SCTE · ISBE

STANDARDS

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-01 2019

IPCablecom 1.5 Part 1: Architecture Framework Technical Report

NOTICE

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

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

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

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

140 Philips Road
Exton, PA 19341

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

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 IPCablecom Overview

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

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

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

1.2 IPCablecom Motivation

The emergence of the Internet Protocol (IP[1]) as the standard transport for packet data networks has enabled a revolution in communications services and applications. This online revolution is demonstrated by the widespread use of email, chat groups, music, video, and the explosive growth of the World Wide Web for entertainment, information exchange, online commerce, and a wide range of new and innovative services. New classes of IP-based information appliances are also emerging, including multimedia personal computers, IP-based set top boxes, and IP-based voice and videophones.

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

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

1.3 IPCablecom Project Phasing

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

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

From time to time, this document refers to the voice communications capabilities of a IPCablecom network in terms of "IP Telephony." The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this document

[1] IPCablecom 1.5 supports only IPv4.

addresses, or is intended to affect, those issues. In particular, while this document uses standard terms such as "call," "call flow," "telephony," etc., it should be recalled that while a 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 NORMATIVE REFERENCES

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1 SCTE References

- No normative references are applicable.

2.2 Standards from Other Organizations

- No normative references are applicable.

2.3 Published Materials

- No normative references are applicable.

3 INFORMATIVE REFERENCES

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

3.1 SCTE References

[1] ANSI/SCTE 165-02 2016, IPCablecom 1.5 Part 2: Audio/Video Codecs.

[2] ANSI/SCTE 165-04 2019, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.

[3] ANSI/SCTE 165-03 2016, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.

[4] ANSI/SCTE 165-09 2019, IPCablecom 1.5 Part 9: Event Messaging.

[5] ANSI/SCTE 165-07 2019, IPCablecom 1.5 Part 7: MTA MIB.

[6] ANSI/SCTE 165-08 2019, IPCablecom 1.5 Part 8: Signaling MIB.

[7] ANSI/SCTE 165-06 2019, IPCablecom 1.5 Part 6: MIBS Framework.

[8] ANSI/SCTE 165-12 2016, IPCablecom 1.5 Part 12: PSTN Gateway Call Signaling Protocol.

[9] ANSI/SCTE 165-05 2019, IPCablecom 1.5 Part 5: Media Terminal Adapter (MTA) Device Provisioning.

[10] ANSI/SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.

[11] ANSI/SCTE 165-18 2016, IPCablecom 1.5 Part 18: CMS to CMS Signaling.

[12] ANSI/SCTE 165-19 2019, IPCablecom 1.5 Part 19: CMS Subscriber Provisioning Specification.

[13] ANSI/SCTE 165-13 2019, IPCablecom 1.5 Part 13: Electronic Surveillance Standard.

[14] ANSI/SCTE 23-01 2017, DOCSIS 1.1 Part 1: Radio Frequency Interface.

3.2 Standards from Other Organizations

[15] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Application, January 1996.

[16] IETF RFC 2327, SDP: Session Description Protocol, IETF RFC 2327, April 1998.

[17] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.

[18] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January 1996.

[19] IETF RFC 1119, Network Time Protocol, September 1989.

[20] IETF RFC 2748, The COPS (Common Open Policy Service) Protocol, January 2000.

[21] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.

[22] IETF RFC 2866, RADIUS Accounting, June 2000.

[23] IETF RFC 3260, New Terminology and Clarifications for Diffserv, April 2002.

[24] IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.

[25] IETF RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP, September 2001.

[26] IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.

[27] IETF RFC 3611, RTP Control Protocol Extended Reports (RTCP XR), November 2003.

[28] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.

[29] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.

[30] IETF RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000.

[31] IETF RFC 3435, Media Gateway Control Protocol (MGCP) Version 1.0, January 2003.

[32] ITU-T Recommendation T.38, Procedures for Real-Time Group 3 Facsimile Communication over IP Networks, April 2004.

[33] ITU-T Recommendation G.711, Pulse Code Modulation (PCM) Of Voice Frequencies, November 1988.

[34] Telcordia GR909, Generic Criteria for Fiber in the Loop Systems, December 2004.

[35] ITU-T Recommendation V.152, Procedures for supporting Voice-Band Data over IP Networks, January 2005.

3.3 Published Materials

- No normative references are applicable.

4 TERMS AND DEFINITIONS

This standard uses the following terms:

Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g., bandwidth) for it on the DOCSIS network.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
Announcement Server	See Audio Server.
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server also known as Announcement Server plays informational announcements in IPCablecom network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user. It is a logical entity consisting of Media Player (MP)and Media Player Controller (MPC).
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set that must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data.
Codec	COder-DECoder
Confidentiality	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptoanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext
Diffserv	(a.k.a. Differentiated Services), an IETF architecture for implementing scalable service differentiation in the Internet. Refer to IETF RFC 3260.

Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate
Digital signature	A data value generated by a public key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum
Downstream	The direction from the head-end toward the subscriber location.
Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU
Errored Second	Any 1-sec interval containing at least one bit error.
Event Message	Message capturing a single portion of a call connection
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated"
Flow [IP Flow]	A unidirectional sequence of packets identified by ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow"). A unidirectional sequence of packets associated with a SID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Gateway	Devices bridging between the 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.
Media Player	Media Player (MP) is responsible for receiving and interpreting commands from the Media Player Controller and for delivering appropriate announcement(s) to the MTA.
Media Player Controller	Media Player Controller (MPC) initiates and manages all announcement services provided by the media player.
Network Management	The functions related to the management of data across the network.
Nonce	A random value used only once that is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
Off-Net Call	Call connecting a IPCablecom subscriber out to a user on the PSTN
On-Net Call	Call placed by one customer to another customer entirely on the IPCablecom Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
Root Private Key	The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.

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

5 ABBREVIATIONS AND ACRONYMS

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

AAA	Authentication, Authorization and Accounting
AF	Assured Forwarding. A Diffserv Per Hop Behavior.
AH	Authentication header is an IPsec security protocol that provides message integrity for complete IP packets, including the IP header.
AMA	Automated Message Accounting., a standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies)
AT	Access Tandem. A switching point in PSTN networks that allows access to an entire calling area.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 or later standard which runs on the MAC layer.
CBC	Cipher block chaining mode is an option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CA	Certification Authority - a trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. In this specification "Call Agent" is part of the CMS that maintains call state, and controls the line side of calls.
CDR	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs
CIC	Circuit Identification Code. In ANSI SS7, a two-octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
CID	Circuit ID (Pronounced "Kid"). This uniquely identifies an ISUP DS0 circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format. A coding format for digital signals.
CIR	Committed Information Rate.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax
CMS	Call Management Server. Controls the audio call connections. Also called a Call Agent in MGCP terminology.
CMTS	Cable Modem Termination System, the device at a cable head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
COPS	Common Open Policy Service. Defined in IETF RFC 2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS 1.0 configuration file.
CSR	Customer Service Representative

DA	Directory Assistance
DE	Default. A Diffserv Per Hop Behavior.
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default - Network Provider DHCP server
DNS	Domain Name System
DSCP	Differentiated Services Code Point. A field in every IP packet header which identifies the Diffserv Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP. See IETF RFC 3260.
DOCSIS	Data Over Cable System Interface Specification.
DPC	Destination Point Code. In ANSI SS7, a 3 octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
DQoS	Dynamic Quality of Service, i.e., assigned on the fly for each call depending on the QoS requested
DTMF	Dual-Tone Multi Frequency (tones)
EF	Expedited Forwarding. A Diffserv Per Hop Behavior.
E-MTA	Embedded MTA – a single node which contains both an MTA and a cable modem.
EO	End Office. A switching point in the PSTN Local Exchange Carrier network that directly connects to subscriber access lines.
ESP	IPsec Encapsulation Security Payload protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute
FGD	Feature Group D signaling. A type of circuit used for exchanging traffic with a PSTN LEC network.
FQDN	Fully Qualified Domain Name.
HFC	Hybrid Fiber/Coaxial cable, HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
HMAC	Hashed Message Authentication Code – a message authentication algorithm, based on either SHA-1 or MD5 hash.
HTTP	Hyper Text Transfer Protocol.
IANA	Internet Assigned Numbers Authority. See http://www.iana.org for details.
IC or IXC	Inter-exchange Carrier. A long distance carrier.
IETF	Internet Engineering Task Force. A standards body responsible, among other things, for developing standards used in the Internet.
IKE	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPsec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE, which requires digital certificates for authentication.
IntraLATA	Within a Local Access Transport Area
IP	Internet Protocol. An Internet network-layer protocol.
IPsec	Internet Protocol Security, a collection of Internet standards for protecting IP packets with encryption and authentication.

