



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

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**

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	7
1.1	PURPOSE	7
1.2	SCOPE	7
1.3	REQUIREMENTS AND CONVENTIONS	8
2	REFERENCES	8
3	ABBREVIATIONS AND ACRONYMS	10
4	TERMS AND DEFINITIONS	17
5	TECHNICAL OVERVIEW	21
5.1	IPCABLECOM QoS ARCHITECTURE REQUIREMENTS	21
5.2	IP QoS ACCESS NETWORK ELEMENTS	23
5.2.1	Multimedia Terminal Adapter (MTA)	23
5.2.2	Cable Modem (CM)	24
5.2.3	Cable Modem Termination System (CMTS)	24
5.2.4	Call Management Server (CMS) and Gate Controller (GC)	24
5.2.5	Record Keeping Server (RKS)	24
5.3	IPCABLECOM DYNAMIC QoS ARCHITECTURE	24
5.4	QoS INTERFACES	25
5.5	FRAMEWORK FOR IPCABLECOM QoS	27
5.6	REQUIREMENTS OF ACCESS NETWORK RESOURCE MANAGEMENT	29
5.6.1	Preventing Theft of Service	29
5.6.2	Two-phase Resource Commitment	29
5.6.3	Segmented Resource Assignment	30
5.6.4	Resource Changes during a Session	30
5.6.5	Dynamic Binding of Resources	30
5.6.6	Dynamic QoS Performance	30
5.6.7	Session Class	30
5.6.8	Intermediate Network Support	31
5.6.9	Backbone QoS Support	31
5.6.10	Handling Multiple Codecs	31
5.6.11	MTA Port-to-Port Calls	32
5.7	THEORY OF OPERATION	32
5.7.1	Basic Session Setup	32
5.7.2	Gate Coordination	33
5.7.3	Changing the Packet Classifiers Associated With a Gate	33
5.7.4	Session Resources	33
5.7.5	Admission Control and Session Classes	34
5.7.6	Resource Renegotiations	34
5.7.7	Dynamic Binding of Resources (Re-reserve)	35
5.7.8	Support for Billing	35
5.7.9	Backbone Resource Management	35
5.7.10	Setting the DiffServ Code Point	36
5.8	SAMPLE MAPPING OF SDP DESCRIPTIONS INTO RSVP FLOWSPECS	36
6	MTA TO CMTS QUALITY-OF-SERVICE PROTOCOL	38
7	EMBEDDED MTA TO CM QoS PROTOCOL (PKT-Q1)	39
7.1	RSVP FLOWSPECS	39
7.1.1	Complex SDP Descriptions with Multiple Codecs	40

7.1.2	<i>Mapping RSVP FlowSpecs into DOCSIS 1.1 QoS Parameters</i>	41
7.1.3	<i>CMTS Authorization and Behavior</i>	47
7.2	DOCSIS 1.1 SUPPORT FOR RESOURCE RESERVATION	48
7.2.1	<i>Two Phase QoS Reservation/Commit</i>	48
7.2.2	<i>Reservation Maintenance</i>	50
7.2.3	<i>Support for Dynamic Binding of Resources</i>	50
7.2.4	<i>QoS Parameter Mapping for Authorization</i>	51
7.2.5	<i>Authorization Block Encoding</i>	53
7.2.6	<i>Payload Header Suppression Handling</i>	53
7.3	USE OF DOCSIS 1.1 MAC CONTROL SERVICE INTERFACE	54
7.3.1	<i>Reservation Establishment</i>	54
7.3.2	<i>Reservation Change</i>	55
7.3.3	<i>Reservation Deletion</i>	55
8	AUTHORIZATION INTERFACE DESCRIPTION (PKT-Q6)	57
8.1	GATES: THE FRAMEWORK FOR QOS CONTROL	57
8.1.1	<i>Classifier</i>	57
8.1.2	<i>Gate</i>	58
8.1.3	<i>Gate Identification</i>	58
8.1.4	<i>Gate Transition Diagram</i>	59
8.1.5	<i>Gate Coordination</i>	61
8.2	COPS PROFILE FOR IPCABLECOM	63
8.3	GATE CONTROL PROTOCOL MESSAGE FORMATS	64
8.3.1	<i>COPS Common Message Format</i>	64
8.3.2	<i>Additional COPS Objects for Gate Control</i>	65
8.3.3	<i>Definition of Gate Control Messages</i>	71
8.4	GATE CONTROL PROTOCOL OPERATION	73
8.4.1	<i>Initialization Sequence</i>	73
8.4.2	<i>Operation Sequence</i>	74
8.4.3	<i>Procedures for Allocating a New Gate</i>	74
8.4.4	<i>Procedures for Authorizing Resources Through a Gate</i>	75
8.4.5	<i>Procedures for Querying a Gate</i>	77
8.4.6	<i>Procedures for Committing a Gate</i>	77
8.4.7	<i>Procedures for Closing a Gate</i>	77
8.4.8	<i>Procedures for Deleting a Gate</i>	77
8.4.9	<i>Termination Sequence</i>	78
8.4.10	<i>Failure Scenario</i>	78
8.5	CMS USE OF GATE PROTOCOL	78
8.6	GATE-COORDINATION	78
8.6.1	<i>Connecting a Call</i>	79
8.6.2	<i>Terminating a Call</i>	79
9	TIMER DEFINITIONS AND VALUES	81
9.1	TIMER T0	81
9.2	TIMER T1	81
9.3	TIMER T2	81
9.4	TIMER T3	81
9.5	TIMER T4	81
9.6	TIMER T5	81
9.7	TIMER T6	82
9.8	TIMER T7	82
9.9	TIMER T8	82

APPENDIX I	THEFT OF SERVICE SCENARIOS	83
I.1	SCENARIO #1: CUSTOMERS ESTABLISHING HIGH QoS CONNECTIONS THEMSELVES	83
I.2	SCENARIO #2: CUSTOMERS USING PROVISIONED QoS FOR NON-VOICE APPLICATIONS	83
I.3	SCENARIO #3: MTA ALTERING THE DESTINATION ADDRESS IN VOICE PACKETS	84
I.4	SCENARIO #4: USE OF HALF-CONNECTIONS	84
I.5	SCENARIO #5: EARLY TERMINATION LEAVING A HALF-CONNECTION	84
I.6	SCENARIO #6: FORGED GATE COORDINATION MESSAGES	84
I.7	SCENARIO #7: FRAUD DIRECTED AGAINST UNWANTED CALLERS	84
APPENDIX II	COPS (COMMON OPEN POLICY SERVICE)	85
II.1	COPS PROCEDURES AND PRINCIPLES	85
II.2	COMPARISON OF COPS AND LDAP FOR POLICY	86
APPENDIX III	RSVP (RESOURCE RESERVATION PROTOCOL)	87
APPENDIX IV	TCP CONSIDERATIONS	88
IV.1	REQUIREMENTS	88
IV.2	RECOMMENDED CHANGES	88
IV.3	TCP CONNECTION ESTABLISHMENT IMPACTING POST-DIAL DELAY	89
IV.4	NEED LOW LATENCY FOR PACKETS BETWEEN THE GC AND CMTS, EVEN UNDER LOSS	89
IV.5	HEAD OF LINE BLOCKING	90
IV.6	TCP SLOW START	90
IV.7	DELAYING OF PACKETS: NAGLE'S ALGORITHM	90
IV.8	NON-BLOCKING INTERFACE	91

List of Figures

FIGURE 1.	QoS SIGNALING INTERFACES IN IPCABLECOM NETWORK	26
FIGURE 2.	RESOURCE MANAGEMENT PHASE 1	32
FIGURE 3.	RESOURCE MANAGEMENT PHASE 2	33
FIGURE 4.	AUTHORIZED, RESERVED, AND COMMITTED RESOURCES	34
FIGURE 5.	DSA AND DSC EXCHANGES BETWEEN CM AND CMTS	49
FIGURE 6.	RESERVATION ESTABLISHMENT	55
FIGURE 7.	RESERVATION CHANGE	55
FIGURE 8.	RESERVATION DELETION	56
FIGURE 9.	GATE STATE TRANSITION DIAGRAM	62
FIGURE 10.	QoS ADMISSION CONTROL LAYOUT	63
FIGURE 11.	COMMON COPS MESSAGE HEADER	64
FIGURE 12.	COMMON COPS OBJECT FORMAT	65
FIGURE 13.	COPS CONNECTION ESTABLISHMENT	73
FIGURE 14.	COPS KEEP-ALIVE EXCHANGE	73
FIGURE 15.	SAMPLE SIGNALING OF GATE-ALLOC	75
FIGURE 16.	SAMPLE SIGNALING OF GATE-SET	76
FIGURE 17.	COORDINATION OF CALL CONNECTION	79
FIGURE 18.	COORDINATION OF CALL TERMINATION	79
FIGURE 19.	COPS PROTOCOL	85
FIGURE 20.	COPS AND LDAP MODEL	86

List of Tables

TABLE 1 - DSA-REQ.....	49
TABLE 2 - DSC-REQ.....	50

1 INTRODUCTION

1.1 Purpose

This standard describes a dynamic Quality-of-Service (QoS) mechanism for the IPCablecom project. It was issued to facilitate design and field-testing leading to the manufacture and interoperability of conforming hardware and software by multiple vendors.

IPCablecom is a set of protocols developed to deliver Quality of Service enhanced communications services using packetized data transmission technology to a consumer's home over the cable network. IPCablecom utilizes a network superstructure that overlays the two-way data-ready cable television network. While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice and Packet Video, the long-term project vision encompasses a large family of packet-based services.

1.2 Scope

This document addresses requirements for a client device to obtain access to IPCablecom network resources. In particular, it specifies a comprehensive mechanism for a client device to request a specific Quality of Service from the DOCSIS[®] network. Extensive examples illustrate the use of the specification.

The scope of this specification is to define the QoS Architecture for the "Access" portion of the IPCablecom network, provided to requesting applications on a per-flow basis. The access portion of the network is defined to be between the Multi-media Terminal Adapter (MTA) and the Cable Modem Termination System (CMTS), including the DOCSIS network. The method of QoS allocation over the backbone is unspecified in this document. Interface to the managed IP backbone and issues related to IP multicast are not within the scope of this document. This specification also recognizes that per-flow reservations may be required within the customer premises, and the protocol developed addresses this potential need.

To summarize, the scope of this document is:

- Allocation of QoS between the MTA and the CMTS.
- Specification of the interfaces which are available for control and delivery of QoS in IPCablecom Networks.
- Support for IPCablecom embedded MTAs.
- Support for Network-based Call Signaling (NCS) [10].

This specification assumes that DOCSIS QoS (specifically RFI version 1.1 [9], or greater) is used to control and deliver QoS across the DOCSIS networks. Use of the term DOCSIS 1.1 is used throughout this specification and signifies any DOCSIS version 1.1 or greater.

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 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 should be recalled that while an IPCablecom network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, and that these differences may be significant for legal/regulatory purposes. Moreover, while reference is made here to "IP Telephony," it should be recognized that this term embraces a number of different technologies and network architecture, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this term.

1.3 Requirements and Conventions

Throughout this document, the 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.

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.

- [1] IETF RFC 2205, *Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification*, September 1997.
- [2] IETF RFC 2210, *The Use of RSVP with IETF Integrated Services*, September 1997.
- [3] IETF RFC 2748, *The COPS (Common Open Policy Service) Protocol*, January 2000.
- [4] IETF RFC 3006, *Integrated Services in the Presence of Compressible Flows*, November 2000.
- [5] IETF RFC 3209, *RSVP-TE: "Extensions to RSVP for LSP Tunnels"*, December 2001.
- [6] IETF RFC 2753, *A Framework for Policy Based Admission Control*, January 2000.
- [7] IETF RFC 3084, *COPS Usage for Policy Provisioning*, March, 2001.
- [8] IETF RFC 1890, *RTP Profile for Audio and Video Conferences with Minimal control*, January 1996.
- [9] ANSI/SCTE 23-01 2010, *DOCSIS 1.1 Part 1: Radio Frequency Interface*.
- [10] 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*.
- [11] ANSI/SCTE 24-10 2016, *IPCablecom 1.0 Part 10: Security Specification*.
- [12] IETF RFC 1321, *MD5 Message-Digest Algorithm*, April 1992.
- [13] IETF RFC 2113, *IP Router Alert Option*, February 1997.
- [14] IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, June 2000.

- [15] IETF RFC 2866, *RADIUS Accounting*, June 2000.
- [16] IETF RFC 2327, *SDP: Session Description Protocol*, April 1998.
- [17] ANSI/SCTE 24-01 2016, IPCablecom 1.0 Part 1: Architecture Framework for the Delivery of Time-Critical Services Over Cable Television Networks Using Cable Modems.
- [18] IETF RFC 2996, *Use and Format of the DCLASS Object with RSVP Signaling*, November 2000.
- [19] ANSI/SCTE 24-09 2016, IPCablecom 1.0 Part 9: Event Message Requirements.
- [20] 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.
- [21] IETF RFC 2749, *COPS Usage for RSVP*, January 2000.
- [22] IETF RFC 2961, *RSVP Refresh Overhead Reduction Extensions*, April 2001.
- [23] IETF RFC 2750, *RSVP Extensions for Policy Control*, January 2000.
- [24] ITU-T Recommendation G.114 (05/00) - One-way transmission time.
- [25] ITU-T Recommendation G.711 (02/00) - Pulse code modulation (PCM) of voice frequencies.
- [26] ITU-T Recommendation G.729 – Annex E (02/00) - Coding of speech at 8 kbit/s using (CS-ACELP).
- [27] ITU-T Recommendation G.726 Adaptive differential pulse code modulation (ADPCM) (12/90)
- [28] ITU-T Recommendation G.728 (09/92) – Coding of speech at 16 kbit/s using low-delay code-excited linear prediction.
- [29] IETF RFC 3168, *The Addition of Explicitly Congestion Notification (ECN) to IPI*, September 2001.
- [30] IETF RFC 0791, *Internet Protocol*, September, 1981.
- [31] IETF RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, December 1988.

3 ABBREVIATIONS AND ACRONYMS

The following is a master list of abbreviations used by IPCablecom 1.0:

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 DSO circuit on a Media Gateway. It is a combination of the circuit’s SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format.
CIR	Committed Information Rate.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax.
CMS	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.
CMTS	Cable Modem Termination System. The device at a cable headend which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.

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

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

MGC	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the IPCablecom and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
MIB	Management Information Base.
MIC	Message Integrity Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a Message Authentication Code (MAC).
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSB	Most Significant Bit.
MSO	Multi-System Operator. A cable company that operates many headend locations in several cities.
MSU	Message Signal Unit.
MTA	Multimedia Terminal Adapter. Contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part. A set of two protocols (MTP 2, MTP 3) within the SS7 suite of protocols that are used to implement physical, data link, and network-level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay.
NANP	North American Numbering Plan.
NANPNAT	North American Numbering Plan Network Address Translation.
NAT Network Layer	Network Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture. This layer provides services to establish a path between open systems.
NCS	Network Call Signaling.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP).
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.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
QCIF	Quarter Common Intermediate Format.
QoS	Quality of Service. Guarantees network bandwidth and availability for applications.
RADIUS	Remote Authentication Dial-In User Service. An internet protocol (IETF RFC 2865 and RFC 2866) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use.
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	Rivest Cipher 4. A variable length stream cipher. Optionally used to encrypt the media traffic in IPCablecom.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html .
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.
RKS	Record Keeping Server. The device, which collects and correlates the various Event Messages.
RSA	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource Reservation Protocol.
RTCP	Real-Time Control Protocol.
RTO	Retransmission Timeout.
RTP	Real-time Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC 1889.
SA	Security Association. A one-way relationship between sender and receiver offering security services on the communication flow.
SAID	Security Association Identifier. Uniquely identifies SAs in the DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.

SCCP	Signaling Connection Control Part. A protocol within the SS7 suite of protocols that provides two functions in addition to those provided within MTP. The first function is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.
SCTP	Stream Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information delivered as a unit between peer service access points.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID. A 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). Upstream Service Flow IDs and Downstream Service Flow IDs are allocated from the same SFID number space.
SFR	Service Flow Reference. A 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular, the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1. A one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
S-MTA	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
SNMP	Simple Network Management Protocol.
SOHO	Small Office/Home Office.
SS7	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Service Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. A node within an SS7 network that routes signaling messages based on their destination address. This is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
TCP	Transmission Control Protocol.
TD	Timeout for Disconnect.
TFTP	Trivial File Transfer Protocol.
TFTP-D	Default – Trivial File Transfer Protocol.
TGS	Ticket Granting Server. A sub-system of the KDC used to grant Kerberos tickets.

TGW	Telephony Gateway.
TIPHON	Telecommunications and Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value. A tuple within a DOCSIS configuration file.
TN	Telephone Number.
ToD	Time-of-Day Server.
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a DiffServ domain, the TOS byte is treated as the DiffServ Code Point, or DSCP.
TSG	Trunk Subgroup.
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
VAD	Voice Activity Detection.
VBR	Variable Bit Rate.
VoIP	Voice-over-IP.

4 TERMS AND DEFINITIONS

The following is a master list of terms and definitions used by 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 public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server plays informational announcements in IPCablecom network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.
Authorization	The act of giving access to a service or device if one has permission to have the access.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key-management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.
Confidentiality	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext.
Digital certificate	A binding between an entity’s public key and one or more attributes relating to its identity, also known as a public key certificate.
Digital signature	A data value generated by a public-key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum.

Downstream	The direction from the headend toward the subscriber location.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or Multipoint Conference Unit (MCU).
Errored Second	Any 1-second interval containing at least one bit error.
Event Message	A message capturing a single portion of a connection.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow") A unidirectional sequence of packets associated with a Service ID (SID) and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Flow [IP Flow]	A unidirectional sequence of packets identified by OSI Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Gateway	Devices bridging between the IPCablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway, which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway, which sends and receives circuit switched network signaling to the edge of the IPCablecom network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T H.245 protocol for communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area.
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.

Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.
Network Management OSS	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.
Nonce	A random value used only once that is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
Off-Net Call	A communication connecting an IPCablecom subscriber out to a user on the PSTN.
On-Net Call	A communication placed by one customer to another customer entirely on the IPCablecom Network.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information, thereby eliminating the need for a host to support the service.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key, for encryption and decryption, also known as an asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
Root Private Key	The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures generated with the corresponding root private key.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.

Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
Signed and Sealed	An “envelope” of information which has been signed with a digital signature and sealed using encryption.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and single source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
Systems Management	Functions in the application layer related to the management of various Open Systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.
Transit Delays	The time difference between the instant at which the first bit of a Protocol Data Unit (PDU) crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch that carries user media content and may carry voice signaling (M_F , R_2 , etc.).
Tunnel Mode	An IPsec (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPsec ESP or AH transform are taken out.
Upstream	The direction from the subscriber location toward the headend.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

5 TECHNICAL OVERVIEW

Enhanced Quality of Service is required for supporting interactive multimedia applications. Resources may be constrained in segments of the network, requiring allocation of resources in the network. The scope of this specification is to define the Quality of Service Architecture for the "Access" portion of the IPCablecom network. The access portion of the network is defined to be between the Multimedia Terminal Adapter (MTA) and the Cable Modem Termination System (CMTS), including the DOCSIS network. This specification also recognizes that per-flow reservations may be required within the customer premises, and the protocols developed herein address this potential need. Although some segments of the backbone network may require resource reservation to provide adequate quality of service, the protocols for backbone resource management are considered to be outside the scope of this specification.

Resources are allocated on the DOCSIS network for individual flows associated with each session of an application, per subscriber, on an authorized and authenticated basis. A DQoS session, or simply a session, is defined by this specification to be a single bi-directional data flow between two clients. When a multi-media application needs multiple bi-directional data flows (e.g., one for voice and a separate for video), separate DQoS sessions are established for each. Applications may use only half of the session's bi-directional data flow, thereby providing send-only or receive-only services. For example, in a typical voice communications application, a simple communication between two parties is implemented by a single session, while complex, multiparty communications (e.g., "conference calls") are implemented by multiple simultaneous sessions.

Network-based Call Signaling (NCS) is the defined IPCablecom Call Signaling Protocol. This Dynamic QoS specification is the underlying QoS framework for this call signaling protocol. QoS is allocated for flows associated with a session in concert with the signaling protocol.

This specification introduces the concept of a segment-by-segment QoS framework. It exploits the information available from signaling protocols to perform the QoS on both the "local" segment (on the DOCSIS network close to the originating party) and the "remote" segment (the DOCSIS network close to the terminating party). Thus, this specification allows different providers to use the most appropriate mechanisms for the segment that they are managing. Using a concatenation of the segments with QoS, end-to-end QoS assurance for the session is provided.

The Dynamic QoS specification incorporates protocols to enable providers of packet-based voice communications using the IPCablecom framework to use different charging models, including both flat-rate charging as well as usage-based charging. It is the intent of this specification to ensure that enhanced QoS is provided only to authorized and authenticated users. The specific techniques used for authorizing and authenticating a user are beyond the scope of this specification.

This Dynamic QoS specification recognizes the requirements of a commercially viable voice communications service analogous to that offered by means of the public switched telephone network. It is important to ensure that resources are available before the two parties involved in the session are invited to communicate. Thus, resources are reserved before the recipient of the communication is notified that someone is trying to initiate a communication. If there are insufficient resources for a session, then the session is blocked.

The protocols developed in this specification explicitly recognize the need to ensure that there is no potential for fraud or theft of service by end-points that do not wish to cooperate with the call signaling and QoS signaling protocols with the intent of avoiding being charged for usage. This specification introduces the concept of a two-phase for resource reservation (reserve and commit). The two-phases allow a provider to both allocate resources only when they are required (when the voice path is cut-through) which may be used for billing. Further, because the second phase to commit resources requires an explicit request from the MTA, it enables the provider to prevent fraud and theft of service.

5.1 IPCablecom QoS Architecture Requirements

The following list presents the QoS requirements for supporting multimedia applications over IPCablecom networks.

1. Provide IPCablecom accounting for the QoS resources on a per-session basis.

It is anticipated that, from a billing perspective, one of the resources that will need to be accounted for is the use of QoS in the DOCSIS network. Thus, information needs to be identified and tracked that allows reconciliation of the use of the DOCSIS QoS resource with IPCablecom session activity.

2. Both two-phase (reserve-commit) and single phase (commit) QoS activation models.

Under application control it should be possible to utilize either a two-phase or single-phase QoS activation model. In the two-phase model the application reserves the resource, and later commits it. In the single phase model both reservation and commitment occur as a single autonomous operation. As in the DOCSIS model, resources that are reserved but not yet committed are available for temporary assignment to other (e.g., best effort) service flows. The current specification provides mechanisms for both two-phase and single-phase activation for embedded MTAs.

3. Provide IPCablecom defined policies to control QoS in both the DOCSIS network and the IP backbone.

It should be possible for different types of sessions to have different QoS characteristics. For example, sessions within a single MSO provider's domain may receive different QoS than sessions outside the domain (e.g., international sessions including links to the PSTN). This dynamic QoS specification may allow an MSO to provide different QoS for different types of customers (e.g., higher QoS for subscribers of a business service at certain times of the day compared to residential customers), or different types of applications for a single customer.

4. Prevent (minimize) abusive QoS usage.

Two types of abusive QoS usage are identified: that which is accurately billed but leads to denying service to others, and that which is not accurately billed and leads to theft of service. Subscriber applications and IPCablecom applications (either embedded or PC-based) may inadvertently or intentionally abuse their QoS privileges (e.g., use of enhanced QoS, which the provider wants limited to voice applications, by an FTP application). Even though the DOCSIS network is expected to enforce a subscriber's access to QoS, rich packet classification and signaling control mechanisms should exist to keep the subscriber (and the subscriber devices) from fraudulent use of QoS. Admission control procedures should be employed to reduce denial-of-service attacks.

5. Provide admission control mechanisms for both upstream and downstream directions in the DOCSIS network.

Both upstream and downstream QoS should be subject to per-session admission control.

6. DOCSIS QoS.

It should be possible to police (defined as marking, dropping, or delaying packets) all aspects of QoS defined in the service at the CMTS using the DOCSIS QoS mechanisms. Furthermore, it should be possible to support multiple flow mapping models – single IPCablecom session to a single Service Flow and multiple IPCablecom sessions to a single Service Flow.

7. Policy is enforced by the CMTS.

Ultimate policy control is entrusted to the CMTS. The philosophy is that any client can make any QoS request, but the CMTS (or an entity behind the CMTS) is the only entity entrusted to grant or deny QoS requests.

8. IPCablecom entities must be as unaware as possible of specific DOCSIS QoS primitives and parameters.

For IPCablecom, like any other application that uses the IP-network, the design objective is to minimize the amount of access-link-specific knowledge contained within the application layer. The less access-link knowledge in the application layer, the more applications will be available for development and deployment, and the fewer testing and support-problems will be encountered.

9. Reclamation of QoS resources for dead/stale sessions.

It is necessary to re-claim and re-allocate precious QoS resources for sessions that are no longer active, but have not been properly torn down. There should be no resource 'leaks' in the DOCSIS link. For example, if an IPCablecom client module malfunctions in the midst of an IPCablecom session, all DOCSIS QoS resources used by the session should be released within a reasonable period of time.

10. Dynamic QoS policy changes.

It is desirable to dynamically change QoS policies for subscribers. For example, this requirement addresses the ability to change a customer's service level (e.g., upgraded from a "bronze" service to a "gold" service) on-the-fly without resetting the cable modem.

11. Absolute minimum session setup latency time and post pickup delay.

The IPCablecom network should allow for emulation and enhancement of the PSTN experience to the user, and should be equally good, if not better, in session setup and post pickup delay metrics.

12. Multiple concurrent sessions.

It is desirable to allocate QoS resources (e.g., bandwidth) for not only individual point-to-point sessions, but also for multiple point-to-point sessions (e.g., conference calls, combined audio/video calls).

13. Dynamic adjustment of QoS parameters in the middle of IPCablecom sessions.

It should be possible for the IPCablecom service to change QoS mid-session, e.g., network-wide resource adjustments or creation of compatible CODEC parameters (necessitating QoS changes), or user defined feature to vary QoS levels, or detection of fax or modem streams (necessitating change from compressing CODEC to G.711).

14. Support multiple QoS control models.

Strong cases can be made for both subscriber-side and network-side initiation of QoS signaling. In subscriber side signaling, an application can initiate its request for QoS immediately when the application believes it needs QoS. Also, subscriber side signaling supports application models that are peer-to-peer. In network-side signaling, implementation of the end-point application can be completely unaware of QoS (especially in the DOCSIS network). Network-side signaling supports application models that are client-server (with the server being trusted). It is expected that both models will be present in IPCablecom (and other DOCSIS application) networks. The current specification is for subscriber-side signaling only.

15. Support both embedded-MTA and standalone-MTA QoS signaling.

It should be possible to signal QoS from both an embedded-MTA and standalone-MTA. This specification only covers the embedded-MTA using direct access to the DOCSIS MAC signaling (via an internal interface as suggested in the DOCSIS RFI [9] specification).

5.2 IP QoS Access Network Elements

The following network elements are employed to support QoS for IPCablecom networks.

5.2.1 Multimedia Terminal Adapter (MTA)

The IPCablecom network client device (i.e., the MTA) can be one of the following devices. These devices reside at the customer site and are connected through the DOCSIS 1.1 channel to the network. All MTAs are assumed to implement some multimedia signaling protocol, such as or NCS [10]. An MTA may be either a device with a standard two-wire telephone set in the MTA-1 configuration, or may add video input/output capabilities in the MTA-2 configuration. It may have minimal capabilities, or may implement this functionality on a multimedia personal computer, and have all of the capabilities of the PC at its disposal.

From the point of view of QoS, there are two types of MTAs:

1. Embedded/Integrated MTA.

This is a client multimedia terminal which incorporates a DOCSIS MAC-layer interface to the DOCSIS network.

2. Standalone MTA.

This is a Client that implements the multimedia functionality without incorporating a DOCSIS MAC-layer interface. The standalone MTA will typically use Ethernet, USB, or IEEE 1394 as the physical interconnect to a DOCSIS Cable Modem. The standalone MTA may be connected to a customer network, and use transport

facilities of the customer network (possibly including intermediate IP routers) to establish sessions over the DOCSIS network.

5.2.2 Cable Modem (CM)

This is an IPCablecom network element as defined by the DOCSIS specification. The CM is responsible for classifying, policing and marking packets once the traffic flows are established by the signaling protocols described herein.

5.2.3 Cable Modem Termination System (CMTS)

The CMTS is responsible for allocating and scheduling upstream and downstream bandwidth in accordance with MTA requests and QoS authorizations established by the network administrator. The CMTS acts as a Policy Enforcement Point (PEP) per the IETF Resource Allocation Protocol (RAP) Framework [6].

The CMTS implements an "IPCablecom Dynamic QoS Gate" (hereafter called just "Gate") between the DOCSIS cable network and an IP Backbone. The Gate is implemented using the packet classification and filtering functions defined for DOCSIS 1.1.

The CMTS may or may not also be configured as an "IS-DS Boundary" entity. An IS-DS Boundary interfaces to an inter-network using the Integrated Services (IntServ) model of QoS control and some other model, e.g., Differentiated Services (DiffServ).

5.2.4 Call Management Server (CMS) and Gate Controller (GC)

The IPCablecom Call Management Server (CMS) entity performs services that permit MTAs to establish Multimedia sessions (including voice communications applications such as "IP telephony" or "VoIP"). The term Gate Controller (GC) is used to refer to the portion of either type of CMS that performs the Quality of Service related functions.

In the IPCablecom Dynamic QoS Model, the Gate Controller controls the operation of the Gates implemented on a CMTS. The GC acts as a Policy Decision Point (PDP) per the IETF Resource Allocation Protocol (RAP) Framework [6].

5.2.5 Record Keeping Server (RKS)

The Record Keeping Server is an IPCablecom network element that only receives information from IPCablecom elements described in this document. The RKS can be used as a billing server, diagnostic tool, etc.

5.3 IPCablecom Dynamic QoS Architecture

The IPCablecom QoS architecture is based upon DOCSIS 1.1, RSVP, and Integrated Services Guaranteed QoS.

Specifically, the IPCablecom QoS architecture uses the protocol as defined in the DOCSIS 1.1 specification within the cable network. These messages support static and dynamic installation of packet classifiers (i.e., Filter-Specs) and flow scheduling (i.e., FlowSpecs) mechanisms to deliver enhanced IP quality of service. DOCSIS QoS is based upon the objects which describe traffic and flow specifications, similar to the TSpec and RSpec objects as defined in the IETF Resource reSerVation Protocol (RSVP) [1]. This allows QoS resource reservations to be defined on a per flow basis.

In the DOCSIS QoS architecture, traffic flows are considered as unidirectional – thus, an interactive session comprises two flows, each subject to the operations shown below. For each (unidirectional) flow:

The CM, where traffic enters the IP QoS enabled cable network, is responsible for:

- Classification of IP traffic into IP QoS flows based on defined filter specifications.
- Performing traffic shaping and policing as required by the flow specification.
- Maintaining state for active flows.
- Altering the TOS field in the upstream IP headers based on the network operator's policy.

- Obtaining the required IP QoS from the CMTS (DOCSIS QoS).
- Applying DOCSIS QoS mechanisms appropriately.

The CMTS is responsible for:

- Providing the required QoS to the CM based upon policy configuration.
- Allocating upstream bandwidth in accordance to CM requests and network QoS policies.
- Classifying each arriving packet from the network side interface and assigning it to a QoS level based on defined filter specifications.
- Policing the TOS field in received packets from the cable network to enforce TOS field settings per network operator policy.
- Altering the TOS field in the downstream IP headers based on the network operator's policy.
- Performing traffic shaping and policing as required by the flow specification.
- Forwarding downstream packets to the DOCSIS network using the assigned QoS.
- Forwarding upstream packets to the backbone network devices using the assigned QoS.
- Maintaining state for active flows.

The backbone network may either utilize Integrated Services based mechanisms or use Differentiated Services mechanisms. In a DiffServ backbone, network routers forward a packet, providing the appropriate IP QoS, based on the setting of the TOS field. In a DiffServ backbone, no per-flow state is required in the core network devices.

