5 REQUIRED SERVICES AND CAPABILITIES	30
6.2	ADDITIONAL IPCABLECOM SUPPORTED SERVICES AND CAPABILITIES	30
6.2.1	<i>IPCablecom Multimedia</i>	31
6.3	ASSUMPTIONS	31
7	EVENT MESSAGES ARCHITECTURE.....	33
7.1	IPCABLECOM EVENT MESSAGE COLLECTION	33
7.2	IPCABLECOM NETWORK ELEMENTS	33
7.2.1	<i>Call Management Server (CMS)</i>	34
7.2.2	<i>Media Gateway Controller (MGC)</i>	34
7.2.3	<i>Cable Modem Termination System (CMTS)</i>	34
7.2.4	<i>Record Keeping Server (RKS)</i>	35
7.3	GENERAL IPCABLECOM NETWORK ELEMENT REQUIREMENTS.....	36
7.4	EVENT MESSAGE INTERFACES.....	37
7.4.1	<i>CMS to CMTS (pkt-em1*)</i>	37
7.4.2	<i>CMS to MGC (pkt-em2)</i>	37
7.4.3	<i>CMS to RKS (pkt-em3)</i>	38
7.4.4	<i>CMTS to RKS (pkt-em4)</i>	38
7.4.5	<i>MGC to RKS (pkt-em5)</i>	38

7.4.6	CMS to CMS (pkt-em6).....	38
7.4.7	Security Requirements	38
8	IPCABLECOM SERVICES AND THEIR ASSOCIATED EVENT MESSAGES	39
8.1	IPCABLECOM CALL CONFIGURATIONS	39
8.1.1	On-Net to On-Net Call Configuration.....	39
8.1.2	On-Net to Off-Net Call Configuration (Outgoing PSTN Interconnect).....	40
8.1.3	Off-Net to On-Net Service (Incoming PSTN Interconnection).....	40
8.2	SPECIFIC SERVICES	41
8.2.1	911 Service.....	41
8.2.2	Other N11 Services (311, 411, 611).....	41
8.2.3	Toll-Free Services	41
8.2.4	Operator Services.....	42
8.2.5	Call Block Service.....	42
8.2.6	Call Waiting Service	42
8.2.7	Call Forwarding Service.....	43
8.2.8	Return Call Service	44
8.2.9	Repeat Call Service.....	44
8.2.10	Voice Mail Service	45
8.2.11	Message Waiting Indicator Service.....	45
8.2.12	Three-Way Call Service	45
8.2.13	Customer Originated Trace Service.....	46
8.2.14	Account Code and Authorization Code Service	46
9	IPCABLECOM EVENT MESSAGE STRUCTURE	48
9.1	EVENT MESSAGE STRUCTURE	51
9.2	SERVICE_INSTANCE	51
9.3	SERVICE_ACTIVATION.....	53
9.4	SIGNALING_START	53
9.5	SIGNALING_STOP	55
9.6	SERVICE_DEACTIVATION	56
9.7	DATABASE_QUERY	57
9.8	INTELLIGENT_PERIPHERAL_USAGE_START	58
9.9	INTELLIGENT_PERIPHERAL_USAGE_STOP.....	58
9.10	INTERCONNECT_START	58
9.11	INTERCONNECT_STOP	59
9.12	CALL_ANSWER.....	59
9.13	CALL_DISCONNECT	60
9.14	QoS_RESERVE.....	61
9.15	QoS_RELEASE	62
9.16	TIME_CHANGE.....	62
9.17	QoS_COMMIT	63
9.18	RTP_CONNECTION_PARAMETERS EVENT MESSAGE	63
9.19	MEDIA_ALIVE.....	63
9.20	MEDIA_STATISTICS	66
10	IPCABLECOM EVENT MESSAGE ATTRIBUTES	67
10.1	EM_HEADER ATTRIBUTE STRUCTURE.....	77
10.1.1	Billing Correlation ID (BCID) Field Structure.....	79
10.1.2	Status Field Structure.....	80
10.2	CALL_TERMINATION_CAUSE ATTRIBUTE STRUCTURE	80
10.3	TRUNK GROUP ID ATTRIBUTE STRUCTURE	81
10.4	QoS DESCRIPTOR ATTRIBUTE STRUCTURE	82

10.5	REDIRECTED-FROM-INFO ATTRIBUTE STRUCTURE	83
10.6	ELECTRONIC-SURVEILLANCE-INDICATION ATTRIBUTE STRUCTURE	83
10.7	ATTRIBUTES FOR CONFERENCE PARTIES	84
11	TRANSPORT INDEPENDENT EVENT MESSAGE ATTRIBUTE TLV FORMAT	85
12	IPCABLECOM EVENT MESSAGE FILE FORMAT	86
12.1	FILE BIT / BYTE ORDER	86
12.2	FILE HEADER	86
12.3	FILE NAMING CONVENTION	87
12.3.1	<i>Filename Components</i>	87
12.4	CONFIGURATION ITEMS	88
12.5	FILE EM STRUCTURE HEADER	88
13	TRANSPORT PROTOCOL	89
13.1	RADIUS ACCOUNTING PROTOCOL	89
13.1.1	<i>Reliability</i>	89
13.1.2	<i>RADIUS Client Reliability</i>	89
13.1.3	<i>Authentication and Confidentiality</i>	90
13.1.4	<i>Standard RADIUS Attributes</i>	90
13.1.5	<i>IPCablecom Extensions</i>	91
13.2	FILE TRANSPORT PROTOCOL (FTP)	92
13.2.1	<i>Required FTP Server Capabilities</i>	92
APPENDIX I	PCES SUPPORT	93
I.1	SERVICE_INSTANCE	93
I.2	SIGNALING_START	94
I.3	SIGNALING_STOP	95
I.4	CALL_ANSWER	96
I.5	CALL_DISCONNECT	97
I.6	QoS_RESERVE	97
I.7	QoS_RELEASE	97
I.8	QoS_COMMIT	97
I.9	MEDIA_REPORT	98
I.10	SIGNAL_INSTANCE	99
I.11	TERMINAL_DISPLAY_INFO ATTRIBUTE STRUCTURE	101
I.12	CONFERENCE_PARTY_CHANGE	102
I.13	SURVEILLANCE_STOP	103
I.14	REDIRECTION	104