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	Remote Access Dial-In User Service, 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
RTO	Retransmission Timeout
RTP	Real-time Transport Protocol, a protocol defined in IETF RFC 1889 for transporting real-time streams such as voice and video.
S-MTA	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g., Ethernet).
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 BPI+ security protocol, part of the DOCSIS specification.
SCCP	The Signaling Connection Control Part is a protocol within the SS7 suite of protocols that provides two functions in addition to those that are provided within MTP. The first is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	A Service Control Point is a Signaling Point within the SS7 network, identifiable by a Destination Point Code, that provides database services to the network.
SDP	Session Description Protocol. See IETF RFC 2327.
SDU	Service Data Unit. Information that is 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. Any 32-bit SFID must not conflict with a zero-extended 14-bit SID. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs are allocated from the same SFID number space.
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. A SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network.
SHA – 1	Secure Hash Algorithm 1 - a one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
SIP	Session Initiation Protocol, an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. See IETF RFC 3261.
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Security Parameters Index - a field in the IPSEC header that along with the destination IP address provides a unique number for each SA.
SS7	Signaling System Number 7. SS7 is 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. An STP is a node within an SS7 network that routes signaling messages based on their destination address. It 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 used to grant Kerberos tickets.
TGW	Telephony Gateway
TIPHON	Telecommunications & Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value 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
WBEM	Web-Based Enterprise Management (WBEM) is the umbrella under which the DMTF (Desktop Management Task Force) will fit its current and future specifications. The goal of the WBEM initiative is to further management standards using Internet technology in a manner that provides for interoperable management of the Enterprise. There is one DMTF standard today within WBEM and that is CIM (Common Information Model). WBEM compliance means adhering to the CIM. See http://www.dmtf.org

6 IPCABLECOM 1.5

IPCablecom 1.5 is a CableLabs definition for the specifications that define the IPCablecom 1.5 reference architecture.

In this version of the architecture framework, the emphasis is on specification of:

- the subscriber environment and its interface requirements to the IPCablecom network including the DOCSIS HFC access network, Call Management Server, PSTN gateway, and MTA device provisioning components (refer to Section 6.1 and subsequent sections for a description of these components);
- communication across IPCablecom zones and domains to enable end-to-end IP-based connections (refer to Section 6.2 and subsequent sections for a description of zones and domains);
- reliability mechanisms such as availability during power failure;
- electronic surveillance capabilities.

The requirements for these functional components and the standardized interfaces between components are defined in detail in the IPCablecom 1.5 specifications.

IPCablecom 1.5 consists of a variety of functional components, each of which must work in harmony to create a consistent and cost-effective delivery mechanism for packet-based services. This distributed architecture allows incremental development and deployment of new features and services, leaving room for implementation flexibility and product innovation. A key focus of the IPCablecom 1.5 release is the definition of low-cost subscriber equipment and a network architecture that supports digital voice services. Follow-on phases of this project will continue to add support for more advanced functionality. This may require evolution in the IPCablecom call signaling, QoS security, provisioning, billing and security protocols.

IPCablecom 1.5 allows the use of proprietary vendor-specific solutions for interfaces not defined in specifications.

6.1 IPCablecom Architecture Framework

At a very high level, the IPCablecom 1.5 architecture contains three networks: the "DOCSIS HFC Access Network", the "Managed IP Network" and the PSTN. The Cable Modem Termination System (CMTS) provides connectivity between the "DOCSIS HFC Access Network" and the "Managed IP Network". Both the Signaling Gateway (SG) and the Media Gateway (MG) provide connectivity between the "Managed IP Network" and the PSTN. The reference architecture for IPCablecom 1.5 is shown in Figure 1.

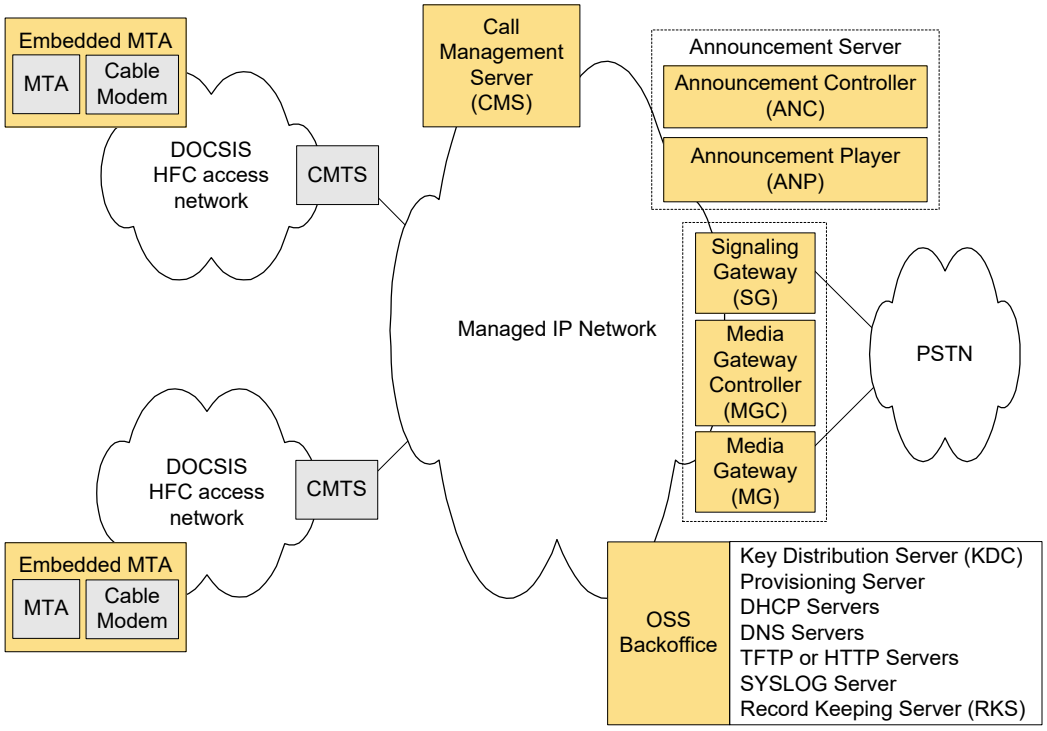

Figure 1. IPCablecom Reference Architecture

The DOCSIS HFC access network provides high-speed, reliable, and secure transport between the customer premise and the cable headend. The access network provides DOCSIS capabilities, including Quality of Service. The DOCSIS HFC access network includes the following functional components: the Cable Modem (CM), the Multimedia Terminal Adapter (MTA), and the Cable Modem Termination System (CMTS).

The Managed IP network serves several functions. First, it provides interconnection between the basic IPCablecom functional components that are responsible for signaling, media, provisioning, and the establishment of Quality of Service on the access network. In addition, the managed IP network provides long-haul IP connectivity between other Managed IP and DOCSIS HFC networks. The Managed IP network includes the following functional components: Call Management Server (CMS), several Operational Support System (OSS) back-office servers, Signaling Gateway (SG), Media Gateway (MG), and Media Gateway Controller (MGC).

The individual network components that are shown in Figure 1 are described in detail in Section 7.

6.2 IPCablecom Zones and Domains

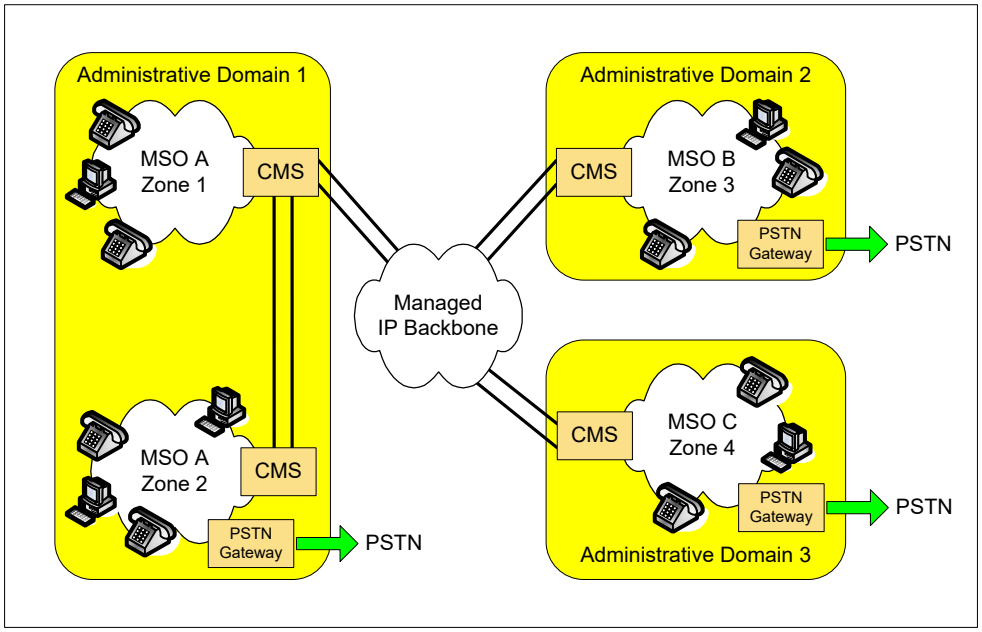

Figure 2. Zones and Administrative Domains

A IPCablecom zone consists of the set of MTAs in one or more DOCSIS HFC access networks that are managed by a single functional CMS as shown in Figure 2. IPCablecom 1.5 defines both interfaces between functional components within a single zone and interfaces between zones (e.g., CMS-CMS).

A IPCablecom domain is made up of one or more IPCablecom zones that are operated and managed by a single administrative entity. A IPCablecom domain may also be referred to as an administrative domain. IPCablecom 1.5 defines interfaces between domains.

6.3 IPCablecom 1.5 Analog Trunking Specifications

IPCablecom 1.5 consists of the twenty-one Specifications and one Technical Report shown in Table 1.

