

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-01 2019

**IPCablecom 1.5 Part 1: Architecture Framework Technical
Report**

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

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

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

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

All Rights Reserved

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

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

Table of Contents

1	INTRODUCTION	6
1.1	IPCablecom Overview	6
1.2	IPCablecom Motivation	6
1.3	IPCablecom Project Phasing	6
2	NORMATIVE REFERENCES	8
2.1	<i>SCTE References</i>	<i>8</i>
2.2	<i>Standards from Other Organizations</i>	<i>8</i>
2.3	<i>Published Materials</i>	<i>8</i>
3	INFORMATIVE REFERENCES	9
3.1	SCTE References	9
3.2	Standards from Other Organizations	9
3.3	Published Materials	10
4	TERMS AND DEFINITIONS	11
5	ABBREVIATIONS AND ACRONYMS	15
6	IPCABLECOM 1.5	21
6.1	IPCablecom Architecture Framework	22
6.2	IPCablecom Zones and Domains	23
6.3	IPCablecom 1.5 Analog Trunking Specifications	23
6.4	IPCablecom 1.5 Design Considerations	24
6.4.1	<i>General Architectural Goals</i>	<i>24</i>
6.4.2	<i>Call Signaling</i>	<i>25</i>
6.4.3	<i>Quality of Service</i>	<i>25</i>
6.4.4	<i>CODEC and Media Stream</i>	<i>26</i>
6.4.5	<i>Device Provisioning and OSS</i>	<i>26</i>
6.4.6	<i>Security</i>	<i>26</i>
6.4.7	<i>Electronic Surveillance</i>	<i>26</i>
7	IPCABLECOM FUNCTIONAL COMPONENTS	27
7.1	Multimedia Terminal Adapter (MTA)	27
7.1.1	<i>MTA Functional Requirements</i>	<i>27</i>
7.1.2	<i>MTA Attributes</i>	<i>28</i>
7.2	Cable Modem (CM)	28
7.3	HFC Access Network	28
7.4	Cable Modem Termination System (CMTS)	29
7.4.1	<i>CMTS Gate</i>	<i>29</i>
7.5	Call Management Server (CMS)	29
7.6	PSTN Gateway	30
7.6.1	<i>Media Gateway Controller (MGC)</i>	<i>30</i>
7.6.2	<i>Media Gateway (MG)</i>	<i>31</i>
7.6.3	<i>Signaling Gateway (SG)</i>	<i>31</i>
7.7	OSS Back Office Components	31
7.7.1	<i>Security Server – Key Distribution Center (KDC)</i>	<i>32</i>
7.7.2	<i>Dynamic Host Configuration Protocol Server (DHCP)</i>	<i>32</i>
7.7.3	<i>Domain Name System Server (DNS)</i>	<i>32</i>
7.7.4	<i>Trivial File Transfer Protocol Server or Hypertext Transfer Protocol Server (TFTP or HTTP)</i>	<i>32</i>
7.7.5	<i>SYSLOG Server (SYSLOG)</i>	<i>32</i>
7.7.6	<i>Record Keeping Server (RKS)</i>	<i>32</i>
7.8	Announcement Server (ANS)	32
7.8.1	<i>Announcement Controller (ANC)</i>	<i>32</i>

7.8.2	<i>Announcement Player (ANP)</i>	33
8	PROTOCOL INTERFACES	34
8.1	Call Signaling Interfaces.....	34
8.1.1	<i>Network-based Call Signaling (NCS) Framework</i>	35
8.1.2	<i>PSTN Signaling Framework</i>	35
8.1.3	<i>CMS to CMS Signaling Framework</i>	36
8.2	Media Streams.....	36
8.2.1	<i>Real-time Transport Control Protocol (RTCP)</i>	38
8.3	MTA Device Provisioning.....	38
8.4	SNMP Element Management Layer Interfaces.....	39
8.5	Event Messages Interfaces.....	39
8.5.1	<i>Event Message Framework</i>	39
8.6	Quality of Service (QoS).....	41
8.6.1	<i>QoS Framework</i>	41
8.6.2	<i>Dynamic Quality of Service</i>	43
8.7	CMS Subscriber Provisioning.....	43
8.8	Electronic Surveillance.....	45
8.9	Security.....	46
8.9.1	<i>Overview</i>	46
8.9.2	<i>Device Provisioning Security</i>	49
9	NETWORK DESIGN CONSIDERATIONS	51
9.1	Time Keeping and Reporting Issues.....	51
9.2	Timing for Playout Buffer Alignment with Coding Rate.....	51
9.3	IP Addressing.....	51
9.4	Dynamic IP Address Assignment.....	51
9.5	Fully Qualified Domain Name (FQDN) Assignment.....	52
9.6	Priority Marking of Signaling and Media Stream Packets.....	52
9.7	Fax Support.....	52
9.8	Analog Modem Support.....	53
9.9	DTMF Relay.....	53

