SCTE · ISBE

STANDARDS

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.

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

List of Figures

List of Tables

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 IPCablecom 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 IPCablecom 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 IPCablecom voice, video and other multimedia services, OpenCable™ services such as Video-On-Demand, Pay-Per-View and DOCSIS® high-speed data services.

The IPCablecom 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.

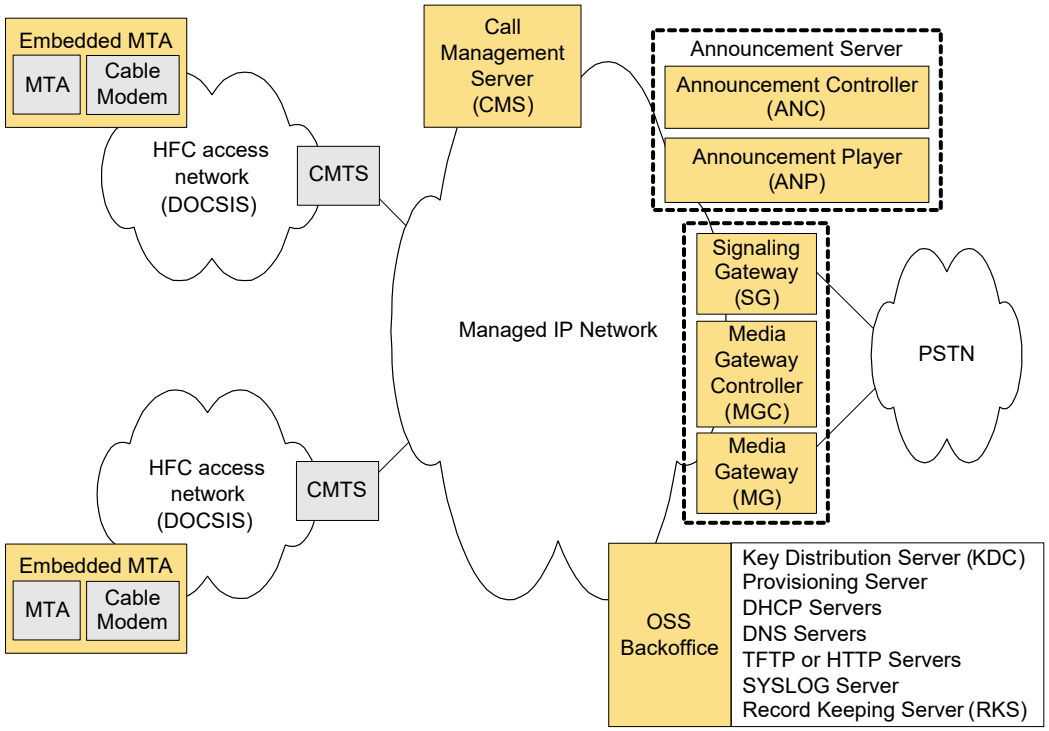

Figure 1. IPCablecom Network Component Reference Model

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.

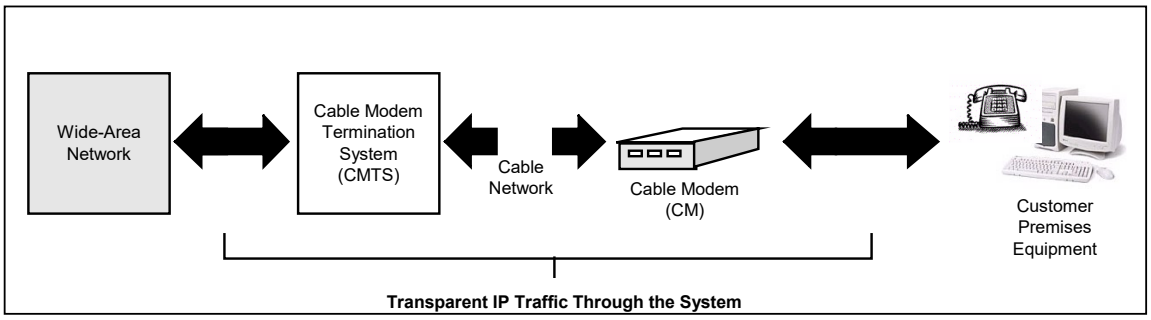

Figure 2. Transparent IP Traffic through the Data-Over-Cable System

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 □ describing the Event Message architecture itself. Section 8 describes the services IPCablecom 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 IPCablecom 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 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. 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 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 to the edge of the IPCablecom 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 IPCablecom. "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 IPCablecom 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 IPCablecom services, bringing along their full structure would make it difficult to support the real-time nature of certain enhanced IPCablecom services. This standard leverages the value of the information content from the existing billing formats, augmenting that with the distributed nature of the IPCablecom architecture.

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

The IPCablecom Event Messages contain sufficient per-call information to support customer billing for service as well as settlement between IPCablecom network providers for access. The information contained in the Event Messages supports a wide variety of billing and settlement models. IPCablecom 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. IPCablecom neither mandates nor precludes the use of a clearinghouse for settlements.

The IPCablecom 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 IPCablecom 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 IPCablecom 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 IPCablecom 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 IPCablecom Event Message standard details these requirements.

For the purposes of settlements, each IPCablecom 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 IPCablecom 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 IPCablecom features such as pre-paid calling card, real-time fraud prevention, and real-time credit enforcement.

The IPCablecom 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 IPCablecom 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 IPCablecom, do not establish any such dedicated paths.

To the contrary, the IPCablecom 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.

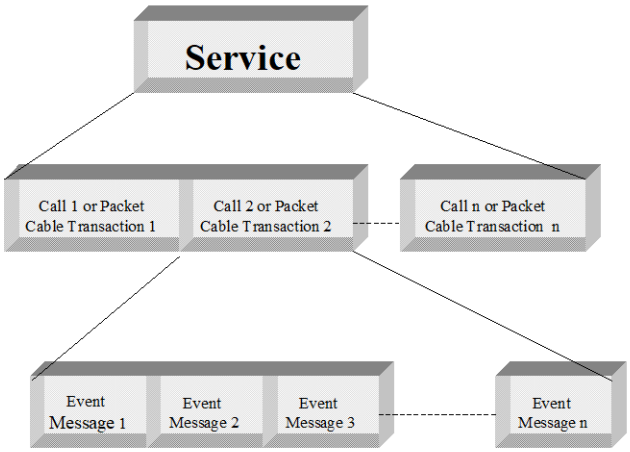

Figure 3. IPCablecom Terminology

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).

7 EVENT MESSAGES ARCHITECTURE

Figure 4 shows a representative IPCablecom Event Messages Architecture. By standardizing the transport, syntax and collection of appropriate Event Message attributes from a distributed set of network elements, the IPCablecom architecture provides a single reference point to interface to existing billing, settlement, reconciliation, and other systems**.** Note that only the shaded components are included within the scope of the IPCablecom 1.5 architecture. Interfaces between the RKS and the shaded IPCablecom network elements are within scope of IPCablecom 1.5. Interfaces between the RKS and back office servers or applications are NOT within the scope of IPCablecom 1.5. It should be understood that the back office servers and applications shown Figure 4 are representative, and are not mandated by the IPCablecom 1.5 architecture.

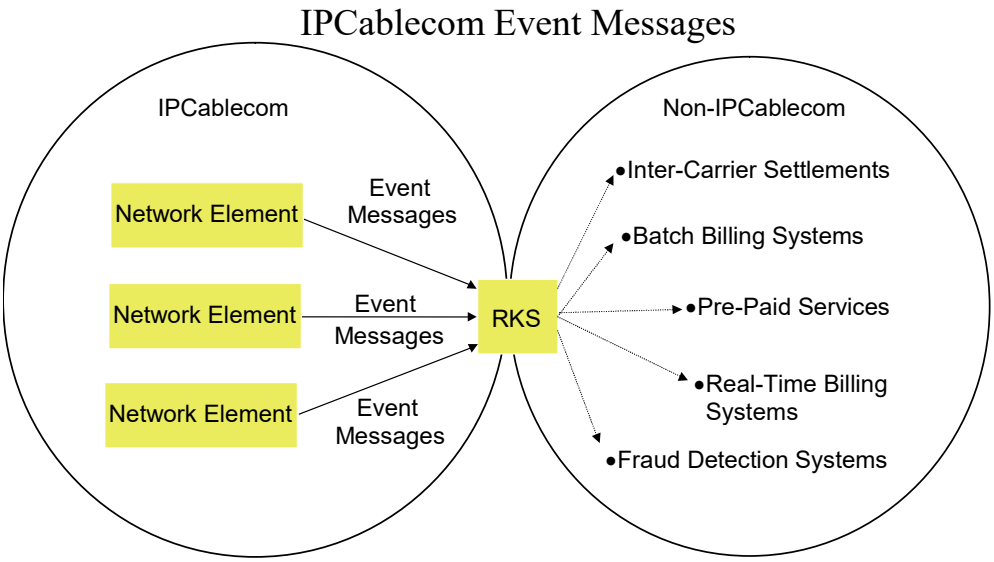

Figure 4. Representative IPCablecom Event Messages Architecture

7.1 IPCablecom Event Message Collection

Event Message collection occurs as follows: when trigger events occur [such as call signaling starts, activation of QoS service resources, call signaling stops, etc.], the relevant IPCablecom network element generates an Event Message. These messages may be sent immediately to the RKS, or a group of messages may be collected and sent at a later time. In either case, the actual time of the trigger event is reported allowing the back office applications to accurately calculate time-based resource usage. As these Event Messages are accumulated within the RKS, the network operator can then export them into their billing systems based on their business requirements. The data from multiple network elements are linked to a transaction [e.g., call] via a unique BCID, which can be leveraged for reconciliation and non-repudiation purposes.

7.2 IPCablecom Network Elements

The IPCablecom architecture supports a system capable of creating, collecting, and delivering usage data from a subset of IPCablecom network elements to a cable operator's back office applications. Trusted IPCablecom 1.5 network elements that create Event Messages include the Call Management Server (CMS) and Cable Modem Termination System (CMTS), Media Gateway Controller (MGC).

The IPCablecom architecture contains trusted and untrusted network elements. Trusted network elements are typically located within a MSO's facility and are controlled by the MSO. Untrusted network elements are typically located within the consumer's home or outside of the MSO's facility or exclusive control. In the IPCablecom 1.5 architecture, Event Messages are only accepted from trusted IPCablecom network elements.

The IPCablecom Architecture Document [13] contains a detailed description of the IPCablecom network elements. A brief explanation of the IPCablecom network elements that will most likely generate IPCablecom Event Messages is listed in this section for completeness.

7.2.1 Call Management Server (CMS)

The Call Management Server (CMS) provides signaling services necessary for voice communications. The primary purpose of the CMS is to establish standard "calls," as that term is used in the IPCablecom context. The media servers also provide support services for the media streams such as conference mixing bridges and announcement servers.

The CMS MUST create a BCID:

- on receipt of an NCS-signaling NTFY message from an MTA, or
- when an Event Message not associated with any call is generated.

The CMS MUST send the BCID and other data as defined in Table 1 to the CMTS via the DQoS GateSet message as specified in the DQoS specification [3].

Table 1. IPCablecom Event Reporting Common Elements

BCID (see Table 39)
IP address and port number of the primary RKS
IP address and port number of the secondary RKS
Flag indicating if CMTS should send Event Messages to the RKS in real-time

The CMS MUST generate the appropriate Event Messages as defined in this standard.

7.2.2 Media Gateway Controller (MGC)

The Media Gateway Controller (MGC) is the overall controller function of the PSTN gateway. It receives, mediates, and routes call signaling information between the IPCablecom and PSTN domains and it maintains and controls the overall call state for all calls connecting to and from the PSTN. It controls the Media Gateway function and communicates with the Signaling Gateway function via the MGC-SG protocol defined for the major protocol family in question, i.e., ISUP, In-band or TCAP.

The MGC MUST create a BCID on receipt of:

- an SS7 IAM message or
- a TCGP NTFY with digits (operator services),
- when an Event Message not associated with any call is generated.

The MGC MUST generate the appropriate Event Messages as defined in this standard.

7.2.3 Cable Modem Termination System (CMTS)

The Cable Modem Termination System terminates the connection from the cable modem on the customer premises into the IPCablecom network. The CMTS generates QoS Event Messages. QoS event messages are generated individually for both upstream and downstream bandwidth.

The CMTS MUST generate the appropriate Event Messages as defined in this standard. For all EM messages it generates other than Time_Change, the CMTS MUST use the unique Billing-Correlation-ID assigned by the CMS and received from the CMS in the Event-Generation-Info object of the DQoS Gate-Set message as defined in Section 5.3.2.7 of DQoS [3]. See Section 9.16 for the generation of BCID in Time_Change events.

DOCSIS provides a mechanism by which multiple sessions can be placed on a single upstream service flow. DQoS supports this feature and refers to it as multiple grants per interval. There are two side effects to event messages when an MTA uses multiple grants per interval. The service flow ID (SFID) will be common among the events for

all sessions that share that flow. The QoS Descriptor attribute relects the total bandwidth of all sessions using the flow.

7.2.4 Record Keeping Server (RKS)

The Record Keeping Server (RKS) is a trusted network element function. In many cases, for simplicity reasons, the RKS is depicted in this document as a separate standalone element, but this standard does not preclude a CMS, Billing System, or other application from performing the RKS functionality. The RKS is the mediation layer between the call signaling and transport layer and the back-office applications. The RKS is expected to pre-process the data from the Call Signaling and Transport layer and present it to the back-office applications in the format and within the time constraints deemed necessary by the MSO.

The RKS also, at a minimum, is a short-term repository for IPCablecom Event Messages. It receives Event Messages from various trusted IPCablecom network elements. The RKS assembles the Event Messages into coherent sets, which are then made available to a usage-processing platform and potentially to several other back office systems. It acts as the demarcation point between the IPCablecom network and the back office applications.

Figure 5 gives a representative RKS deployment for information only and does not imply an implementation requirement.

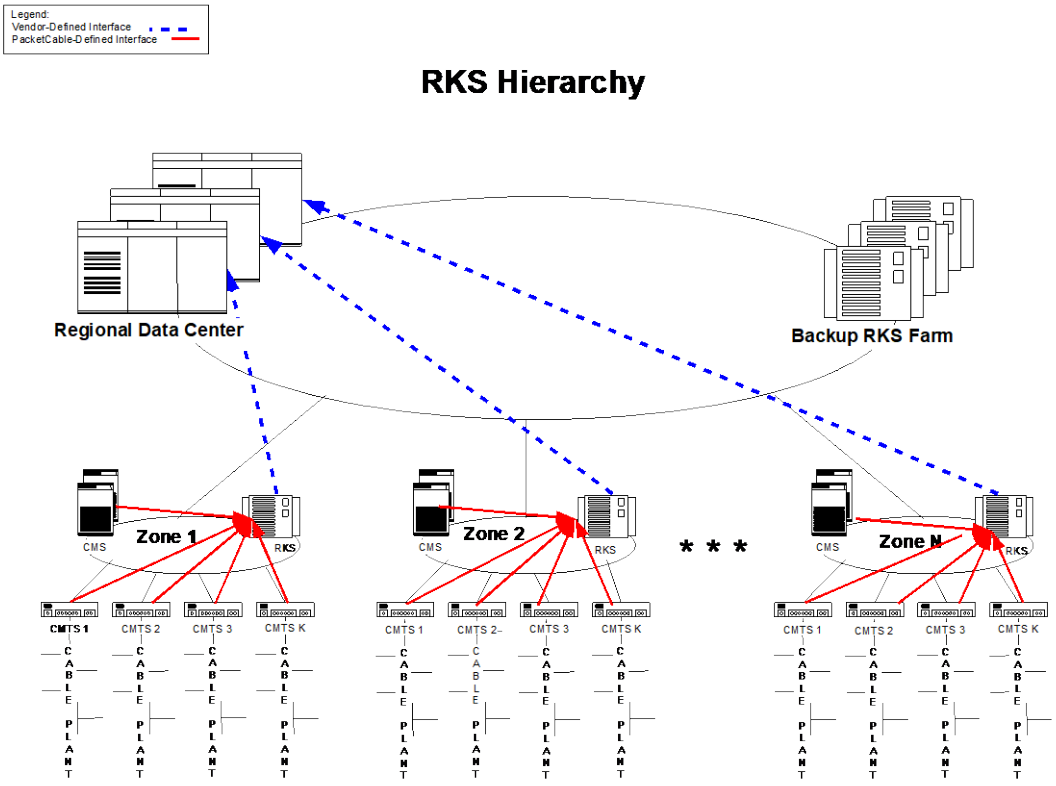

Figure 5. Example RKS Architecture

The RKS is expected to perform the following functions:

- The RKS MUST receive Event Messages.
- The RKS MUST be capable of correlating all Event Messages related to an individual call and have an extensible output to meet the needs of the downstream applications.

- The RKS MUST assemble Events and Determine Completeness. This MUST include the capability to distinguish Event Messages, and recognize when a complete set, representing a coherent set of billing data is available for transport to the back office system.
- The RKS MUST provide interface network functions that require real time or near real time based on priority and where messages are being sent, as defined in Section 9. For example, a call may be sent real-time and a report may be sent at night. The correlation process MUST be user definable to support the various call events defined herein and defined in the future.
- The RKS MUST have the ability to store the Event Messages for at least one week or until sent to the other back office systems and successful receipt is acknowledged from those systems.
- The RKS MUST have the ability to dump the Event Messages to some other type of offline storage device on a regular basis (CD, tape, or other media) for retrieval and regulatory purposes.

The following list deals with other possible capabilities of an RKS. They are therefore beyond the scope of the requirements of this current document, and are included here for informational use only. Decisions on these optional requirements will be based upon the MSO response to many regulatory and business variables.

- An RKS-RKS security interface MAY be required. IPCablecom 1.5 does not define this interface. The security interface between the RKS and other IPCablecom trusted network elements is defined in [2].
- The RKS MAY support Backup and Recovery. This includes a nominal ability to restore the state and contents of billing data in the event of application or platform failures.
- The RKS MAY support distribution of billing data to all appropriate systems. This includes the implementation of a protocol that ensures data integrity and reliability on the usage collator interface.
- The RKS MAY support monitoring and reporting. This includes the ability to produce and send alarms to a network management system, and create various audit and measurement reports.
- The RKS MAY allow remote testing and maintenance capability.
- The RKS MAY support a Service Creation Environment.
- The RKS MAY support user defined fault handling in the case of incomplete Event Messages or other such anomalies.
- The RKS MAY support multiple downstream applications, and various transport methodologies.
- The RKS MAY support full auditability of data and processes.
- The RKS MAY support a user definable long-term storage mechanism.
- The RKS MAY support disaster planning and recovery processing.

7.3 General IPCablecom Network Element Requirements

This section lists requirements placed on the IPCablecom network elements:

The CMS, CMTS, and MGC MUST create a security relationship with each RKS that these network elements will send Event Messages as defined in the IPCablecom Security Specification [2].

The CMS MUST support multiple sets of primary and secondary RKSes, which might be required in cases in which total Event Message traffic exceeds the throughput capability of a single RKS.

For each call, the CMS or the MGC MUST create a unique BCID, identify the primary and secondary RKS and determine whether the Event Messages are to be delivered in real time or batched and sent at a later time.

- The trusted IPCablecom network elements that generate Event Messages MUST timestamp Event Messages in 1 millisecond granularity +/- 100 milliseconds based on information reported by network time sources such as edge devices (Clients and Gateways).

- All IPCablecom network elements that generate Event Messages MUST synchronize their clocks at least once per hour to a network clock source. This synchronization MUST assure the reporting device's own clock remains within ±100 milliseconds real time of the last synchronization value.
- IPCablecom network elements that generate Event Messages MUST support Network Time Protocol (NTP) time synchronization as defined in [10].
- The IPCablecom network elements MUST support transport to a primary RKS and failover to a secondary RKS when communication with the primary RKS fails for any reason (including situations where the primary RKS becomes inoperable).
- IPCablecom network elements MUST support the transport of a single Event Message as well as a batch of Event Messages (batch mode = multiple Event Message per single Radium message).
- Each trusted IPCablecom network element that generates an Event Message MUST identify itself with a static, unique element ID.
- Implementations that combine CMS and MGC functionality MAY share a single element ID. Event Messages generated by a combined CMS/MGC MUST indicate which IPCablecom functional element (e.g., MGC or CMS) initiated the message using the Element_Type field in the EM_Header.

7.4 Event Message Interfaces

This section describes the interfaces between the IPCablecom network elements that are involved in the Event Messages process. It should be noted that additional requirements are imposed on these by other IPCablecom specifications and that the requirements listed in this document are specific to Event Messages. It should also be noted that additional requirements are specified for these interfaces and these IPCablecom network elements in other sections of this document.

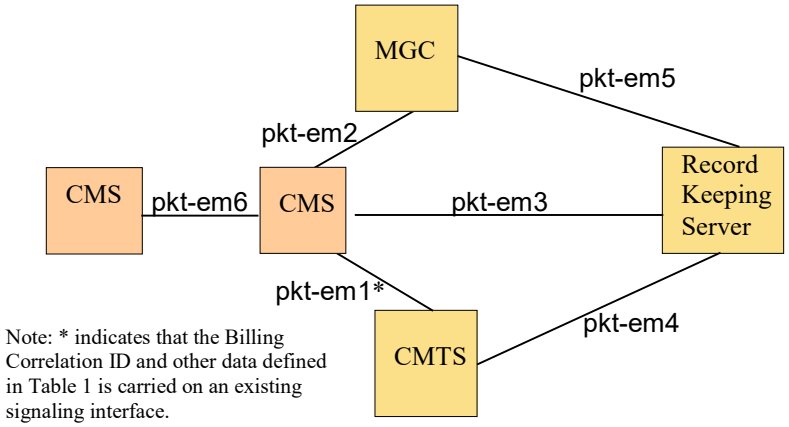

Figure 6. Event Message Billing Interfaces

7.4.1 CMS to CMTS (pkt-em1*)

The CMS to CMTS interface is defined by the IPCablecom DQoS protocol [3].

The CMS sends the BCID and other data as defined in Table 1 to the CMTS via the DQoS GateSet message as specified in the DQoS specification [3].

7.4.2 CMS to MGC (pkt-em2)

The CMS to MGC interface is defined by the IPCablecom CMSS specification [7]. The CMS and MGC exchange originating/terminating information such as BCID, FEID, etc. across this interface as defined in [7].

7.4.3 CMS to RKS (pkt-em3)

The CMS to RKS interface is defined by the IPCablecom security specification [2] and also by the Event Message transport and syntax rules defined in this document.

7.4.4 CMTS to RKS (pkt-em4)

The CMTS to RKS interface is defined by the IPCablecom security specification [2] and by the Event Message transport and syntax rules defined in this document.

7.4.5 MGC to RKS (pkt-em5)

The MGC to RKS interface is defined by the IPCablecom security specification [2] and by the Event Message transport and syntax rules defined in this document.

7.4.6 CMS to CMS (pkt-em6)

The CMS to CMS interface is defined by the IPCablecom CMSS specification [7]. The originating CMS and terminating CMS exchange originating/terminating information such as BCID, FEID, etc., across this interface as defined in [7].

7.4.7 Security Requirements

When the network IPSec Security Associations are established, security keys MUST be created and exchanged between each RKS (primary, secondary, etc.) and every CMS, CMTS, and MGC that will send Event Messages to any of those RKSes. The Event Messages are sent from the CMS, CMTS, and MGC to the RKS using one of the supported transport mechanisms, each of which it must be possible to secure with IPSec. Refer to the IPCablecom Security Specification [2] for a detailed description of the security requirements for the IPCablecom Event Message interfaces.

8 IPCABLECOM SERVICES AND THEIR ASSOCIATED EVENT MESSAGES

This section defines the supported IPCablecom 1.5 Services and their associated Event Messages. Although many of the IPCablecom 1.5 services can be billed using the Event Messages and attributes defined in this document, the services described in this section are currently limited to IPCablecom 1.5 services.

In order to identify appropriate Event Messages required for each service, representative call flows were developed for IPCablecom 1.5 basic call configurations. The IPCablecom Call Flow documents [16], [17], [17], provide a description of the call configuration along with any assumptions made about a specific service and an example call flow. It is not the intention of these call flow documents to limit the realization of any of these services to any specific implementation.

8.1 IPCablecom Call Configurations

This section describes the three basic IPCablecom 1.5 call configurations: On-Net to On-Net, On-Net to Off-Net, and Off-Net to On-Net. A required minimum set of Event Messages MUST be generated for each of these three basic call configurations. If specific services are initiated along with the basic call, then refer to Section 9 for a list of additional Event Messages for these specific services.

8.1.1 On-Net to On-Net Call Configuration

A single-zone On-Net to On-Net call is within a single MSO's network, using two different MTAs that are both connected to the same CMS. For IPCablecom 1.5, it is assumed that both the originating and terminating MTAs are using the same CMS and possibly two different CMTSes.

Refer to the IPCablecom Call Flow document [16] for a complete description of an example single-zone On-Net to On-Net call configuration including an example call flow showing the triggers for these Event Messages.

Both intra-domain and inter-domain On-Net to On-Net call configurations use two different MTAs that are both connected to two different CMSes.

For any On-Net to On-Net call configuration, the originating half and the terminating half of the call MUST each generate a complete set of Event Messages.

Table 2. On-Net to On-Net Call Configuration

Event Message	Required or Optional	Comments
Database_Query	O	If LNP is required
Signaling_Start	R	CMS is starting signaling to support a call start
QoS_Reserve	R	CMTS is reserving QoS
QoS_Commit	R	CMTS is committing QoS
Intelligent_Peripheral_Usage_Start	O	e.g., if an announcement is needed NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	e.g., if an announcement is needed NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Call_Answer	R	Indicates start of media stream
Call_Disconnect	R	Indicates termination of media steam
QoS_Release	R	CMTS is releasing QoS
Signaling_Stop	R	Signaling for the service is complete
Media_Statistics	O	Media stream statistics reported by the gateway

8.1.2 On-Net to Off-Net Call Configuration (Outgoing PSTN Interconnect)

The only Off-Net interconnection supported by IPCablecom 1.5 is to the PSTN. Therefore the CMS sends all Off-Net calls to the PSTN. The Interconnect_Start Event Message identifies the type of Off-Net trunk, for example SS7/FG-D trunks, Type 1/DTMF trunks or some other type of trunks as required. The Off-Net call (i.e., non-special access codes calls e.g., 800, 900, N11 etc.) may require an LNP query. The CMS MUST generate a database query Event Message each time a LNP database is accessed (regardless of whether this query is requested from a PSTN database or IP database).

Refer to the IPCablecom Call Flow document [17] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

For any On-Net to Off-Net call configuration, the originating half and the terminating half of the call MUST each generate a complete set of Event Messages.

Table 3. On-Net to Off-Net Call Configuration

Event Message	Required or Optional	Comments
Database_Query	O	If LNP is Required
Signaling_Start	R	Starting signaling to support a call start
QoS_Reserve	R	CMTS reserves QoS
QoS_Commit	R	CMTS commits QoS
Intelligent_Peripheral_Usage_Start	O	e.g., if an announcement is needed NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	e.g., if an announcement is needed NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Interconnect_Start	R	For call setup
Call_Answer	R	Indicates start of media stream
Call_Disconnect	R	Indicates termination of media steam
Interconnect_Stop	R	For call tear-down
QoS_Release	R	CMTS releases bandwidth
Signaling_Stop	R	Indicates end of signaling
Media_Statistics	O	Media stream statistics reported by the gateway

8.1.3 Off-Net to On-Net Service (Incoming PSTN Interconnection)

The CMS receives calls that are incoming from other entities and establishes communications with the MTA on the MSO's network. For IPCablecom 1.5, it is assumed that all incoming calls are from the PSTN.

Refer to the IPCablecom Call Flow document [17] for a complete description of this call configuration including an example call flow showing the triggers for these Event Messages.

For any Off-Net to On-Net call configuration, the originating half and the terminating half of the call MUST each generate a complete set of Event Messages.

Table 4. Off-Net to On-Net Call Configuration

Event Message	Required or Optional	Comments
Signaling_Start	R	Starting signaling to service a request to start a call
Interconnect_Start	R	For call setup

Event Message	Required or Optional	Comments
QoS_Reserve	R	CMTS reserves bandwidth
QoS_Commit	R	CMTS commits bandwidth
Intelligent_Peripheral_Usage_Start	O	e.g., if an announcement is needed NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	e.g., if an announcement is needed NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Call_Answer	R	Indicates start of media stream
Call_Disconnect	R	Indicates termination of media steam
Interconnect_Stop	R	For call tear-down
QoS_Release	R	CMTS releases bandwidth.
Signaling_Stop	R	Indicates end of signaling
Media_Statistics	O	Media stream statistics reported by the gateway

8.2 Specific Services

A basic set of Event Messages MUST be generated based on the type of call configuration: On-Net to On-Net, On-Net to Off-Net, Off-Net to On-Net. The basic set of Event Messages is described in Section 8.1.

This section describes additional Event Messages that MUST be generated along with the basic set in order to describe specific IPCablecom 1.5 services. This section also describes optional Event Messages that MAY be generated along with the basic set and any additional required Event Messages. These additional required and optional Event Messages are identified in the tables in this section. It is expected that these additional Event Messages will be able to be generated regardless of the particular implementation of the service.

8.2.1 911 Service

A 911 call follows the standard On-Net to Off-Net Event Message flow described above in Section 8.1.2.
911 calls require special treatment. In IPCablecom Release 1.5, it is assumed that the MSO sends 911 calls to the PSTN on a special trunk. The Trunk Group ID is captured in the Interconnect_Start and Interconnect_Stop Event Messages, and it is assumed that the RKS or some element downstream of the RKS has the capability of inferring this trunk group type from that unique Trunk Group ID.

No additional Event Messages are required beyond the basic ones listed for an On-Net to Off-Net call in Section 8.1.2.

8.2.2 Other N11 Services (311, 411, 611)

These calls are identical to the 911 call both from a call flow and Event Message perspective. The determination of whether to bill or not can be performed at the Billing System based on the "Called Party Number" attribute. For example, charges for calls to 411 for directory assistance may be different than charges for 911 emergency calls, which are free, but the Event Messages, which capture the usage for both types of services, are the same. They would differ only in the content of specific attribute values such as the Called_Party_Number (411 vs. 911) within the Call_Answer Event Message. The billing system is expected to make a determination as to how much to bill the customer based on these attributes together with other factors such as whether the call is completed or not.

8.2.3 Toll-Free Services

Toll-Free Services follow the standard On-Net to Off-Net Event Message flow described above in Section 8.1.2. In IPCablecom 1.5, toll-free calls can be handled two ways:

- Send all Toll-free calls to the PSTN on a special trunk. The call is treated exactly like the 911 case discussed in Section 8.2.1 in terms of Event Messages, meaning that no additional Event Messages are required.
- Initiate a query to the toll-free SCP (in IP or PSTN) and, depending on the specified Carrier Identification Code, route the call to the appropriate network. A Database_Query Event Message MUST be generated to record the query to the toll-free database.

Table 5. Toll-Free Services

Additional Event Messages	Required or Optional	Comments
Database_Query	R	Not used for Scenario 1 but required for Scenario 2

8.2.4 Operator Services

Operator Services follow the standard On-Net to Off-Net Event Message configuration described above in Section 8.1.2. There are no new additional Event Messages beyond those already described for the On-Net to Off-Net calls in that section. The CMS sends that call to the designated Operator Service Provider using the PSTN. There may be multiple Operator Service Providers with which the MSO has contracts. The caller just dials "0."

The CMS generates an event identifying that call as 0- (denoting the single digit "0" dialed without any subsequent digits) with "0" in the Called number field. The CMS replaces the "0" in the Called Number field with the number of the Operator Service Provider (OSP). These parameters are sent to PSTN so that call can be sent via PSTN to the OSP. It is assumed dedicated private lines to the OSP from each IP-switch are impractical and expensive for MSO and not considered as an option.

For the purposes of IPCablecom 1.5, it is assumed that operator services encompasses only 0- services. 0+ service, in which the customer keys the dialed number in together with the initial "0", is not supported in IPCablecom 1.5.

8.2.5 Call Block Service

Event Messages are generated for Call Block Service only if the CMS blocks a call. Call Blocking is supported by all of the three basic call configurations: On-Net to On-Net, On-Net to Off-Net, and Off-Net to On-Net.

The CMS can block calls depending on the policies laid out by the MSO. For example, the MSO may allow the end-user to block all 900 calls at the user's request. As another example, the MSO may recognize some calls as fraudulent and block those fraudulent calls. In this case an Event Message needs to be generated with some reason attributes as to why the call was blocked. In addition, depending on the type of blockage, the MSO may desire to play an appropriate announcement (e.g., "Sorry your time is up ….").

The CMS may initiate another call to the Announcement Server via the PSTN and play it to the caller. A series of Event Messages will be generated for this call, using the same BCID as the standard Event Messages associated with the off-hook, dialing, etc., which is not expected to be used for billing this call to the end-user.

Table 6. Call Block Service

Additional Event Messages	Required or Optional	Comments
Service_Instance	R	None
Intelligent_Peripheral_Usage_Start	O	NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	NOTE: This Event Message will be defined in a future release of this IPCablecom standard.

8.2.6 Call Waiting Service

At any given time the caller may be talking and will hear the call waiting tone when another call is incoming. It is understood that at some point prior to this call, the called party subscribed to call waiting service. The called party

can switch back and forth between the two calls by using the flash hook. Call Waiting can be supported by any of the three basic call configurations: On-Net to On-Net, On-Net to Off-Net, and Off-Net to On-Net.

The call flow is as follows:

- There is an existing call to a number connected via the MTA/CMTS/CMS. Another call attempt is made to that number, the CMS:
  - Verifies that an existing call is already in progress,
  - Checks its internal database to verify whether the called party has subscribed to Call Waiting, if yes:
  - Establishes a voice connection to the Announcement Server (which will play the call waiting tone),
  - Creates an Event Message indicating that Call Waiting is being initiated,
  - Mixes the two voice calls (the currently established voice call and the Call Waiting tone voice call) so that the called party can hear the call waiting tone.

It is assumed that Call Waiting only supports two calls (one active and the other on hold) in IPCablecom 1.5. The call on hold will not be connected to any announcement server.

Both of the calls between which the subscriber is switching generate a complete set of Event Messages on their own as detailed in Sections 8.1.2 and 8.1.3, but there may also be three additional Event Messages associated with this instance of Call Waiting, as detailed below. If the Announcement Server is located on the PSTN, then the previously discussed Call_Answer and Call_Disconnect Event Messages are generated for this call.

Table 7. Call Waiting Service

Event Message	Required or Optional	Comments
Interconnect_Start	O	Required only if Announcement Server for Call Waiting tone is Off-Net on PSTN
Interconnect_Stop	O	Required only if Announcement Server for Call Waiting tone is Off-Net
Intelligent_Peripheral_Usage_Start	O	Required only if Announcement Server On-Net NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	Required only if Announcement Server On-Net NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Service_Instance	R	None

8.2.7 Call Forwarding Service

Call Forwarding Service applies only to calls terminating On-Net as described in Sections 8.1.1 and 8.1.3.

The CMS gets notification that a call needs to be completed to a specific dialed number/end device. The CMS checks its internal database and determines that the called number has subscribed to Call Forwarding, Call Forwarding is currently active, and the forwarding number is XYZ. The CMS initiates another call to the forwarded number on behalf of the original calling party.

The CMS MUST generate a Service_Instance Event Message with the Calling_Party_Number attribute containing the original calling party number, the Charge_Number attribute containing the original called party number (the party number of the subscriber who has call forwarding service enabled), and the Called_Party_Number containing the forwarded number XYZ. Event Messages are generated for the fact that a Call Forwarding service instance was initiated. The BCID for this leg is different than the first call. The rationale for using the Related BCID as the common identifier for call forwarding is that it may be desirable to flag calls made automatically by invocation of call forwarding on the subscriber's monthly statement in order to make it clear the reason those calls were placed.

For all purposes the original call and the forwarded call are two different billable calls. This will require the RKS to replace the Calling Party Number with the value of the Charge Number for the forwarded call's AMA record.

The Calling_Party_Number attribute in the Service_Instance Event Messages is consistent with Telcordia Technologies' GR-580-CORE [27], GR-586-CORE [28] call forwarding specifications and the GR-317-CORE [29] specification.

Table 8. Call Forwarding Service

Event Message	Required or Optional	Comments
Service_Instance	R	None

8.2.8 Return Call Service

This service applies only to calls originating On-Net, described in Sections 8.1.1 and 8.1.2. The CMS MUST keep a register with the Calling Party Number of the last call.

Return Call Service returns the last call that was made to an MTA. Upon instantiation of Return Call feature, the CMS initiates another call with the Calling Party Number of the last call, retrieved from the register just described, as the Dialed number. Event Messages are generated for the fact that the Return Call feature was initiated, using the BCID of this call. If the Calling Party Number of the last call had Caller ID privacy restrictions, then CMS may conference in a recording from an announcement server saying that this call cannot be completed.

Table 9. Return Call Service

Event Message	Required or Optional	Comments
Service_Instance	R	None
Interconnect_Start	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is Off-Net on PSTN.
Interconnect_Stop	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is Off-Net on PSTN.
Intelligent_Peripheral_Usage_Start	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is On-Net. NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	Required only if Announcement Server for delivering the Message indicating reason Return Call cannot be activated is On-Net. NOTE: This Event Message will be defined in a future release of this IPCablecom standard.

8.2.9 Repeat Call Service

Repeat Call Service applies only to calls terminating On-Net as described in Sections 8.1.1 and 8.1.3.

Repeat Call can be initiated when the caller dials a number and gets a busy signal. With this feature the caller dials a special pre-determined string of digits (*66 in the United States of America) which then instructs the network to keep polling the called and calling party and when both free, establish the communication. In IPCablecom 1.5, the originating CMS will keep trying to establish communications to the called number for a pre-determined amount of time.

Table 10. Repeat Call Service

Event Message	Required or Optional	Comments
Service_Instance	R	None
Interconnect_Start	O	Required if Announcement Server for delivering the Message indicating reason Repeat Call cannot be activated is Off-Net on PSTN.
Interconnect_Stop	O	Required only if the appropriate Interconnect_Start was activated.
Intelligent_Peripheral_Usage_Start	O	Required only if Announcement Server for delivering the Message indicatin reason Repeat Call cannot be activated is On-Net. NOTE: This Event Message will be defined in a future release of this IPCablecom standard.
Intelligent_Peripheral_Usage_Stop	O	Required only if Announcement Server for delivering the Message indicating reason Repeat Call cannot be activated is On-Net, NOTE: This Event Message will be defined in a future release of this IPCablecom standard.

NOTE: There may be multiple Interconnect_Start and Stops capturing the multiple different times the originating CMS tries to make an Off-Net call to try to complete a Repeat Call request.

8.2.10 Voice Mail Service

Voice Mail Service only applies to calls terminating On-Net, described in Sections 8.1.1 and 8.1.3.

It is assumed that the voice mail server will be located Off-Net for IPCablecom 1.5. It is therefore assumed if voicemail billing is usage sensitive, that connections to the Off-Net voicemail system will be counted in the same way whether they are voicemail messages being left for the subscriber (deposit) or calls to retrieve the messages on the voicemail server.

Voice mail deposit and retrieval scenarios are treated as separate transactions that have associated Event Messages. Event Messages for voice mail deposit look like a standard On-Net to Off-Net call. When the call is transferred to the Voice Mail Server, the Routing Number MUST be captured and populated with the Voice Mail Server Address.

The connection time to the Voice Mail Server MAY also be derived through the standard On-Net to Off-Net Event Messages. Since the Voice Mail Server is located Off-Net, Event Messages for voice mail retrieval MAY only be generated if the retrieval is initiated from a device within the MSO's network (e.g., On-Net to Off-Net call).

8.2.11 Message Waiting Indicator Service

It is assumed that an Off-Net voicemail system is used as described in Section 8.2.10. Because it seems unreasonable for the CMS to have to place a separate call to the Off-Net system each time a voicemail subscriber goes off-hook, it is assumed that a mechanism exists which allows the Off-Net voicemail system pass the information to the CMS indicating which subscribers have voicemail waiting. A further assumption is that the MTA is capable of delivering the audible stutter-tone message-waiting indicator to the subscriber's MTA port going off-hook, on the command of the CMS.

Under the scenario described in the assumptions section, and given the fact that billing is not based on any per use delivery of the stutter tone, there are no Event Messages required for this service. Billing is based on a combination of information obtained from the Voicemail send/retrieve Event Messages discussed in Section 8.2.10 and provisioning information indicating when a subscriber has signed up for voicemail services.

