



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

ANSI/SCTE 24-1 2016

**IPCablecom 1.0 Part 1: Architecture Framework for
the Delivery of Time-Critical Services over Cable
Television Networks Using Cable Modems**

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) 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 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.

SCTE 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. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. 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 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 web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2016
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.

Table of Contents

1	INTRODUCTION	5
1.1	IPCABLECOM OVERVIEW	5
2	REFERENCES	6
2.1	NORMATIVE REFERENCES	6
2.2	INFORMATIVE REFERENCES	6
3	TERMS AND DEFINITIONS	8
4	ABBREVIATIONS AND ACRONYMS	12
5	IPCABLECOM 1.0	18
5.1	IPCABLECOM ARCHITECTURE FRAMEWORK	18
5.2	IPCABLECOM ZONES AND DOMAINS	19
5.3	IPCABLECOM 1.0 SPECIFICATIONS	19
5.4	IPCABLECOM 1.0 DESIGN CONSIDERATIONS	20
5.4.1	<i>General Architectural Goals</i>	<i>20</i>
5.4.2	<i>Call Signaling</i>	<i>21</i>
5.4.3	<i>Quality of Service</i>	<i>22</i>
5.4.4	<i>CODEC and Media Stream</i>	<i>22</i>
5.4.5	<i>Device Provisioning and OSS</i>	<i>22</i>
5.4.6	<i>Security</i>	<i>22</i>
6	IPCABLECOM 1.0 FUNCTIONAL COMPONENTS	23
6.1	MULTIMEDIA TERMINAL ADAPTER (MTA)	23
6.1.1	<i>MTA Functional Requirements</i>	<i>23</i>
6.1.2	<i>MTA Attributes</i>	<i>24</i>
6.2	CABLE MODEM (CM)	25
6.3	HFC ACCESS NETWORK	25
6.4	CABLE MODEM TERMINATION SYSTEM (CMTS)	25
6.4.1	<i>CMTS Gate</i>	<i>25</i>
6.5	CALL MANAGEMENT SERVER (CMS)	25
6.6	PSTN GATEWAY	26
6.6.1	<i>Media Gateway Controller (MGC)</i>	<i>26</i>
6.6.2	<i>Media Gateway (MG)</i>	<i>27</i>
6.6.3	<i>Signaling Gateway (SG)</i>	<i>28</i>
6.7	OSS BACK OFFICE COMPONENTS	28
6.7.1	<i>Security Server – Key Distribution Center (KDC)</i>	<i>28</i>
6.7.2	<i>Dynamic Host Configuration Protocol Server (DHCP)</i>	<i>29</i>
6.7.3	<i>Domain Name System Server (DNS)</i>	<i>29</i>
6.7.4	<i>Trivial File Transfer Protocol Server or Hypertext Transfer Protocol Server (TFTP or HTTP)</i>	<i>29</i>
6.7.5	<i>SYSLOG Server (SYSLOG)</i>	<i>29</i>
6.7.6	<i>Record Keeping Server (RKS)</i>	<i>29</i>
7	PROTOCOL INTERFACES	30
7.1	CALL SIGNALING INTERFACES	30
7.1.1	<i>Network-based Call Signaling (NCS) Framework</i>	<i>31</i>
7.1.2	<i>PSTN Signaling Framework</i>	<i>31</i>
7.2	MEDIA STREAMS	32
7.2.1	<i>Real-time Transport Control Protocol (RTCP)</i>	<i>33</i>
7.3	MTA DEVICE PROVISIONING	34