Table 1. IPCablecom 1.5 Specifications and Reports

IPCablecom Specification Reference Number	Specification Name
SCTE 165-2	Audio/Video Codecs
SCTE 165-4	Dynamic Quality-of-Service
SCTE 165-3	Network-based Call Signaling (NCS)
SCTE 165-9	Event Messages
SCTE 165-6	MIBS Framework
SCTE 165-7	MTA MIB
SCTE 165-20	MTA Extension MIB
SCTE 165-8	Signaling MIB
SCTE 165-21	Signaling Extension MIB
SCTE 165-15	Management Event MIB

IPCablecom Specification Reference Number	Specification Name
SCTE 165-5	MTA Device Provisioning
SCTE 165-10	Security
SCTE 165-12	PSTN Gateway Call Signaling Protocol
SCTE 165-17	Audio Server Protocol
SCTE 165-16	Management Event Mechanism
SCTE 165-14	Embedded MTA Analog Interface and Powering
SCTE 165-19	CMS Subscriber Provisioning
SCTE 165-18	CMS to CMS Signaling
SCTE 165-13	Electronic Surveillance Standard
IPCablecom Technical Report Reference Number	**Technical Report Name**
SCTE 165-1	Architecture Framework (this document)

6.4 IPCablecom 1.5 Design Considerations

In order to enable real-time multimedia communications across the cable network infrastructure, IPCablecom 1.5 specifications define protocols in the following areas:

- Call Signaling;
- Quality of Service;
- Media Stream Transport and Encoding;
- Device Provisioning;
- Event Messaging;
- Security;
- Electronic Surveillance;
- Operational Support Systems.

This section provides an overview of the high-level design goals and concepts used in developing the specifications that define the IPCablecom 1.5 reference architecture. Individual IPCablecom specifications should be consulted to obtain detailed protocol requirements for each of these areas.

6.4.1 General Architectural Goals

- Enable voice quality capabilities similar to or better than the PSTN as perceived by the end-user;
- Provide a network architecture that is scalable and capable of supporting millions of subscribers;
- Ensure the one-way delay for local IP access and IP egress (i.e., excluding the IP backbone network) is less than 45ms;
- Leverage existing protocol standards. IPCablecom strives to specify open, approved industry standards that have been widely adopted in other commercial communication networks. This includes protocols approved by the ITU, IETF, IEEE, Telcordia and other communications standards organizations;
- Leverage and build upon the data transport and Quality of Service capabilities provided by DOCSIS;
- Define an architecture that allows multiple vendors to develop low-cost interoperable solutions rapidly, in order to meet Member time-to-market requirements;
- Ensure that the probability of blocking a call can be engineered to be less than 1% during the High Day Busy Hour (HDBH);

- Ensure that call cutoffs and call defects can be engineered to be less than 1 per 10,000 completed calls;
- Support modems (up to V.90 56 kbps) and fax (up to 14.4 kbps);
- Ensure that frame slips due to unsynchronized sampling clocks or due to lost packets occur at a rate of less than 0.25 per minute.

6.4.2 Call Signaling

- Define a network-based signaling architecture;
- Provide end-to-end call signaling for the following call models:
    - calls that originate from the PSTN and terminate on the cable network;
    - calls that originate on the cable network and terminate on the cable network;
    - calls that originate from the cable network and terminate on the PSTN.
    - calls that traverse zones (intradomain) and domains (interdomain)
- Provide signaling to support custom calling features such as:
    - Call Waiting;
    - Cancel Call Waiting;
    - Call Forwarding (no-answer, busy, variable);
    - Three-way Calling;
    - Voice mail Message Waiting Indicator.
- Provide signaling to support Custom Local Area Signaling Services (CLASS) features such as:
    - Calling Number Delivery;
    - Calling Name Delivery;
    - Calling Identity Delivery On Call Waiting;
    - Calling Identity Delivery Blocking;
    - Anonymous Call Rejection;
    - Automatic Callback;
    - Automatic Recall;
    - Distinctive Ringing/Call Waiting;
    - Customer Originated Trace.
- Support signaling consistent with existing IP telephony standards for use within a cable operator's IPCablecom network and when connecting to the PSTN;
- Support ability to dial any domestic or international telephone number (E.164 address) directly;
- Support ability to receive a call from any domestic or international telephone number supported by the PSTN;
- Ensure that a new subscriber may retain a current phone number via Local Number Portability (LNP);
- Support ability to use the IXC of choice for intra-LATA toll (local toll) and inter-LATA (long distance) calls. This includes pre-subscription and "dial-around" (10-1X-XXX);
- Support Call Blocking/Call Blocking Toll restrictions, (e.g., blocking calls to 900-, 976-, etc.);
- Support Operator Services such as emergency and operator-assisted calls, and busy-line-verify.

6.4.3 Quality of Service

- Provide a rich set of policy mechanisms to enable and manage QoS for IPCablecom services over the access network;
- Provide admission control mechanisms for both upstream and downstream directions;
- Allow dynamic changes in QoS while a IPCablecom call is under way;
- Minimize abusive QoS usage, including theft-of-service and denial-of-service attacks. Ensure QoS policy is set and enforced by trusted IPCablecom network elements;
- Provide a priority mechanism for 911 and other priority-based signaling services.

6.4.4 CODEC and Media Stream

- Minimize the effects of latency, packet-loss, and jitter on voice quality in the IP telephony environment;
- Define a minimum set of audio codecs that must be supported on all IPCablecom endpoint devices (MTAs and MGs). Evaluation criteria for mandatory codecs are selected as those most efficient with respect to voice quality, bandwidth utilization, and implementation complexity;
- Accommodate evolving narrow-band and wide-band codec technologies;
- Specify echo cancellation and voice activity detection mechanisms;
- Support for transparent, error-free Dual-Tone Multi Frequency (DTMF) transmission and detection via both inband transmission and DTMF relay;
- Support terminal devices for the deaf and hearing impaired;
- Provide mechanisms for codec switching when fax and modem services are required;
- Support fax relay for reliable transmission of fax over IP networks;
- Support reliable transmission of modem signals over IP networks;
- Support calculation and reporting of VoIP Metrics to monitor voice quality.

6.4.5 Device Provisioning and OSS

- Support dynamic and static provisioning of customer premise equipment (MTA and Cable Modem);
- Common provisioning changes should not require reboot of MTA;
- Allow dynamic assignment and management of IP addresses for subscriber devices;
- Ensure that real-time provisioning and configuration of MTA software does not adversely affect subscriber service;
- Define MIB modules for managing customer premise equipment (MTA) using the IETF Simple Network Management Protocol (SNMP).

6.4.6 Security

- Enable residential voice capabilities with the same or higher level of perceived privacy as in the PSTN;
- Provide protection against attacks on the MTA;
- Protect the MSO from various denial of service, network disruption and theft-of-service attacks;
- Design considerations include confidentiality, authentication, integrity, and access control.

6.4.7 Electronic Surveillance

- Support the ability to perform electronic surveillance by reporting call data and call content.

7 IPCABLECOM FUNCTIONAL COMPONENTS

This section describes the functional components present in a IPCablecom 1.5 network. Component descriptions are not intended to define or imply product implementation requirements but rather to describe the functional role of each of these components in the reference architecture. Note that specific product implementations may combine functional components as needed. Not all components are required to be present in a particular instance of a IPCablecom Network.

The IPCablecom architecture contains trusted and untrusted network elements. Trusted network elements are typically located within a Cable Operator's managed backbone network. Untrusted network elements, such as the MTA and its embedded CM, are typically located within the subscriber's home and are therefore outside of the MSO's facility.

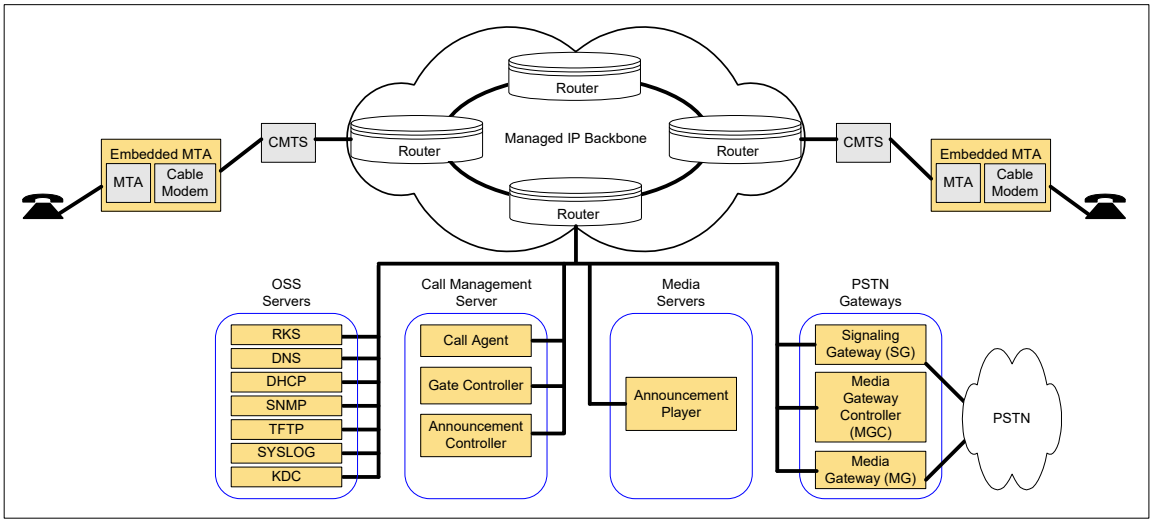

Figure 3. IPCablecom Component Reference Model

7.1 Multimedia Terminal Adapter (MTA)

An MTA is a IPCablecom client device that contains a subscriber-side interface to the subscriber's CPE (*e.g.*, telephone) and a network-side signaling interface to call control elements in the network. An MTA provides codecs and all signaling and encapsulation functions required for media transport and call signaling.

MTAs reside at the customer site and are connected to other IPCablecom network elements via the HFC access network (DOCSIS). IPCablecom 1.5 MTAs are required to support the Network-based Call Signaling (NCS) protocol.

A IPCablecom 1.5 MTA is a hardware device that incorporates a DOCSIS cable modem; since it contains an embedded cable modem, a IPCablecom 1.5 MTA is sometimes called an "embedded MTA", or "E-MTA". Figure 4 shows a representative functional diagram of an E-MTA.

7.1.1 MTA Functional Requirements

An MTA is responsible for providing the following functionality:

- NCS call signaling with the CMS;
- QoS signaling with the CMTS;
- Authentication, confidentiality and integrity of some messages between the MTA and other IPCablecom network elements;
- Mapping media streams to the MAC services of the DOCSIS access network;
- Encoding/decoding of media streams;
- Providing multiple audio indicators to phones, such as ringing tones, call-waiting tones, stutter dial tone, dial tone, etc.;

- Standard PSTN analog line signaling for audio tones, voice transport, caller-id signaling, DTMF, and message waiting indicators;
- The G.711 audio codec [33] and low bit-rate audio codecs;
- One or more telephone interfaces (e.g., RJ11 analog interface as defined by Telcordia (formerly Bellcore) GR-909).

Additional MTA functionality is defined in other IPCablecom specifications such as NCS Signaling [3], Dynamic Quality-of-Service [2], Audio-Video Codecs [1], MIBS [5] [6], Security [10], and MTA Device Provisioning [9] (note: this is not an exhaustive list).

7.1.2 MTA Attributes

The following attributes characterize the E-MTA:

- An embedded MTA has two MAC addresses, one for the cable modem and one for the MTA;
- An embedded MTA has two IP addresses, one for the cable modem and one for the MTA;
- An embedded MTA has two Fully Qualified Domain Names (FQDN), one for the cable modem and one for the MTA;
- At least one telephone number per configured physical port;
- Device capabilities;
- The MTA's associated CMSs.

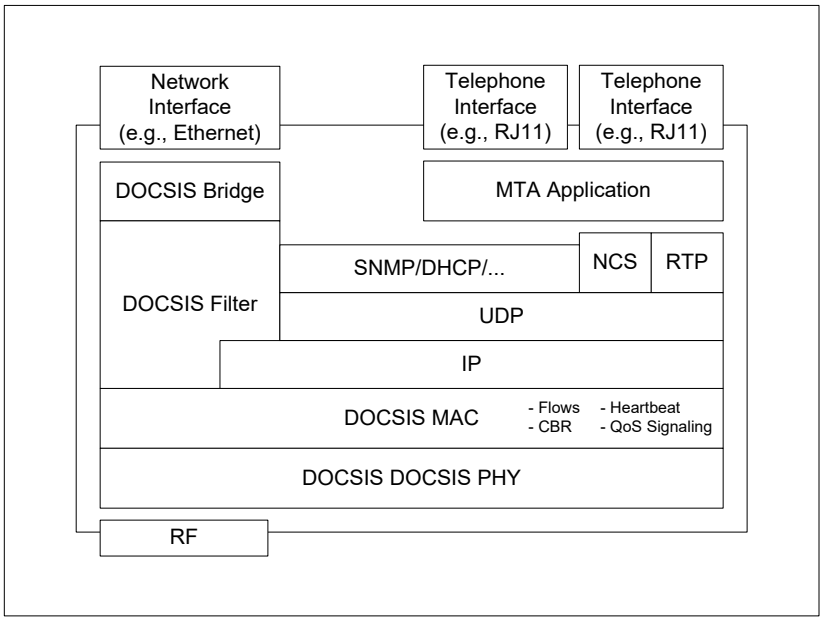

Figure 4. E-MTA Conceptual Functional Architecture

7.2 Cable Modem (CM)

The cable modem (CM) is a network element that is defined by DOCSIS [14]. The CM is a modulator/demodulator residing on the customer premises that provides data transmission over the cable network using the DOCSIS protocol. In IPCablecom, the CM plays a key role in handling the media stream and provides services such as classification of traffic into service flows, rate shaping, and prioritized queuing.

7.3 HFC Access Network

IPCablecom-based services are carried over the Hybrid Fiber/Coax (HFC) access network. The access network is a bi-directional, shared-media system that consists of the Cable Modem (CM), the Cable Modem Termination System (CMTS), and the DOCSIS MAC and PHY access layers.

7.4 Cable Modem Termination System (CMTS)

The CMTS provides data connectivity and complementary functionality to cable modems over the HFC access network (DOCSIS). It also provides connectivity to wide area networks. The CMTS is located at the cable television system head-end or distribution hub.

The CMTS is responsible for the following functions:

- Providing the required QoS to the CM based upon DOCSIS requests which are checked against policy;
- Allocating upstream bandwidth in accordance with CM requests and network QoS policies;
- Classifying each arriving packet from the backbone-side interface and assigning it to a QoS level based on defined filter specifications;
- Policing the TOS field in packets received from the cable network, in order 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;
- Converting QoS Gate parameters into DOCSIS QoS parameters;
- Recording usage of access network resources per call using IPCablecom Event Messages.

7.4.1 CMTS Gate

The CMTS is responsible for allocating and scheduling upstream and downstream bandwidth in accordance with MTA requests and QoS authorizations established by the Gate Controller.

The CMTS implements a IPCablecom Dynamic QoS Gate or CMTS Gate between the DOCSIS cable network and an IP Backbone. The CMTS Gate is a functional component of the CMTS that performs traffic classification and enforces QoS policy on media streams as directed by the Gate Controller (GC). The CMTS Gate is controlled by the Gate Controller (GC), a logical QoS management component within the CMS that coordinates all Quality of Service authorization and control.

7.5 Call Management Server (CMS)

The Call Management Server provides call control and signaling related services for the MTA, CMTS, and PSTN gateways in the IPCablecom network. The CMS is a trusted network element that resides on the managed IP portion of the IPCablecom network.

A IPCablecom 1.5 CMS consists of the following logical IPCablecom components:

- **Call Agent (CMS/CA)** – Call Agent is a term that is often used interchangeably with CMS, especially in the MGCP specification. In IPCablecom, Call Agent (CA) refers to the control component of the CMS that is responsible for providing signaling services using the NCS protocol to the MTA. In this context, Call Agent responsibilities include but are not limited to:
    - Implementing call features;
    - Maintaining call state;
    - Guide the use of codecs within the subscriber MTA device;
    - Collecting and processing dialed digits;
    - Collecting and classifying user actions (e.g., hook-state actions);
    - Control the usage of Voice Metrics by the MTA.
- **Gate Controller (CMS/GC)** – The Gate Controller (GC) is a logical QoS management component within the CMS that coordinates all Quality of Service authorization and control. Gate Controller functionality is defined in the IPCablecom Dynamic Quality of Service (DQoS) specification [2].

The CMS may contain the following logical components:

- **Media Gateway Controller** - The MGC is a logical signaling management component used to control PSTN Media Gateways. The MGC function is defined in detail later in this section.

The CMS may also provide functions such as:

- Call management and CLASS features;
- Directory Services and Address translation;
- Call routing;
- Record usage of local number portability services.

For the purposes of this standard, protocols that implement the functionality of the CMS are specified as terminating at the CMS – actual implementations may distribute the functionality in one or more servers that sit "behind" the Call Management Server.

7.6 PSTN Gateway

IPCablecom allows MTAs to interoperate with the current PSTN through the use of PSTN Gateways.

In order to enable operators to minimize cost and optimize their PSTN interconnection arrangements, the PSTN Gateway is decomposed into three functional components:

- **Media Gateway Controller (MGC)** – The MGC maintains the call state and controls the overall behavior of the PSTN gateway.
- **Signaling Gateway (SG)** – The SG provides a signaling interconnection function between the PSTN SS7 signaling network and the IP network.
- **Media Gateway (MG)** – The MG terminates the bearer paths and transcodes media between the PSTN and IP network.

7.6.1 Media Gateway Controller (MGC)

The Media Gateway Controller (MGC) receives and mediates call-signaling information between the IPCablecom network and the PSTN. It maintains and controls the overall call state for calls requiring PSTN interconnection.

The MGC controls the MG by instructing it to create, modify, and delete connections that support the media stream over the IP network. The MGC also instructs the MG to detect and generate events and signals such as continuity test tones for ISUP trunks. Each trunk is represented as an endpoint.