8.2.12 Three-Way Call Service

The Three-Way Call Service allows a subscriber to add a third party to an active call. Three-Way Call Service applies to the originating and terminating CMS. To operate Three-Way Call Service, the subscriber dials the first call party. While on the first call, the subscriber presses the switch hook or flash key to place the first party on hold, and, after listening for a dial tone, dials a second party number. The second party answers, the subscriber may speak privately or create a Three-Way Call by depressing the hook switch or pressing the flash key once again to merge

the two calls. The Three-Way Call Service is then initiated and the Service_Instance Event Message is generated by the subscriber's CMS.

Table 11. Three-Way Call Service

Event Message	Required or Optional	Comments
Service_Instance	R	If the Three-Way Call Service is supported by the CMS, the CMS MUST generate a Service_Instance Event Message when the Three-Way Call service is initiated.

8.2.13 Customer Originated Trace Service

The Customer Originated Trace Service (COT) allows subscribers to activate an immediate trace on an annoyance or nuisance call. After a nuisance call is terminated, a subscriber who wishes to trace the call picks up the handset and goes off-hook, listens to dial tone, and then dials the Customer Originated Trace activation code (for example, in the United States, the Customer Originated Trace activation code is *57).

Table 12. Customer Originated Trace Service

Event Message	Required or Optional	Comments
Service_Activation	R	If the Customer Originated Trace Service is supported by the CMS, the CMS MUST generate a Service_Activation Event Message when the Customer Originated Trace Service is initiated.

Note that when the COT Service is activated, it only applies to one call (the last call received by the subscriber), and no Service_Deactivation Event Message is generated.

8.2.14 Account Code and Authorization Code Service

The Account Code and Authorization Code Service defines two service capabilities as one service in support of account & authorization codes. The account and authorization codes may be used by Business Support Systems (BSS) to apply various accounting and charging rules based on the codes.

Account codes allow call charging to user projects, departments or special accounts, etc. A subscriber may activate the Account Code service capability when initiating a call (usually a long distance call) in order to have the call accounting recorded under a special project or account. The account code may then be used in the BSS systems for various purposes including call accounting & charging; it is usually not subject to verification by the CMS.

Authorization codes provide the capability for a subscriber to override call restrictions for a single call. A subscriber may be restricted from making toll calls and may decide to activate the Authorization Code service capability when placing a long distance phone call in order to remove the default call restrictions for that one call. The subscriber can typically override the restriction by dialing an authorization code that grants enough privileges to make long distance calls. The Authorization Code Service capability is used in a business group environment where multiple authorization codes may be assigned to grant various call privileges. Some authorization codes may be used to logically segment a given account code.

The Telcordia Technologies General Requirements document GR-605-CORE [26] defines multiple mechanisms for "Authorization Codes for Automatic Flexible Routing (AFR) and Account Codes for Basic Business Group and AFR". A CMS MAY implement one or more of the mechanisms defined in GR-605-CORE [26]. However, IPCablecom CMS network elements MUST support the generation of Service_Instance Event Messages and report the account or authorization code entered by the subscriber as defined in this standard if any GR-605-CORE mechanisms are supported.

Table 13. Account Code and Authorization Code Service

Event Message	Required or Optional	Comments
Service_Instance	R	If the Account Code and Authorization Code Service is supported by the CMS, the CMS MUST generate a Service_Instance Event Message when either the account or authorization code service capability is initiated.

The CMS MUST generate a Service_Instance Event Message when the Account Code and Authorization Code Service is initiated even when the dialed code is invalid and the call is not successfully made. The Call_Termination_Cause attribute MUST be present in the Service_Instance Event Message for this service and it MUST be encoded as defined in Section 10.2 to report the appropriate Call Completion Code (GR-1100-CORE [6], Table 235). This attribute indicates whether the service is successfully completed or the reason for the service failure (for e.g., the dialed code provided by the subscriber is not authorized or invalid).

A successful call completion code reported in the Service_Instance Event Message only means that the Account Code and Authorization Code Service is successfully attempted and that the call signaling may proceed (other errors could occur resulting in a call failure during the call setup which may be reported in other Event Messages, like the Signaling_Stop Event Message for example).

9 IPCABLECOM EVENT MESSAGE STRUCTURE

This section describes the various Event Messages, together with their associated list of attributes. Refer to Section 10 for a detailed description of the attributes described in this section. Refer to Section 8 for a detailed description of the services and their associated Event Messages.

The description of each event message in this Section includes:

- A summary of the EM purpose and conditions under which it is sent.
- Mandatory requirements for triggers that cause the EM to be created and timestamped during a call that is completely set up and terminates normally. Throughout Section 9, the timestamp triggers for each EM are clearly defined. When a timestamp requirement exists for an Event Message, there is an assumption that the event message will be generated as well, however when the message is actually transmitted depends on whether the NE is operating in immediate or batch mode (see Section 7.1).
- A table showing mandatory and optional attributes in the EM.

Note that, even though only mandatory EM trigger requirements for normal completed calls are specified, the NEs are expected to implement reasonable triggers for all call and exception scenarios. Additionally, NEs are expected to implement reasonable triggers if they have not implemented all IPCablecom interfaces (for example, if CMS-to-CMS signaling is not used for CMS to MGC communication).

The following tables show the association between IPCablecom 1.5 services, supported by the aforementioned call configurations, and proposed Event Messages that may be generated for each service. Voice communications services that IPCablecom 1.5 provides are based on three main call configurations:

- On-Net to On-Net
- On-Net to Off-Net
- Off-Net to On-Net

Table 14 provides a list of IPCablecom Event Messages defined in this document. More than one set of Event Messages MAY be generated during a particular service instance.

Table 14. IPCablecom Event Message Summary

Event Message ID	IPCablecom Event Message	Description
0	Reserved	
1	Signaling_Start	Start of signaling for originating or terminating part of the call
2	Signaling_Stop	Stop of signaling for originating or terminating part of the call
3	Database_Query	An inquiry into an external database; for example a toll-free number database
4	Intelligent_Peripheral_Usage_Start	Deferred
5	Intelligent_Peripheral_Usage_Stop	Deferred
6	Service_Instance	Indicates an occurrence of a service
7	QoS_Reserve	Reservation of QoS for originating or terminating part of the call
8	QoS_Release	Release of QoS for originating or terminating part of the call.
9	Service_Activation	Indicates a subscriber has activated a service.
10	Service_Deactivation	Indicates a subscriber has deactivated a service.
11	Media_Report	Indicates a change in media session information.

Event Message ID	IPCablecom Event Message	Description
12	Signal_Instance	Indicates an NCS signal instance.
13	Interconnect_(Signaling)_Start	Start of network interconnect signaling (between IPCablecom and PSTN) for originating or terminating part of the call.
14	Interconnect_(Signaling)_Stop	Stop of network interconnect signaling (between IPCablecom and PSTN) for originating or terminating part of the call.
15	Call_Answer	Indicates that all network resources for have been allocated for originating or terminating part of the call.
16	Call_Disconnect	Indicates that all network resources for have been released for originating or terminating part of the call.
17	Time_Change	Indicates time change on a network element.
19	QoS_Commit	Commitment of QoS for originating or terminating part of the call.
20	Media_Alive	Indicates if the call is still active.
21	Conference_Party_Change	A party is added, placed on hold, or retrieved from hold in a call involving multiple parties.
22	Media_Statistics	Media stream statistics reported by the gateway.
23	Surveillance_Stop	Indicates end of call content and/or call data. Generally, this will mean the end of a call. However, this can also indicate that call content and/or call data can no longer be intercepted (e.g., a call has been forwarded to another service provider's network and cannot be intercepted).
24	Redirection	Indicates that a call involving the surveillance subject has been redirected by either the surveillance subject or an associte in those scenarios where a Service_Instance is not sent.
31-39	Reserved	Reserved for IPCablecom Multimedia.

The Signaling_Start, Signaling_Stop, Call_Answer, and Call_Disconnect messages are important for accounting purposes and tracking the signaling overhead for media session establishment. The following are some assumptions on how these messages will be used:

- Signaling_Start and Signaling_Stop messages bracket the timeframe during which the CMS or MGC is processing dialed digits, performing signaling, and maintaining state for a call. Thus, the timestamp on a Signaling_Start is timestamped as early in the flow as possible on both the originating and terminating side after the message containing routable digits from the originator. A routable set of digits can be defined as a set of digits that are collected by the MTA matching the digit map, and will trigger call routing processing (e.g., *69 would not be considered routable digits, but 00 would). The timestamp on the Signaling_Stop is timestamped when signaling for the call is completed, generally when a DLCX is sent to an endpoint.
- A Signaling_Stop is generated if and only if a Signaling_Start was generated. Under normal circumstances, an RKS can expect a Signaling_Start and Signaling_Stop message for each set of event messages it receives for a specific BCID.
- Call_Answer and Call_Disconnect messages bracket the time-frame during which 2-way media path is active. The timestamps on these messages are used to calculate call time and duration for any calls that have usage billing. The timestamp on the Call_Answer will closely match the time at which the terminating party goes off-hook, and the timestamp on the Call_Disconnect will closely match the time at which the media path is torn down.

- A Call_Disconnect is generated if and only if a Call_Answer was generated. Existence of these two EMs in a set of EMs for a BCID indicates that all the conditions for a 2-way media path were met.
- The Called_Party_Number in Signaling_Start is the E.164 number of the terminating party. This number is intended to capture the destination of the call as specified by the originator. It often indicates the dialed-digits from the originator (e.g., for the 3 digit calls like 911, 411, this attribute captures this 3 digit number). However, there are several cases in which this field does not reflect the actual input of the user (e.g., in case of features like speed dial, it is populated with the digits configured for the speed dial digits). A few examples:
    1. Subscriber is in area code 972 and has 7 digit dial plan. When the subscriber dials 234-1234, the Called_Party_Number in Signaling_Start is populated with the 10 digit number including the area code, 9722341234.
    2. Subscriber has speed dial feature and configured 11 to 972-234-1234. When the subscriber dials 11#, the Called_Party_Number in Signaling_Start is populated with the 10 digit number configured for the speed dial 11, 9722341234.
    3. When a subscriber dials 911 for emergency call, the Called_Party_Number in Signaling_Start is populated with 3 digit 911.
    4. When the subscriber dials 1-919-234-1234, the Called_Party_Number in Signaling_Start is populated with the 10 digit number without the prefix, 9192341234.
    5. When the subscriber dials a dial around code, 1010288, and then dials 919-234-1234, the Called_Party_Number in Signaling_Start is populated with the 10 digit number without the dial around code, 9192341234.
    6. When the subscriber dials 1-800-228-8288, the Called_Party_Number in Signaling_Start is populated with 8002888288, and the Routing_Number is populated with the translated number after the database dip.

Table 15. Services Supported by On-Net to On-Net call Configuration

Service	Event Message ID																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19	20	21	22
Basic	X	X	X	X	X		X	X			X	X			X	X		X	X		X
Call Block	X	X		X	X	X	X	X	X	X	X	X			X	X		X			X
Call Waiting	X	X		X	X	X	X	X	X	X	X	X			X	X		X			X
Call Forwarding	X	X		X	X	X	X	X	X	X	X	X			X	X		X			X
Return Call	X	X		X	X	X	X	X			X	X			X	X		X			X
Repeat Call	X	X		X	X	X	X	X			X	X			X	X		X			X
Voice Mail	X	X		X	X		X	X			X	X			X	X		X			X
Three-Way Call	X	X		X	X	X	X	X				X			X	X		X		X	X
Customer Originated Trace	X	X		X	X		X	X	X			X			X	X		X			X

Table 16. Services Supported by On-Net to Off-Net call Configuration

Service	Event Message ID																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19	20	21	22
Basic	X	X	X	X	X		X	X			X	X	X	X	X	X		X	X		X
Call Block	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X			X
Call Waiting	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X			X
Return Call	X	X		X	X	X	X	X			X	X	X	X	X	X		X			X
Repeat Call	X	X		X	X	X	X	X			X	X	X	X	X	X		X			X
911	X	X	X	X	X		X	X			X	X	X	X	X	X		X			X

Service	Event Message ID																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19	20	21	22
N11	X	X	X	X	X		X	X			X	X	X	X	X	X		X			X
Toll-Free	X	X	X	X	X		X	X			X	X	X	X	X	X		X			X
Operator	X	X		X	X		X	X			X	X	X	X	X	X		X			X
Three-Way Call	X	X		X	X	X	X	X				X	X	X	X	X		X		X	X

Table 17. Services Supported by Off-Net to On-Net call Configuration

Service	Event Message ID																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	19	20	21	22
Basic	X	X	X	X	X		X	X			X	X	X	X	X	X		X	X		X
Call Block	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X			X
Call Waiting	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X			X
Repeat Call	X	X		X	X	X	X	X			X	X	X	X	X	X		X			X
Call Forwarding	X	X		X	X	X	X	X	X	X	X	X			X	X		X			X
Voice Mail	X	X		X	X		X	X			X	X	X	X	X	X		X			X
Three-Way Call	X	X		X	X	X	X	X				X	X	X	X	X		X		X	X
Customer Originated Trace	X	X		X	X		X	X	X			X	X	X	X	X		X			X

9.1 Event Message Structure

An event message contains a header followed by attributes. The header is required on every event message. The attributes vary based on the type of service the Event Message is describing. Refer to Table 38 for a description of the Event Message Header (EM_Header Attribute Structure).

9.2 Service_Instance

This event captures the fact that a service event has happened. The Event_Time attribute in the EM_Header Structure (see Table 38) MUST contain the time at which the service occurred.

This event message indicates the time at which the CMS provides an instance of a call control/feature service. For example, the time at which a call is put on hold, the time at which a call is forwarded, the time at which a last call return service is provided, the time at which a call-waiting service is provided, etc.

The CMS MUST timestamp these messages immediately upon operation of the service instance being reported.

The following generic call scenarios and BCIDs are used to specify the call leg for which the CMS sends the Service_Instance Event Message for Call Forwarding, Call Waiting and Three-Way Call Services:

1. For Call Forwarding, Subscriber A (BCID-A) calls Subscriber B (BCID-B1), Subscriber B (BCID-B2) forwards to Subscriber C (BCID-C). In this case, the CMS managing Subscriber B MUST generate a Service_Instance Event Message with the BCID (BCID-B2) in the EM_Header attribute and the Related_Call_Billing_Correlation_ID attribute MUST be BCID(BCID-B1).
2. For Call Waiting, Subscriber A (BCID-A) calls Subscriber B (BCID-B1) and after the call is established, Subscriber C (BCID-C) calls Subscriber B (BCID-B2), who uses call waiting to talk to Subscriber C. In this case, the CMS managing Subscriber B MUST generate the Service_Instance Event Message with the BCID (BCID-B2) in the EM_Header attribute and the Related_Call_Billing_Correlation_ID attribute MUST be BCID (BCID-B1).

3. For Three-Way Call, Subscriber A (BCID-A1) calls Subscriber B (BCID-B1) and after call is established, either A or B can make Three-Way Call to Subscriber C. When A (BCID-A2) makes Three-Way Call to Subscriber C (BCID-C), the CMS managing Subscriber A MUST generate the Service_Instance Event Message with BCID (BCID-A2) in the EM_Header attribute and the Related_Call_Billing_Correlation_ID attribute MUST be BCID (BCID-A1). When Subscriber B (BCID-B2) makes a Three-Way Call to Subscriber C (BCID-C), the CMS managing Subscriber B MUST generate the Service_Instance Event Message with BCID(BCID-B2) in the EM_Header attribute and the Related_Call_Billing_Correlation_ID attribute MUST be BCID (BCID-B1).

The following services are part of the IPCablecom EM 1.5 supported service capabilities (see Section 6.2.1):

- Three_Way_Call
- Acct_Auth_Code (Account and Authorization Code Service).

When a Service_Instance Event Message is generated with a Service_Name of Acct_Auth_Code, at least one of the attributes Account_Code or Authorization_Code MUST be present, and both MAY be present.

Table 18. Service_Instance Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Service_Name	R	The Service_Name attribute MUST be present. Class Service Name: Call_Block Call_Forward Call_Waiting Repeat_Call Return_Call Three_Way_Call Acct_Auth_Code
Call_Termination_Cause	O	The Call_Termination_Cause attribute MUST be present if the Service_Name is Call_Block or Acct_Auth_Code. If the Service_Name is Acct_Auth_Code, the Source_Document field of the Call_Termination_Cause attribute MUST indicate that the source document is GR-1100-CORE - Table 235 and the Cause_Code field MUST include the Call Completion Code as defined in GR-1100-CORE - Table 235.
Related_Call_Billing_Correlation_ID	O	The Related_Call_Billing_Correlation_ID attribute MUST be present if Service_Name is Call_Forward, Call_Waiting or Three_Way_Call.
Charge_Number	O	The Charge_Number attribute MUST be present if Service_Name is Call_Forward, Call_Waiting, Repeat_Call Return_Call or Three_Way_Call.
First_Call_Calling_Party_Number	O	The First_Call_Calling_Party_Number attribute MUST be present if Service_Name is Call_Waiting.
Second_Call_Calling_Party_Number	O	The Second_Call_Calling_Party_Number attribute MUST be present if Service_Name is Call_Waiting.
Called_Party_Number	O	The Called_Party_Number attribute MUST be present if Service_Name is Call_Waiting.
Routing_Number	O	The Routing_Number attribute MUST be present if Service_Name is Repeat_Call or Return_Call
Calling_Party_Number	O	The Calling_Party_Number attribute MUST be present if Service_Name is Repeat_Call or Return_Call.
Account_Code	O	The Account_Code attribute MAY be present if Service_Name is Acct_Auth_Code.

Attribute Name	Required or Optional	Comment
Authorization_Code	O	The Authorization_Code attribute MAY be present if Service_Name is Acct_Auth_Code.

9.3 Service_Activation

This event captures a subscriber activating a service. The Event_Time attribute in the EM_Header Structure (see Table 38) MUST contain the time when the service was activated.

This Event Message indicates the time at which the CMS records an attempt to activate a service. For example, the time at which call-forwarding is activated by the MTA user, the time at which the call-waiting service is activated by the MTA user, etc. These service activations are typically requested via a *XX dial-string.

The CMS MUST timestamp this message immediately upon successful activation of the requested service.[1]

The CMS MUST create a new BCID for this Event Message even if a service is activated during an existing call.

Table 19. Service_Activation Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Service_Name	R	The Service_Name attribute MUST be present. Class Service Name: Call_Block Call_Forward Call_Waiting Customer_Originated_Trace
Calling_Party_Number	R	The Calling_Party_Number attribute MUST be present if the Service_Name is Call_Forward. The Calling_Party_Number attribute MUST be present if the Service_Name is Call_Waiting, Call_Block or Customer_Originated_Trace and if the calling party number is known. Otherwise, this attribute may be omitted
Charge_Number	R	The Charge_Number attribute MUST be present.
Forwarded_Number	O	The Forwarded_Number attribute MUST be present if Service_Name is Call_Forward.

9.4 Signaling_Start

This Event Message indicates the time at which signaling starts. It is intended to capture the point at which the NE starts processing a call once a routable set of digits have been obtained from the originator.

The CMS or MGC MUST timestamp this message prior to digit translation. Note that the attributes contained in this Event Message contain information that is obtained after digit translation. In the event that a database dip is required, then the Signaling_Start message MUST be generated after the response from the database dip.

Originating CMS

In all scenarios, the originating CMS MUST timestamp this message immediately upon receipt of an NCS-signaling NTFY message with a routable set of digits that indicate a call attempt.

[1] Failed activation attempts are not reported at this time.

Terminating CMS

In the single-zone scenario, the terminating CMS MUST timestamp this Event Message based on a vendor-proprietary trigger.

In the intra-domain and inter-domain scenarios, the terminating CMS MUST timestamp this Event Message immediately upon receipt of an INVITE message with a routable set of dialed digits.

Originating MGC (off-on)

The originating MGC MUST timestamp this message immediately upon receipt of an SS7 IAM message or a TGCP NTFY with digits (operator services).

Terminating MGC (on-off)

The terminating MGC MUST timestamp this message immediately upon receipt of an INVITE message with a routable set of dialed digits. If the MGC is integrated with the CMS, the terminating MGC MUST timestamp this message based on vendor proprietary trigger. The proprietary trigger MAY be based on when the IAM is transmitted. The Trunk_Group_Number in the Trunk_Group_ID attribute in this message is the trunk group number used to formulate the first IAM transmitted to the Signaling Gateway that communicates with PSTN SS7 network for this call. It is referenced to the first IAM because potentially due to reattempt handling another IAM may be attempted to complete the same call.

Table 20. Signaling_Start Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Direction_Indicator	R	The Direction_Indicator attribute MUST be present.
MTA_Endpoint_Name	O	If the originating CMS generates this message, MTA_Endpoint_Name attribute MUST contain the endpoint name of the originating MTA. If the terminating CMS generates this message, MTA_Endpoint_Name attribute MUST contain the endpoint name of the terminating MTA. If the originating MGC generates this message, MTA_Endpoint_Name attribute MAY contain the endpoint ID of the originating MG. If the terminating MGC generates this message, the MTA_Endpoint_Name attribute MAY contain the endpoint ID of the terminating MG.
Calling_Party_Number	O	The Calling_Party_Number attribute MUST be included in the Signaling_Start Event Message whenever it is available in SS7 or CMSS signaling. For example, in the off-net to on-net scenario, this attribute may not be present when the Originating MGC and Terminating CMS do not have the Calling Party Number attribute available from SS7 signaling.
Called_Party_Number	R	The Called_Party_Number attribute MUST be present, it holds the formatted digits (E.164 [9] format) dialed by the subscriber. Refer to Section 9 for examples of how to populate this field.
Routing_Number	R	The Routing_Number attribute MUST be present, it indicates a routable number.
Location_Routing_Number	O	The Location_Routing_Number attribute MUST be included if a LNP lookup returns a LRN.
Carrier_Identification_Code	O	The Carrier_Identification_Code attribute MUST be included in MGC generated messages in which the call is being routed to an inter-exchange carrier and the information is available.
Trunk_Group_ID	O	The Trunk_Group_ID attribute MUST be included when the MGC generates this message.
Intl_Code	O	The Intl_Code attribute MUST be included for call origination of an internationally routed call.

Attribute Name	Required or Optional	Comment
Dial_Around_Code	O	The Dial_Around_Code attribute MUST be included for call origination where the inter-exchange carrier was specified by keying in a dial-around code (e.g., 1010288).
Jurisdiction_Information_Parameter	O	If the originating MGC generates this messages, the Jurisdiction_Information_Parameter (JIP) MUST be included when JIP was received in SS7 message (reference: GR-317-CORE) or if the incoming trunk group is provisioned with LRN of remote end. If the originating CMS generates this messages, the Jurisdiction_Information_Parameter MUST be included when the calling party number is ported-in number. In this case, JIP is per CMS provisioning. Note that this may be present even if the calling party is not ported in number. If the terminating CMS generates this messages, the Jurisdiction_Information_Parameter MUST be included when JIP is received in CMSS interface.
Called_Party_NP_source	O	Number Portability source. The Called_Party_NP_Source indicates how CMS or MGC obtained LRN of called party.
Calling_Party_NP_source	O	Number Portability source. The Calling_Party_NP_Source indicates how CMS or MGC obtained local number portability information for calling party.
Ported_In_Calling_Number	O	If the originating CMS generates this messages, the Ported_In_Calling_Number attribute MUST be included when the calling party number is ported-in number.
Ported_In_Called_Number	O	If the terminating CMS generates this messages, the Ported_In_Called_Number attribute MUST be included when the called party number is ported-in number.
Billing_Type	O	The Billing_Type attribute MUST be included for call origination where the originating endpoint is a measured rate subscriber.
Related_ICID	O	If the CMS or MGC generates this message as a result of receiving a SIP INVITE, the Related_ICID attribute MUST contain the ICID as received in the P-Charging-Vector SIP Header. Otherwise, the CMS or MGC MUST populate the Related_ICID attribute based on the ICID created by the CMS or MGC and placed in the P-Charging-Vector SIP header of an outbound INVITE message. If the ICID is not provided or received, this attribute may be omitted.

9.5 Signaling_Stop

This Event Message indicates the time at which signaling terminates. It is intended to capture the point at which the NE processes the final signaling message for the call. A Signaling_Stop message MUST NOT be generated unless a Signaling_Start message with the same BCID has been generated for the call. A Signaling_Stop message MUST be generated if a Signaling_Start message with the same BCID has been generated for the call (in exception cases, this may be the result of a proprietary time-out or clean-up process).

Originating CMS

In the single-zone scenario, the originating CMS MUST timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.

In the intra-domain or inter-domain scenarios, the originating CMS MUST timestamp this message upon transmission of the last signaling event in the following list:

- Transmission of the NCS-signaling DLCX message, or
- Transmission of the CMSS-signaling BYE message or CANCEL message.

Terminating CMS

In the single-zone scenario, the terminating CMS MUST timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.

In the intra-domain or inter-domain scenarios, the terminating CMS MUST timestamp this message upon transmission of the last signaling event in the following list:

- Transmission of the NCS-signaling DLCX message, or
- Transmission of the CMSS-signaling BYE message or the transmission of the CMSS-signaling acknowledgment response message to a CANCEL request.

Originating MGC (off-net to on-net)

The originating MGC MUST timestamp this EM message immediately upon the last signaling event in the following list:

- transmission/receipt of an RLC to/from the Signaling Gateway that communicates with the SS7 network,
- transmission of the MGC-issued TGCP DLCX message,
- receipt of an MG-issued TGCP DLCX, or
- transmission of the CMSS-signaling BYE message or CANCEL message.

Terminating MGC (on-net to off-net)

The terminating MGC MUST timestamp this EM message immediately upon transmission of the TGCP-signaling DLCX message.

Table 21. Signaling_Stop Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Related_Call_Billing_Correlation_ID	O	If the originating CMS or MGC generates this message, the Related_Call_Billing_Correlation_ID attribute MUST contain the BCID of the terminating CMS or MGC when terminating CMS or MGC is known. If the terminating CMS or MGC is not known, this attribute may be omitted. If the terminating CMS or MGC generates this message, the Related_Call_Billing_Correlation_ID attribute MUST contain the BCID of the originating CMS or MGC if known. If the BCID of the originating CMS or MGC is not known this attribute may be omitted.
FEID	O	If the originating CMS or MGC generates this message, the FEID attribute MUST contain the FEID of the terminating CMS or MGC when terminating CMS or MGC is known. If the terminating CMS or MGC is not known, this attribute may be omitted. If the terminating CMS or MGC generates this message, the FEID attribute MUST contain the FEID of the originating CMS or MGC.
Call_Termination_Cause	R	The Call_Termination_Cause code MUST be present.

9.6 Service_Deactivation

This Event Message indicates the time at which the CMS records an attempt to deactivate a service. For example, the time at which call-forwarding is deactivated by the MTA user, the time at which the call-waiting service is deactivated by the MTA user, etc. These service deactivations are typically requested via a *XX dial-string.

The CMS MUST timestamp this message immediately upon successful deactivation of the requested service. Failed Deactivation attempts are not reported at this time.

The CMS MUST create a new BCID for this Event Message even if a service is deactivated during an existing call.

Table 22. Service_Deactivation Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Service_Name	R	The Service_Name attribute MUST be present. Class Service Name: Call_Block Call_Forward Call_Waiting
Calling_Party_Number	R	The Calling_Party_Number attribute MUST be present.
Charge_Number	R	The Charge_Number attribute MUST be present.

Note that in the case of the Call_Waiting Service, the service deactivation or cancellation only applies to the duration of one call. If the subscriber has Call_Waiting Service, by default, any call placed or received after the Call_Waiting Service deactivation will have call waiting enabled. As a consequence, no Service_Activation Event Message is generated to activate this service again.

9.7 Database_Query

This Event Message indicates the time at which a one-time request/response transaction or database dip is completed by an intelligent peripheral (800 number database, LNP database, etc.).

The CMS originating the call MUST timestamp this message immediately upon a receipt of the response from the Intelligent Peripheral.

Table 23. Database_Query Event Message

Attribute Name	Required or Optional	Comment
EM_Header, see (Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Database_ID	R	None
Query_Type	R	Toll Free Number Lookup, LNP lookup, etc.
Called_Party_Number	R	None

Attribute Name	Required or Optional	Comment
Returned_Number	R	Note 1: In the PSTN, only a single number is returned per a query for Toll-free/LNP/Calling Name service ([21],[22],[23]). There may be multiple numbers returned such as the 800 translation results in a ported number in an optimized response available in AIN 0.2 ([18], [20]). This is optional for use in TCAP query of these services. If multiple numbers are returned, this attribute SHOULD reflect the result associated with the original query as indicated in the attribute Query_Type in this message. Any additional database dip result SHOULD be included in the corresponding specific attribute. In the case of LNP as a bundled response to the toll free query, the Location_Routing_Number SHOULD be included to convey the additional returned number result from a single database query to the SCP. As an alternative, the Returned_Number MAY be included for each number returned, but SHOULD be included as a pair with Query_Type in an ordered sequence. The first pair denotes the returned number associated with the original query type. The next pair denotes the next returned number of the next bundled database dip of the same original query. This repeats until the last returned number is conveyed. Note 2: For a calling name database query, this field should contain the calling party number provided to the database for which the name is being requested.
Location_Routing_Number	O	See note above.
Query_Type	O	As a pair with Returned_Number for each of the subsequent database dip result within a single original database query. See note in the Returned_Number comment column above.
Returned_Number	O	As a pair with Query_Type for each of the subsequent database dip result within a single original database query. See note above.

9.8 Intelligent_Peripheral_Usage_Start

Deferred.

9.9 Intelligent_Peripheral_Usage_Stop

Deferred.

9.10 Interconnect_Start

This Event Message indicates the time at which the start of network interconnect occurs. Only the MGC is permitted to issue this event message.

The MGC MUST timestamp this message immediately upon transmission/receipt of an IAM to/from the Signaling Gateway that communicates with the SS7 network.

The terminating MGC MUST generate this message only after the ACM/ANM is received. This is so that if another IAM is attempted due to reattempt handling with a different trunk group number before the ACM/ANM is received, the Interconnection_Start reports the latest trunk group number along with the latest timestamp of the final IAM used to complete the call. (The Signaling_Start reports the first IAM attempted trunk group number of the same call.)

The originating MGC MAY generate this message when the ACM is transmitted although it is timestamp upon receipt of an IAM.

The MGC MUST timestamp this message immediately upon transmission/receipt of digits to/from the Media Gateway that communicates with the MF/DTMF network.

The originating MGC MUST generate this message only after call answer is transmitted. The Interconnection_Start reports the latest trunk group number along with the latest timestamp of answer used to complete the call. (The Signaling_Start reports the first attempted trunk group number of the same call.)

The terminating MGC MAY generate this message when call answer is received although it is timestamp upon sending the digits to the Media Gateway that communicates with the MF/DTMF network.

Table 24. Interconnect_Start Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Carrier_Identification_Code	O	CIC Code of connecting operator. This attribute MUST be present when the call is routed off-net to an inter-exchange carrier. For example, this attribute can be omitted for operator and emergency (911) trunks.
Trunk_Group_ID	R	TGID of the trunk over which the interconnection is occurring
Routing_Number	R	None

9.11 Interconnect_Stop

This Event Message indicates the termination of bandwidth between the IPCablecom network and the PSTN. Only the MGC is permitted to issue this Event Message.

The MGC MUST timestamp this message immediately upon transmission/receipt of an RLC to/from the Signaling Gateway that communicates with the SS7 network.

The MGC MUST timestamp this message immediately upon transmission/receipt of an Release Complete to/from the Media Gateway that communicates with the MF/DTMF network.

Table 25. Interconnect_Stop Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Carrier_Identification_Code	O	CIC Code of connecting operator. This attribute MUST be present when the call is routed off-net to an inter-exchange carrier. For example, this attribute can be omitted for operator and emergency (911) trunks.
Trunk_Group_ID	R	TGID of the trunk over which the interconnection is occurring

9.12 Call_Answer

This Event Message indicates that the media connection is open because answer has occurred. It is intended to capture the earliest point at which the NE can determine that the termination side has gone off-hook, resulting in a 2-way media path.

Originating CMS

In the single-zone scenario, the originating CMS MUST timestamp this Event Message based on its knowledge of media connection establishment. This trigger should correspond as closely as possible to the time at which the terminating side has determined that off-hook has occurred.

In the multi-zone scenario, the originating CMS MUST timestamp this Event Message message immediately upon receipt of the CMSS signaling 200 OK sent in response to the original INVITE message indicating call answer.

Terminating CMS

The terminating CMS MUST timestamp this message immediately upon receipt of the NCS-signaling NTFY message indicating off-hook at the terminating MTA.

Originating MGC (off-on)

The originating MGC MUST timestamp this message immediately upon:

- transmission of an SS7 ANM message to the PSTN via the SG, or
- commanding the MG to generate answer indication on the operator services trunk.

Terminating MGC (on-off)

The terminating MGC MUST timestamp this message immediately upon

- receipt of an SS7 ANM message from the PSTN via the SG or
- an answer indication from the MG indicating answer has occurred on an operator services trunk.

Table 26. Call_Answer Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Charge_Number	R	The Charge_Number attribute MUST contain the charge number in the appropriate cases such as collect call, calling-card call, call billed to a 3rd party, or others.
Related_Call_Billing_Correlation_ID	O	If the originating CMS or MGC generates this message, the Related_Call_Billing_Correlation_ID attribute MUST contain the BCID of the terminating CMS or MGC when terminating CMS or MGC is known. If the terminating CMS or MGC is not known, this attribute may be omitted. If the terminating CMS or MGC generates this message, the Related_Call_Billing_Correlation_ID attribute MUST contain the BCID of the originating CMS or MGC if known. If the BCID of the originating CMS or MGC is not known this attribute may be omitted.
FEID	O	If the originating CMS or MGC generates this message, the FEID attribute MUST contain the FEID of the terminating CMS or MGC when terminating CMS or MGC is known. If the terminating CMS or MGC is not known, this attribute may be omitted. If the terminating CMS or MGC generates this message, the FEID attribute MUST contain the FEID of the originating CMS or MGC.

9.13 Call_Disconnect

This Event Message indicates the time at which the media connection is closed because the calling party has terminated the call by going on-hook, or that the destination party has gone on-hook and the called-party's call-continuation timer[2] has expired. The call termination cause attribute must be included as an attribute in a Call_Disconnect message; its structure is defined in Table 41 and its Cause_Code sub-field is normatively defined in [6], Table 411.

Call_Disconnect should be timestamped by the NE as closely as possible to the time that the media connection is torn down. A Call_Disconnect message MUST NOT be generated unless a Call_Answer message with the same BCID has been generated for the call. A Call_Disconnect message MUST be generated if a Call_Answer message

[2] In the current telephony network, when the called party goes on-hook, a 10-11 second timer is started. If the calling party remains off-hook, and the called party goes off-hook again within that time period, the call continues.

with the same BCID has been generated for the call (in exception cases, this may be the result of a proprietary time-out or clean-up process).

Originating CMS

The originating CMS MUST timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message (for calls that have reached the state where the terminating party has gone off-hook and the Call_Answer message was sent).

Terminating CMS

The terminating CMS MUST timestamp this message immediately upon transmission of the DLCX or upon expiration of the terminating MTA's call-continuation timer.

Originating MGC (off-net to on-net)

The originating MGC MUST timestamp this EM message upon receipt of an SS7 REL message from the PSTN via the SG, or upon sending a CMSS-signaling 200-OK message in response to a BYE message from the terminating CMS.

Terminating MGC (on-net to off-net)

The terminating MGC MUST timestamp this message upon receipt of an SS7 RLC message from the PSTN via the SG, an indication from the MG that an operator services trunk has disconnected, or upon sending a 200-OK message in response to a BYE message from the originating CMS.

Table 27. Call_Disconnect Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Call_Termination_Cause	R	Normal Termination

9.14 QoS_Reserve

This Event Message indicates the time at which the CMTS reserves bandwidth on the IPCablecom access network. The CMTS MUST also generate this event if the Reserved bandwidth changes or if the service flow is authorized by another gate (through the association of a different Gate than originally authorized the flow).

The originating and terminating CMTS MUST timestamp this message immediately upon:

Table 28. QoS Reserve Timestamp Generation

Client Initiated	CMTS Initiated
Client initiated DSA-REQ or DSC-REQ	CMTS initiated DSA-REQ or DSC-REQ
Reception of a DSA/DSC-ACK acknowledging a successful DSA/DSC-RSP (confirmation code == success).	Transmission of a DSA/DSC-ACK acknowledging a successful DSA/DSC-RSP (confirmation code == success)
If a DSA/DSC-ACK is not received, the CMTS MUST NOT generate this message.	If a DSA/DSC-ACK is not transmitted, the CMTS MUST NOT generate this message.

If the DSA/DSC-RSP confirmation code is not successful, the CMTS MUST NOT generate this message.

Table 29. QoS_Reserve Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.

Attribute Name	Required or Optional	Comment
QoS_Descriptor	O	None
MTA_UDP_Portnum	R	None
SF ID	R	None
Flow_Direction	R	None

9.15 QoS_Release

This Event Message indicates the time at which the CMTS released its bandwidth commitment on the IPCablecom access network.

The originating and terminating CMTS MUST timestamp this message immediately upon:

- transmission of a DSC-RSP that indicates that authorization and admission control for a DSC-REQ against an existing service flow have succeeded against a separate Gate, indicating that the previous Gate will be deleted, or
- transmission of a DSD-RSP that indicates the request to delete bandwidth contained in the DSD-REQ from the MTA was successful.
- transmission of a DSC-RSP that indicates the request to delete bandwidth contained in the DSC-REQ from the MTA was successful. This occurs when the MTA is utilizing multiple grants per interval to place multiple sessions on a single service flow and uses a DSC-REQ to delete bandwidth for one of the sessions.

Table 30. QoS_Release Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
SF_ID	R	None
Flow Direction	R	None

9.16 Time_Change

This event captures an instance of a time change. Whenever the (IPCablecom) clock on the network element (CMS,MGC or CMTS) is changed by more than 200 milliseconds, the network element MUST generate a Time Change message. This includes time shift events (Daylight savings time), step adjustments to synchronize with the NTP reference clock and manual time setting changes, The Event_Time attribute in the EM_Header Structure (Table 38) MUST reflect the new (adjusted) notion of time. Note that Time_Change message is not required for slew adjustments performed by NTP.

The network element (CMS, MGC and CMTS) MUST send the Time Change event message to the active (current primary) RKS. The Time Change event message MUST be generated when one or more calls are active or in the process of being set up. For the CMS and MGC active or in process is after a Signaling Start event has been generated. For the CMTS active or in process is indicated by the presence of a DQoS gate. The Time Change event message need not be generated when calls are not active or in the process of being set up. Only one Time Change event message is sent to each primary RKS (if there is more than one primary RKS) regardless of how many calls may be active.

The BCID in the EM_Header of the Time Change event message MUST be generated locally by the network element at the time of the event. The BCID is not associated with any call related BCID, it is a unique BCID for this event.

Table 31. Time_Change Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Time_Adjustment	R	None

9.17 QoS_Commit

This Event Message indicates the time at which the CMTS commits bandwidth on the IPCablecom access network. The CMTS MUST also generate this event if the Committed bandwidth changes or if the service flow is authorized by another gate (through the association of a different Gate than originally authorized the flow).

The originating and terminating CMTS MUST timestamp this message immediately upon:

Table 32. QoS Commit Timestamp Generation

Client Initiated	CMTS Initiated
Client initiated DSC-REQ or a DSA-REQ (when the CMTS reserves and commits the bandwidth in one-step).	CMTS initiated DSC-REQ or a DSA-REQ (when the CMTS reserves and commits the bandwidth in one-step).
reception of a DSA/DSC-ACK acknowledging a successful DSA-RSP/DSC-RSP (confirmation code == success).	transmission of a DSA/DSC-ACK acknowledging a successful DSA/DSC-RSP (confirmation code == success).
If a DSA/DSC-ACK is not received, the CMTS MUST NOT generate this message.	If a DSC-ACK is not transmitted, the CMTS MUST NOT generate this message.

If the DSA/DSC-RSP confirmation code is not successful, the CMTS MUST NOT generate this message.

Table 33. QoS_Commit Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
QoS_Descriptor	O	None
MTA_UDP_Portnum	R	None
SF_ID	R	None
Flow_Direction	R	None

9.18 RTP_Connection_Parameters Event Message

Deferred.

9.19 Media_Alive

If the IPCablecom architecture is expected to support this Media_Alive Event Message, then it is recommended that all CMS, CMTS, and MGC be pre-configured with the same Media_Alive generation time.

This Event Message indicates that service is active due to the continued existence of a bearer connection. This Event Message MAY be generated by any trusted IPCablecom network element (CMS, CMTS, MGC) as defined below.

If a NE is configured to generate the optional Media_Alive event message, it must check for the status of all calls at the configured Media_Alive generation time. At the configured Media_Alive generation time, (e.g., 00:00 means

midnight, 23:59 means 11:59 PM) the NE checks if any of the active calls are equal to or older than 1440 minutes. (24 hours). Only if a call is equal to or older than 1440 minutes, a Media_Alive event message for that call MUST be generated.

The call starting time for different NE types are specified by:

- CMTS: the first QoS_Commit event message EM_Header attribute Event_time for a gate.
- CMS: the Call_Answer event message EM_Header attribute Event_time. The EM_Header attribute Event_time is timestamped as per Section 9.12 Call_Answer.
- MGC: the Call_Answer event message EM_Header attribute Event_time. The EM_Header attribute Event_time is timestamped as per Section 9.12 Call_Answer.

NEs MUST (when configured to generate the Media_Alive EMs) generate the Media_Alive EMs at the Media_Alive EM generation time. Even though the Media_Alive EM generation time is configurable, the default value for the Media_Alive EM generation time MUST be midnight. Thus a service provider can have a synchronized network simply by accepting the default value from all NEs. If a service provider wants different time for Media_Alive EM generation time, it is up to the service provider to configure the different Media_Alive EM generation time.

Figure 7 illustrates how a long duration call is identified.

Assumption: the Media_Alive EM generation on the NE has been configured to midnight (00:00) (the default value).

Call A is not a long duration call because its duration is less than 24 hours (or 1440 minutes) long.

Call B is not a long duration call because its duration is longer than 24 hours but it is less than 1440 minutes long at the Media_Alive EM generation time (midnight).

Call C is a long duration call because at the second midnight after the call was established, its duration is longer than 1440 minutes. (actually 2340 minutes long). Only one Media_Alive is generated because it is terminated prior to the next Media_Alive EM generation time (midnight).

Call D is also a long duration call because it meets the same criterion as Call C. Because it stays up across the midnight boundary after becoming a long duration call, two Media_Alive EMs are generated.

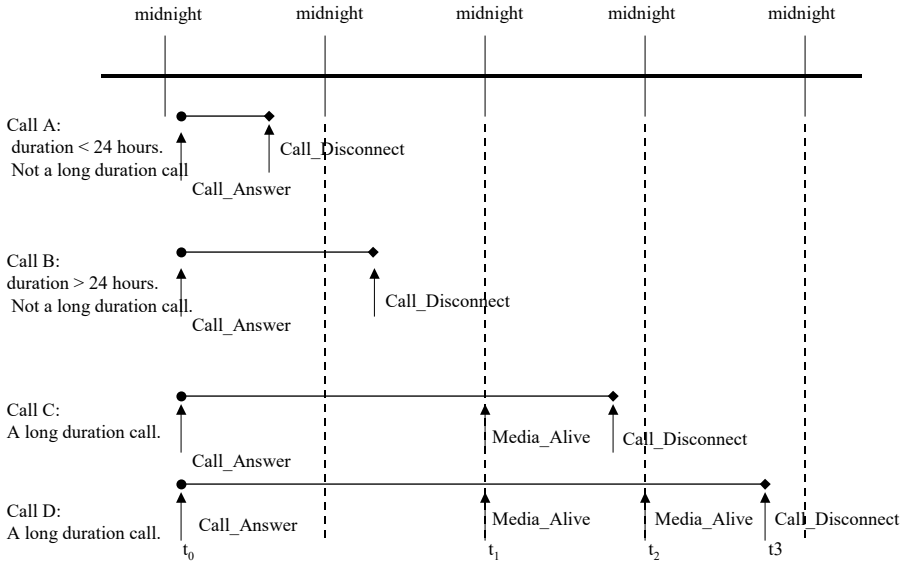

Figure 7. Long Duration Call Identification

From the above diagram, Call D will be used to illustrate the contents of the long duration call records belonging to a same call id (BCID).

In the above scenario, there will be three records generated from Call D, let's identify these as record 1, 2, and 3:

The Call D starts on day 0 at 9:00:00 AM. (t0 July 27, 2001).

At first midnight crossing, the call is 900 minutes long (or 5400 seconds). So no record is generated.

At second midnight crossing (t1), the call is 2340 minutes long (or 140400 seconds). So a Media_Alive Event Message is generated with the following value:

- EM Header.Event_time = 20010729000000.000

At third midnight crossing (t2), the call is 3780 minutes long (or 226800 seconds). A Media_Alive event message with the following value is generated:

- EM Header.Event_time = 20010730000000.000

At 5:00pm, following the third midnight, the call is terminated. (t3). The overall duration of the call is 4800 minutes long (or 288000 seconds). A Call_Disconnect event message with the following value is generated for this call BCID.

- EM Header.Event_time = 20010730170000.000

Table 34. Media_Alive Event Message

Attribute Name	Required or Optional	Comment
EM_Header, see (Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.

9.20 Media_Statistics

This Event Message is generated when a gateway returns VoIP Metrics in NCS or TGCP messages.

CMSs and MGCs MAY generate and timestamp this message when an NCS or TGCP signaling message is received from the MTA/MG that contains VoIP Metrics data. If this optional Event Message is generated, it MUST contain all of the VoIP metrics data received as specified in Table 35. VoIP metrics data is defined as that contained within the Local and Remote XR_Blocks, RTCP data is not considered VoIP metrics data even though it is contained in this message. See [1] for more information on how this data is represented in NCS signaling, and to determine which NCS messages may carry this data. CMSs and MGCs MUST NOT generate this message when no VoIP Metrics data is received in the NCS or TGCP signaling messages.

Within the NCS or TGCP Signaling response from the MTA/MG, the RTCP_Data metrics are found in the P: parameter, the Local_XR_Block metrics are found in the XRM/LVM: parameter, and the Remote_XR_Block metrics are found in the XRM/RVM parameter. The CMS and MGC MUST remove the parameter name, and copy the metrics as they appear in NCS or TGCP into the appropriate Media_Statistics attribute.

Note that in a very common case, VoIP Metrics data is included in the response to a DLCX message. In this case, the timestamp is later than the Signaling_Stop message. Thus, it is not valid to assume that the Signaling_Stop message is necessarily the last message associated with a voice connection.

Table 35. Media_Statistics Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
RTCP_Data	O	The RTCP_Data attribute MUST be present if an NCS or TGCP message was received with any RTCP report data included.
Local_XR_Block	O	The _XR_Block MUST be present if an NCS or TGCP message was received with any local VoIP metrics data included.
Remote_XR_Block	O	The Remote_XR_Block MUST be present if an NCS or TGCP message was received with any remote VoIP metrics data included.

10 IPCABLECOM EVENT MESSAGE ATTRIBUTES

This section describes the IPCablecom attributes included in the IPCablecom Event Messages. Event Messages and attributes denoted by an asterisk "*" in Table 36 indicate that the message or attribute is specific to electronic surveillance Event Messages. Electronic surveillance specific Event Messages and/or attributes MUST NOT be sent to the RKS.

Table 36 shows a mapping of the IPCablecom Event Messages and their associated IPCablecom attributes. Table 37 contains a detailed description of the IPCablecom attributes.

Table 36. IPCablecom Attributes Mapped to IPCablecom Event Messages

EM Attribute ID	EM Attribute Name	Event Message ID																						
		1 – Signaling_Start	2 – Signaling_Stop	3 – Database_Query	4 – Deferred	5 – Deferred	6 – Service_Instance	7 – QoS_Reserve	8 – QoS_Release	9 – Service_Activation	10 – Service_Deactivation	11 - Media_Report*	12 - Signal_Instance*	13 – Interconnect_Start	14 – Interconnect_Stop	15 – Call_Answer	16 – Call_Disconnect	17 – Time_Change	19 – QoS_Commit	20 – Media_Alive	21-Conference_Party_Change*	22-Media_Statistics	23 Surveillance_Stop*	24 – Redirection *
0	Reserved																							
1	EM_Header	X	X	X			X	X	X	X	X	X*	X*	X	X	X	X	X	X	X	X*	X	X*	X*
2	Undefined																							
3	MTA_Endpoint_Name	X																						
4	Calling_Party_Number	X					X			X	X													
5	Called_Party_Number	X		X			X																	
6	Database_ID			X																				
7	Query_Type			X																				
8	Undefined																							
9	Returned_Number			X																				
10	Undefined																							
11	Call_Termination_Cause		X				X										X							
12	Undefined																							
13	Related_Call_Billing_Correlation_ID		X				X									X								X*
14	First_Call_Calling_Party_Number						X																	
15	Second_Call_Calling_Party_Number						X																	
16	Charge_Number						X			X	X					X								

EM Attribute ID	EM Attribute Name	Event Message ID																						
17	Forwarded_Number									X														
18	Service_Name						X			X	X													
19	Undefined																							
20	Intl_Code	X																						
21	Dial_Around_Code	X																						
22	Location_Routing_ Number	X		X																				
23	Carrier_Identification_ Code	X					X*							X	X									X*
24	Trunk_Group_ID	X												X	X									
25	Routing_Number	X					X							X										
26	MTA_UDP_Portnum							X											X					
27	Undefined																							
28	Undefined																							
29	Channel_State											X*												
30	SF_ID							X	X										X					
31	Error_Description																							
32	QoS_Descriptor							X											X					
33	Undefined																							
34	Undefined																							
35	Undefined																							
36	Undefined																							
37	Direction_indicator	X																						
38	Time_Adjustment																	X						
39	SDP_Upstream											X*												
40	SDP_Downstream											X*												
41	User_Input	X*																						
42	Translation_Input	X*																						
43	Redirected_From_Inf	X*																						
44	Electronic_Surveillance_ Indication	X*																				X*		
45	Redirected_From_Party_Number						X*																	X*
46	Redirected_To_Party_ Number						X*																	X*
47	Undefined																							
48	CCC_ID							X*	X*			X*							X*					
49	FEID		X													X								

EM Attribute ID	EM Attribute Name	Event Message ID																						
50	Flow_Direction							X	X			X*							X					
51	Signal_Type												X*											
52	Alerting_Signal												X*											
53	Subject_Audible_Signal												X*											
54	Terminal_Display_Info												X*											
55	Switch_Hook_Flash												X*											
56	Dialed_Digits												X*											
57	Misc_Signaling_Information												X*											
61-79	Reserved																							
80	Account_Code						X																	
81	Authorization_Code						X																	
82	Jurisdiction_Information_Parameter	X																						
83	Called_Party_NP_Source	X																						
84	Calling_Party_NP_Source	X																						
85	Ported_In_Calling_Number	X																						
86	Ported_In_Called_Number	X																						
87	Billing_Type	X																						
88	Signaled_To_Number												X*											
89	Signaled_From_Number												X*											
90	Communicating_Party																				X*			
91	Joined_party																				X*			
92	Removed_Party																				X*			
93	RTCP_Data																					X		
94	Local_XR_Block																					X		
95	Remote_XR_Block																					X		
96	Surveillance_Stop_Type*																						X*	
97	Surveillance_Stop_Destination*																						X*	
98	Related_ICID	X																						

Table 37 provides a detailed list of the IPCablecom Event Message attributes. A data value of an attribute may be represented by a simple data format (one data field) or by a more complex data format (Data Structure). Data Structure formats of the appropriate attributes are detailed in Table 38 through Table 44. It should be noted that Event Message 17 is not service dependent.

Table 37. IPCablecom Event Message Attributes

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
0	Reserved			
1	76 bytes	EM_Header	Data structure (See Table 38)	Common data required on every IPCablecom Event Message
2	Undefined			
3	variable length, maximum of 247 bytes (247 is maximum length of vendor specific attribute)	MTA_Endpoint_Name	ASCII character string	Physical Port name (aaln/#) as defined in the IPCablecom NCS Spec [1]
4	20 bytes	Calling_Party_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the Originating party. In the future other numbering plans will be addressed.
5	20 bytes	Called_Party_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.
6	Variable length, maximum of 247 bytes (247 is maximum length of vendor specific attribute)	Database_ID	Right justified, space padded ASCII character string	A unique identifier of the referenced database
7	2 bytes	Query_Type	Unsigned integer	Query type: 0=Reserved 1=Toll Free Number Lookup 2=LNPNumberLookup 3=Calling Name Delivery Lookup
8	Undefined			
9	20 bytes	Returned_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number resulting from a database query. In the future other numbering plans will be addressed.
10	Undefined			
11	6 bytes	Call_Termination_Cause	Data structure (See Table 41)	Termination code identifier
12	Undefined			

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
13	24 bytes	Related_Call_ Billing_ Correlation_ID	Data structure. (See Table 39)	BCID for possible use in value added services or to identify the matching originating/terminating half of the service.
14	20 bytes	First_Call_Calling_ Party_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the calling party. In the future other numbering plans will be addressed.
15	20 bytes	Second_Call_ Calling_Party_ Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9]formatted address specifying the number of the calling party. In the future other numbering plans will be addressed.
16	20 bytes	Charge_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the billable party. In the future other numbering plans will be addressed.
17	20 Bytes	Forwarded_ Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the Forwarded Number. In the future other numbering plans will be addressed.
18	32 Bytes	Service_Name	Right justified, space padded ASCII character string	Class Service Name. Allowed names are: Call_Block Call_Forward Call_Waiting Repeat_Call Return_Call Three_Way_Call Customer_Originated_Trace
19	Undefined			
20	4 Bytes	Intl_Code	Right justified, space padded ASCII character string	International Country Code
21	8 Bytes	Dial_Around_Code	Right justified, space padded ASCII character string	Dial-around code used for per-call selection of inter-exchange carrier
22	20 bytes	Location_Routing_ Number	Right justified, space padded ASCII character string	For LNP uses IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.
23	8 bytes	Carrier_ Identification_ Code	Right justified, space padded ASCII character string	If the MSO provides a service for a telecommunications operator, the Carrier Identification Code (CIC) or other identification is recorded in this field.
24	6 bytes	Trunk_Group_ID	Data structure (See Table 42)	Trunk group identification
25	20 bytes	Routing_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the terminating party. In the future other numbering plans will be addressed.

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
26	4 bytes	MTA_UDP_ Portnum	Unsigned Integer	MTA Endpoint UDP Port Number. Destination port field value in DQoS Gate-spec object received in DQoS Gate-Set message.
27	Undefined			
28	Undefined			
29	2 bytes	Channel_State	Unsigned Integer	Channel State: 0=Not Used/Reserved 1=Open 2=Change 3=Close
30	4 bytes	SF_ID	Unsigned integer	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RFMAC domain. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs are allocated from the same SFID number space.
31	32 bytes	Error_Description	Right justified, space padded ASCII character string.	A user-defined description of the error conditions. (See Table 40)
32	Variable; Min 8 bytes	QoS_Descriptor	Data structure See Table 43.	QoS parameters data (See Appendix C of [15])
37	2 bytes	Direction_ indicator	Unsigned integer	Specifies if a device acts on behalf of an originating or terminating part of the call at the time an Event Message is being generated. 0=undefined 1=Originating 2=Terminating
38	8 bytes	Time_Adjustment	signed integer	Time adjustment of an element's (CMS, CMTS, MGC) clock. This time is in milliseconds, detailing the amount of the time change.
39	variable	SDP_Upstream	ASCII character string	Description of upstream packet flow
40	variable	SDP_Downstream	ASCII character string	Description of downstream packet flow
41	variable	User_Input	ASCII character string	Sequence of dialed digits as entered by user
42	20 bytes	Translation_Input	Right justified, space padded ASCII character string	E.164 [9] address of the input to an external translation lookup
43	42 bytes	Redirected_From_I nfo	Data Structure	Information about previous redirections of this call
44	variable	Electronic_ Surveillance_ Indication	Data Structure	Additional destination of CCC and CDC for redirected call
45	20 bytes	Redirected_From_ Party_Number	Right justified, space padded ASCII character string	E.164 [9] address of the party initiating a redirection

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
46	20 bytes	Redirected_To_ Party_Number	Right justified, space padded ASCII character string	E.164 [9] address of the destination party of a redirection
47	Undefined			
48	4 bytes	CCC_ID	Unsigned integer	Call Content identifier assigned by CMS or MGC
49	Variable length, maximum of 247 bytes	FEID	ASCII character string.	Financial Entity ID. The first 8 bytes constitute MSO defined data. By default, the first 8 bytes are zero filled. From the 9th byte on the field contains the MSO's domain name which uniquely identifies the MSO for billing and settlement purposes. The MSO's domain name is limited to 239 bytes.
50	2 bytes	Flow Direction	Unsigned integer	Flow direction: 0=Reserved 1=Upstream 2=Downstream
51	2 bytes	Signal_Type	Unsigned Integer	Type of signal: 0 = Reserved 1 = Network_Signal 2 = Subject_Signal
52	4 bytes	Alerting_Signal	Unsigned Integer	Type of alerting signal[3]: 0 = Reserved 1 = Ringing (rg) 2 = Distinctive ringing 2 (r2) 3 = Distinctive ringing 3 (r3) 4 = Distinctive ringing 4 (r4) 5 = Ringsplash (rs) 6 = Call waiting tone 1 (wt1) 7 = Call waiting tone 2 (wt2) 8 = Call waiting tone 3 (wt3) 9 = Call waiting tone 4 (wt4) 10 = Reserved 11 = Distinctive ringing 0 (r0) 12 = Distinctive ringing 1 (r1) 13 = Distinctive ringing 5 (r5) 14 = Distinctive ringing 6 (r6) 15 = Distinctive ringing 7 (r7)

[3] The values are the standard values defined for a circuit-switched environment to report alerting signals for voice services to law enforcement. The "Reserved" values are for alerting signals that are not relevant to an IPCablecom environment, and have been reserved to achieve consistent reporting across different voice environments.

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
53	4 bytes	Subject_Audible_Signal	Unsigned Integer	Type of audible signal4: 0 = Reserved 1 = Dial tone (dl) 2 = Stutter dial tone (sl) 3 = Ring back tone (rt) 4 = Reorder tone (ro) 5 = Busy tone (bz) 6 = Confirmation tone (cf) 7 = Reserved 8 = Message waiting indicator (mwi) 9 = Off-hook warning tone (ot) 10 = Reserved 11 = Reserved 12 = Reserved 13 = Reserved 14 = Reserved 15 = Reserved 16 = Reserved 17 = Reserved 18 = Reserved 19 = Reserved 20 = Reserved 21 = Reserved
54	Variable length, maximum of 201 bytes	Terminal_Display_Info	Data Structure (see Table 69)	Provides information signaled for display on surveillance subject's terminal.
55	Variable length, maximum of 128 bytes	Switch_Hook_Flash	ASCII character string	Indicates signaling of a flash hook. Value is "FLASHHOOK" for Flash hook signal (hf).
56	Variable length, maximum of 128 bytes	Dialed_Digits	ASCII character String	Provides digits dialed. Value is digits received for DTMF digits signal (0-9,*,#,A,B,C,D).
57	Variable length, maximum of 128 bytes	Misc_Signaling_Information	ASCII character string	Provides miscellaneous signaling information. Attribute is populated as follows: - Value is digits sent for DTMF digits signal (0-9,*,#,A,B,C,D). - Value is "FAX TONE" for Fax tone signal (ft). - Value is "MODEM TONE" for Modem tone signal (mt). - Value is "TDD TONE" for TDD signal (TDD).
61-79				Reserved for IPCablecom Multimedia

[4] The values are the standard values defined for a circuit-switched environment to report audible signals for voice services to law enforcement. The "Reserved" values are for audible signals that are not relevant to an IPCablecom environment, and have been reserved to achieve consistent reporting across different voice environments.