7.4	SNMP ELEMENT MANAGEMENT LAYER INTERFACES	35
7.5	EVENT MESSAGES INTERFACES	35
7.5.1	<i>Event Message Framework</i>	35
7.6	QUALITY OF SERVICE (QoS)	36
7.6.1	<i>QoS Framework</i>	36
7.6.2	<i>Dynamic Quality of Service</i>	39
7.7	SECURITY	39
7.7.1	<i>Overview</i>	39
7.7.2	<i>Device Provisioning Security</i>	43
8	NETWORK DESIGN CONSIDERATIONS	45
8.1	TIME KEEPING AND REPORTING ISSUES	45
8.2	TIMING FOR PLAYOUT BUFFER ALIGNMENT WITH CODING RATE	45
8.3	IP ADDRESSING	45
8.4	DYNAMIC IP ADDRESS ASSIGNMENT	45
8.5	FULLY QUALIFIED DOMAIN NAME (FQDN) ASSIGNMENT	46
8.6	PRIORITY MARKING OF SIGNALING AND MEDIA STREAM PACKETS	46
8.7	FAX SUPPORT	47
8.8	ANALOG MODEM SUPPORT	47

List of Tables

FIGURE 1.	IPCABLECOM REFERENCE ARCHITECTURE	18
FIGURE 2.	ZONES AND ADMINISTRATIVE DOMAINS	19
FIGURE 3.	IPCABLECOM COMPONENT REFERENCE MODEL	23
FIGURE 4.	E-MTA CONCEPTUAL FUNCTIONAL ARCHITECTURE	24
FIGURE 5.	CALL SIGNALING INTERFACES	30
FIGURE 6.	RTP MEDIA STREAM FLOWS IN AN IPCABLECOM NETWORK	32
FIGURE 7.	RTP PACKET FORMAT	33
FIGURE 8.	IPCABLECOM PROVISIONING INTERFACES	34
FIGURE 9.	REPRESENTATIVE EVENT MESSAGES ARCHITECTURE	35
FIGURE 10.	EVENT MESSAGE INTERFACES	36
FIGURE 11.	IPCABLECOM QoS INTERFACES	37
FIGURE 12.	IPCABLECOM SECURITY INTERFACES	41

List of Tables

TABLE 1.	IPCABLECOM 1.0 SPECIFICATIONS AND TECH REPORT	20
TABLE 2.	CALL SIGNALING INTERFACES	30
TABLE 3.	RTP MEDIA STREAM FLOWS	32
TABLE 4.	DEVICE PROVISIONING INTERFACES	34
TABLE 5.	EVENT MESSAGE INTERFACES	36
TABLE 6.	QoS INTERFACES	37
TABLE 7.	QoS INTERFACES	38
TABLE 8.	SECURITY INTERFACES	42

1 INTRODUCTION

This document provides the architectural framework that will enable cable television operators to provide time critical services over their networks that have been enhanced to support cable modems.

1.1 IPCablecom Overview

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 [11]. 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 1.0, which is the subject of this Technical Report, is designed to provide digital voice and telephony services. Note: IPCablecom 1.0 only supports IPv4.

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 1.0 specifications as listed in Section 5.3.

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 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 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 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 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

This technical report does not use any normative references.

2.2 Informative References

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

- [1] ANSI/SCTE 24-02 2016, IPCablecom 1.0 Part 2: Audio Codec Requirements for the Provision of Bi-directional Audio Service Over Cable Television Networks Using Cable Modems.
- [2] ANSI/SCTE 24-04 2016, IPCablecom 1.0 Part 4: Dynamic Quality of Service for the Provision of Real-Time Services over Cable Television Networks Using Data Modems.
- [3] ANSI/SCTE 24-03 2016, IPCablecom 1.0 Part 3: Network Call Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems.
- [4] ANSI/SCTE 24-09 2016, IPCablecom 1.0 Part 9: Event Message Requirements.
- [5] ANSI/SCTE 24-07 2016, IPCablecom 1.0 Part 7: Media Terminal Adapter (MTA) Management Information Base (MIB) Requirements.
- [6] ANSI/SCTE 24-08 2016, IPCablecom 1.0 Part 8: Network Call Signaling Management Information Base (MIB) Requirements
- [7] ANSI/SCTE 24-06 2016, IPCablecom 1.0 Part 6: Management Information Base (MIB) Framework.
- [8] ANSI/SCTE 24-12 2016, IPCablecom 1.0 Part 12: Trunking Gateway Control Protocol (TGCP).
- [9] ANSI/SCTE 24-05 2016, IPCablecom 1.0 Part 5: Media Terminal Adapter (MTA) Device Provisioning Requirements for the Delivery of Real-Time Services over Cable Television Using Cable Modems.
- [10] ANSI/SCTE 24-10 2016, IPCablecom 1.0 Part 10: Security Specification.
- [11] ANSI/SCTE 23-01 2010, DOCSIS 1.1 Part 1: Radio Frequency Interface.
- [12] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Application, January 1996.
- [13] IETF RFC 2327, SDP: Session Description Protocol, IETF RFC 2327, April 1998.
- [14] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.
- [15] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January 1996.
- [16] IETF RFC 1119, Network Time Protocol, September 1989.
- [17] IETF RFC 2748, The COPS (Common Open Policy Service) Protocol, January 2000.
- [18] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.
- [19] IETF RFC 2866, RADIUS Accounting, June 2000.
- [20] IETF RFC 3260, New Terminology and Clarifications for Diffserv, April 2002.
- [21] IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.