List of Figures

FIGURE 1. IPCABLECOM NETWORK COMPONENT REFERENCE MODEL	10
FIGURE 2. TRANSPARENT IP TRAFFIC THROUGH THE DATA-OVER-CABLE SYSTEM.....	11
FIGURE 3. IPCABLECOM TERMINOLOGY	28
FIGURE 4. REPRESENTATIVE IPCABLECOM EVENT MESSAGES ARCHITECTURE	33
FIGURE 5. EXAMPLE RKS ARCHITECTURE	35
FIGURE 6. EVENT MESSAGE BILLING INTERFACES	37
FIGURE 7. LONG DURATION CALL IDENTIFICATION	65

List of Tables

TABLE 1. IPCABLECOM EVENT REPORTING COMMON ELEMENTS.....	34
TABLE 2. ON-NET TO ON-NET CALL CONFIGURATION	39
TABLE 3. ON-NET TO OFF-NET CALL CONFIGURATION	40
TABLE 4. OFF-NET TO ON-NET CALL CONFIGURATION	40
TABLE 5. TOLL-FREE SERVICES	42
TABLE 6. CALL BLOCK SERVICE	42
TABLE 7. CALL WAITING SERVICE.....	43
TABLE 8. CALL FORWARDING SERVICE	44
TABLE 9. RETURN CALL SERVICE	44
TABLE 10. REPEAT CALL SERVICE.....	45
TABLE 11. THREE-WAY CALL SERVICE	46
TABLE 12. CUSTOMER ORIGINATED TRACE SERVICE	46
TABLE 13. ACCOUNT CODE AND AUTHORIZATION CODE SERVICE.....	47
TABLE 14. IPCABLECOM EVENT MESSAGE SUMMARY	48
TABLE 15. SERVICES SUPPORTED BY ON-NET TO ON-NET CALL CONFIGURATION	50
TABLE 16. SERVICES SUPPORTED BY ON-NET TO OFF-NET CALL CONFIGURATION	50
TABLE 17. SERVICES SUPPORTED BY OFF-NET TO ON-NET CALL CONFIGURATION	51
TABLE 18. SERVICE_INSTANCE EVENT MESSAGE	52
TABLE 19. SERVICE_ACTIVATION EVENT MESSAGE	53
TABLE 20. SIGNALING_START EVENT MESSAGE	54
TABLE 21. SIGNALING_STOP EVENT MESSAGE.....	56
TABLE 22. SERVICE_DEACTIVATION EVENT MESSAGE.....	57
TABLE 23. DATABASE_QUERY EVENT MESSAGE.....	57
TABLE 24. INTERCONNECT_START EVENT MESSAGE.....	59
TABLE 25. INTERCONNECT_STOP EVENT MESSAGE	59
TABLE 26. CALL_ANSWER EVENT MESSAGE	60
TABLE 27. CALL_DISCONNECT EVENT MESSAGE.....	61
TABLE 28. QoS RESERVE TIMESTAMP GENERATION.....	61
TABLE 29. QoS_RESERVE EVENT MESSAGE	61
TABLE 30. QoS_RELEASE EVENT MESSAGE.....	62
TABLE 31. TIME_CHANGE EVENT MESSAGE	63
TABLE 32. QoS COMMIT TIMESTAMP GENERATION	63
TABLE 33. QoS_COMMIT EVENT MESSAGE	63
TABLE 34. MEDIA_ALIVE EVENT MESSAGE	65
TABLE 35. MEDIA_STATISTICS EVENT MESSAGE	66
TABLE 36. IPCABLECOM ATTRIBUTES MAPPED TO IPCABLECOM EVENT MESSAGES	67
TABLE 37. IPCABLECOM EVENT MESSAGE ATTRIBUTES	70

TABLE 38. EM_HEADER ATTRIBUTE STRUCTURE	77
TABLE 39. BCID FIELD DESCRIPTION	79
TABLE 40. STATUS FIELD DESCRIPTION	80
TABLE 41. CALL TERMINATION CAUSE DATA STRUCTURE	81
TABLE 42. TRUNK GROUP ID DATA STRUCTURE	81
TABLE 43. QoS DESCRIPTOR DATA STRUCTURE	82
TABLE 44. QoS STATUS BITMASK	82
TABLE 45. DATA STRUCTURE OF THE REDIRECTED-FROM-INFO ATTRIBUTE	83
TABLE 46. DATA STRUCTURE OF THE ELECTRONIC-SURVEILLANCE-INDICATION ATTRIBUTE	83
TABLE 47. COMMUNICATING_PARTY, JOINED_PARTY, AND REMOVED_PARTY ATTRIBUTES	84
TABLE 48. EVENT MESSAGE ATTRIBUTE TLV-TUPLE FORMAT	85
TABLE 49. BIT / BYTE ORDER FOR THE EVENT MESSAGE FILE	86
TABLE 50. FILE HEADER FOR IPCABLECOM EVENT MESSAGE FILE FORMAT	86
TABLE 51. FILENAME COMPONENTS	87
TABLE 52. REQUIRED CONFIGURATION ITEMS	88
TABLE 53. FILE-BASED EM PACKET STRUCTURE	88
TABLE 54. RADIUS MESSAGE HEADER	90
TABLE 55. MANDATORY RADIUS ATTRIBUTES	90
TABLE 56. RADIUS ACCT_STATUS_TYPE	90
TABLE 57. RADIUS VSA STRUCTURE FOR IPCABLECOM ATTRIBUTES	91
TABLE 58. CONCATENATED ATTRIBUTES	92
TABLE 59. SERVICE_INSTANCE EVENT MESSAGE FOR PCES	93
TABLE 60. SIGNALING_START EVENT MESSAGE FOR PCES	94
TABLE 61. SIGNALING_STOP EVENT MESSAGE	96
TABLE 62. QoS_RESERVE EVENT MESSAGE FOR PCES	97
TABLE 63. QoS_RELEASE EVENT MESSAGE FOR PCES	97
TABLE 64. QoS_COMMIT EVENT MESSAGE FOR PCES	98
TABLE 65. MEDIA_REPORT EVENT MESSAGE FOR PCES	98
TABLE 66. SIGNALS SENT TOWARD INTERCEPT SUBJECT	99
TABLE 67. SIGNALS RECEIVED FROM INTERCEPT SUBJECT	99
TABLE 68. SIGNAL_INSTANCE EVENT MESSAGE FOR PCES	100
TABLE 69. TERMINAL_DISPLAY_INFO ATTRIBUTE DATA STRUCTURE	101
TABLE 70. TERMINAL_DISPLAY_STATUS_BITMASK	102
TABLE 71. CONFERENCE_PARTY_CHANGE EVENT MESSAGE	102
TABLE 72. SURVEILLANCE_STOP EVENT MESSAGE FOR PCES	104
TABLE 73. REDIRECTION EVENT MESSAGE FOR PCES	105

This page left blank intentionally.