The following functions are performed by the Media Gateway Controller:

- Call Control Function – maintains and controls the overall PSTN Gateway call state for the portion of a call that traverses the PSTN Gateway. The function communicates with external PSTN elements as needed for PSTN Gateway call control, e.g., by generating TCAP queries.
- IPCablecom Signaling – terminates and generates the call signaling from and to the IPCablecom side of the network.
- MG Control – The MG Control function exercises overall control of endpoints in the Media Gateway:
    - Event Detection instructs the MG to detect events: e.g., in-band tones, on the endpoint and possibly on connections;
    - Signal Generation instructs the MG to generate in-band tones and signals on the endpoint and possibly on connections;
    - Connection Control instructs the MG how to handle connections with endpoints in the MG;
    - Attribute Control instructs the MG regarding the attributes to apply to an endpoint and/or connection: e.g., encoding method, use of echo cancellation, security parameters, etc.;
- External Resource Monitoring – maintains the MGC's view of externally visible MG resources and packet network resources: e.g., endpoint availability;
- Call Routing – makes call routing decisions;
- Security – ensures that any entity communicating with the MGC adheres to the security requirements;
- Usage Recording via Event Messages – records usage of resources per call.

7.6.2 Media Gateway (MG)

The Media Gateway provides bearer connections between the PSTN and the IPCablecom IP network. Each bearer is represented as an endpoint, and the MGC instructs the MG to set-up and control media connections to other endpoints on the IPCablecom network. The MGC also instructs the MG to detect and generate events and signals relevant to the call state known to the MGC.

7.6.2.1 Media Gateway Functions

The following functions are performed by the Media Gateway:

- Terminates and controls physical circuits in the form of bearer channels from the PSTN;
- Detects events on endpoints and connections as requested by the MGC;
- Generates signals on endpoints and connections as instructed by the MGC (e.g., continuity tests);
- Creates, modifies, and deletes connections to and from other endpoints as instructed by the MGC;
- Controls and assigns internal media processing resources to specific connections on receipt of requests from the Media Gateway Controller;
- Performs media transcoding between the PSTN and the IPCablecom network. This includes all aspect of the transcoding, such as codecs, echo cancellation, etc.
- Ensures that any entity communicating with the MG adheres to the security requirements;
- Determines usage of relevant resources and attributes associated with those resources: e.g., number of media bytes sent and received;
- Reports usage of network resources to the MGC.

7.6.3 Signaling Gateway (SG)

The Signaling Gateway function sends and receives circuit-switched network signaling at the edge of the IPCablecom network. For IPCablecom 1.5, the signaling gateway function supports only non-facility associated signaling in the form of SS7.

7.6.3.1 SS7 Signaling Gateway Functions

The following functions are performed by the Signaling Gateway function:

- Terminates physical SS7 signaling links from the PSTN (A, F links);
- Implements security features, to ensure that the Gateway security is consistent with IPCablecom and SS7 network security requirements;
- Terminates Message Transfer Part (MTP) level 1, 2 and 3;
- Implements MTP network management functions as required for any SS7 signaling point;
- Performs ISUP Address Mapping to support flexible mapping of Point Codes (both Destination Point Code and Origination Point Code) and/or Point Code/CIC code combination contained within SS7 ISUP messages to the appropriate Media Gateway Controller (MGC) (either a domain name or an IP address). The addressed MGC will be responsible for controlling the Media Gateway, which terminates the corresponding trunks;
- Performs TCAP Address Mapping to map Point Code/Global Title/Signaling Connectionless Control Part (SCCP) Subsystem Number combinations within SS7 TCAP messages to the appropriate Media Gateway Controller or Call Management Server;
- Provides mechanism for certain trusted entities ("TCAP Users") within the IPCablecom network, such as Call Agents, to query external PSTN databases via TCAP messages sent over the SS7 network;
- Implements the transport protocol required to transport the signaling information between the Signaling Gateway and the Media Gateway Controller.

7.7 OSS Back Office Components

The OSS back office contains business, service, and network management components supporting the core business processes. As defined by the ITU TMN framework, the main functional areas for OSS are fault management, performance management, security management, accounting management, and configuration management.

IPCablecom 1.5 defines a limited set of OSS functional components and interfaces to support MTA device provisioning and Event Messaging to carry billing information.

7.7.1 Security Server – Key Distribution Center (KDC)

For IPCablecom, the term KDC is utilized for a Kerberos security server. The Kerberos protocol with the public key PKINIT extension is used for key management on the interfaces between the MTA and the CMS and Provisioning Server. Refer to [10] for more information.

Following MTA authentication using the PKINIT protocol, the KDC grants Kerberos tickets to the MTA. A ticket contains information used to configure security for the call signaling between the MTA and the CMS (if the MTA is to communicate with the CMS using a secured interface) and for the management interface between the MTA and the Provisioning Server (if the MTA is to be managed over a secured interface). Tickets are issued:

- during device provisioning. In the case when the MTA reboots and a saved ticket is still valid, then the MTA will not need to execute the PKINIT exchange to request a new ticket from the KDC.
- when a ticket expires. Under normal circumstances, tickets expire roughly once per week.

7.7.2 Dynamic Host Configuration Protocol Server (DHCP)

The DHCP server is a back office network element used during the MTA device provisioning process to allocate IP addresses and other client configuration information. See IETF RFC2131 [17].

7.7.3 Domain Name System Server (DNS)

The DNS server is a back office network element used to map between domain names and IP addresses.

7.7.4 Trivial File Transfer Protocol Server or Hypertext Transfer Protocol Server (TFTP or HTTP)

The TFTP server is a back office network element used during the MTA device provisioning process to download a configuration file to the MTA. An HTTP server may be used for the same purpose instead of a TFTP server.

7.7.5 SYSLOG Server (SYSLOG)

The SYSLOG server is an optional back office network element used to collect event notification messages indicating that certain events such as device errors have occurred.

7.7.6 Record Keeping Server (RKS)

The RKS is a trusted network element component that receives IPCablecom Event Messages from other trusted IPCablecom network elements such as the CMS, CMTS, and MGC. The RKS also, at a minimum, is a short-term repository for IPCablecom Event Messages. The RKS may assemble or correlate the Event Messages into coherent sets or Call Detail Records (CDRs), which are then made available to other back office systems such as billing or fraud detection.

7.8 Announcement Server (ANS)

An Announcement Server (ANS) is a network component that manages and plays informational tones and messages in response to events that occur in the network. An ANS is a logical entity composed of an Announcement Controller (ANC) and an Announcement player (ANP).

7.8.1 Announcement Controller (ANC)

The ANC initiates and manages all announcement services provided by the Announcement Player. The ANC requests the ANP to play announcements based on call state as determined by the CMS. When information is collected from the end-user by the ANP, the ANC is responsible for interpreting this information and manage the session accordingly. Hence, the ANC may also manage call state.

7.8.2 Announcement Player (ANP)

The Announcement Player is a media resource server. It is responsible for receiving and interpreting commands from the ANC and for delivering the appropriate announcement(s) to the MTA. The ANP also is responsible for accepting and reporting user inputs (e.g., DTMF tones). The ANP functions under the control of the ANC.

8 PROTOCOL INTERFACES

Protocol specifications have been defined for most of the component interfaces in the IPCablecom 1.5 architecture. An overview of each protocol interface is provided within this section. The individual IPCablecom specifications should be consulted for the complete protocol requirements.

It is possible that some of these interfaces may not exist in a given vendor's product implementation. For example, if several functional IPCablecom components are combined then it is possible that some of these interfaces are internal to that component.

8.1 Call Signaling Interfaces

Call signaling requires multiple interfaces within the IPCablecom architecture. These interfaces are identified in Figure 5. Each interface in the diagram is labeled, and further described in the subsequent Table 2.

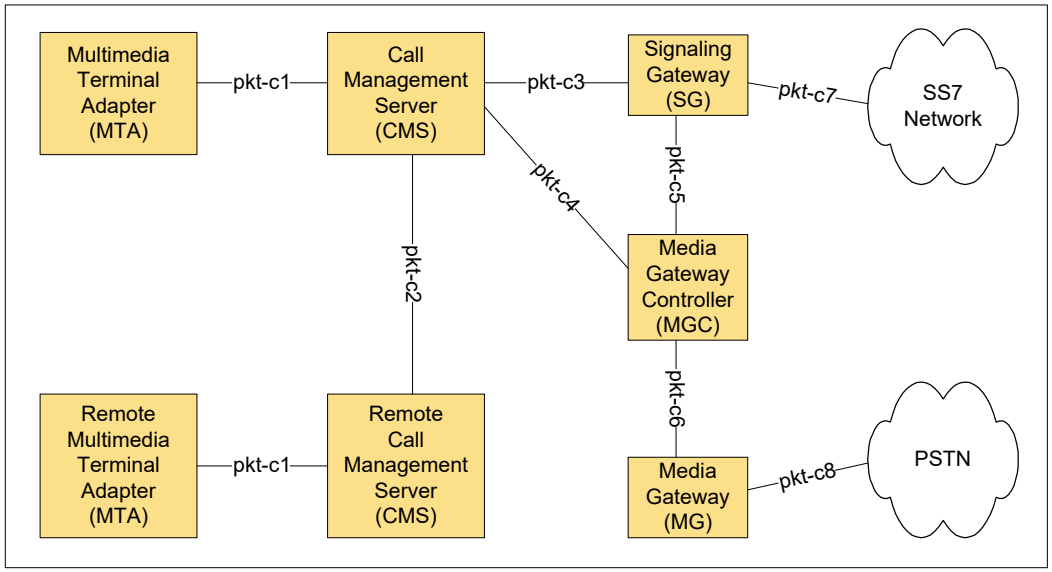

Figure 5. Call Signaling Interfaces

Table 2. Call Signaling Interfaces

Interface	IPCablecom Functional Component	Description
pkt-c1	MTA – CMS	Call signaling messages exchanged between the MTA and CMS using the NCS protocol, which is a profile of MGCP.
pkt-c2	CMS-CMS	Call signaling messages exchanged between CMSes. The protocol for this interface is CMSS.
pkt-c3	CMS – SG	Call signaling messages exchanged between the CMS and SG. The protocol for this interface is not defined in IPCablecom 1.5.
pkt-c4	CMS – MGC	Call signaling messages exchanged between the CMS and MGC. The protocol for this interface is CMSS.
pkt-c5	SG – MGC	Call signaling messages exchanged between the MGC and SG. The protocol for this interface is not defined in IPCablecom 1.5.
pkt-c6	MGC – MG	Interface for control of the Media Gateway using the TGCP protocol, which is a profile of MGCP similar (but not identical) to NCS.

Interface	IPCablecom Functional Component	Description
pkt-c7	SG – SS7	The SG terminates physical SS7 signaling links from the PSTN (A, F links). The following protocols are supported: ISUP User Interface. Provides an SS7 ISUP signaling interface to external PSTN carriers. TCAP User Interface. Provides mechanism for certain trusted entities ("TCAP Users") within the IPCablecom network, such as Call Agents, to query external PSTN databases via TCAP messages sent over the SS7 network.
pkt-c8	MG – PSTN	This interface defines bearer channel connectivity from the Media Gateway to the PSTN.

8.1.1 Network-based Call Signaling (NCS) Framework

The IPCablecom Network-based Call Signaling (NCS) protocol (pkt-c1) is a profile of the MGCP call signaling protocol defined in IETF RFC 3435 [31]. The NCS architecture places call state and feature implementation in a centralized component, the Call Management Server (CMS), and places device control intelligence in the MTA. The MTA passes device events to the CMS, and responds to commands issued from the CMS. The CMS, which may consist of multiple geographically or administratively distributed systems, is responsible for setting up and tearing down calls, providing services such as CLASS and custom calling features, performing call authorization, and generating billing event records, etc.

The signaling functions necessary to provide service are divided between the MTA and the CMS. For example, a simple basic call could be implemented by the following sequence: the CMS instructs the MTA to inform the CMS when the phone goes off hook and seven DTMF digits have been entered. When this sequence of events occurs, the MTA notifies the CMS. The CMS then instructs the MTA to create a connection, reserve QoS resources through the access network for the pending voice connection, and also to play a locally generated ringback tone. The CMS in turn communicates with a remote CMS (or MGC) to set up the call. When the CMS detects answer from the far end, it instructs the MTA to stop the ringback tone, activate the media connection between the MTA and the far-end MTA, and begin sending and receiving media stream packets.

By centralizing call state and service processing in the CMS, the service provider is in a position to manage centrally the service provided. In addition, the service provider has access to all the call-control software and hardware in the event that a defect occurs that impacts subscriber services. Software is controlled, and may be updated in debugging and resolution cycles that do not require deployment of field personnel to the customer premise. Additionally, the service provider has direct control over the services provided and their associated revenue streams.

8.1.2 PSTN Signaling Framework

PSTN signaling interfaces are summarized in Table 2 (pkt-c3 through pkt-c8). These interfaces provide access to PSTN-based services and to PSTN subscribers from the IPCablecom network.

The IPCablecom PSTN signaling framework consists of a PSTN gateway that is divided into three functional components:

- Media Gateway Controller (MGC)
- Media Gateway (MG)
- Signaling Gateway (SG)

The Media Gateway Controller and the Media Gateway are analogous to, respectively, the CMS and MTA in the NCS framework. The Media Gateway provides bearer and in-band signaling connectivity to the PSTN. The Media Gateway Controller implements all the call state and intelligence and controls the operation of the Media Gateway through the TGCP protocol (pkt-c6) [8]. This includes creation, modification and deletion of connections. TGCP is a profile of the MGCP call signaling protocol defined in IETF RFC 3435 and is very similar (but not identical) to NCS.

The CMS and the MGC may each send TCAP queries (e.g., 800 number lookup, LNP lookup) to an SS7 Service Control Point (SCP) via the SG (pkt-c3 and pkt-c5). The MGC, via the SG, also exchanges ISUP signaling with the PSTN's SS7 entities for trunk management and control. The interface SG and the CMS or MGC is not defined in IPCablecom 1.5.

8.1.3 CMS to CMS Signaling Framework

IPCablecom 1.5 supports both inter-domain and intra-domain CMS-CMS and CMS-MGC signaling as defined in the IPCablecom CMSS specification [11]. The CMSS signaling architecture is based on the IETF Session Initiation Protocol (SIP) (IETF RFC 3261 [26]). CMSS defines a call signaling protocol. It does not address routing in the network.

The CMS contains a SIP User Agent Client (UAC) and User Agent Server (UAS). The user agent maintains call state during the life of the call, and monitors the MTA for state changes that affect the call. The interface between the CMS and the MTA is NCS. CMSS messages for setting up a new call, or changing the attributes or participants of an active call, are initiated by the CMS. The CMS in turn is typically driven to this by signaling from the MTA, e.g., by receiving an NCS message informing about dialed digits. A CMS includes a Gate Controller (GC) function. The User Agent part of the CMS participates in the CMSS signaling and the Gate Controller part participates in the D-QoS signaling. Together, they control the coordination of the signaling for call setup and resource management.

8.2 Media Streams

The IETF standard Real-time Transport Protocol (RTP) (IETF RFC 1889) is used to transport media streams in the IPCablecom network [15]. IPCablecom uses the RTP profile for audio streams as defined in IETF RFC 1890 [18].

The primary media flow paths in the IPCablecom network architecture are shown in Figure 6. Note that the media paths traverse the CMTSs even though this is not explicitly represented in Figure 6.

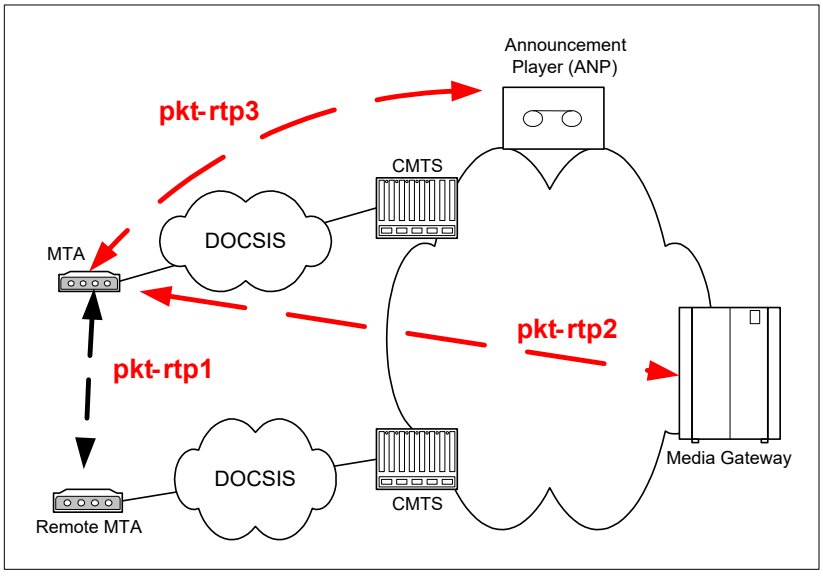

Figure 6. RTP Media Stream Flows in a IPCablecom Network

The primary media flow paths in the IPCablecom network architecture are described in Table 3.

Table 3. RTP Media Stream Flows

Interface	IPCablecom Functional Component	Description
pkt-rtp1	MTA – MTA	Media flow between MTAs. Includes, for example, encoded voice and fax.
pkt-rtp2	MTA – MG	Media flow between the MG and the MTA. Includes, for example, tones, announcements, and PSTN media flow.
pkt-rtp3	MTA – ANP	Media flow between the ANP and the MTA. Includes, for example, tones and announcements sent to the MTA by the Announcement Player.

RTP encodes a single channel of multimedia information in a single direction. Inside each RTP header, a 7-bit Payload Type (PT) indicates which encoding algorithm, e.g.,G.711, is used inside the payload of the packet. Most of the common audio algorithms are assigned to particular PT values in the range 0 through 95. The range 96 through 127 is reserved for "dynamic" RTP payload types, where the binding between the encoding algorithm and the payload type is established through signaling.

The packet format for RTP data transmitted over IP over Ethernet is depicted in Figure 7.

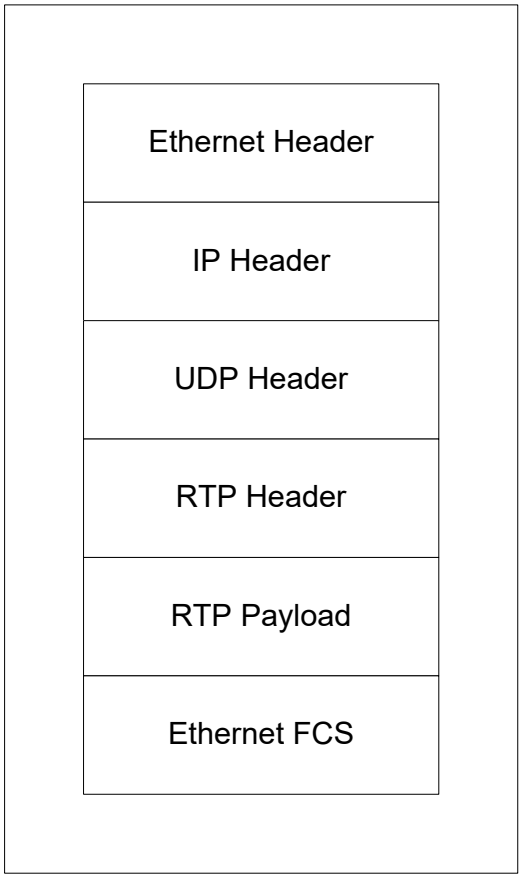

Figure 7. RTP Packet Format

The length of the RTP Payload as well as the frequency with which packets are transmitted depends on the encoding algorithm defined by the Payload Type field.

RTP sessions are established dynamically by the endpoints involved, so there is no "well-known" UDP port number used to receive RTP information. The Session Description Protocol (SDP) [16] was developed by the IETF to

communicate the particular IP address and UDP port used by a particular RTP session. SDP is used by both NCS and TGCP.

The packet header overhead of Ethernet, IP, UDP, and RTP is significant when compared to a typical RTP Payload size, which can be as small as just a few bytes for packetized voice. The DOCSIS specifications address this issue with a Payload Header Suppression feature for abbreviating common headers.

The ITU-T T.38 recommendation [32] is also used to transport facsimile media in IPCablecom networks, refer to Section 9.7 of this document for more details.

8.2.1 Real-time Transport Control Protocol (RTCP)

RTCP is defined in IETF RFC 1889. It is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. RTCP provides feedback on the quality of the data distribution. This is an integral part of the RTP's role as a transport protocol and is related to the flow and congestion control functions of other transport protocols. IPCablecom 1.5 supports the usage of RTCP on all its endpoints.

Extensions to RTCP exist in order to better assess the quality of a voice call and diagnose problems on the network more effectively. These extensions are called RTCP Extended Reports (RTCP XR), and are defined in IETF RFC 3611 [27]. RTCP XR contains many sets of metrics. IPCablecom 1.5 supports only the RTCP XR Voice Metrics on all endpoints.

8.3 MTA Device Provisioning

MTA Device Provisioning enables an MTA to register with the operator network and to provide subscriber services over the HFC network. Provisioning covers initialization, authentication, and registration functions required for MTA device provisioning. The IPCablecom 1.5 MTA Device Provisioning Specification [9] also includes attribute definitions required in the MTA configuration file.

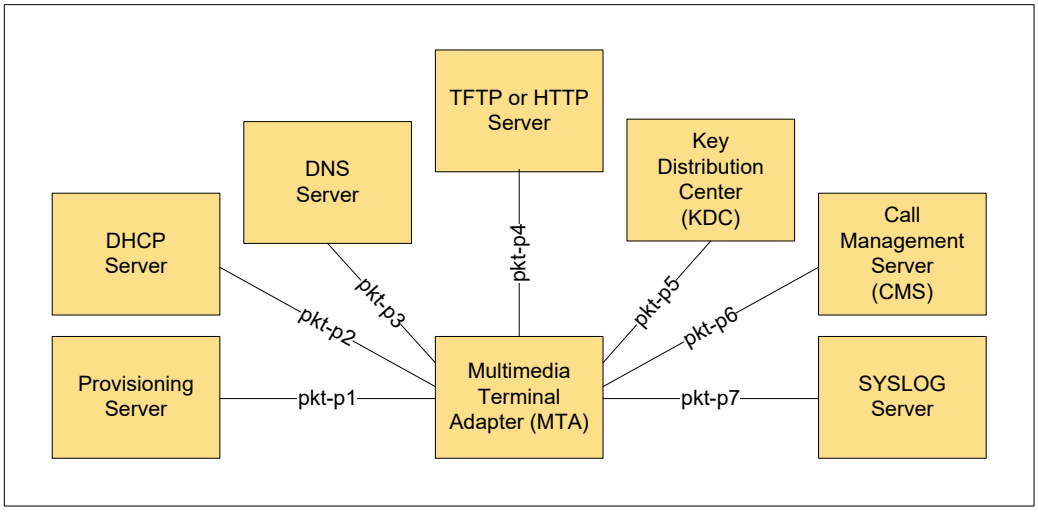

Figure 8. IPCablecom Provisioning Interfaces

Table 4 describes the provisioning interfaces shown in Figure 8.

Table 4. Device Provisioning Interfaces

Interface	IPCablecom Functional Component	Description
pkt-p1	MTA-PROV Server	Interface to exchange device capability as well as MTA device and endpoint information between the MTA and Provisioning Server, using the SNMP protocol. The MTA also uses this interface to send notification that provisioning has completed along with a pass/fail status, using the SNMP protocol.
pkt-p2	MTA- DHCP server	DHCP interface between the MTA and DHCP server; used to assign an IP address to the MTA and to provide additional low-level information used by the MTA when attaching itself to the network.
pkt-p3	MTA – DNS server	DNS interface between the MTA and DNS server; used to obtain the IP address of a IPCablecom server given its fully qualified domain name.
pkt-p4	MTA – HTTP or TFTP server	Interface used by the MTA to download its device configuration file from the TFTP server or HTTP server.
pkt-p5	MTA – KDC	Interface used by the MTA to obtain Kerberos tickets from the Key Distribution Center using the Kerberos protocol.
pkt-p6	MTA – CMS	Interface used between the MTA and the CMS to establish an IPsec Security Association using the Kerberos protocol.
pkt-p7	MTA – SYSLOG	Interface used by the MTA to send network event notifications to a SYSLOG server including information related to the status of the device provisioning.

8.4 SNMP Element Management Layer Interfaces

IPCablecom requires SNMP to interface the MTA to element management systems for MTA device provisioning. IPCablecom specifications rely on standard SNMP protocol operations such as "traps" and "informs" for event reporting, and "sets" and "gets" for device provisioning and management. The IPCablecom MIB modules are defined in the IPCablecom 1.5 MIBs Framework specification [7] and defined in the IPCablecom 1.5 MTA MIB specification [5] and the IPCablecom 1.5 Signaling MIB specification [6].

The IPCablecom 1.5 Signaling MIB module contains Network-based Call Signaling information for provisioning on both a device and a per-endpoint basis. The IPCablecom 1.5 MTA MIB module contains data for device provisioning and for supporting provisioned functions such as event logging.

8.5 Event Messages Interfaces

8.5.1 Event Message Framework

An Event Message is a data record containing information about network usage and activities. A single Event Message may contain a complete set of data regarding usage or it may only contain part of the total usage information. When correlated by the Record Keeping Server (RKS), information contained in multiple Event Messages provides a complete record of the service afforded a call. This complete record of the service is often referred to as a Call Detail Record (CDR). Event Messages or CDRs may be sent to one or more back office applications such as a billing system, fraud detection system, or pre-paid services processor.

The IPCablecom 1.5 Event Messages specification [4] defines the structure of the Event Message data record and defines RADIUS (IETF RFCs 2865 [21] and 2866 [22])as the transport protocol. The Event Message data record format is designed to be flexible and extensible in order to carry information about network usage for a wide variety of services. Figure 9 shows a representative Event Message architecture.