- [22] IETF RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP, September 2001.
- [23] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
- [24] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.
- [25] IETF RFC 3435, Media Gateway Control Protocol (MGCP) Version 1.0, January 2003.
- [26] ITU-T Recommendation G.711, Pulse Code Modulation (PCM) Of Voice Frequencies, November 1988.
- [27] Telcordia GR-909, Generic Criteria for Fiber in the Loop Systems, December 2004.

3 TERMS AND DEFINITIONS

The following is a master list of terms and definitions used in IPCablecom 1.0.

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 a public key cryptography, where encryption and decryption keys are always distinct.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity 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 IPCablecom 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 IPCablecom 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.
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 an 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

4 ABBREVIATIONS AND ACRONYMS

The following is a master list of abbreviations and acronyms used by IPCablecom 1.0.

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 combines (XORs) 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.
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part is a protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ITU	International Telecommunication Union

IVR	Interactive Voice Response System
KDC	Key Distribution Center, a Kerberos security server
LATA	Local Access and Transport Area
LD	Long Distance
LIDB	Line Information Data Base, containing information on telephone customers required for real-time access such as calling card personal identification numbers (PINs) for real-time validation
LLC	Logical Link Control, used here to mean the Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sub layer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same phone 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 sub layer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller
MD5	Message Digest 5 - a one-way hash algorithm which maps variable length plaintext into fixed length (16 byte) ciphertext.
MDU	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high rise buildings
MG	The media gateway provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
MGC	A Media Gateway Controller is the overall controller function of the PSTN gateway. It receives controls and mediates call signaling information between the IPCablecom and PSTN.
MGCP	Media Gateway Control Protocol. See the IPCablecom NCS specification.
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 MAC.
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSO	Multi-System Operator, a cable company that operates many head-end locations in several cities.
MSU	Message Signal Unit
MTA	Media Terminal Adapter – contains the interface to a subscribers' CPE, 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 is 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. The set of rules defining phone numbers in North America.
NAT	Network Address Translation
NAT Network Layer	Network Address Translation Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.
NCS	Network-based Call Signaling

NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a 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 which defines the analog color television, broadcast standard used today in North America.
OSP	Operator Service Provider
OSS	Operations Systems Support. The back office software used for configuration, performance, fault, accounting and security management.
PAL	Phase Alternate Line – the European color television format which evolved from the American NTSC standard.
PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standards, published by RSA Data Security Inc. Describes 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	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
PHS	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
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.
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.
POTS	Plain Old Telephone Service
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service, guarantees network bandwidth and availability for applications.
RADIUS	<u>R</u> emote <u>A</u> ccess <u>D</u> ial- <u>I</u> n <u>U</u> ser <u>S</u> ervice, an internet protocol (IETF RFCs 2865 and 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.
RFC	Request for Comments. Technical documents approved by the IETF which are available on the World Wide Web at http://www.ietf.org/rfc.html
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
RKS	Record Keeping Server, the device which collects and correlates the various Event Messages
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol