



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-2 2009

IPCablecom 1.5 Part 2: Audio/Video Codecs

NOTICE

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

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

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

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

All Rights Reserved

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

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

Contents

1	SCOPE.....	1
1.1	INTRODUCTION AND OVERVIEW	1
1.2	PURPOSE OF THE DOCUMENT.....	1
1.3	ORGANIZATION OF DOCUMENT	1
1.4	REQUIREMENTS SYNTAX	2
1.5	PHASING OF REQUIREMENTS	2
2	REFERENCES	3
2.1	NORMATIVE REFERENCES	3
2.2	INFORMATIVE REFERENCES	4
2.3	REFERENCE ACQUISITION.....	5
3	TERMS AND DEFINITIONS	6
4	ABBREVIATIONS AND ACRONYMS.....	10
5	BACKGROUND.....	16
5.1	IPCABLECOM VOICE COMMUNICATIONS QUALITY REQUIREMENTS	16
5.2	NETWORK PREPARATION FOR CODEC SUPPORT	16
5.2.1	<i>Packet Loss Control.....</i>	<i>16</i>
5.2.2	<i>Latency Control</i>	<i>16</i>
5.2.3	<i>Codec Transcoding Minimization.....</i>	<i>18</i>
5.2.4	<i>Bandwidth Minimization.....</i>	<i>18</i>
6	DEVICE REQUIREMENTS FOR AUDIO CODEC SUPPORT.....	19
6.1	DYNAMIC UPDATE CAPABILITY	19
6.2	MAXIMUM SERVICE OUTAGE	19
6.3	MINIMUM PROCESSING CAPABILITY	19
6.4	MINIMUM AUDIO CODEC STORAGE CAPABILITY	20
7	AUDIO CODECS SPECIFICATIONS.....	21
7.1	FEATURE SUPPORT	21
7.1.1	<i>DTMF Support.....</i>	<i>21</i>
7.1.2	<i>Fax and Modem Support.....</i>	<i>21</i>
7.1.3	<i>Echo Compensation Support.....</i>	<i>22</i>
7.1.4	<i>Asymmetrical Services Support.....</i>	<i>22</i>
7.1.5	<i>Hearing-impaired Services Support</i>	<i>22</i>
7.1.6	<i>A-law and μ-law Support.....</i>	<i>23</i>
7.1.7	<i>Packet Loss Concealment.</i>	<i>23</i>
7.1.8	<i>Fax Relay.....</i>	<i>23</i>
7.1.9	<i>DTMF Relay</i>	<i>24</i>
7.1.10	<i>V.152 Transmission</i>	<i>25</i>
7.1.11	<i>Security Considerations.....</i>	<i>27</i>
7.2	MANDATORY CODECS.....	27
7.2.1	<i>G.711</i>	<i>27</i>
7.3	RECOMMENDED CODECS.....	27
7.3.1	<i>iLBC.....</i>	<i>27</i>
7.3.2	<i>BV16</i>	<i>27</i>
7.4	OPTIONAL CODECS.....	28
7.4.1	<i>G.728</i>	<i>28</i>
7.4.2	<i>G.729 Annex E.....</i>	<i>28</i>
7.4.3	<i>G.722</i>	<i>28</i>

7.5	OPTIONAL FEATURES	28
7.5.1	Wideband Codecs	28
7.5.2	Optional Codecs	28
7.5.3	Voice Activity Detection (VAD)	28
7.6	SESSION DESCRIPTION OF CODECS	28
7.6.1	iLBC Session Description	32
7.6.2	BV16 Session Description.....	33
7.6.3	G.722 Session Description.....	33
8	VIDEO REQUIREMENTS	34
8.1	OVERVIEW.....	34
8.2	IPCABLECOM VIDEO DEVICES	34
8.3	VIDEO ENCODER REQUIREMENTS	34
8.4	VIDEO FORMAT REQUIREMENTS	34
8.5	H.263 ANNEXES	36
8.6	MULTIPOINT CONFERENCING SUPPORT.....	38
8.6.1	Freeze Picture Request.....	38
8.6.2	Fast Update Request.....	38
8.6.3	Freeze Picture Release	38
8.6.4	Continuous Presence Multipoint (CPM).....	38
8.7	SIGNALING MESSAGES	39
9	RTP AND RTCP USAGE	41
9.1	RTP REQUIREMENTS	41
9.2	RTCP REQUIREMENTS	41
9.2.1	General Requirements of the IPCablecom RTCP Profile.....	41
9.2.2	Security Requirements for RTP and RTCP in IPCablecom	42
9.2.3	Extended RTCP Reports	42
	APPENDIX A. CODEC COMPARISON TABLES	48

LIST OF TABLES

TABLE 1. - FRAME SIZES OF THE CODECS.....	17
TABLE 2. - MTA PROCESSING CAPABILITY	19
TABLE 3. - CODEC RTP MAP PARAMETERS	29
TABLE 4. - MAPPING OF SESSION DESCRIPTION PARAMETERS TO RSVP FLOWSPEC.....	30
TABLE 5. - NUMBER OF PIXELS PER LINE AND NUMBER OF LINES FOR EACH PICTURE FORMAT	35
TABLE 6. - H. - 263 ANNEXES AND THEIR APPLICABILITY TO IPCABLECOM	38
TABLE 7. - H.245 COMMANDS THAT ARE APPLICABLE TO IPCABLECOM	39
TABLE 8. - METRICS RELATED TO PACKET LOSS AND DISCARD.....	43
TABLE 9. - METRICS RELATED TO DELAY.....	43
TABLE 10. - METRICS DUE TO SIGNAL	44
TABLE 11. - METRICS RELATED TO CALL QUALITY.....	45
TABLE 12. - IE AND BPL PARAMETERS FOR IPCABLECOM VOCODERS.....	45
TABLE 13. - PARAMETERS RELATED TO ENDPOINT CONFIGURATION	47
TABLE 14. - ITU IETF AND CABLELABS SPEECH CODERS.....	48
TABLE 15. - NORTH AMERICAN WIRELESS SPEECH CODERS.....	49
TABLE 16. - BANDWIDTH ATTRIBUTES OF CODECS.....	50

1 SCOPE

This document addresses interfaces between IPCablecom client devices for audio and video communication. Specifically, it identifies the audio and video codecs necessary to provide the highest quality and the most resource-efficient service delivery to the customer. This document also specifies the performance required in client devices to support future IPCablecom codecs. Additionally, this document describes a suggested methodology for optimal network support for codecs.

1.1 Introduction and Overview

The quality of audio and video delivered over the IPCablecom architecture will depend on multiple factors: the end device performance, the network's inherent quality, and the intelligence of the system resource allocation policy. This document defines mandated codecs and capabilities supporting audio and video applications, with a particular emphasis on the stringent requirements of IP-based voice communications.

Acceptable voice communications functionality imposes strict latency and packet-loss criteria on IP implementations and will thus stress system resources, particularly if bandwidth becomes congested or saturated. Video applications — while more forgiving to dropped packets and latency — require bandwidth of at least an order of magnitude more than audio applications. The IPCablecom architecture is designed to support both types of applications simultaneously.

Speech and video compression are evolving technologies. New algorithms are being enabled as more sophisticated and higher performing processors become available at lower cost. Additionally, the system infrastructure and mechanisms for allocating resources will evolve. Due to this dynamism, the priority in designing the architecture is to define a robust system to accommodate evolving technology without creating a legacy burden.

Therefore, the IPCablecom philosophy is to establish cost-effective envelopes for network and device performance to enable the most appropriate current technology, while allowing upgrades as technology and market needs evolve. To address near-term market needs, this document also specifies codec and performance mandates to deliver the quality-of-service necessary for launching competitive services.

1.2 Purpose of the Document

The purpose of this document is to extend the existing IPCablecom 1.0 Codec specification by introducing two new low-bit codecs, ITU-T T.38 fax relay for reliable fax transmission, IETF RFC 2833 DTMF Relay for reliable DTMF transmission, and metrics to measure voice quality. It is issued to facilitate design and field-testing leading to the manufacturability and interoperability of conforming hardware and software by multiple vendors.

1.3 Organization of Document

This document covers the following major topics:

- Network issues affecting and influenced by codecs, along with a discussion of codec implications on network design (Section 5).
- Client device requirements necessary to support codecs (Section 6).
- Audio codec specifications (Section 7).
- Video codec requirements and specifications (Section 8).
- RTP and RTCP usage (Section 9).

1.4 Requirements Syntax

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 specification 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 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. These differences may be significant for legal/regulatory purposes.

1.5 Phasing of Requirements

The codec requirements contained in this specification cover both audio and video Multimedia Terminals (MTAs) and Trunking Gateways (Media Gateway). The term MTA-2 is used to define a terminal supporting video.

In the initial phase of IPCablecom, MTAs are not required to support the MTA-2 requirements as defined in Section 8 of this specification. MTAs **MUST** support the requirements for audio terminals as defined in Sections 5, 6, 7, and 9.

Support for video terminals will be **REQUIRED** in later phases of IPCablecom. All MTA-2s **MUST** support the requirements defined in Section 8.

2 REFERENCES

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

2.1 Normative References

- [1] SCTE 165-1 2009, IPCablecom 1.5 Part 1: Architecture Framework.
- [2] SCTE 165-4 2009, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.
- [3] SCTE 165-3 2009, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.
- [4] ANSI T1.521-1999, A Packet Loss Concealment Technique for Use with ITU-T Recommendation G.711.
- [5] IMTC Voice-Over-IP Forum Service Interoperability Implementation Agreement 1.0, dated December 1, 1997.
- [6] "Current Methods of Speech Coding." R.V. Cox. *International Journal of High Speed Electronics & Systems*, Vol 8, No 1 (1997) pp 13–68.
- [7] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January 1996.
- [8] IETF RFC 2327, SDP: Session Description Protocol, April 1998.
- [9] IETF RFC 0821, Simple Mail Transfer Protocol, August 1982.
- [10] IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, February 1997.
- [11] IETF RFC 1945, Hypertext Transfer Protocol -- HTTP/1.0, May 1996.
- [12] IETF RFC 2068, Hypertext Transfer Protocol -- HTTP/1.1, January 1997.
- [13] IETF RFC 3435, Media Gateway Control Protocol (MGCP) Version 1.0, January 2003.
- [14] IETF RFC 2138, Remote Authentication Dial In User Service (RADIUS), April 1997.
- [15] IETF RFC 2139, RADIUS Accounting, April 1997.
- [16] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996.
- [17] ITU-T Recommendation G.711, Pulse Code Modulation (PCM) Of Voice Frequencies, November 1988.
- [18] ITU-T Recommendation G.165, Echo Cancellers, March 1993.
- [19] ITU-T Recommendation G.168, Digital Network Echo Cancellers, June 2002.
- [20] ITU-T Recommendation T.38, Procedures for Real-Time Group 3 Facsimile Communication over IP Networks, April 2004.
- [21] ITU-T Recommendation V.18, Operational and Interworking Requirements for DCEs Operating in the Text Telephone Mode, November 2000.
- [22] ITU-T Recommendation G.728, Coding of Speech at 16 kbit/S Using Low-Delay Code Excited Linear Prediction, September 1992.
- [23] ITU-T Recommendation G.729 Annex E, Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP) 11.8 kbit/s CS-ACELP speech coding algorithm, September 1998.
- [24] IETF RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Signals, May 2000.
- [25] Telcordia, "LSSGR: Signaling for Analog Interfaces", Generic Requirements Gr-506–Core Issue 1 June 1996, Revision 1 November 1996, Morristown, New Jersey.

-
- [26] SIA DC-05-1999.09, Digital Communication Standard - Ademco ® Contact ID Protocol - for Alarm System Communications, Security Industry Association Copyright 1999, Ademco Group Publication Order Number: 14085.
 - [27] ETSI ES 201 235-2 V1.2.1 (2002-05) ETSI Standard "Access and Terminals (AT); Specification of Dual-Tone Multi-Frequency (DTMF) Transmitters and Receivers; Part 2: Transmitters."
 - [28] ETSI ES 201 235-3 V1.2.1 (2002-05) ETSI Standard "Access and Terminals (AT); Specification of Dual-Tone Multi-Frequency (DTMF) Transmitters and Receivers; Part 3: Receivers."
 - [29] IETF RFC 3611 Real Time Control Protocol Extended Reports (RTCP XR), T. Friedman et al., November 2003.
 - [30] ITU Recommendation P.56, Objective Measurement of Active Speech Level, March 1993.
 - [31] ITU Recommendation P.561, In-Service, Non-Intrusive Measurement Device, 1996.
 - [32] ITU Recommendation G.107, The E Model, a computational model for use in transmission planning, May 2003.
 - [33] ITU Recommendation P.862, Perceptual Estimation of Speech Quality (PESQ), an objective method for end-to-end speech quality assessment of narrowband telephone networks and speech codecs, February 2001.
 - [34] IETF RFC 3952, Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech, December 2004.
 - [35] IETF RFC 3951, Internet Low Bit Rate Codec (iLBC), December 2004.
 - [36] iLBC Speech Codec Fixed Point Reference Code for PacketCable, Version 1.0.3, October 2003. (For further information, contact PacketCable, Cable Television Laboratories, Inc.)
 - [37] IETF RFC 4298, RTP Payload Format for BroadVoice Speech Codecs, December 2005.
 - [38] ANSI/SCTE 24-21 2006, BV16 Speech Codec Specification for Voice over IP Applications in Cable Telephony.
 - [39] ITU-T Recommendation V.152, Procedures for supporting Voice-Band Data over IP Networks, January 2005.
 - [40] IETF RFC 2198, RTP Payload for Redundant Audio Data, September 1997.
 - [41] IETF RFC 3407, Session Description Protocol (SDP) Simple Capability Declaration, October 2002.
 - [42] ITU-T Recommendation G.722, 7 kHz audio-coding within 64 kbit/s, November 1988.
 - [43] ITU-T Recommendation G.722 Appendix III, A High Quality Packet Loss Concealment Algorithm for G.722.
 - [44] ITU-T Recommendation G.722 Appendix IV, A Low-Complexity Algorithm for Packet Loss Concealment with G.722.
 - [45] ITU-T Recommendation G.711 Appendix II, A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems, February 2000.

2.2 Informative References

This document uses the following informative references.

- [46] SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.
- [47] SCTE 165-9 2009, IPCablecom 1.5 Part 9: Event Messages.
- [48] SCTE 165-5 2009, IPCablecom 1.5 Part 5: MTA Device Provisioning.
- [49] SCTE 165-12 2009, IPCablecom 1.5 Part 12: PSTN Gateway Call Signaling Protocol Specification.
- [50] SCTE 165-17 2009, IPCablecom 1.5 Part 17: Audio Server Protocol.

-
- [51] ITU-T Recommendation G.729 Annex A, Reduced Complexity 8 kbit/s CS-ACELP Speech Codec, November 1996.
 - [52] ITU-T Recommendation H.243, Procedures for establishing communication between three or more audiovisual terminals using digital channels up to 1920 kbit/s, February 2000.
 - [53] ITU-T Recommendation H.245, Control protocol for multimedia communication, July 2003.
 - [54] ITU-T Recommendation H.261, Video codec for audiovisual services at p x 64 kbit/s, March 1993.
 - [55] ITU-T Recommendation H.263, Video coding for low bit rate communication, February 1998.
 - [56] ITU-T Recommendation H.323, Packet-based multimedia communications systems, July 2003.
 - [57] ITU-T Recommendation H.324, Terminal for low bit-rate multimedia communication, March 2002.

2.3 Reference Acquisition

- ATIS Document center: www.atis.org
- ETSI Standards: www.etsi.org/services_products/e-shop/home.htm.
- Internet Engineering Task Force (IETF) Secretariat, 46000 Center Oak Plaza, Sterling, VA 20166, Phone +1-571-434-3500, Fax +1-571-434-3535, <http://www.ietf.org>.
- ITU-T Recommendations: www.itu.int/ITU-T/publications/recs.html.
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; <http://www.cablelabs.com>.
- Telcordia: http://www.telcordia.com/services/testing/lab_access/gr-listing.html.
- Security Industry Association: www.siaonline.org.

3 TERMS AND DEFINITIONS

This document uses 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 the permission to have the access.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set, which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.
Confidentiality	A way to ensure that information is not disclosed to any one 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 head-end toward the subscriber location.
Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.

Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU.
Errored Second	Any 1-sec interval containing at least one bit error.
Event Message	Message capturing a single portion of a connection.
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 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 ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Gateway	Devices bridging between the IP/Cablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway which sends and receives circuit switched network signaling to the edge of the IP/Cablecom network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T H.245 protocol for communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local and 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.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
On-Net Call	A communication placed by one customer to another customer entirely on the IPCablecom Network.
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 any one 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 source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.

Systems Management	Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.
Transit Delays	The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch 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 head-end.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

4 ABBREVIATIONS AND ACRONYMS

This document uses 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.
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 head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
Codec	COder-DECoder
COPS	Common Open Policy Service Protocol. Defined in RFC 2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS configuration file.

CSR	Customer Service Representative
DA	Directory Assistance
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard
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.
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. See [2].
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.
FEC	Forward Error Correction
ETSI	European Telecommunications Standards Institute
FEID	Financial Entity ID
FGD	Feature Group D signaling
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated".
FQDN	Fully Qualified Domain Name. Refer to [9] for details.
GTT	Global Title Translation
HFC	Hybrid Fiber/Coaxial cable. An HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the head-end 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 [10].
HTTP	Hypertext Transfer Protocol. Refer to [11] and [12].
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.
IC	Inter-exchange Carrier
ICMP	Internet Control Message Protocol. An extension to the Internet Protocol, ICMP supports packets containing error, control, and information messages.
IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used on the Internet.
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 X509 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
ISP	Internet Service Provider
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 Telecommunications Union–Telecommunications Standardization Sector
IVR	Interactive Voice Response System
KDC	Key Distribution Center
LATA	Local Access and Transport Area
LD	Long Distance
LIDB	Line Information Database. Contains information on customers 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.
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.
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.
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 IP/Cablecom and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF RFC [13].
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 head-end 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, 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 Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture. This layer provides services to establish a path between open systems.
Network Layer	
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)
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.
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