List of Figures

Figure 1. IPCablecom Reference Architecture	22
Figure 2. Zones and Administrative Domains	23
Figure 3. IPCablecom Component Reference Model	27
Figure 4. E-MTA Conceptual Functional Architecture	28
Figure 5. Call Signaling Interfaces	34
Figure 6. RTP Media Stream Flows in a IPCablecom Network	36
Figure 7. RTP Packet Format	37
Figure 8. IPCablecom Provisioning Interfaces	38
Figure 9. Representative Event Messages Architecture.....	40
Figure 10. Event Message Interfaces.....	40
Figure 11. IPCablecom QoS Interfaces	41
Figure 12. CMS Subscriber Provisioning Interfaces	44
Figure 13. Electronic Surveillance Interfaces.....	45
Figure 14. IPCablecom Security Interfaces	47

List of Tables

Table 1. IPCablecom 1.5 Specifications and Reports	23
Table 2. Call Signaling Interfaces	34
Table 3. RTP Media Stream Flows.....	37
Table 4. Device Provisioning Interfaces.....	39
Table 5. Event Message Interfaces	40
Table 6. QoS Interfaces	41
Table 7. QoS Interfaces	42
Table 8. CMS Subscriber Provisioning Interfaces.....	44
Table 9. Electronic Surveillance Interfaces	46
Table 10. Security Interfaces	48

1 INTRODUCTION

1.1 IPCablecom Overview

IPCablecom is a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies. The IPCablecom project defines interface specifications that can be used to develop interoperable equipment capable of providing packet-based voice, video and other high-speed multimedia services over hybrid fiber coax (HFC) cable systems utilizing the DOCSIS® protocol [14]. Any reference to DOCSIS in this document is understood to be DOCSIS version 1.1 or later.

IPCablecom defines a communication services architecture that overlays the two-way data-ready broadband cable access network. Within the overall IPCablecom framework, IPCablecom version 1.5, which is the subject of this Technical Report, is designed to provide digital voice and telephony services.

The objective of this IPCablecom Architecture Technical Report is to provide a high-level reference framework that identifies the functional components and defines the interfaces necessary to implement the capabilities detailed in the individual IPCablecom 1.5 specifications as listed in Section 6.3.

1.2 IPCablecom Motivation

The emergence of the Internet Protocol (IP¹) as the standard transport for packet data networks has enabled a revolution in communications services and applications. This online revolution is demonstrated by the widespread use of email, chat groups, music, video, and the explosive growth of the World Wide Web for entertainment, information exchange, online commerce, and a wide range of new and innovative services. New classes of IP-based information appliances are also emerging, including multimedia personal computers, IP-based set top boxes, and IP-based voice and videophones.

In recent years the growth of a worldwide IP-based data network, coupled with the rapid growth in the number of households that have online access, have resulted in an environment that allows service providers to offer integrated voice and data services over a common broadband cable access network and IP transport backbone. While the initial application of Voice over IP (VoIP) technology was for toll bypass services (particularly high-cost international toll service) the technology is now sufficiently mature that it is feasible to offer IP-based voice communication services similar to those offered by telecommunications carriers on the Public Switched Telephone Network (PSTN).

With the success of the DOCSIS standardization effort, the Quality of Service (QoS) enhancements of DOCSIS, and the acceleration of major cable system upgrades for two-way capability, the infrastructure is in place for development and deployment of packetized voice and video applications. These applications can be deployed with limited incremental cost, providing a technically distinctive and cost-effective alternative for subscribers' voice communications needs, as well as a platform for introducing the next generation of voice and other real-time multimedia services.

1.3 IPCablecom Project Phasing

The IPCablecom architecture is designed to be a robust, complete, end-to-end broadband architecture that supports voice, video, and other multimedia services. The architecture is capable of supporting millions of subscribers over multiple cable operator networks.

It is understood that the initial focus of the IPCablecom architecture must support the time-to-market business considerations of parties interested in deploying packet-based services. Going forward, the IPCablecom architecture must continue to evolve to meet Member business requirements and to accommodate advances resulting from the maturing of IP-based technology. The IPCablecom project will release specifications that define this architecture in a phased approach according to technical feasibility and business priority. As new IPCablecom specifications are released, they will complement the previously released specifications.

From time to time, this document refers to the voice communications capabilities of a 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

¹ IPCablecom 1.5 supports only IPv4.

addresses, or is intended to affect, those issues. In particular, while this document uses standard terms such as "call," "call flow," "telephony," etc., it should be recalled that while a IP-Cablecom network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, 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 architectures, each potentially with different associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this term.

2 NORMATIVE REFERENCES

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document 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 SCTE References

- No normative references are applicable.

2.2 Standards from Other Organizations

- No normative references are applicable.

2.3 Published Materials

- No normative references are applicable.

3 INFORMATIVE REFERENCES

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

3.1 SCTE References

- [1] ANSI/SCTE 165-02 2016, IPCablecom 1.5 Part 2: Audio/Video Codecs.
- [2] ANSI/SCTE 165-04 2019, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.
- [3] ANSI/SCTE 165-03 2016, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.
- [4] ANSI/SCTE 165-09 2019, IPCablecom 1.5 Part 9: Event Messaging.
- [5] ANSI/SCTE 165-07 2019, IPCablecom 1.5 Part 7: MTA MIB.
- [6] ANSI/SCTE 165-08 2019, IPCablecom 1.5 Part 8: Signaling MIB.
- [7] ANSI/SCTE 165-06 2019, IPCablecom 1.5 Part 6: MIBS Framework.
- [8] ANSI/SCTE 165-12 2016, IPCablecom 1.5 Part 12: PSTN Gateway Call Signaling Protocol.
- [9] ANSI/SCTE 165-05 2019, IPCablecom 1.5 Part 5: Media Terminal Adapter (MTA) Device Provisioning.
- [10] ANSI/SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.
- [11] ANSI/SCTE 165-18 2016, IPCablecom 1.5 Part 18: CMS to CMS Signaling.
- [12] ANSI/SCTE 165-19 2019, IPCablecom 1.5 Part 19: CMS Subscriber Provisioning Specification.
- [13] ANSI/SCTE 165-13 2019, IPCablecom 1.5 Part 13: Electronic Surveillance Standard.
- [14] ANSI/SCTE 23-01 2017, DOCSIS 1.1 Part 1: Radio Frequency Interface.

3.2 Standards from Other Organizations

- [15] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Application, January 1996.
- [16] IETF RFC 2327, SDP: Session Description Protocol, IETF RFC 2327, April 1998.
- [17] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.
- [18] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January 1996.
- [19] IETF RFC 1119, Network Time Protocol, September 1989.
- [20] IETF RFC 2748, The COPS (Common Open Policy Service) Protocol, January 2000.
- [21] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.
- [22] IETF RFC 2866, RADIUS Accounting, June 2000.
- [23] IETF RFC 3260, New Terminology and Clarifications for Diffserv, April 2002.
- [24] IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- [25] IETF RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP, September 2001.
- [26] IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.
- [27] IETF RFC 3611, RTP Control Protocol Extended Reports (RTCP XR), November 2003.
- [28] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
- [29] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.

- [30] IETF RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000.
- [31] IETF RFC 3435, Media Gateway Control Protocol (MGCP) Version 1.0, January 2003.
- [32] ITU-T Recommendation T.38, Procedures for Real-Time Group 3 Facsimile Communication over IP Networks, April 2004.
- [33] ITU-T Recommendation G.711, Pulse Code Modulation (PCM) Of Voice Frequencies, November 1988.
- [34] Telcordia GR909, Generic Criteria for Fiber in the Loop Systems, December 2004.
- [35] ITU-T Recommendation V.152, Procedures for supporting Voice-Band Data over IP Networks, January 2005.

3.3 Published Materials

- No normative references are applicable.

4 TERMS AND DEFINITIONS

This standard 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".
Announcement Server	See Audio Server.
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server also known as Announcement Server plays informational announcements in IPCablecom network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user. It is a logical entity consisting of Media Player (MP) and Media Player Controller (MPC).
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 that 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.
Codec	COder-DECoder
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.
Cryptoanalysis	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
Diffserv	(a.k.a. Differentiated Services), an IETF architecture for implementing scalable service differentiation in the Internet. Refer to IETF RFC 3260.

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 call 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 [IP Flow]	A unidirectional sequence of packets identified by ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow"). A unidirectional sequence of packets associated with a SID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Gateway	Devices bridging between the IP/Cablecom IP Telephony 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 calls for the use of the H.225/H.245 protocol for call 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 call
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.

Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
Media Player	Media Player (MP) is responsible for receiving and interpreting commands from the Media Player Controller and for delivering appropriate announcement(s) to the MTA.
Media Player Controller	Media Player Controller (MPC) initiates and manages all announcement services provided by the media player.
Network Management	The functions related to the management of data across the network.
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	Call connecting a IPCablecom subscriber out to a user on the PSTN
On-Net Call	Call placed by one customer to another customer entirely on the IPCablecom Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to 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 there by eliminating a host from having to support the services themselves.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key which can decrypt messages sent encrypted by the user's public key.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
Root Private Key	The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.

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

5 ABBREVIATIONS AND ACRONYMS

The suite of IPCablecom standards uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
AF	Assured Forwarding. A Diffserv Per Hop Behavior.
AH	Authentication header is 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)
AT	Access Tandem. A switching point in PSTN networks that allows access to an entire calling area.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 or later standard which runs on the MAC layer.
CBC	Cipher block chaining mode is 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.
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. In this specification "Call Agent" is part of the CMS that maintains call state, and controls the line side of calls.
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. A coding format for digital signals.
CIR	Committed Information Rate.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax
CMS	Call Management Server. Controls the audio call connections. Also called a Call Agent in MGCP terminology.
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.
COPS	Common Open Policy Service. Defined in IETF RFC 2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS 1.0 configuration file.
CSR	Customer Service Representative

DA	Directory Assistance
DE	Default. A Diffserv Per Hop Behavior.
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default - Network Provider DHCP server
DNS	Domain Name System
DSCP	Differentiated Services Code Point. A field in every IP packet header which 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 IETF RFC 3260.
DOCSIS	Data Over Cable System Interface Specification.
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, i.e., assigned on the fly for each call depending on the QoS requested
DTMF	Dual-Tone Multi Frequency (tones)
EF	Expedited Forwarding. A Diffserv Per Hop Behavior.
E-MTA	Embedded MTA – a single node which contains both an MTA and a cable modem.
EO	End Office. A switching point in the PSTN Local Exchange Carrier network that directly connects to subscriber access lines.
ESP	IPsec Encapsulation Security Payload protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute
FGD	Feature Group D signaling. A type of circuit used for exchanging traffic with a PSTN LEC network.
FQDN	Fully Qualified Domain Name.
HFC	Hybrid Fiber/Coaxial cable, 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.
HTTP	Hyper Text Transfer Protocol.
IANA	Internet Assigned Numbers Authority. See http://www.iana.org for details.
IC or IXC	Inter-exchange Carrier. A long distance carrier.
IETF	Internet Engineering Task Force. A standards body responsible, among other things, for developing standards used in the Internet.
IKE	Internet Key Exchange is 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, which requires digital certificates for authentication.
IntraLATA	Within a Local Access Transport Area
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.