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
80	24 bytes	Account_Code	Right justified, space padded ASCII character string	Account code used for this call.
81	24 bytes	Authorization_ Code	Right justified, space padded ASCII character string	Authorization code used for this call; it may be used to segment an account code.
82	6 bytes	Jurisdiction_Information_Parameter	Right justified, space padded ASCII character string	The originating network element's JIP as per GR-317-CORE.
83	2 bytes	Called_Party_NP_ Source	Unsigned integer	Provisioned data Signaling Information NPDB
84	2 bytes	Calling_Party_NP_ Source	Unsigned integer	Provisioned data Signaling Information NPDB
85	2 bytes	Ported_In_Calling_ Number	Unsigned integer	Value: 0= Not ported In 1= ported In
86	2 bytes	Ported_In_Called_ Number	Unsigned integer	Value: 0= Not ported In 1= ported In
87	2 bytes	Billing_Type	Unsigned integer	Indicates if the call is measured rate or flat rate. Value: 1 = Measured rate (aligned with BAF call type 1 that indicates a local message rate call or a measured call) 3 = Flat rate (aligned with BAF call type 3 that indicates local message rate that is not timed)
88	20 bytes	Signaled_To_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the Originating party. In the future other numbering plans will be addressed.
89	20 bytes	Signaled_From_Number	Right justified, space padded ASCII character string	IPCablecom 1.5 will use E.164 [9] formatted address specifying the number of the Originating party. In the future other numbering plans will be addressed.
90	26 bytes	Communicating_Party	Data Structure (see Table 47)	CCC_ID and Party ID of the communicating party in the conference.
91	26 bytes	Joined_Party	Data Structure (see Table 47)	CCC_ID and Party ID of the party that joined the conference.
92	26 bytes	Removed_Party	Data Structure (see Table 47	CCC_ID and Party ID of the party removed from the conference.
93	variable	RTCP_Data	ASCII character string	RTCP metrics available on a connection.
94	variable	Local_XR_Block	ASCII character string	Local RTCP-XR VoIP Metrics Block data available on a connection.
95	variable	Remote_XR_Block	ASCII character string	Remote RTCP-XR VoIP Metrics Block data available on a connection.

EM Attribute ID	EM Attribute Length	EM Attribute Name	EM Attribute Value Type	Attribute Data Description
96	2 bytes	Surveillance_Stop_ Type	Unsigned Integer	Value: 0 = Reserved 1 = End of surveillance (CDC and, if present, CCC) 2 = End of CCC only (CDC will continue)
97	2 bytes	Surveillance_Stop_ Destination	Unsigned Integer	Value: 0 = Reserved 1 = Surveillance_Stop applies to local surveillance only 2 = Surveillance_Stop applies to both local and remote surveillance 3 = Surveillance_Stop applies only to remote surveillance
98	variable	Related_ICID	ASCII character string	IMS Charging Identifier (ICID) is used to allow correlation of Event Messages generated by CMSes and MGCs with Accounting Events generated by other network elements [7].

10.1 EM_Header Attribute Structure

Table 38 contains a detailed description of the fields in the EM_Header attribute structure. This Event Message Header attribute MUST be the first attribute in every IPCablecom Event Message.

Table 38. EM_Header Attribute Structure

Field Name	Semantics	Value Type	Length
Version_ID	Identifies version of this structure. 1 = IPCablecom 1.0 2 = IPCablecom 1.1[5] 3 = IPCablecom Multimedia 4 = IPCablecom 1.5 The CMS, MGC and CMTS network element MUST set the value of the Version_ID to 4. Note: A value of >= 2 indicates the Event_Object field in this header is used.	Unsigned integer	2 bytes
BCID	Unique identifier for a transaction within a network. See following section.	Data Structure (See Table 39)	24 bytes
Event_Message_Type	Identifies the type of Event Message. Refer to Table 14 for a list of Event message types.	Unsigned integer	2 bytes
Element_Type	Identifies Type of Originating Element: 0 = Reserved 1 = CMS 2 = CMTS 3 = Media Gateway Controller	Unsigned integer	2 bytes
Element_ID	Network wide unique identifier 5 digits (statically configured element number unique within an IPCablecom domain in the range of 0-99,999)	Right justified, space padded ASCII Character String	8 bytes

[5] Note that PacketCable 1.1 was an interim PacketCable release that has now been subsumed by 1.5. This value was left to aid in release transitioning.

Field Name	Semantics	Value Type	Length
Time_Zone	Identifies daylight savings time and offset from universal time (UTC). Daylight Savings Time: 0 = Standard Time 1 = Daylight Savings The Daylight-Savings Time indicator MUST be set to a value of 1 if the network element is in a region that implements DST and then only during the daylight-saving-time period (usually the summer months). Since there may be areas in which the daylight-saving-time offset indicates a time-change other than 1 hour, the receiving system (e.g., RKS) needs to correctly calculate local time based on knowledge of the area(s) in which the subscriber and the network element reside. UTC offset: + HHMMSS The offset is reported from the network element (CMS/MGC/CMTS) point of view; not based on the subscriber point of view. The UTC offset represents the time offset from universal time (formerly called Greenwich Mean Time, or GMT) when standard time is in effect and MUST NOT change on transition into or out of daylight-saving-time. For example: the Time_Zone field of a network element in Boston in December is "0-050000". The same network element in Boston in July is "1-050000".	ASCII character string	1 byte 7 bytes
Sequence_Number	Each network element MUST assign a unique and monotonically increasing unsigned integer for each Event Message sent to a given RKS pair (primary/secondary). For the purpose of this standard, monotonically increasing is to be interpreted as increasing by 1. This is used by the RKS to determine if Event Message are missing from a given network element.	Unsigned integer	4 bytes
Event_time	Event generation time and date. Millisecond granularity. This specifies the local time. i.e.after applying Time_Zone UTC offset and Daylight Savings Time adjustment to UTC time. Format: yyyymmddhhmmss.mmm	ASCII character string	18 bytes
Status	Status indicators	See Table 40	4 bytes
Priority	Indicates the importance to assign relative to other event messages. The processing of event message priority is defined as: -as long as there are higher priority messages within the system, lower priority messages SHOULD NOT be processed. -arrival of a higher priority message will not interrupt current lower priority message processing. Only after the completion of the message processing, the newly arrived higher message will be processed. For IPCablecom Release 1.5, values for this field will be service provider assigned. 255 = highest priority 0 = lowest priority 128 = default.	Unsigned integer	1 byte
Attribute_Count	Indicates the number of attributes that follow (or are appended to) this header in the current Event Message.	Unsigned integer	2 bytes

Field Name	Semantics	Value Type	Length
Event_Object	The Event_Object field allows for a grouping of services. 0 = Accounting Event Message 1 = PCES Event Message The CMS, CMTS and MGC network elements MUST set the value of the Event_Object field to 0 if the Event Message is sent to the RKS. The RKS MUST discard EM messages when the Event_Object field is set to 1. The CMS, CMTS and MGC network elements MUST set the value of the Event_Object field to 1 if the Event Message is sent to the DF. The DF MUST discard EM messages when the Event Object field is set to a value different than 1.	Unsigned integer	1 byte

10.1.1 Billing Correlation ID (BCID) Field Structure

Table 39 describes the Billing Correlation ID field (BCID). The RKS, or some other back office application, uses the BCID to correlate Event Messages that are generated for a single transaction. It is one of the fields in the Event Message Header attribute. The BCID is unique for each transaction in the network. All Event Messages with the same BCID SHOULD be sent to the same primary RKS except in failover circumstances in which case the Event Messages MUST be sent to secondary RKS.

Table 39. BCID Field Description

Field Name	Semantics	Value Type	Length
Timestamp	High-order 32 bits of NTP time reference	Unsigned integer	4 bytes
Element_ID	Network wide unique identifier 5 digits (statically configured element number unique within an IPCablecom domain in the range of 0-99,999)	Right justified, space padded ASCII character string	8 bytes
Time_Zone	Identifies daylight savings time and offset from universal time (UTC). Daylight Savings Time: 0 = Standard Time 1 = Daylight Savings The Daylight-Savings Time indicator MUST be set to a value of 1 if the network element is in a region that implements DST and then only during the daylight-saving-time period (usually the summer months). Since there may be areas in which the daylight-saving-time offset indicates a time-change other than 1 hour, the receiving system (e.g., RKS) needs to correctly calculate local time based on knowledge of the area(s) in which the subscriber and the network element reside. UTC offset: + HHMMSS The offset is reported from the network element (CMS/MGC/CMTS) point of view; not based on the subscriber point of view The UTC offset represents the time offset from universal time (formerly called Greenwich Mean Time, or GMT) when standard time is in effect and MUST NOT change on transition into or out of daylight-saving-time. For example: The Time_Zone field of a network element in Boston in December is "0-050000". The same network element in Boston in July is "1-050000".	ASCII character string	1 byte 7 bytes

Field Name	Semantics	Value Type	Length
Event_Counter	Monotonically increasing for each transaction. For the purpose of this standard, monotonically increasing Event_Counter is to be interpreted as a increasing number that is greater than the preceding number.	Unsigned integer	4 bytes

The Related_Call_Billing_Correlation_ID attribute structure is shown in Table 39.

The Remote_Surveillance_Subject_BCID attribute Structure is shown in Table 39.

10.1.2 Status Field Structure

The Status field of the Event Message Header attribute is a 32-bit mask. Bit 0 is the low-order bit; the field is treated as a 4 byte unsigned integer. Table 40 presents Status field description.

Table 40. Status Field Description

Bit	Semantics	Bit Count
0-1	Error Indicator: 0 = No Error 1 = Possible Error 2 = Known Error 3 = Reserved Notes: a) If the Error Indicator bit of the Status field is set to 2 (Known Error), the Error_Description attribute (EM attribute ID 31) MUST be included in the Event Message corresponding to this header. b) If the Error Indicator bit of the Status field is set to 1 (Possible Error), the Error_Description attribute (EM attribute ID 31) MAY be included in the Event Message corresponding to this header.	2
2	Event Origin: 0 = Trusted Element 1 = Untrusted Element	1
3	Event Message Proxied: 0 = Not proxied, all data known by sending element 1 = proxied, data sent by a trusted element on behalf of an untrusted element	1
4-31	Reserved. The Status field bits 4 to 31 MUST be set to 0.	28

10.2 Call_Termination_Cause Attribute Structure

Table 41 describes the data structure of the Call_Termination_Cause attribute. It is important to note that in some cases, the Call_Termination_Cause attribute may include a Call Completion Code that may indicate a successful call completion.

Table 41. Call Termination Cause Data Structure

Field Name	Semantics	Value Type	Length
Source_Document	Identifies the source Document of the Cause Codes: 0 = Reserved 1 = Telcordia Technologies Generic Requirements GR-1100-CORE, Section 2.9, Table 411 [6] 2 = Telcordia Technologies Generic Requirements GR-1100-CORE, Section 2.9, Table 235 [6]. A Source_Document value of 2 must only be used with the Service_Instance Event Message. 3 and above for future use.	Unsigned integer	2 bytes
Cause_Code	Cause Code Identifier. Meaning determined by Source_Document defined in previous field. The Cause_Code attribute is a 4 byte value. In the case where Source_Document = 1, the IPCablecom Cause_Code is populated based only on the GR-1100-CORE [6] (Table 411) definition of character 2 (Cause Category) and characters 3-5 inclusive (Cause Indication), and encoding these 4 characters as an unsigned integer. Characters 1 and 6 of Table 411 are not relevant. For example, the encoding of a Cause_Code with Cause Category of ITU Standard (0) and a Cause Indication of "Normal Call Clearing" (016) is the unsigned integer value 0016. In the case where Source_Document = 2, the IPCablecom Cause_Code is populated based on the GR-1100-CORE [6] - Table 235 character 1. For example, the encoding of a Cause_Code with a Call Completion Code "Not completed: Invalid authorization code" (3) is the unsigned integer value of 0003.	Unsigned integer	4 bytes

10.3 Trunk Group ID Attribute Structure

Table 42 describes the Trunk Group ID Data Structure.

Table 42. Trunk Group ID Data Structure

Field Name	Semantics	Value Type	Length
Trunk_Type	1 = when Non-SS7 (MF) direct trunk group is used 2 = Not Used 3 = when an SS7 signaling trunk is directly connected to IC/INC, SS7 direct trunk group number 4 = when an SS7 signaling trunk is connected to IC via AT and SS7 from AT to EO 5 = Not Used 6 = when Non-SS7 trunk is used between the EO and AT and SS7 signaling trunk is used between AT and IC. (Terminating only) 9 = Signaling type not specified	Unsigned integer Value is the Trunk Group Signaling Type Indicator as defined in Telcordia GR-1100-CORE [6], Table 83.	2 bytes
Trunk_Group_Number	ASCII Identifier. Values in the range 0000-9999.	Right justified, space padded ASCII character string	4 bytes

10.4 QoS Descriptor Attribute Structure

Table 43 describes the QoS Descriptor Data Structure.

Table 43. QoS Descriptor Data Structure

Field Name	Semantics	Value Type	Length
Status_Bitmask	Bitmask describing structure contents. (See Table 38)	Bit map	4 bytes
Service_Class_Name	Service profile name	Right justified, space padded ASCII character string	16 bytes
QoS_Parameter_Array	QoS Parameters. Contents determined by Status Bitmask.	Unsigned integer array	Variable length array of 32-bit unsigned integers

Table 44 describes the QoS Status Bitmask field of the QoS Descriptor attribute. Bits 2-17 describe the contents of the QoS_Parameter_Array. Each of these bits indicates the presence (bit=1) or absence (bit=0) of the named QoS parameter in the array. The location of a particular QoS parameter in the array matches the order in which that parameter's bit is encountered in the bitmask, starting from the low-order bit.

Each QoS parameter present in the QoS_Parameter_Array must occupy four bytes. The definition and encoding of the QoS parameters can be found in Appendix C of [15]. QoS parameters whose definition specifies less than four bytes must be right-justified (where the 4 bytes are to be treated as an unsigned integer) in the four bytes allocated for the array element.

Table 44. QoS Status Bitmask

Start Bit	Semantics	Bit Count
0	State Indication: 0 = Illegal Value 1 = Resource Reserved but not Activated 2 = Illegal Value 3 = Resource Reserved & Activated	2
2	Service Flow Scheduling Type	1
3	Nominal Grant Interval	1
4	Tolerated Grant Jitter	1
5	Grants Per Interval	1
6	Unsolicited Grant Size	1
7	Traffic Priority	1
8	Maximum Sustained Rate	1
9	Maximum Traffic Burst	1
10	Minimum Reserved Traffic Rate	1
11	Minimum Packet Size	1
12	Maximum Concatenated Burst	1
13	Request/Transmission Policy	1
14	Nominal Polling Interval	1
15	Tolerated Poll Jitter	1
16	IP Type of Service Override	1
17	Maximum Downstream Latency	1

10.5 Redirected-From-Info Attribute Structure

Table 45 describes the data structure of the Redirected-From-Info.

Table 45. Data Structure of the Redirected-From-Info Attribute

Field Name	Semantics	Value Type	Length
Last_Redirecting_Party	E.164 [9] address of most recent redirecting party	ASCII string	20 bytes
Original_Called_Party	E.164 [9] address of the original called party	ASCII string	20 bytes
Number_of_Redirections	Number of times this call has been redirected	Unsigned integer	2 bytes

10.6 Electronic-Surveillance-Indication Attribute Structure

Table 46 describes the data structure of the Electronic-Surveillance-Indication. The Electronic-Surveillance-Indication attribute appears in the Signaling_Start EM or Surveillance_Stop EM.

This attribute creates a "chain" of DFs as calls are redirected from one endpoint to another. In such scenarios, the DF associated with each CMS will be responsible for forwarding the call content and/or call data to the next DF in the chain. The last DF in the chain will then report the call content and/or call data to the appropriate LEA. If multiple surveillances are being performed, a DF in the middle of the chain may report the call content and/or call data to the appropriate LEA, as well as forward the call content and/or call data to the next DF in the chain.

This attribute is included in a Signaling_Start EM to indicate to the DF where to forward call content and/or call data for a particular intercept. For example, in a CMSS environment, a CMS may perform surveillance at the request of another CMS due to a redirection by the subject. In such a scenario, the CMS would send call content and/or call data to its DF, and the DF would then forward the call data and call content to the DF responsible for delivering the call content and/or call data to the appropriate Law Enforcement Agency (LEA).

This attribute is included in a Surveillance_Stop EM when a CMS needs to indicate that surveillance will end, but the DF is not part of the surveillance chain as described above. This will occur in a CMSS environment when a CMS is redirected, and surveillance is requested as part of the redirection. In such a scenario, the CMS will normally request that the redirected-to CMS perform surveillance on behalf of the redirecting CMS, and a chain will be established between the redirected-to CMS and the redirecting CMS. However, the redirecting CMS may be in a jurisdiction in which surveillance cannot be performed. As a result, the CMS would send a Surveillance_Stop EM, and include the Electronic-Surveillance-Indication attribute, to ensure that the EM is forwarded to the DF of the redirecting CMS.

Table 46. Data Structure of the Electronic-Surveillance-Indication Attribute

Field Name	Semantics	Value Type	Length
DF_CDC_Address	IP address of the electronic surveillance Delivery Function of the forwarding party for event messages	IP Address	4 bytes
DF_CCC_Address	IP address of the electronic surveillance Delivery Function of the forwarding party for call content packets	IP Address	4 bytes
CDC_Port	Port number to which to send a copy of event messages	Unsigned integer	2 bytes
CCC_Port	Port number to which to send a copy of call content packets	Unsigned integer	2 bytes
Local_CCC_ID	Call Content Identifier assigned by CMS or MGC	Unsigned integer	4 bytes
Remote_CCC_ID	Call Content Identifier assigned by CMS or MGC	Unsigned integer	4 bytes
Remote_Surveillance_Subject_BCID	BCID of the surveillance subject at the redirecting CMS	Data Structure (See Table 39)	24 Bytes

10.7 Attributes For Conference Parties

Table 47 describes the data structure of the attributes Communicating_Party, Joined_Part, and Removed_Party.

Table 47. Communicating_Party, Joined_Party, and Removed_Party Attributes

Field Name	Semantics	Value Type	Length
Party_ID	E.164 [9] formatted address specifying the number of the party. In the future other numbering plans will be addressed.	Right justified, space padded ASCII character String.	20 bytes
CCC_ID_Valid	When CCC_ID is present this field is set to 1; otherwise it is set to 0.	Unsigned integer	2 bytes
CCC_ID	The CCC_ID associated with the call leg for the Party_ID. When the subject is one of the party in the conference, any of the active CCC_IDs can be used. When CCC_ID_Valid is not set (CCC_ID not valid in the case of Call Data), this field is filled with the default binary value of all ones.	Unsigned integer	4 bytes

11 TRANSPORT INDEPENDENT EVENT MESSAGE ATTRIBUTE TLV FORMAT

Every Event Message Attribute is defined by a Type Length Value (TLV) tuple. An attribute TLV tuple has the format shown in Table 48:

Table 48. Event Message Attribute TLV-tuple Format

Field Name	Semantics	Field Length
Attribute_Type	IPCablecom Attribute Type	1 byte (refer to Table 37)
Attribute_Length	IPCablecom Attribute Length	1 byte (refer to Table 37) Note: Value is Attribute Length + 2
Attribute_Value	IPCablecom Attribute Value	Attribute Length bytes

12 IPCABLECOM EVENT MESSAGE FILE FORMAT

The IPCablecom Event Message File Format has the following basic structure:

12.1 File Bit / Byte Order

Table 49 defines the Bit / Byte order for the Event Message file. For fields that span multiple bytes, the high-order bit of the field is the highest order bit of the lowest-numbered byte. Conversely, the low-order bit of a multi-byte field is the lowest-order bit of the highest-numbered byte.

Table 49. Bit / Byte Order for the Event Message File

Bit / Byte Order		High-order Bit							Low-order Bit
Binary		7	6	5	4	3	2	1	0
High-order Byte	Byte 1								
…	…								
Low-order Byte	Byte n								

12.2 File Header

The header shown in Table 50 MUST be written at the start of a file formatted using the IPCablecom Event Message File Format:

Table 50. File Header for IPCablecom Event Message File Format

Field Name	Semantics	Length	Type
Format_Version	Identifies the version of this file format. The value must be 1 to comply this version of the EM standard.	4 bytes	Unsigned int
EM_Count	Number of EMs in File	8 bytes	Unsigned int
File_Creation_Timestamp	YYYYMMDDHHMMSS.MMM	18 bytes	ASCII
File_Sequence_Number	Monotonically increasing for each new file. For the purpose of this standard, monotonically increasing is to be interpreted as increasing by 1.	8 bytes	Unsigned int
Element_ID	Network wide unique identifier 5 digits (statically configured element number unique within an IPCablecom domain in the range of 0-99,999)	8 bytes	Right justified, space padded ASCII character string
Time_Zone	Identifies daylight savings time and offset from universal time (UTC). Daylight Savings Time: 0 = Standard Time 1 = Daylight Savings The Daylight-Savings Time indicator MUST be set to a value of 1 if the network element is in a region that implements DST and then only during the daylight-saving-time period (usually the summer months. Since there may be areas in which the daylight-saving-time offset indicates a time-change other than 1 hour, the receiving system (e.g., RKS) needs to correctly calculate local time based on knowledge of the area(s) in which the subscriber and the network element reside. UTC offset: +HHMMSS	1 byte 7 bytes	ASCII character string

Field Name	Semantics	Length	Type
	The UTC offset represents the time offset from universal time (formerly called Greenwich Mean Time, or GMT) when standard time is in effect and MUST NOT change on transition into or out of daylight-saving-time. For example: the Time_Zone field of a network element in Boston in December is "0-050000". The same network element in Boston in July is "1-050000".		
File_Completion_Timestamp	YYYYMMDDHHMMSS.MMM	18 bytes	ASCII

NOTE: There is no checksum included in the file header. It is assumed that the transport mechanism is responsible for delivery of damage-free files. For example, both of the IP transport protocols, UDP and TCP, contain a checksum to protect against damaged messages.

12.3 File Naming Convention

Files created using the IPCablecom Event Message File Format MUST use the following naming convention: "PKT-EM_yyyymmddhhmmss_pri_type_elementid_seq.bin."

12.3.1 Filename Components

Table 51 describes each of the components of the filename:

Table 51. Filename Components

Component	Semantics	Type	Length
File_ID	Identifies this file as containing IPCablecom Event Messages	Literal string 'PKT-EM'	6 characters
Timestamp	Time at which file was opened by the network element	yyyymmddhhmmss	14 characters
Priority	Priority of this file When processing multiple files with differing priorities, files of higher priority must be processed before the lower priority files. File priority should be established by the application creating the file.	Integer in the range 1-4 4 is the highest 1 is the lowest A default value of 3 is recommended.	1 character
Record_Type	This flag identifies the record type contined in the file. Primary records indicate new, while secondary records indicate previously transmitted	Binary If the file contains primary usage data this will be a 0 (zero) if it contains a 1 (one) the file contains secondary data.	1 characters
Element_ID	Network wide unique identifier 5 digits (statically configured element number unique within an IPCablecom domain in the range of 0-99,999) with leading zeros for padding. e.g., element id = 99 PKT-EM_yyyymmddhhmmss_pri_type_00099_seq.bin	Right justified, zero padded ASCII character string	5 characters

Component	Semantics	Type	Length
Sequence_Number	Monotonically increasing sequence number for each new file. For the purpose of this standard, monotonically increasing is to be interpreted as increasing by 1.	A fixed length character string that allows only the characters 0-9, with an interger range of 000001-999999. Left most positions are always padded with zero.	6 characters

Each element of the filename components is separated by an underscore "_" character. The segment delimiter will also enable segments to be distinguishable simply by a parsing process.

12.4 Configuration Items

The items shown in Table 52 MUST be configurable by the IPCablecom network element creating the file:

Table 52. Required Configuration Items

Name	Semantics	Type	Length
Maximum File Length	Maximum size of file, in bytes, to which flat file can grow before being closed for transport.	Unsigned integer	4 octets
Maximum Open Time	Maximum amount of time, in seconds, before file must be closed for transport.	Unsigned integer	4 octets

The IPCablecom Network Element that created the file MUST close any currently open flat file at the first occurrence of either of the following events:

- The file size exceeds the Max File Length
- The file open duration exceeds the Maximum Open Time

12.5 File EM Structure Header

When an EM is written out to a file, each event message MUST be identified by a structure header.

Table 53 identifies the File-based EM Packet Structure:

Table 53. File-based EM Packet Structure

Field Name	Semantics	Description
ID	Indicates an EM structure	2 byte, value of 0xAA 55. The value 0xAA 55 is chosen to enable synchronization of the EM boundary if there are any errors within an event message.
Length	Indicate the length of the entire EM structure	2 bytes, length of all attributes + 4
attributes	Refer to Table 48. Event Message Attribute TLV-tuple format.	Event Message attributes

13 TRANSPORT PROTOCOL

This section specifies the possible transport protocols used between the IPCablecom network elements that generate Event Messages (CMS, CMTS, MGC) and the Record Keeping Server (RKS). These network elements MUST support RADIUS Accounting (RFC2866) with IPCablecom extensions as defined in this document. The optional transport protocol is FTP as defined in this document.

The following are the IPCablecom transport requirements:

- The transport protocol MAY support confidentiality of Event Messages.
- End-to-end security across multiple administrative domains is not required.
- RADIUS protocol parameters:
- Retry interval and Retry count.
- For each RKS that may receive Event Messages, its IP address and UDP port.
- The IP address of each RADIUS server that it may communicate with.

13.1 RADIUS Accounting Protocol

The RADIUS Accounting protocol is a client/server protocol that consists of two message types: Accounting-Request and Accounting-Response. IPCablecom network elements that generate Event Messages are RADIUS clients that send Accounting-Request messages to the RKS. The RKS is a RADIUS server that sends Accounting-Response messages back to the IPCablecom network elements indicating that it has successfully received and stored the Event Message.

The Event Messages are formatted as RADIUS Accounting-Request and Accounting-Response packets as specified in RFC 2866 [5]. Although IPCablecom 1.5 specifies RADIUS as the transport protocol, alternate transport protocols MAY be supported in future IPCablecom releases.

13.1.1 Reliability

The RADIUS messages are transported over UDP, which does not guarantee reliable delivery of messages, hence the request/response nature of the protocol (see RFC 2865 [4] for the technical justification of choosing UDP over TCP for the transport of Authentication, Authorization, and Accounting messages).

When an RKS receives and successfully records all IPCablecom Event Messages in a RADIUS Accounting-Request message, it MUST send an Accounting-Response message to the client. If the IPCablecom network element does not receive an Accounting- Response within the configured retry interval, it MUST re-send the same Accounting Request either to the same RKS or the alternate RKS (retries may alternate between primary and secondary RKS in a vendor-specific way). The IPCablecom network element MUST continue resending the Accounting-Request until it receives an acknowledgement from an RKS or the maximum number of retries is reached. The RADIUS server MUST NOT transmit any Accounting-Response reply if it fails to successfully record the Event Message.

Once a Network Element succeeds in sending event messages to the secondary RKS server, a failover to the secondary RKS should occur. This is a non-revertive failover, meaning that the secondary RKS becomes active, and is the new primary RKS. For calls in progress, all subsequent event messages should be sent to the now active secondary RKS. For all new calls, the CMS should instruct the CMTS and MGC to use the new active RKS as the primary (i.e., the previous secondary RKS becomes the new primary for subsequent calls).

13.1.2 RADIUS Client Reliability

All Network Elements MUST store Event Messages until they have received an Acknowledgement (Ack) from an RKS that the data was correctly received and stored, or until the maximum number of retries has been reached. Only when an Ack is received or the maximum retries reached are the NEs allowed to delete these Event Messages. If the maximum retries is reached, the NEs SHOULD write the Event Messages to an error file before deleting these Event Messages.

In order to guarantee the reliable transfer of the data, the Radius Client should implement a user configurable Radius message Ack interval and the number of times the client needs to retransmit the event or message. The time interval should be configurable (suggested: 10msec to 10 sec), the number of retries should be configurable (suggested: 0 to 9). The number of retries should be attempted on both the primary RKS and secondary RKS. After exhausting the number of retries, the event message SHOULD be written to an error file and the event message can then be deleted from the network element.

NOTE: 1) The Radius Client MIB (RFC2620) does not contain these parameters.
2) This requirement implies that the RKSes use highly reliable storage media and are also highly available.

13.1.3 Authentication and Confidentiality

Refer to the IPCablecom security specification [2] for details concerning the use of IPSec to provide both authentication and confidentiality of the RADIUS messages, and the details of the correct usage of the RADIUS shared secret.

13.1.4 Standard RADIUS Attributes

Each RADIUS message starts with the standard RADIUS header shown in Table 54.

Table 54. RADIUS Message Header

Field Name	Semantics	Field Length
Code	Accounting-Request = 4 Accounting-Response = 5	1 byte
Identifier	Used to match accounting-request and accounting-response messages.	1 byte
Length	Total length of RADIUS message min value = 20 max value = 4096	2 bytes
Authenticator	Computed as per RADIUS Specification [5]	16 bytes

Two standard RADIUS attributes MUST follow the RADIUS Message Header: NAS-IP-Address and Acct_Status_Type. These two fields are included to improve interoperability with existing RADIUS server implementations since they are mandatory attributes in a RADIUS Accounting-Request packet.

The NAS-IP-Address indicates the originator of the Accounting-Request message and MUST contain the IP address of the originating IPCablecom network element.

The Acct-Status-Type attribute typically indicates whether the Accounting-Request marks the beginning of the user service (Start) or the end (Stop). Since an IPCablecom Accounting-Request message may contain multiple Event Message Packets, it could contain Event Messages which mark both the beginning and end of the user service. For this reason, an Acct-Status-Type value of Interim-Update is used to represent IPCablecom Event Messages.

Table 55. Mandatory RADIUS Attributes

Name	Type	Length	Value
NAS-IP-Address	4	6	IP address of originating IPCablecom network element
Acct-Status-Type	40	6	Interim-Update=3

Table 56. RADIUS Acct_Status_Type

Type	Length	Value
40	6 bytes	Interim-Update = 3

IPCablecom attributes are defined in Section 10 of this document. IPCablecom attributes are encoded in the RADIUS Vendor Specific Attributes (VSA) structure as described in this section. Additional IPCablecom or vendor-specific attributes can be added to existing Event Messages by adding additional RADIUS VSAs to the message.

The Vendor-Specific attribute includes a field to identify the vendor, and the Internet Assigned Numbers Authority (IANA) has assigned IPCablecom an SMI Network Management Private Enterprise Number of 4491 for the encoding of these attributes. The RKS server SHOULD ignore Event Messages where the IPCablecom "Event Message type" is unidentified. The RKS server SHOULD also ignore IPCablecom event attributes where the event attribute type is unidentified.

Table 57. Radius VSA Structure for IPCablecom Attributes

Field Name	Semantics	Field Length
Type	Vendor Specific = 26	1 byte
Length	Total Attribute Length Note: value is Vendor Length + 8	1 byte
Vendor ID	CableLabs = 4491	4 bytes
Vendor Attribute Type	IPCablecom Attribute Type	1 byte (refer to Table 37)
Vendor Attribute Length	IPCablecom Attribute Length	1 byte (refer to Table 37) Note: value is Vendor Length +2
Vendor Attribute Value	IPCablecom Attribute Value	Vendor Length bytes

13.1.5 IPCablecom Extensions

13.1.5.1 IPCablecom RADIUS Accounting-Request Packet Syntax

```
<<RADIUS Accounting-Request> ::==
                  <RADIUS message Header>
                  <RADIUS NAS-IP-Address Attribute>
                  <RADIUS Acct-Status-Type Attribute>
                  <Packet Cable EM List>

<Packet Cable EM List> ::==
                  <Packet Cable EM> |
                  <Packet Cable EM List> <Packet Cable EM>

<Packet Cable EM> ::==
                  <RADIUS VSA for IPCablecom EM Header Attribute>
                  <IPCablecom EM Attribute List>

<IPCablecom EM Attribute List> ::==
                  <RADIUS VSA for IPCablecom EM Attribute> |
                  <IPCablecom EM Attribute List>
<RADIUS VSA for Packet Cable EM Attribute>
```

The potential of a high Event Message volume raised the concern that the RADIUS mechanism for ensuring reliability via request/response may consume too much bandwidth or be too computationally intensive. This led to the requirement that it be possible to transmit multiple IPCablecom Event Messages in a single RADIUS message. The use of this 'batch mode' is left to the discretion of the IPCablecom network element and will likely depend on the latency requirements of the particular event type. The number of Event Messages encapsulated in a single RADIUS message is still subject to the maximum RADIUS message length restriction of 4096 bytes.

The Event Message Header MUST be the first attribute within a given Event Message. If multiple Event Messages are sent in a single RADIUS Accounting-Request, the Event Message Header attribute indicates the start of a new Event Message. The order of the Event Message attributes which follow the Event Message Header is arbitrary.

IPCablecom extends RADIUS Accounting, by introducing new attributes and new values for existing attributes. Since the RADIUS protocol is extendable in this manner, it is expected that existing RADIUS server implementations will require minimal modifications to support the batch collection of IPCablecom Event Messages.

13.1.5.2 Concatenation of Attributes

The Vendor Specific Attribute (VSA) limits the size of the attribute value to 247 bytes (see Table 57). However there may be instances where the attribute value cannot fit into a single VSA, for example, the SDP attributes used in electronic surveillance. In cases where the value of an attribute is greater than 247 bytes, the network element MUST create multiple attributes of the same type in the RADIUS message. The attributes MUST be adjacent to one another within the message and MUST be sequential such that the order of the original attribute value is maintained. The recipient in this case MUST concatenate the multiple attributes into a single attribute value. Note that regardless of multiple attributes being present in an event message, the message is subject to the maximum RADIUS message length restriction of 4096 bytes. Attributes that are concatenated in this manner MUST be from the list presented in Table 58.

Table 58. Concatenated Attributes

EM Attribute Name	EM Attribute ID
SDP_Upstream	39
SDP_Downstream	40
RTCP_Data	93
Local_XR_Block	94
Remote_XR_Block	95

13.2 File Transport Protocol (FTP)

The File Transfer Protocol (FTP) [24] MAY be used by an IPCablecom network element to transport Event Messages to the RKS. The RKS MUST have FTP Server support. If this transport protocol is used, the RKS hosts an FTP server to accept files transferred by the IPCablecom network element. The IPCablecom network element acts as the FTP client, pushing the files to the RKS for processing.

If FTP is used as a transport protocol, then the file MUST be formatted using the IPCablecom Event Message File Format.

13.2.1 Required FTP Server Capabilities

The FTP Server at the RKS MUST have at minimum the following capabilities:

- Minimum implementation as described in Internet Protocol Standards - STD9 [24] Section 5.1.
- PASV Mode (passive mode) command
- Data Type I, Image (binary)
- Authentication support (PASS command)
- File Transfer logging

The FTP client should listen for the 226 response to the STOR (close data connection) to indicate the file was successfully transferred and excepted by the RKS before marking the file as transferred. The NE should attempt to resend the file during the next scheduled FTP session if a response other than 226 is received.

Appendix I PCES Support

This section details the IPCablecom Event Messages and their associated attributes that MUST be generated to support IPCablecom Electronic Surveillance as defined in [8]. The following requirements apply to all PCES Event Messages:

- The appropriate network element (CMS,CMTS, MGC) MUST send the PCES Event Message to the DF in real-time as defined in [8].
- The PCES Event Message sent to the DF MUST NOT affect the monotonically increasing Sequence-Number that appears in the Event Message header sent to the RKS.
- All PCES Event Messages MUST have the Event_Object field in the EM_Header attribute set to one.
- PCES Event Messages MUST NOT be sent to the RKS.

The following requirements apply to all PCES components responsible for sending or receiving Event Messages:

- Intercept Access Points (e.g., CMS, CMTS, MGC) and Delivery Function (DF) MUST support the Radius Protocol over UDP as defined in Section 13 except for 13.1.1 and 13.1.2.
- If an IAP does not receive an Accounting-Response message within the configured retry interval, it MUST continue resending the same Accounting-Request until it receives an acknowledgement from the DF or the maximum number of retries is reached. The IAP MAY drop the request after the maximum retries is reached.
- When a DF receives PCES Event Message in a Radius Accounting-Request message from an IAP, it MUST send an Accounting-Response message to the IAP.

I.1 Service_Instance

If the service is under surveillance as defined in [8], the Service_Instance Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters.

Table 59. Service_Instance Event Message for PCES

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Service_Name	R	The Service_Name attribute MUST be present. Class Service Name: Call_Block Call_Forward Call_Waiting Repeat_Call Return_Call Three_Way_Call
Call_Termination_Cause	O	The Call_Termination_Cause attribute MUST be present if Service_Name is Call_Block.
Redirected_From_Party_Number	O	2 = The Redirected_From_Party_Number attribute MUST be present if Service_Name is Call_Forward.
Redirected_To_Party_Number	O	The Redirected_To_Party_Number attribute MUST be present if Service_Name is Call_Forward.
Carrier_Identification_Code	O	The Carrier_Identification_Code attribute MUST be present if Service_Name is Call_Forward and transit carrier is used to transport the redirected call.
Related_Call_Billing_Correlation_ID	O	The Related_Call_Billing_Correlation_ID attribute MUST be present if Service_Name is Call_Forward, Call_Waiting or Three_Way_Call.

Attribute Name	Required or Optional	Comment
Charge_Number	O	The Charge_Number attribute MUST be present if Service_Name is Call_Forward, Call_Waiting, Repeat_Call, Return_Call or Three_Way_Call.
First_Call_Calling_Party_Number	O	The First_Call_Calling_Party_Number attribute MUST be present if Service_Name is Call_Waiting.
Second_Call_Calling_Party_Number	O	The Second_Call_Calling_Party_Number attribute MUST be present if Service_Name is Call_Waiting. The Called_Party_Number MUST also be present for Return_Call when it's not included in the Signaling_Start message .
Called_Party_Number	O	The Called_Party_Number attribute MUST be present if Service_Name is Call_Waiting.
Routing_Number	O	The Routing_Number attribute MUST be present if Service_Name is Repeat_Call or Return_Call.
Calling_Party_Number	O	The Calling_Party_Number attribute MUST be present if Service_Name is Repeat_Call or Return_Call.

I.2 Signaling_Start

If the service is under surveillance as defined in [8], this Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters.

The MGC MUST generate, timestamp, and send this event to the DF for a terminating call under surveillance to a PSTN Gateway.

- The MGC MUST timestamp this message coincident with sending the SS7 IAM message or transmitting the dialed digits on an MF-trunk.
- For an originating call from an MTA or from a PSTN Gateway, if the MGC receives notification via signaling from the terminating CMS that the call is to be intercepted but the terminating device is unable to perform the interception, the MGC MUST timestamp and send an additional Signaling_Start event message to the Electronic Surveillance Delivery Function prior to delivering a response to the originating MTA or PSTN Gateway. This Signaling_Start event message MUST contain the Electronic_Surveillance_Indication attribute, and the value of the Direction_Indicator attribute MUST be integer 2 (2=Terminating).
- The CMS MUST generate, timestamp, and send this event to the DF if the originating call from an MTA is under surveillance.
- The CMS MUST timestamp and send this event message DF after all translation of the dialed digits is complete, whether the translation is successful or not. This includes unroutable digits reported to the CMS (i.e., partially dialed digits).
- The CMS MUST generate, timestamp, and send this event to the DF. for a terminating call to an MTA under surveillance, or for a terminating call under surveillance to an MTA.
- The CMS MUST timestamp and send this event message to the Electronic Surveillance Delivery Function prior to invoking any termination features.

Table 60. Signaling_Start Event Message for PCES

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Direction_Indicator	R	None
MTA_Endpoint_Name	O	If the originating CMS generates this message, this attribute MUST

Attribute Name	Required or Optional	Comment
		contain the endpoint name of the originating MTA. If the terminating CMS generates this message, this attribute MUST contain the endpoint name of the terminating MTA. If the originating MGC generates this message, this attribute MAY contain the endpoint ID of the originating MG. If the terminating MGC generates this message, this attribute MAY contain the endpoint ID of the terminating MG.
Calling_Party_Number	O	The Calling_Party_Number attribute MUST be included whenever it is available in SS7 or CMSS signaling. For example, in the off-net to on-net scenario, this attribute may not be present when the Originating MGC and Terminating CMS do not have the Calling Party Number attribute available from SS7 signaling.
Called_Party_Number	R	Terminating address (E.164 [9] format)
Routing_Number	R	Routable number
Location_Routing_Number	O	The Location_Routing_Number attribute MUST be included if a LNP lookup returns a LRN.
Carrier_Identification_Code	O	This attribute MUST be included in MGC generated messages in which the call is being routed to an inter-exchange carrier and the information is available.
Trunk_Group_ID	O	This attribute MUST be included when the MGC generates this message.
User_Input	O	MUST be present for a call origination event, and MUST contain the original dialed digits received from MTA or from PSTN Gateway.
Translation_Input	O	MUST be present if an external database was consulted for translation, and the input for that external translation was different than the value of User-Input.
Redirected_From_Info	O	MUST be included for a call termination if information is available about previous redirections.
Electronic_Surveillance_Indication	O	The Electronic_Surveillance_Indication attribute MUST be present in events sent to DF for terminating calls that have been redirected by a surveillance subject.

I.3 Signaling_Stop

If the service is under surveillance as defined in [8], this Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters.

This Event Message indicates the time at which signaling terminates. It is intended to capture the point at which the NE processes the final signaling message for the call. A Signaling_Stop message MUST NOT be generated unless a Signaling_Start message with the same BCID has been generated for the call. A Signaling_Stop message MUST be generated if a Signaling_Start message with the same BCID has been generated for the call (in exception cases, this may be the result of a proprietary time-out or clean-up process).

Originating CMS

In the single-zone scenario, the originating CMS MUST timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.

In the intra-domain or inter-domain scenarios, the originating CMS MUST timestamp this message upon transmission of the last signaling event in the following list:

- Transmission of the NCS-signaling DLCX message, or
- Transmission of the CMSS-signaling BYE message or CANCEL message.

Terminating CMS

In the single-zone scenario, the terminating CMS MUST timestamp this EM message immediately upon transmission of the NCS-signaling DLCX message.

In the intra-domain or inter-domain scenarios, the terminating CMS MUST timestamp this message upon transmission of the last signaling event in the following list:

- Transmission of the NCS-signaling DLCX message, or
- Transmission of the CMSS-signaling BYE message or the transmission of the CMSS-signaling acknowledgment response message to a CANCEL request.

Originating MGC (off-net to on-net)

The originating MGC MUST timestamp this EM message immediately upon the last signaling event in the following list:

- Transmission/receipt of an RLC to/from the Signaling Gateway that communicates with the SS7 network,
- Transmission of the MGC-issued TGCP DLCX message,
- Receipt of an MG-issued TGCP DLCX, or
- Transmission of the CMSS-signaling BYE message or CANCEL message.

Terminating MGC (on-net to off-net)

The terminating MGC MUST timestamp this EM message immediately upon transmission of the TGCP-signaling DLCX message.

Table 61. Signaling_Stop Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Related_Call_Billing_Correlation_ID	O	If the originating CMS or MGC generates this message, the Related_Call_Billing_Correlation_ID attribute MUST contain the BCID of the terminating CMS or MGC when terminating CMS or MGC is known. If the terminating CMS or MGC is not known, this attribute may be omitted. If the terminating CMS or MGC generates this message, the Related_Call_Billing_Correlation_ID attribute MUST contain the BCID of the originating CMS or MGC if known. If the BCID of the originating CMS or MGC is not known this attribute may be omitted.
FEID	O	If the originating CMS or MGC generates this message, the FEID attribute MUST contain the FEID of the terminating CMS or MGC when terminating CMS or MGC is known. If the terminating CMS or MGC is not known, this attribute may be omitted If the terminating CMS or MGC generates this message, the FEID attribute MUST contain the FEID of the originating CMS or MGC.
Call_Termination_Cause	R	The Call_Termination_Cause code MUST be present.

I.4 Call_Answer

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters and with the additional required electronic surveillance parameters.

The CMS or MGC MUST send this Event Message to the DF.

I.5 Call_Disconnect

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the standard required parameters.

The CMS or MGC MUST send this Event Message to the DF.

I.6 QoS_Reserve

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the parameters described in Table 62 below.

The CMTS MUST generate this message if:

1. The CMTS generates a QoS_Reserve Event Message as defined in Section 9.14, AND
2. The COPS Electronic-Surveillance-Parameters object was included in the Gate-Set message to the CMTS, and the flag indicates dup-event

Table 62. QoS_Reserve Event Message for PCES

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
QoS_Descriptor	R	None
MTA_UDP_Portnum	R	None
SF_ID	R	None
Flow_Direction	R	None
CCC_ID	R	None

I.7 QoS_Release

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the parameters described in Table 63 below.

The CMTS MUST generate this message if:

1. The CMTS generates a QoS_Release event message as defined in Section 9.15, AND
2. The Electronic-Surveillance-Parameters object was included in the Gate-Set message to the CMTS, and the flag indicates dup-event.

Table 63. QoS_Release Event Message for PCES

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
SF_ID	R	None
Flow_Direction	R	None
CCC_ID	R	None

I.8 QoS_Commit

If the service is under surveillance as defined in [8], then this Event Message MUST be generated with all the parameters described in Table 64 below.

The CMTS MUST generate this message if:

1. The CMTS generates a QoS Commit Event Message as defined in Section 9.17, AND
2. The COPS Electronic-Surveillance-Parameters object was included in the Gate-Set message to the CMTS, and the flag indicates dup-event.

Table 64. QoS_Commit Event Message for PCES

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
QoS_Descriptor	R	None
MTA_UDP_Portnum	R	None
SF_ID	R	None
Flow_Direction	R	None
CCC_ID	R	None

I.9 Media_Report

This Event Message is used by the CMS and MGC to report media stream status and session description information (SDP) to the DF. The CMS and MGC MUST send this message:

1. When it opens a new media channel and receives confirmation containing SDP. Typically the sending of this message would be triggered by the positive acknowledgement of an NCS or TGCP modify connection in which reservations were requested. The "Channel_State" attribute is set to "Open" in this case. [6]
2. When it closes a media channel. Typically the sending of this message would be triggered by the positive acknowledgement of an NCS or TGCP delete connection. The "Channel_State" attribute is set to "Close" in this case.[7]
3. When it receives new SDP for an open media channel. Typically the sending of this message would be triggered by the positive acknowledgement of an NCS or TGCP modify connection in which SDP was received. The "Channel_State" attribute is set to "Change" in this case.[8]

The CMS or MGC MUST timestamp this message on receipt of response from an endpoint that triggered the sending of the message (e.g., response from a modify or delete connection).

Table 65. Media_Report Event Message for PCES

Attribute Name	Required or Optional	Comments
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM
CCC_ID	O	The CCC_ID attribute MUST be present for call content surveillance. CMS and MGC provide CCC_ID. The CCC_ID attribute MUST NOT be present for call data surveillance.
SDP_Upstream	O	The SDP_Upstream attribute MUST be included if SDP is received from the surveillance subject's associate.
SDP_Downstream	O	The SDP_Downstream attribute MUST be included if SDP is received from the surveillance subject

[6] This is the message that the DF uses to trigger sending a CCOpen message to the CF (refer to [8]).
[7] This is the message that the DF uses to trigger sending a CCClose message to the CF (refer to [8]).
[8] This is the message that the DF uses to trigger sending a CCChange message to the CF (refer to [8]).

Attribute Name	Required or Optional	Comments
Channel_State	R	The Channel_State attribute MUST be included and set to "Open" if a new channel has been opened, "Change" if SDP is being provided for an opened channel, "Close" if the media channel has been closed.
Flow_Direction	R	The Flow_Direction attribute MUST be included and indicates direction of flow: Upstream or Downstream.

I.10 Signal_Instance

If the service is under surveillance as defined in [8], the Signal_Instance message MUST be generated and timestamped when any of the following events occurs, unless the information reported in the Signal_Instance message would be redundant with the information reported by other Event Messages (e.g., Signaling_Start):

1. The CMS receives a positive acknowledgement in response to a NotificationRequest command that requested immediate generation of a signal contained in Table 66 toward the surveillance subject.
2. The CMS receives a Notify command that indicates the surveillance subject's initiation of a signal contained in Table 67. For DTMF tones, the CMS MUST not generate the Signal_Instance message until it has received all of the digits provided by the surveillance subject.

Table 66. Signals Sent Toward Intercept Subject

NCS Code	Description (Name)
0-9,*,#,A,B,C,D	DTMF tones
bz	Busy tone
cf	Confirmation tone
ci(ti,nu,na)	Caller Id
dl	Dial tone
mwi	Message waiting indicator
ot	Off-hook warning tone
r0,r1,r2,r3,r4,r5,r6,r7	Distinctive ringing
rg	Ringing
ro	Reorder tone
rs	Ringsplash
rt	Ring back tone
sl	Stutter dial tone
vmwi	Visual message waiting indicator
wt1,wt2,wt3,wt4	Call waiting tone

Table 67. Signals Received From Intercept Subject

NCS Code	Description (Name)
0-9,*,#,A,B,C,D	DTMF tones
ft	Fax tone
hf	Flash hook
mt	Modem tones
TDD	Telecomm Devices for the Deaf (TDD) tones

When the generation of the Signal_Instance message is due to Condition 1 in the above requirement, the Signal_Type attribute in Table 68 MUST be set to a value of "1". The value of "1" identifies the other attributes in Table 68 that are relevant to this condition, namely the Alerting_Signal, Subject_Audible_Signal, Terminal_Display_Info, and Misc_Signaling_Information attributes. These attributes MUST be present in the Signal_Instance message generated per Condition 1 if the condition presented in the Comment column of the corresponding table row is met.

When the generation of the Signal_Instance message is due to Condition 2 in the above requirement, the Signal_Type attribute in Table 68 MUST be set to a value of "2". The value of "2" identifies the other attributes in Table 68 that are relevant to this condition, namely the Switch_Hook_Flash, Digits_Dialed and Misc_Signaling_Information attributes. These attributes MUST be present in the Signal_Instance message generated per Condition 2 if the condition presented in the Comment column of the corresponding table row is met.

Table 68. Signal_Instance Event Message for PCES

Attribute Name	Required or Optional	Comment
Event Message Header (Table 38)	R	The EM_Header MUST be present as the first attribute of the EM.
Signal_Type	R	1 = Network_Signal 2 = Subject_Signal
Signaled_To_Number	O	MUST be present if Signal_Type =1 MUST NOT be present if Signal_Type =2
Signaled_From_Number	O	MUST NOT be present if Signal_Type =1 MUST be present if Signal_Type =2
Alerting_Signal	O	MUST be present if Signal_Type =1 and the following signals are detected: r0,r1,r2,r3,r4,r5,r6,r7 rg rs wt1,wt2,wt3,wt4
Subject_Audible_Signal	O	MUST be present if Signal_Type =1 and the following signals are detected: bz cf dl mwi ot ro rt sl
Terminal_Display_Info	O	MUST be present if Signal_Type =1 and the following signals are detected: ci(ti,nu,na) vmwi
Switch_Hook_Flash	O	MUST be present if Signal_Type =2 and the following signals are detected: hf
Dialed_Digits	O	MUST be present if Signal_Type =2 and the following signals are detected: 0-9,*,#,A,B,C,D

Attribute Name	Required or Optional	Comment
Misc_Signaling_Information	O	MUST be present if the following signals are detected: 0-9,*,#,A,B,C,D (for Signal_Type 1) ft mt TDD

I.11 Terminal_Display_Info Attribute Structure

Table 69 describes the data structure of the Terminal_Display_Info attribute.

Table 69. Terminal_Display_Info Attribute Data Structure

Field Name	Semantics	Value Type	Length
Terminal_Display_Status_Bitmask	Bitmask describing structure contents (see Table 70)	Bit map	1 byte
General_Display	Used to report undefined display-related signals sent toward the surveillance subject. Field is populated with text that describes the signal.	Right justified, space padded ASCII character string	80 bytes
Calling_Number	Calling number information for Caller Id signal (ci/nu) that is displayed on the surveillance subject's terminal. Field is populated as follows: - If signal includes a calling number, value is number. - If signal indicates privacy ("P") for calling number, value is "private". - If signal indicates unavailability ("O") for calling number, value is "unavailable". - If signal does not include anything (number, "P" or "O") for calling number, Calling_Number field is not included in Terminal_Display_Info attribute.	Right justified, space padded ASCII character string	40 bytes
Calling_Name	Calling name information for Caller Id signal (ci/na) that is displayed on the surveillance subject's terminal. Field is populated as follows: - If signal includes a calling name, value is name. - If signal indicates privacy ("P") for calling name, value is "private". - If signal indicates unavailability ("O") for calling name, value is "unavailable". - If signal does not include anything (number, "P" or "O") for calling name, Calling_Name field is not included in Terminal_Display_Info attribute.	Right justified, space padded ASCII character string	40 bytes
Message_Waiting_Notif	Information for Visual message waiting indicator signal (vmwi). Field is populated as follows: - If indicator is turned on by signal, value is "VMWI ON". - If indicator is turned off by signal, value is "VMWI OFF".	Right justified, space padded ASCII character string	40 bytes

Table 70 describes the Terminal_Display_Status_Bitmask field of the Terminal_Display_Info attribute. Bits 0-3 describe the contents of the Terminal_Display_Info attribute fields. Each of these bits indicates the presence (bit=1) or absence (bit=0) of the named Terminal_Display_Info attribute field.

Table 70. Terminal_Display_Status_Bitmask

Bit	Semantics	Bit Count
0	General_Display	1
1	Calling_Number	1
2	Calling_Name	1
3	Message_Waiting_Notif	1
4	Reserved	1
5	Reserved	1
6	Reserved	1
7	Reserved	1

I.12 Conference_Party_Change

This Event Message is used by a CMS to report the change in the participants of a conference call. The CMS MUST generate this Event Message for a conference call that was initiated by the user under surveillance, when:

- The subject adds a third, or additional parties, to an existing to call to form a conference call.
- A party in a subject-initiated conference call is placed on hold.
- A party in a subject-initiated conference call is retrieved from hold.

When the subject adds a party, all the parties to the call (including the newly added party) are reported as communicating parties, and the newly added party is also reported as a joined party. When a party is placed on hold, all the remaining parties are reported as communicating parties, and the party on hold is reported as a removed party. When a party is retrieved from hold, all the parties (including the retrieved party) are reported as communicating parties, and the party retrieved from hold is also reported as a joined party. Multiple parties may be added, placed on hold, or retrieved from hold at the same time. All parties would be reported within the same Conference_Party_Change message. Note that the Signaling_Stop message is used to indicate when a party in a subject-initiated conference call is dropped, released, or otherwise disconnected from the conference call.

Example 1 - A (the subject) calls B, and A creates a conference that includes A, B and C. This Event Message is generated with A,B, and C listed as communicating parties, and C listed as the joined party.

Example 2 – A (the subject), B and C are in a conference created by A. When C goes on hold, this Event Message is generated with A and B listed as communicating parties and C listed as removed party.

Example 3 – A (the subject), B and C are in a conference created by A but C has gone on hold. When C joins the conference again, this Event Message is generated with A,B and C listed as communicated parties and C listed as joined party.

Table 71. Conference_Party_Change Event Message

Attribute Name	Required or Optional	Comment
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM. Within the EM_Header, the BCID MUST be one of the BCIDs associated with a call leg participating in the conference call.
Communicating_Party	O	This attribute MUST be included when known, to identify all communicating party identity(ies), when the conference is established by the intercept subject's service. This attribute may appear multiple times, one for each communicating party in the call. This attribute may appear independently or in combination with other attributes.

Attribute Name	Required or Optional	Comment
Joined_Party	O	This attribute MUST be included when known, to identify a communicating party identity(ies) when added to the conference established by the intercept subject's service. This attribute may appear multiple times, one for each added party. This attribute may appear independently or in combination with other attributes.
Removed_Party	O	This attribute MUST be included when known, to identify a previously communicating party identity(ies), when removed (e.g., placed on hold) from the conference established by the intercept subject's service. This attribute may appear multiple times, one for each removed party. This attribute may appear independently or in combination with other attributes.

I.13 Surveillance_Stop

Surveillance_Stop indicates the end of call content and/or call data. Generally, this will mean the end of a call. However, this can also indicate that call content and/or call data can no longer be intercepted (e.g., a call has been forwarded to another service provider's network and cannot be intercepted).

The CMS MUST timestamp this EM immediately upon:

1. The end of a call. A call has ended when a Signaling_Stop is sent for the call leg under surveillance and the call has not been redirected. The Surveillance_Stop_Type would be set to 1 "End of surveillance".
2. The CMS determining that surveillance cannot be started, or can no longer be performed. For example:
   - A call is redirected to a jurisdiction in which surveillance cannot be requested, a CMS may continue to perform call data surveillance, but not call content surveillance. In such a case, the CMS would send a Surveillance_Stop indicating that call content will end. The Surveillance_Stop_Type would be set to 2 "End of CCC only".
   - A call is redirected to a jurisdiction in which surveillance cannot be requested, and CMS will no longer be part of the call path. In such a case, the call has not ended, but the CMS would still send a Surveillance_Stop indicating that both call content and call data surveillance will end. The Surveillance_Stop_Type would be set to 1 "End of surveillance".

Generally, a DF that receives a Surveillance_Stop will be part of a "chain" of DFs (for more information, refer to Section 10.6) that are responsible for forwarding call data and call content down the chain. A chain is established when the CMS has already sent a Signaling_Start with the Electronic_Surveillance_Indication attribute. In this case, the Electronic_Surveillance_Indication attribute MUST NOT be included in the Surveillance_Stop. However, under certain scenarios a CMS may send a Surveillance_Stop to its DF even though the DF is not part of the surveillance chain being stopped. In this case, the CMS MUST include the Electronic_Surveillance_Indication attribute in the Surveillance_Stop EM to identify the remote surveillance session that is to be stopped. For example, consider the case where a CMS receives a SIP Redirect with a request to perform surveillance, and the redirect is to a jurisdiction in which surveillance cannot be performed. In such a scenario, the CMS would send a Surveillance_Stop to its DF, and the DF would then forward the Surveillance_Stop EM to the appropriate DF based on the information in the Electronic_Surveillance_Indication attribute. Note that in this scenario the BCID in the EM_Header would not be bound to the remote surveillance session being stopped; therefore the Electronic_Surveillance_Indication attribute is required in order to ensure the Surveillance_Stop EM is forwarded to the appropriate DF.

Table 72. Surveillance_Stop Event Message for PCES

Attribute Name	Required or Optional	Comments
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Surveillance_Stop_Type	R	1 = End of surveillance (CDC and, if present, CCC) 2 = End of CCC only (CDC will continue)
Surveillance_Stop_Destination	O	In certain CMSS scenarios, a CMS may continue to perform surveillance on a local subject, but can no longer perform surveillance (call content and/or call data) on behalf of another CMS. This parameter indicates to the DF which subject (local and/or remote) the Surveillance_Stop EM applies to. 1 = Surveillance_Stop applies to local surveillance only 2 = Surveillance_Stop applies to both local and remote surveillance 3 = Surveillance_Stop applies only to remote surveillance
Electronic_Surveillance_Indication	O	This structure MUST be included when the local DF is not part of the DF chain (i.e., the CMS has not established a DF chain by not including the Electronic_Surveillance_Indication attribute in a Signaling_Start EM). This structure MUST NOT be included when the local DF is part of the DF chain (i.e., the CMS has established a DF chain by including the Electronic_Surveillance_Indication attribute in a Signaling_Start EM).

I.14 Redirection

The Redirect Event Message allows the DF to generate the Redirection ESP Message for those cases where a Service_Instance Event Message is not reported from the CMS to the DF. The Redirection message MUST be sent to the DF if a call involving a surveillance subject is redirected, and:

- The CMS is aware of the redirection
- No Service_Instance is generated for the redirection.

The CMS is aware of the redirection as a result of the following triggers:

- The subject or associate is on the same CMS that is responsible for the surveillance and that party initiates a redirection via a call transfer.
- The subject or associate is on the same CMS that is responsible for the surveillance and call forwarding is activated for that party.
- The CMS responsible for the surveillance receives a CMSS 302 REDIRECT indicating that the call has been forwarded at a remote CMS.
- The CMS responsible for the surveillance receives a CMSS REFER indicating that the call has been transferred at a remote CMS.

Table 73. Redirection Event Message for PCES

Attribute Name	Required or Optional	Comments
EM_Header (see Table 38)	R	The EM_Header attribute MUST be present as the first attribute of the EM.
Related_Call_Billing_Correlation_ID (See Table 39)	O	Included when the redirected call will be identified by a different Call_ID in future CDC messages.
Redirected_From_Party_Number	O	Identifies the redirected-from party. This field MUST be included when the subject is performing the redirection.
Redirected_To_Party_ Number	R	Identifies the redirected-to party (forwarded-to or trasferred-to party)
Carrier_Identification_Code	O	Included when a transit carrier is used to transport the redirected call and the carrier information is available to the CMS