5.4 QoS Interfaces

Quality of service signaling interfaces are defined between many of the components of the IPCablecom network as shown in Figure 1. Signaling involves communication of QoS requirements at the application layer (e.g., SDP parameters), network layer (e.g., RSVP), and at the data-link layer (e.g., DOCSIS 1.1 QoS). Also, the requirement for policy enforcement and system linkages between the OSS subscriber provisioning, admission control within the managed IP backbone, and admission control within the DOCSIS network creates the need for additional interfaces between components in the IPCablecom network.

An expanded explanation of QoS architecture framework is contained in the IPCablecom Architecture Framework Technical Report [17], and is shown in Figure 1.

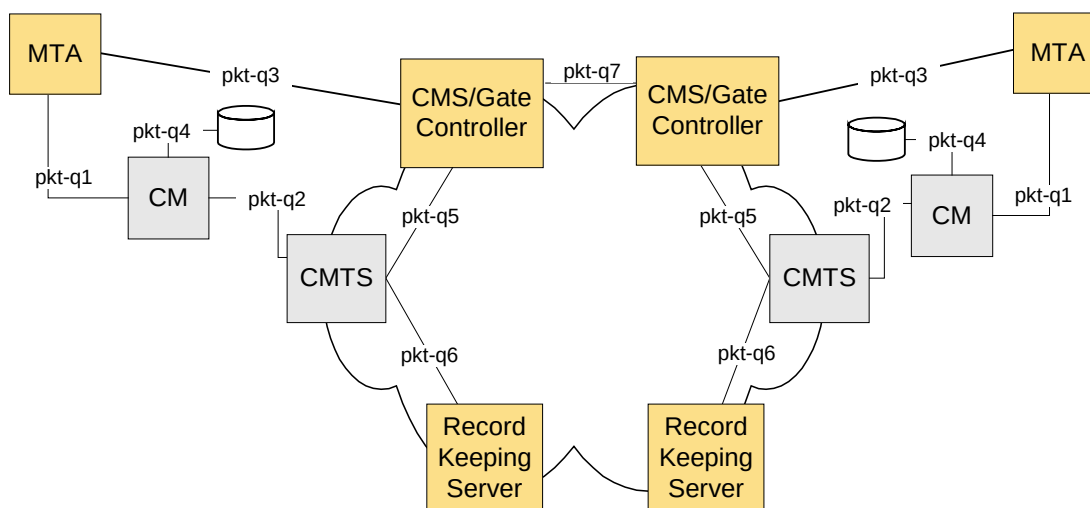


Figure 1. QoS Signaling Interfaces in IPCablecom Network

Interfaces Pkt-q1 through Pkt-q7 are available for controlling and processing QoS. Not all interfaces are used in all configurations and protocol variations. All but the Pkt-q5 interface are utilized by DQoS. The following matrix briefly identifies each interface and how each interface is used in this Dynamic QoS Specification (DQoS).

Interface	Description	Notes
Pkt-q1	MTA – CM	E-MTA, MAC Control Service Interface
Pkt-q2	CM – CMTS (DOCSIS)	DOCSIS, CM-initiated
Pkt-q3	MTA – GC/CMS	NCS
Pkt-q4	CM – Provisioning Server	N/A
Pkt-q5	GC – CMTS	Gate Management
Pkt-q6	CMTS – RKS	Billing
Pkt-q7	CMS to CMS	CMS to CMS Signaling

Pkt-q1: Interface between the MTA and CM

This interface is only defined for the embedded MTA. The interface decomposes into three sub-interfaces:

- Control: used to manage DOCSIS service-flows and their associated QoS traffic parameters and classification rules.
- Synchronization: used to synchronize packetization and scheduling for minimizing latency and jitter.
- Transport: used to process packets in the media stream and perform appropriate per-packet QoS processing.

This interface is conceptually defined in Appendix E of the DOCSIS RFI specification [9]. For standalone MTAs no instance of this interface is defined.

Pkt-q2: DOCSIS QoS Interface between CM and CMTS

This is the DOCSIS RFI QoS interface (control, scheduling, and transport). Control functions can be initiated from either the CM or the CMTS. However the CMTS is the final policy arbiter and granter of resources by performing admission control for the DOCSIS network. This interface is defined in the DOCSIS RFI specification [9].

Pkt-q3: Application Layer signaling between GC/CMS and MTA

This is the IPCablecom Network-Based Call Signaling Protocol (NCS). Many parameters are signaled across this interface such as the media stream, IP addresses, port numbers, and the selection of Codec and packetization characteristics. This interface is defined in the IPCablecom NCS specification [10].

Pkt-q4: Signaling from the DOCSIS/IPCablecom Provisioning to the DOCSIS CM.

This interface is not utilized for QoS signaling in DQoS.

Pkt-q5: Interface between the GC/CMS and CMTS

This interface is used to manage the dynamic Gates for media stream sessions. This interface enables the IPCablecom network to request and authorize QoS.

Pkt-q6: CMTS to Record Keeping Server

This interface is used by the CMTS to signal to the RKS all changes in session authorization and usage.

Pkt-q7: CMS to CMS interface

This interface is used for session management and resource coordination between a pair of CMSs.

5.5 Framework for IPCablecom QoS

In order to justify its costs to the end user, a commercial multimedia service (e.g., voice communications capability) may require a high level of transport and signaling performance, including:

- Low delay – end-to-end packet delay needs to be small enough that it does not interfere with normal multimedia interactions. For normal telephony service using the PSTN, the ITU recommends no greater than 300 ms roundtrip delay.¹ Given that the end-to-end backbone propagation delay may absorb a significant amount of this delay budget, it is important to control delay on the access channel, at least for long-distance calls.
- Low packet loss – packet loss needs to be small enough so that voice quality or performance of fax and voice-band modems is not perceptibly impaired. While loss concealment algorithms can be used to reproduce intelligible speech even with high loss rates, the resulting performance cannot be considered to be adequate as a replacement for existing circuit-switched telephone service. Loss requirements for acceptable voice-band modem performance are even more stringent than those for voice.
- Short post-dial delay – the delay between the user signaling a connection request and receiving positive confirmation from the network needs to be short enough that users do not perceive a difference from the post-dial delay they are accustomed to in the circuit switched network, or believe that the network has failed. This is of the order of one second.
- Short post-pickup delay – the delay between a user picking up a ringing phone and the voice path being cut through needs to be short enough so that the "hello" is not clipped. This should be less than a few hundred milliseconds (ideally less than 100 ms).

A key contribution of the Dynamic QoS framework is a recognition of the need for coordination between signaling, which controls access to application specific services, and resource management, which controls access to network-layer resources. This coordination provides a number of critical functions. It ensures that users are authenticated and authorized before receiving access to the enhanced QoS associated with the service. It ensures that network resources are available end-to-end before alerting the destination MTA. Finally, it ensures that the use of resources is properly accounted for, consistent with the conventions of traditional voice-grade telephone service (to which some IPCablecom services are similar from a customer perspective) in which charging occurs only after the party receiving a communication picks up.

¹ ITU-T Recommendation G.114 states that a one-way delay of 150 ms is acceptable for most user applications. However, highly interactive voice and data applications may experience degradation even when delays are below 150 ms. Therefore any increase in processing delay (even on connections with transmission times well below 150 ms) should be discouraged unless there are clear service and application benefits.

In order to support the above requirements, the QoS protocols assure that all resources are committed to all transport segments before the signaling protocols cause alerting of the destination. Likewise, during tear down of a session, the QoS protocols include measures to assure that all resources dedicated exclusively to the session are released. Without this coordination between the two directions of data flows, it would be possible for users to thwart the QoS controls and obtain free service. For example, if the paying client terminates the session, but the non-paying does not, a "half channel" remains that can be used to fraudulently transfer data in one direction. The QoS protocols approximate the "all or nothing" transaction semantics for session creation and destruction.

It is desired that the mechanisms used to implement the session be based on existing standards and practices, and also that the results of this work be usable to support alternative call models. These desires have led to the use of the IETF Real Time Protocol (RTP) to carry multimedia data, carried over the IETF User Datagram Protocol (UDP). In-band signaling to set up Quality of Service is carried out using DOCSIS Dynamic QoS messages.

The QoS architecture should provide support for new emerging applications that are dependent on multicast data delivery. Although this is not a strict requirement in the QoS architecture, providing support for multicast will enable the future development of a rich set of multimedia applications. It has not yet been examined whether the resource management enhancements introduced here will support multicast seamlessly or not.

For purposes of managing Quality of Service, the bearer channel for a session is managed as three distinct segments: the access network for the originating side of the session, a backbone network, and the access network for the terminating side of the session. DOCSIS network resources are managed as a pair of dynamic service flows, using the mechanisms defined in the DOCSIS 1.1 specification. Backbone resources may be managed either per-flow or, more likely, through an aggregated quality of service mechanism. Management of backbone resources is outside the scope of this specification.

A QoS-defined construct called a gate provides a control point for the connection of access networks to high quality backbone service. A gate is implemented by a CMTS and consists of a packet classifier, a traffic policer, and an interface to an entity that gathers statistics and events (all of these components exist in DOCSIS 1.1). A gate can ensure that only those sessions that have been authorized by the service provider receive high quality service. Gates are managed selectively for a flow.

For IPCablecom-based voice communications service, they are opened for individual calls. Opening a gate involves an admission control check that is performed when a resource management request is received from the client for an individual session, and it may involve resource reservation in the network for the session if necessary. The upstream packet filter in the gate allows a flow of packets to receive enhanced QoS for a session from a specific IP source address and port number to a specific IP destination address and port number. The downstream packet filter in the gate allows a flow of packets to receive enhanced QoS for a session from a specific IP source address to a specific IP destination address and port number.

A Gate is a logical entity that resides in a CMTS. A GateID is associated with an individual session and is meaningful at the Gate; the GateID is an identifier that is locally unique at the CMTS, and is assigned by that CMTS. A Gate is uni-directional in nature. If a Gate is "Closed", then data going upstream/downstream on the DOCSIS 1.1 access network may either be dropped or provided best-effort service. The choice of dropping packets or serving them on a best-effort basis is a policy choice of the provider.

The gate controller is responsible for the policy decision of when and whether the gate should be opened. A gate is established in advance of a resource management request. This allows the policy function, which is at the gate controller, to be "stateless" in that it does not need to know the state of sessions that are already in progress.

While the gate controls the QoS-guaranteed stream, other flows, such as RTCP or signaling messages, are not policed by the gate. The support of enhanced QoS for signaling messages may play a very important role if the cable system is utilizing high best effort data traffic. In order to meet the signaling performance targets given at the beginning of this section it may be crucial to use a dedicated signaling flow with proper QoS constructs. It should further be noted that the exact nature of the QoS that should be given to the dedicated signal flow depends on traffic and the CMTS design and is left as a vendor differentiation point.