1 INTRODUCTION

This standard describes the concept of Event Messages used to collect usage for the purposes of billing within the IP-Cablecom architecture. It details a transport protocol independent Event Message attribute TLV format, an Event Message file format, mandatory and optional transport protocols, the various Event Messages, lists the attributes each Event Message contains, and lists the required and optional Event Messages associated with each type of end-user service supported. In order to support vendor interoperability, implementations must minimally support RADIUS as a transport protocol. It is issued to facilitate design and field-testing leading to manufacturability and interoperability of conforming hardware and software by multiple vendors.

1.1 IP-Cablecom Event Messages

An Event Message is a data record containing information about network usage and activities. A single Event Message may contain a complete set of data regarding usage or it may only contain part of the total usage information. When correlated by the Record Keeping Server (RKS), information contained in multiple Event Messages provides a complete record of the service. This complete record of the service is often referred to as a Call Detail Record (CDR). Event Messages or CDRs may be sent to one or more back office applications such as a billing system, fraud detection system, or pre-paid services processor.

The structure of the Event Message data record is designed to be flexible and extensible in order to carry information about network usage for a wide variety of services. Examples of these services include IP-Cablecom voice, video and other multimedia services, OpenCable™ services such as Video-On-Demand, Pay-Per-View and DOCSIS® high-speed data services.

The IP-Cablecom Event Message standard defines a transport protocol independent Event Message attribute Type-Length-Value (TLV) format, an Event Message file format, as well as the mandatory RADIUS protocol and the optional FTP transport protocol.

1.2 IPCablecom Reference Architecture

Figure 1 shows the reference architecture for the IPCablecom Network. Refer to the IPCablecom Architecture Document [13] for more detailed information on this reference architecture.

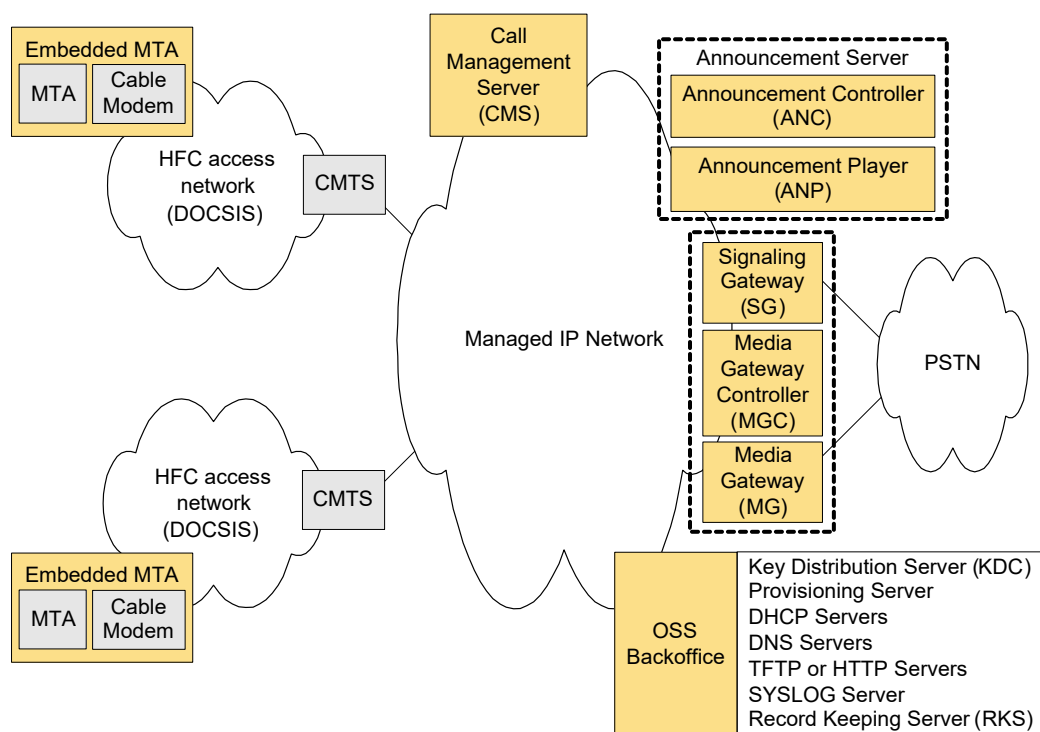


Figure 1. IPCablecom Network Component Reference Model

1.3 IPCablecom, Voice-over-IP over Cable

Cable operators are deploying high-speed data communications systems and offering voice, video, and data services based on bi-directional transfer of Internet protocol (IP) traffic. The transfer takes place between the cable system headend and customer locations, over an all-coaxial or hybrid-fiber/coax (HFC) cable network, defined by the Data-Over-Cable Service Interface specification (DOCSIS). This is shown in simplified form in the following diagram.

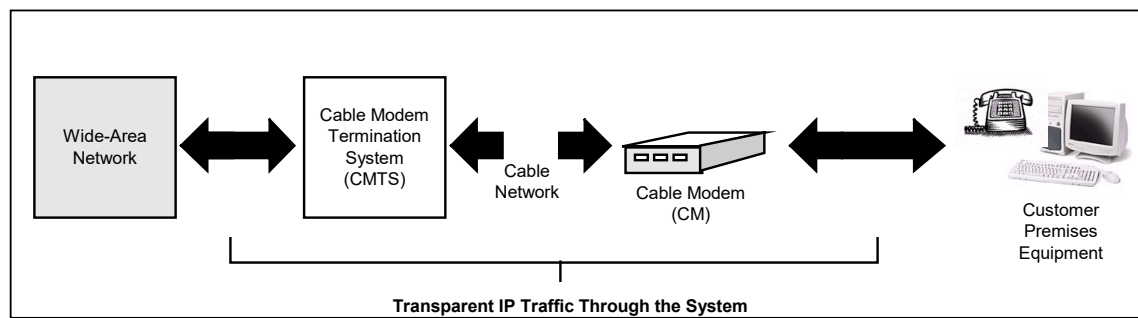


Figure 2. Transparent IP Traffic through the Data-Over-Cable System

The transmission path over the cable system is realized at the headend by a cable modem termination system (CMTS) and at each customer location by a cable modem (CM). At customer locations, the interface is called the cable-modem-to-customer-premises-equipment interface (CMCI) and is specified in [13].

One critical Operations Support System (OSS) function required to operate such a system is the capturing of usage on a call-by-call basis for each subscriber. Such functionality is critical in allowing MSOs to bill for services provided on a usage-sensitive basis, but also plays an important role in areas such as network usage monitoring and fraud management. The usage collection concept lies in requiring network elements involved in key portions of each call to notify a centralized Record Keeping Server (RKS) with what are termed Event Messages detailing the relevant data pertaining to the portion of the call handled by that given network element. This Event Message concept, and the architecture, which underlies it are described in greater detail in this document.

1.4 Document Scope

The scope of this document encompasses the definition of the Event Message architecture; the services for which Event Messages are defined; the set of Event Messages defined for each supported service; the format and coding of the Event Messages; and finally the transport protocol used to pass Event Messages between IPCablecom network elements.

The Event Messages are designed to be flexible and extensible in order to support new and innovative IPCablecom and value-added services. In an effort to describe some of these features and possible uses of these Event Messages, this document may describe interfaces and signaling protocols that are outside the scope of IPCablecom 1.5. It should be understood that the primary purpose of this document is to support the IPCablecom 1.5 architecture and the IPCablecom 1.5 services as defined in this document.

In order to support early deployment of IPCablecom networks, the IPCablecom project is developing specifications in a phased approach. In an effort to keep pace with the larger IPCablecom project and interface specification development effort, the Event Messages are also addressed in a phased approach. Possible future extensions to this document may include topics such as expanded support for fraud detection and other back office applications.

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.

1.5 Document Overview

The document contains the following sections. Section 5 motivates the need for Event Messages. Section 6 describes objectives of the Event Message architecture followed by Section 7 describing the Event Message architecture itself. Section 8 describes the services IP-Cablecom 1.5 will support for which Event Messages need to be generated. Section 9 defines the Event Messages needed in order to bill these supported services. Section 10 defines the IP-Cablecom Event Message attributes. Section 11 describes the transport independent Event Message attribute TLV format. Section 12 describes the Event Message file format. Finally, Section 13 describes the mandatory and optional transport protocols.

1.6 Requirements and Conventions

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

"MUST"	This word or the adjective "REQUIRED" 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 or the adjective "RECOMMENDED" 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 or the adjective "OPTIONAL" 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.

Other text is descriptive or explanatory.

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 standard 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 will be evident from this document that while a IP-Cablecom 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. These differences may be significant for legal/regulatory purposes.

2 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision, and while parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version

2.1 Normative References

In order to claim compliance with this standard, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this standard. Intellectual property rights may be required to implement these references.

- [1] ANSI/SCTE 165-03 2016, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.
- [2] ANSI/SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.
- [3] ANSI/SCTE 165-04 2019, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.
- [4] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2002.
- [5] IETF RFC 2866, RADIUS Accounting, June 2000.
- [6] Telcordia GR-1100-CORE Bellcore Automatic Message Accounting Format (BAF) Requirements Terms and Definitions.
- [7] ANSI/SCTE 165-18 2016, IPCablecom 1.5 Part 18: CMS to CMS Signaling.
- [8] ANSI/SCTE 165-13 2019, IPCablecom 1.5 Part 13: Electronic Surveillance Standard.
- [9] ITU-T Recommendation E.164, The International Public Telecommunication Numbering Plan, May 1997.
- [10] IETF RFC 1305, Network Time Protocol (Version 3), Specification, Implementation and Analysis, March 1992.
- [11] IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications, July 2003.
- [12] IETF RFC 3611, RTP Control Protocol Extended Reports (RTCP XR), November 2003.

2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

- [13] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premises Equipment Interface (CMCI) Specification, CM-SP-CMCI-C01-081104, Cable Television Laboratories, Inc.
- [14] ANSI/SCTE 165-01 2019, IPCablecom 1.5 Part 1: Architecture Framework Technical Report.
- [15] ANSI/SCTE 23-01 2017, DOCSIS 1.1 Part 1: Radio Frequency Interface.
- [16] PacketCable Architecture Call Flow Technical Report, On-Net MTA to On-Net MTA, PKT-TR-CF-ON-ON-C01-071129, November 29, 2007, Cable Television Laboratories, Inc.
- [17] PacketCable Architecture Call Flow Technical Report, On-Net MTA to PSTN, PKT-TR-CF-ON-PSTN-C01-071129, November 29, 2007, Cable Television Laboratories, Inc.
- [18] PacketCable Architecture Call Flow Technical Report, PSTN to On-Net MTA, PKT-TR-CF-PSTN-ON-C01-071129, November 29, 2007, Cable Television Laboratories, Inc.
- [19] GR-1298-CORE, AINGR: Switching Systems (GR-1298).
- [20] GR-1299-CORE, AINGR: Switch - Service Control Point (SCP)/Adjunct Interface (GR-1299).

- [21] GR-533-CORE, LSSGR: Database Services Service Switching Points - Toll-Free Service (FSD 31-01-0000), A Module of LSSGR, FR-64 (GR-533), Telcordia.
- [22] GR-2892-CORE, Switching and Signaling Generic Requirements for Toll-Free Service Using AIN (GR-2892), Telcordia.
- [23] TRQ No. 2, Technical Requirements Number 2, Number Portability Switching Systems (ANSI T1S1.6 Working Group).
- [24] Internet Protocol Standards - STD9, October 1985, J. Postel, J. Reynolds, File Transfer Protocol (FTP)
- [25] ANSI/SCTE 159-01 2017, IPCablecom Multimedia.
- [26] Telcordia GR-605-CORE – LSSGR: Authorization Codes for Automatic Flexible Routing (AFR) and Account Codes for Basic Business Group and AFR (FSD 02-02-1010) – Telecordia.
- [27] Telcordia GR-580-CORE LSSGR: Call Forwarding Variable, Telecordia.
- [28] Telcordia GR-586-CORE LSSGR: Call Forwarding Subfeatures, Telecordia
- [29] Telcordia GR-317-CORE LSSGR: Switching System Generic Requirements for Call Control Using Integrated Services Digital Network User Part (ISDNUP).
- [30] GR-2936-CORE Local Number Portability Capability Specification, Telecordia.

3 TERMS AND DEFINITIONS

IPCablecom standards 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."
Asymmetric Key	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server plays informational announcements in IPCablecom network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
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 that claims to have given the information.
Authorization	The act of giving access to a service or device if one has 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. Also called plaintext.
Confidentiality	A way to ensure that information is not disclosed to anyone other than 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.
Downstream	The direction from the headend toward the subscriber location.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or Multipoint Conference Unit (MCU).

Errored Second	Any 1-second interval containing at least one bit error.
Event Message	A message capturing a single portion of a connection.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow") A unidirectional sequence of packets associated with a Service ID (SID) and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Flow [IP Flow]	A unidirectional sequence of packets identified by OSI 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.
Gateway	Devices bridging between the IP/Cablecom 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 to the edge of the IP/Cablecom network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T H.245 protocol for communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
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.
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.
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.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
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.
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 that 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.
IPCablecom 1.5	The suite of IPCablecom specifications that support telephone service.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
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 anyone other than 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, thereby eliminating the need for a host to support the service.
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 an 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 user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
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 generated with the corresponding root private key.
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 using encryption.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and single 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 Protocol Data Unit (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 that carries user media content and may carry voice signaling (M_F , R_2 , 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 headend.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

4 ABBREVIATIONS AND ACRONYMS

IPCablecom standards use the following abbreviations.

AAA	Authentication, Authorization and Accounting.
AES	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in IPCablecom.
AF	Assured Forwarding. This is a DiffServ Per Hop Behavior.
AH	Authentication header. An IPsec security protocol that provides message integrity for complete IP packets, including the IP header.
AMA	Automated Message Accounting. A standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies).
ASD	Application-Specific Data. A field in some Kerberos key management messages that carries information specific to the security protocol for which the keys are being negotiated.
AT	Access Tandem.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, also known as AMA.
BCID	Billing Correlation ID.
BPI+	Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.
BSS	Business Support System
CA	Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. The part of the CMS that maintains the communication state, and controls the line side of the communication.
CBC	Cipher Block Chaining mode. An option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CDR	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs.
CIC	Circuit Identification Code. In ANSI SS7, a two-octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
CID	Circuit ID (Pronounced "kid"). This uniquely identifies an ISUP DS0 circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format.
CIR	Committed Information Rate.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax.
CMS	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.
CMTS	Cable Modem Termination System. The device at a cable headend which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
CMSS	Call Management Server Signaling.
Codec	COder-DECoder.

COPS	Common Open Policy Service protocol. Defined in RFC2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS configuration file.
CRCX	Create Connection.
CSR	Customer Service Representative.
DA	Directory Assistance.
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard.
DF	Delivery Function.
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default. Network Provider DHCP Server.
DNS	Domain Name Service.
DOCSIS®	Data-Over-Cable Service Interface Specifications.
DPC	Destination Point Code. In ANSI SS7, a 3-octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
DQoS	Dynamic Quality-of-Service. Assigned on the fly for each communication depending on the QoS requested.
DSA	Dynamic Service Add.
DSC	Dynamic Service Change.
DSCP	DiffServ Code Point. A field in every IP packet that identifies the DiffServ Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP.
DTMF	Dual-tone Multi Frequency (tones).
EF	Expedited Forwarding. A DiffServ Per Hop Behavior.
E-MTA	Embedded MTA. A single node that contains both an MTA and a cable modem.
EO	End Office.
ESP	IPsec Encapsulating Security Payload. Protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
FEID	Financial Entity ID.
FGD	Feature Group D signaling.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 2821 for details.
GC	Gate Controller.
GTT	Global Title Translation.
HFC	Hybrid Fiber/Coaxial. An HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the headend and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
HMAC	Hashed Message Authentication Code. A message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104.
HTTP	Hypertext Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.
IC	Inter-exchange Carrier.

IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used on the Internet. See www.ietf.org for details.
IKE	Internet Key Exchange. A key-management mechanism used to negotiate and derive keys for SAs in IPsec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE with X.509 certificates for authentication.
IP	Internet Protocol. An Internet network-layer protocol.
IPsec	Internet Protocol Security. A collection of Internet standards for protecting IP packets with encryption and authentication.
ISDN	Integrated Services Digital Network.
ISTP	Internet Signaling Transport Protocol.
ISUP	ISDN User Part. A protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ITU	International Telecommunication Union.
ITU-T	International Telecommunication Union–Telecommunication Standardization Sector.
IVR	Interactive Voice Response system.
JIP	Jurisdiction Information Parameter. The identity of the originating network element in ISUP.
KDC	Key Distribution Center.
LATA	Local Access and Transport Area.
LD	Long Distance.
LIDB	Line Information Database. Contains customer information required for real-time access such as calling card personal identification numbers (PINs) for real-time validation.
LLC	Logical Link Control. The Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sublayer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
LRN	Location Routing Number.
LSSGR	LATA Switching Systems Generic Requirements.
MAC	Message Authentication Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC.
MAC	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller.
MCU	Multipoint Conferencing Unit.
MD5	Message Digest 5. A one-way hash algorithm that maps variable length plaintext into fixed-length (16 byte) ciphertext.
MDCP	Media Device Control Protocol. A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
MDCX	Modify Connection.
MDU	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high-rise buildings.
MEGACO	Media Gateway Control IETF working group. See www.ietf.org for details.
MF	Multi-Frequency.
MG	Media Gateway. Provides the bearer circuit interfaces to the PSTN and transcodes the media stream.

MGC	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the IPCablecom and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
MIB	Management Information Base.
MIC	Message Integrity Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a Message Authentication Code (MAC).
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSB	Most Significant Bit.
MSO	Multi-System Operator. A cable company that operates many headend locations in several cities.
MSU	Message Signal Unit.
MTA	Multimedia Terminal Adapter. Contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part. A set of two protocols (MTP 2, MTP 3) within the SS7 suite of protocols that are used to implement physical, data link, and network-level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay.
NANP	North American Numbering Plan.
NANPNAT	North American Numbering Plan Network Address Translation.
NAT Network Layer	Network Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture. This layer provides services to establish a path between open systems.
NCS	Network Call Signaling.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP).
NPDB	Number Portability Data Base
NTP	Network Time Protocol. An internet standard used for synchronizing clocks of elements distributed on an IP network.
NTSC	National Television Standards Committee. Defines the analog color television broadcast standard used today in North America.
OID	Object Identification.
OSP	Operator Service Provider.
OSS	Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
OSS-D	OSS Default. Network Provider Provisioning Server.
PAL	Phase Alternate Line. The European color television format that evolved from the American NTSC standard.
PCES	IPCablecom Electronic Surveillance.
PCM	Pulse Code Modulation. A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog-to-digital conversion techniques.
PDU	Protocol Data Unit.
PHS	Payload Header Suppression. A DOCSIS technique for compressing the Ethernet, IP, and UDP headers of RTP packets.

PKCROSS	Public-Key Cryptography for Cross-Realm Authentication. Utilizes PKINIT for establishing the inter-realm keys and associated inter-realm policies to be applied in issuing cross-realm service tickets between realms and domains in support of Intradomain and Interdomain CMS-to-CMS signaling (CMSS).
PKCS	Public-Key Cryptography Standards. Published by RSA Data Security Inc. These Standards describe how to use public key cryptography in a reliable, secure and interoperable way.
PKI	Public-Key Infrastructure. A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	Public-Key Cryptography for Initial Authentication. The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
QCIF	Quarter Common Intermediate Format.
QoS	Quality of Service. Guarantees network bandwidth and availability for applications.
RADIUS	Remote Authentication Dial-In User Service. An internet protocol (IETF RFC 2865 and RFC 2866) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use.
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	Rivest Cipher 4. A variable length stream cipher. Optionally used to encrypt the media traffic in IPCablecom.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html .
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.
RKS	Record Keeping Server. The device, which collects and correlates the various Event Messages.
RSA	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource Reservation Protocol.
RTCP	Real-Time Control Protocol.
RTO	Retransmission Timeout.
RTP	Real-time Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC3550.
SA	Security Association. A one-way relationship between sender and receiver offering security services on the communication flow.
SAID	Security Association Identifier. Uniquely identifies SAs in the DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.
SCCP	Signaling Connection Control Part. A protocol within the SS7 suite of protocols that provides two functions in addition to those provided within MTP. The first function is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.

SCTP	Stream Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information delivered as a unit between peer service access points.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID. A 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). Upstream Service Flow IDs and Downstream Service Flow IDs are allocated from the same SFID number space.
SFR	Service Flow Reference. A 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular, the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1. A one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus. An extension to SIP.
S-MTA	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
SNMP	Simple Network Management Protocol.
SOHO	Small Office/Home Office.
SS7	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Service Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. A node within an SS7 network that routes signaling messages based on their destination address. This is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
TCP	Transmission Control Protocol.
TD	Timeout for Disconnect.
TFTP	Trivial File Transfer Protocol.
TFTP-D	Default – Trivial File Transfer Protocol.
TGS	Ticket Granting Server. A sub-system of the KDC used to grant Kerberos tickets.
TGW	Telephony Gateway.
TIPHON	Telecommunications and Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value. A tuple within a DOCSIS configuration file.
TN	Telephone Number.
ToD	Time-of-Day Server.
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a DiffServ domain, the TOS byte is treated as the DiffServ Code Point, or DSCP.

TSG	Trunk Subgroup.
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
VAD	Voice Activity Detection.
VBR	Variable Bit Rate.
VoIP	Voice-over-IP.

5 BACKGROUND

5.1 Traditional Telephony Billing Formats

The telephony industry has traditionally recorded call detail transactions on telephone switches utilizing various standard and proprietary billing formats such as Automated Message Accounting (AMA), sometimes referred to as Bellcore AMA Format (BAF). The switches generate multiple transactions based upon the type of call the customer placed. These transactions are correlated and packaged into a single Call Detail Record (CDR) at the end of the service instance for billing purposes. In this traditional telephony model, services and awareness of "call state" is usually maintained in one or at most two nodes of the network, which makes such correlation relatively straightforward. The CDR is then delivered to the billing system for the purpose of placing a charge on the customer's account.

5.2 Motivation for Event Based Billing

The event-based approach to capturing information to be used for billing is necessary to accommodate the distributed architecture of IP-Cablecom. "Call state awareness" no longer resides in one or two network elements, but is instead spread out among many. Each network element **MUST** be responsible for generating Event Messages for the portion of the communication pertaining to them.

The primary motivating factor behind articulating the structure and details of these various Event Messages is to support multi-vendor interoperability between network elements and record keeping servers. This standard defines the Event Message syntax and in addition it describes the transport protocols.

Event based billing has the added advantage that it enables IP-Cablecom services to be billed in real-time, making the information about billable communications available as the network equipment processes them. This allows the system as a whole to be more responsive, allowing, for example, fraudulent behavior to be detected sooner, saving revenue for the provider. It also allows a more fully integrated solution, as it becomes possible for the billing system and the network equipment to exchange information about the availability of a service as the customer is requesting that service.

With respect to the Event Message format, there are a large number of formats in use today. The most widely used formats carry the legacy of the traditional CDR, which is generated at the end of the call. While these formats capture much of the information content needed to bill for IP-Cablecom services, bringing along their full structure would make it difficult to support the real-time nature of certain enhanced IP-Cablecom services. This standard leverages the value of the information content from the existing billing formats, augmenting that with the distributed nature of the IP-Cablecom architecture.

5.3 Originating/Terminating Call Model to Support Customer Billing and Settlements

The IP-Cablecom Event Messages contain sufficient per-call information to support customer billing for service as well as settlement between IP-Cablecom network providers for access. The information contained in the Event Messages supports a wide variety of billing and settlement models. IP-Cablecom does not mandate the use of specific billing or settlement models as these models are defined by and based on the specific business requirements of the individual MSOs. IP-Cablecom neither mandates nor precludes the use of a clearinghouse for settlements.

The IP-Cablecom Event Messages are based on a model where a call or service is divided into an originating half and a terminating half. The originating CMS or MGC MUST generate a unique Billing Correlation ID (BCID) to identify all Event Messages associated with the originating half of the call. The terminating CMS or MGC MUST generate a unique BCID to identify all Event messages associated with the terminating half of the call. For each half of the call or service, the set of IP-Cablecom network elements that generate Event Messages (CMS, MGC, CMTS) must provide all necessary information required for billing and/or settlements as appropriate based on the service. The information generated by the originating half MUST be sent to the RKS supporting the originating half. The information generated by the terminating half MUST be sent to the RKS supporting the terminating half. The IP-Cablecom network elements also generate Event Messages that are not associated with any call. For those cases, the network element generating the Event Message MUST generate a unique BCID for the event and send the Event Message to appropriate RKS supporting the network element.

The IP-Cablecom Event Messages support billing and settlement for single-zone, intra-domain and inter-domain architectures. In most cases, the basic set of Event Messages, their associated attributes, and the triggers for the Event Message are identical for these three architectures. In the case of intra-domain and inter-domain architectures, additional triggers exist for a subset of the Event Messages. The IP-Cablecom Event Message standard details these requirements.

For the purposes of settlements, each IP-Cablecom zone is divided into one or more logical Financial Entities. Settlements occur between Financial Entities. Each Financial Entity is identified by a Financial Entity ID (FEID). FEIDs are pre-assigned to every CMS and MGC in the IP-Cablecom network. A single CMS may be assigned at most one FEID. One or more CMSes may be assigned the same FEID.

In the Intra-domain and Inter-domain cases, the originating and terminating CMSes exchange BCIDs and FEIDs. The originating CMS sends its BCID and FEID in the INVITE message. The terminating CMS sends its BCID and FEID in the first response to the INVITE message which is typically the 183 SDP.

5.4 Real-Time Billing

The billing system can be regarded as a functional block of the back office Operations Support System (OSS). The inputs to the billing system are the billing events and the outputs are the account balance and invoice. The billing system relates the billing events to the account balance by rating the events according to the pricing structure and other business logic.

Real-time Billing Systems relate the billing events to the account balance as events occur. As the billing system receives these real-time billing events, its rating engine rates the events and immediately posts balances. Real-time Billing Systems may be required to support advanced IP-Cablecom features such as pre-paid calling card, real-time fraud prevention, and real-time credit enforcement.

The IP-Cablecom Event Message architecture can be used to support both real-time and batch billing systems.

5.5 Real-Time and Batch Event Message Delivery

Event Messages may be delivered to the RKS in real time as they are created. This enables support for a growing number of services that require purchase limits such as prepaid calling cards.

As an alternative, Event Messages may be stored for some period of time and batched together before being sent to the RKS. This approach provides a more efficient use of network resources.

5.6 Terminology and Concepts

This section defines terminology associated with usage data as it relates to IP-Cablecom Services. The concept of a "call" is well understood and used within the telecommunications marketplace today. A traditional telephony "call" involves establishing a dedicated, circuit-switched path between the calling and called parties. Packet-switched architectures, including IP-Cablecom, do not establish any such dedicated paths.

To the contrary, the IP-Cablecom architecture assumes a shared medium between the head-end and the customer, as compared to the dedicated loop plant in traditional telephony; and during a traditional telephone call, as noted above,

a circuit-switched "connection" is established between the parties, whereas packet switching is inherently "connectionless." All that said, the term "call" is sufficiently well entrenched that it will be used in this document to refer to packet-mode voice communications between two parties over an IPCablecom network, even though in technical terms (as will be seen) there is little resemblance to a traditional telephone "call."

It is envisioned that many new voice, video, data and other multimedia services will be developed to take advantage of the inherent extensibility of the IPCablecom architecture. These new services, which likely will not be derived from traditional telephony principals, will be based on the term transaction, which is more indicative of the data flows across the IPCablecom network. The Event Message structure is designed to be flexible and enable the addition of new IPCablecom services and features while maintaining backward compatibility with existing applications. Event Messages MAY support information required for billing of DOCSIS data services, OpenCable video services, and the encapsulation of vendor specific proprietary data.

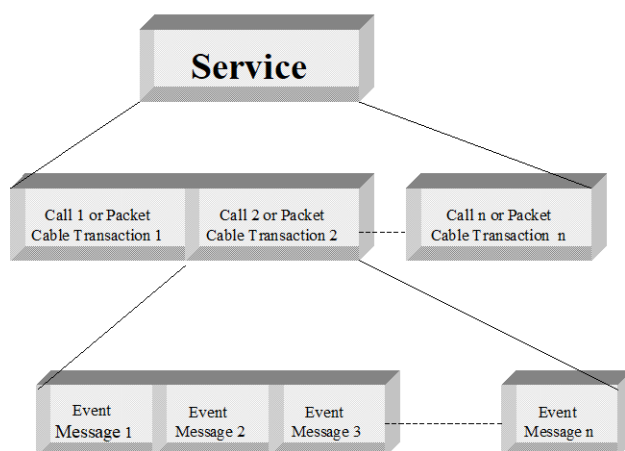


Figure 3. IPCablecom Terminology

5.6.1 Service

A service is an individual or package of communications features a subscriber may select. A service is identified by a set of one or more "calls" or transactions that deliver the desired functionality to the subscriber. Examples of a service include: a voice communication between two local IPCablecom subscribers, a 3-way call, pay-per-view movie, and a web surfing session. A service may be instantaneous or persist over time. Service in the context of IPCablecom 1.5 implies voice communications only and may not necessarily apply to the variety of other services such as Data, traditional IP, E-Commerce, etc.

5.6.2 IPCablecom Transaction

An IPCablecom transaction is a collection of events on the IPCablecom network when delivering a service to a subscriber. Event Messages for the same transaction are identified by one unique BCID (as described in Table 39). For some services, multiple transactions may be required to provide information that is necessary to collect the total usage for the service. Multiple Event Messages may be required to track resources for each individual service used. A Transaction may persist over time.

5.6.3 Call

A call is an instance of user-initiated voice communication capabilities. In traditional telephony, a call is generally considered as the establishment of connectivity directly between two points: originating party and terminating party. In the IPCablecom context, as noted above, the communication between the parties is "connectionless" in the traditional sense.

5.6.4 Event Message

An Event Message is a set of data, representative of an event in the IPCablecom architecture that could be indicative of usage of one or more billable IPCablecom capabilities. An Event Message by itself may not be fully indicative of a customer's billable activities, but an Event Message correlated with other Event Messages builds the basis of a billable Usage Detail Record.

5.6.5 Attribute

An Event Message Attribute is a predefined data element described by an attribute definition and attribute type.

5.7 Supporting Documentation

A number of documents and specifications describe the IPCablecom project. The IPCablecom Architecture Framework [13] is the starting point for understanding the IPCablecom project and the various IPCablecom Interface Specifications, technical reports and other IPCablecom documents.

6 IPCABLECOM OBJECTIVES

6.1 IPCablecom 1.5 Required Services and Capabilities

IPCablecom 1.5 provides basic voice capabilities and therefore **MUST** support Event Messages for the following services. These services are described in more detail in Section 8 of this document.

- Interconnection with circuit-switched PSTN
- Support for 911 emergency services
- n11 (411, 611, etc.) assume outside directory service
- Toll-free services (800, 888, 877...)
- Operator services
- Call block service
- Call waiting service
- Call forwarding/call redirection services
- Return call service
- Repeat call service
- Voice mail service
- Message waiting indicator service (email/voice mail notification)
- Three-Way Call
- Customer Originated Trace

6.2 Additional IPCablecom Supported Services and Capabilities

The following represents a list of possible additional IPCablecom services that **MAY** be supported. The list, though meant as a rough guideline, is by no means comprehensive, and it is expected that as the scope of services grows, this list will be expanded. These services are not defined in more detail in this document.

- Call transfer
- Speed dialing
- Caller name and number
- Caller name and number privacy
- Selective screening services
- Pay-per-communication services (900, etc.)
- Distinctive notification (to identify callee in a multiple-party household)
- Priority notification (to prioritize incoming communications)
- Selective forwarding
- Rejection (activate and deactivate)
- Teletype translation services
- Multi-line hunt group services
- Virtual second line (multiple lines)

- Alternate billing methods (collect, third number billed, credit card, pre-paid services, etc.)

In addition, the following list represents a set of IPCablecom 1.5 services that MAY be supported by IPCablecom CMS network elements, however these services MUST be supported by IPCablecom 1.5 RKS network elements. When these services are supported by an IPCablecom 1.5 compliant CMS, they MUST be supported as defined in this standard. These services are described in more detail in Section 8 of this document.

- Account Code and Authorization Code

6.2.1 IPCablecom Multimedia

The IPCablecom Multimedia standard defines a service delivery framework that provides general-purpose QoS, event-based accounting, and security functionality founded upon the mechanisms defined in IPCablecom 1.5. It is defined in [25]. The IPCablecom Multimedia standard extends this document and the capabilities of the present Event Messages standard; refer to [25] for more details.

6.3 Assumptions

The following assumptions have been made which apply to the entire document:

- IPCablecom 1.5 does not specify the interface between an RKS and a billing system.
- All IP based Intelligent Peripherals (these include Announcement Servers, for example) will be connected to the originating CMS or MGC.
- IPCablecom 1.5 does not support Line Information Database (LIDB) queries. Calls requiring LIDB determination, such as calling card personal identification number validation, are sent directly to the PSTN.
- IPCablecom 1.5 supports local number portability (LNP). Following information and references are applicable to LNP:
 1. Location Routing Number (LRN) identifies routing information for a ported called party number; and Jurisdiction Information Parameter (JIP) identifies the network element where the ported calling party number is currently getting the service from. The JIP parameter received in SS7 message is needed for billing settlement purpose. (References: GR-317-CORE, GR-2936-CORE, and GR-1100-CORE).
 2. The originating half determines if the caller is ported-in and the terminating half determines if the called party is ported-in. The CMS or MGC determines if a number is ported based on different data including a) provisioned data, b) signaling messages c) Number Portability data base. The source of Number Portability information is specified in Technical Requirements on Number portability systems [30] Table 8.
- Non-IPCablecom network elements, such as those residing in the public switched telephone network (PSTN) to which an IPCablecom system may interconnect with, will NOT generate and send Event Messages to the RKS.
- PSTN Intelligent Peripheral Event Messages are generated by the originating CMS.
- IPCablecom 1.5 Event Messages currently only support messages for actual billable events. This document does not specify messages related to provisioning of services by the operator of an IPCablecom network. This document does support Event Messages for Subscriber service activation. This document does not specify messages related to selection of an entity other than the IPCablecom network operator to handle off-network activities (e.g., inter-exchange communications).
- The initiating party number and the terminating party number are the only two attributes defined in IPCablecom 1.5 that can be used to associate a subscriber with usage of network resources.
- IPCablecom 1.5 supports interconnection to both Class 4 and Class 5 Switches.
- IPCablecom supports a 911 Trunk Group.
- IPCablecom 1.5 trusted network elements are expected to be pre-provisioned with a minimum set of data using a vendor-proprietary mechanism. Examples of this data may include:
 - Element Type, identifying the element as a CMTS, CMS, or MGC

- Element ID
- A list of which Event Messages are required and which Event Messages are optional as defined by the MSO.
For each of these Event Messages, identify if the Event Messages are to:
 - 1) be transported to the RKS as a single Event Message in real-time, or
 - 2) batched and transported to the RKS as multiple Event Messages at a later time;
 - 3) provide capability to configure both how many Event Messages are batched before being sent to the RKS.
- Number of days to keep Event Messages for short-term storage
- Others
- Enable or disable Media_Alive Event Message, configure the frequency of Media_Alive message (suggested 0 to 1440 minutes, with 0 being no Media_Alive Events).