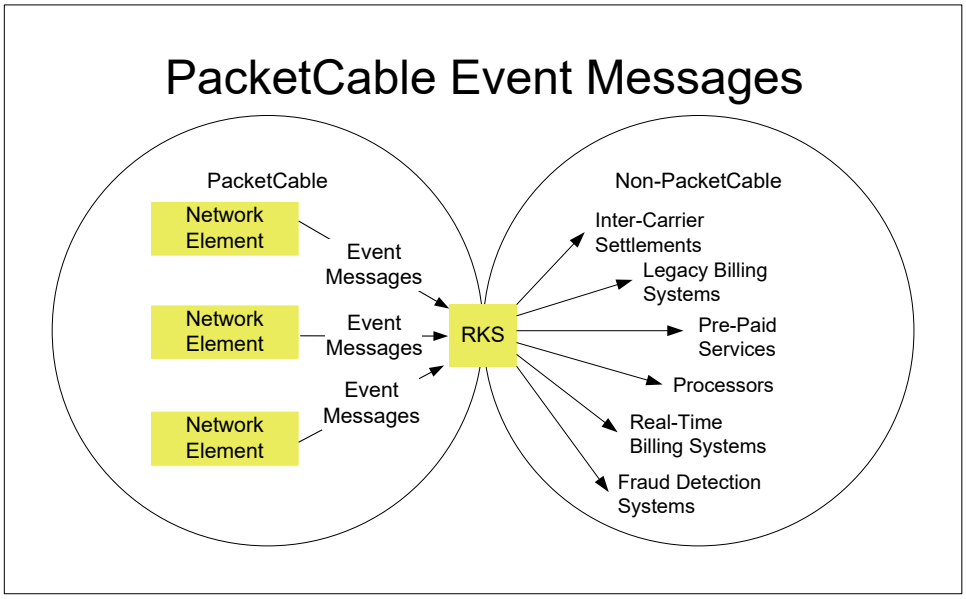

Figure 9. Representative Event Messages Architecture

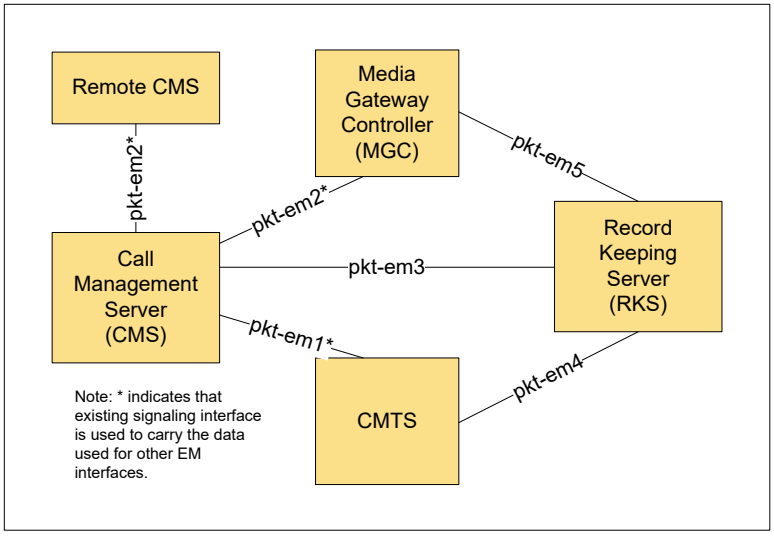

Figure 10. Event Message Interfaces

Table 5 describes the Event Message interfaces shown in Figure 10.

Table 5. Event Message Interfaces

Interface	IPCablecom Functional Component	Description
pkt-em1	CMS-CMTS	DQoS Gate-Set message carrying Billing Correlation ID and other data required for the CMTS to send Event Messages to an RKS.
pkt-em2	CMS-CMS CMS-MGC	The protocol for this interface is CMSS. Used to carry Billing Correlation ID and other data required for billing data.
pkt-em3	CMS-RKS	RADIUS protocol carrying IPCablecom Event Messages.

Interface	IPCablecom Functional Component	Description
pkt-em4	CMTS-RKS	RADIUS protocol carrying IPCablecom Event Messages.
pkt-em5	MGC-RKS	RADIUS protocol carrying IPCablecom Event Messages.

8.6 Quality of Service (QoS)

8.6.1 QoS Framework

The IPCablecom QoS Framework is represented in Figure 11.

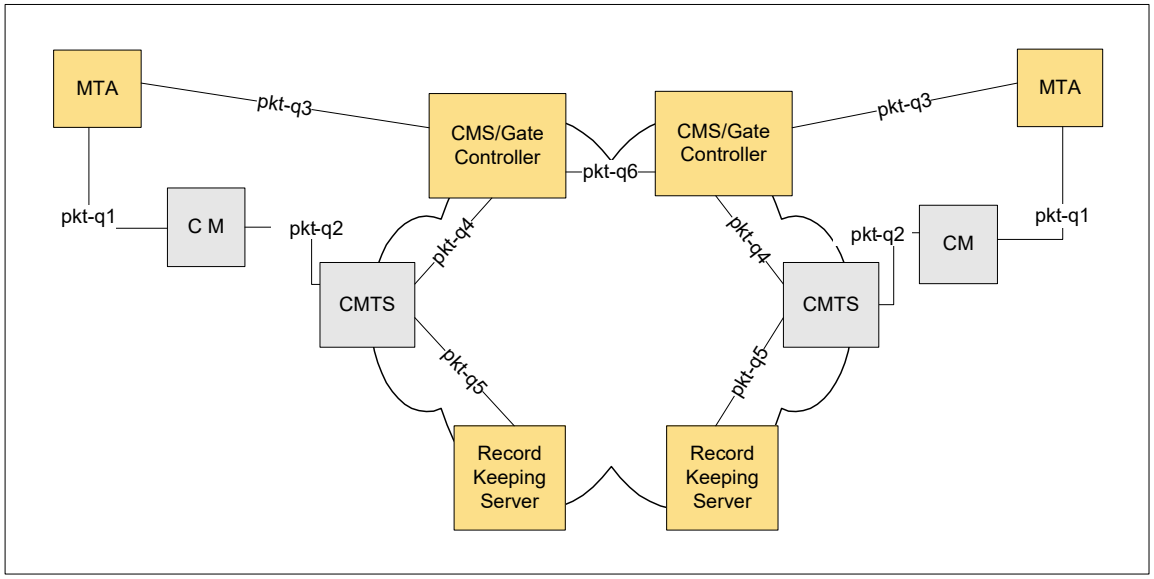

Figure 11. IPCablecom QoS Interfaces

Table 6 briefly identifies each interface and describes how each interface is used in the IPCablecom 1.5 Dynamic QoS Specification (DQoS) [2].

Table 6. QoS Interfaces

Interface	IPCablecom Functional Component	DQoS Description
pkt-q1	MTA – CM	MTA, MAC Control Service Interface (not exposed)
pkt-q2	CM – CMTS (DOCSIS)	DOCSIS, CM-initiated
pkt-q3	MTA – CMS	NCS
pkt-q4	GC – CMTS	Gate Management
pkt-q5	CMTS – RKS	Billing
Pkt-q6	CMS – CMS	Session Establishment

The function of each QoS interface is further described in Table 7.

Table 7. QoS Interfaces

Interface	IPCablecom Functional Component	Description
pkt-q1	MTA – CM	This 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 packet and scheduling for minimization of latency and jitter. • *Transport*: used to process packets in the media stream and perform appropriate per-packet QoS processing. The MTA/CM interface is conceptually defined in the DOCSIS RFI specification [14]. It is not exposed to the IPCablecom layers.
pkt-q2	CM – CMTS	This interface is the DOCSIS QoS interface (control, scheduling, and transport). It should be noted that in IPCablecom 1.5 most control functions can be initiated only by the CM. The CMTS, as always, is the final policy arbiter and granter of admission into the DOCSIS access network. The following capabilities of the DOCSIS MAC are used within IPCablecom: • Multiple service flows, each with its own class of upstream traffic, both single and multiple voice connections per DOCSIS service flow. • Prioritized classification of traffic streams to service flows. • Guaranteed minimum/constant bitrate scheduling service. • Constant bit rate scheduling with traffic activity detection service (slow down, speed up, stop, and restart scheduling). • DOCSIS packet header suppression for increased call density. • DOCSIS classification of voice flows to service flow. • DOCSIS synchronization of CODEC to CMTS clock and Grant Interval. • Two-phase activation of QoS resources. • TOS packet marking at network layer. • Guarantees on latency and jitter. • Internal sub-layer signaling between IPCablecom MTA and DOCSIS. This interface is further defined in the DOCSIS RFI specification [14].
pkt-q3	MTA –CMS	Signaling interface between the MTA and CMS. Many parameters are signaled across this interface such as the media stream, IP addresses, port numbers, and the selection of Codec and packetization characteristics.
pkt-q4	GC – 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-q5	CMTS – RKS	This interface is used by the CMTS to report changes in the QoS resources used by a call. This interface is defined in the Event Messages specification.
pkt-q6	CMS - CMS	This interface is used to establish intradomain and interdomain sessions. This interface includes functionality to ensure QoS resources are available on both ends of the connection before the call is allowed to complete.

8.6.2 Dynamic Quality of Service

IPCablecom Dynamic QoS (DQoS) utilizes the call signaling information at the time that the call is made to authorize resources for the call. This Dynamic QoS architecture prevents various theft of service attack types by integrating the QoS messaging with other protocols and network elements. The network elements that are necessary for a Dynamic QoS control are shown in Figure 11.

The logical entity within the CMTS that defines traffic classification and QoS policy on media streams is called a Gate. The Gate Controller element of the CMS manages Gates for IPCablecom media streams. The following key information is included in signaling between the GC and the CMTS:

- Maximum Allowed QoS Envelope – The maximum allowed QoS envelope defines the maximum QoS resource (e.g., "2 grants of 160 bytes per 10ms") that the MTA is allowed to request for a given media stream bearer flow. If the MTA requests a value greater than the parameters contained within the envelope, then the request is denied.
- Identity of the media stream endpoints – The GC/CMS authorizes the parties that are involved in a media stream bearer flow. Using this information, the CMTS can police the data stream to ensure that the origin and destination of the data stream match the parties that are authorized as endpoints for the flow.
- Destination for Billing Information – The GC/CMS informs the CMTS of the identity of primary and secondary Record Keeping Servers for the call and provides a unique billing id to allow for correlation of records across multiple network elements.

The role of each of the IPCablecom components in implementing DQoS is as follows:

Call Management Server/Gate Controller – The CMS/GC is responsible for QoS authorization. The QoS authorization might depend on the type of call, type of user or other parameters defined by policy. The CMS/GC also uses CMSS to ensure that QoS resources are available on both ends of a call in the event of an intradomain or interdomain call.

CMTS – Using information supplied by the CMS/GC, the CMTS performs admission control on the QoS requests and subsequently polices the admitted data stream to make sure that the source and destination for the data stream match the parties who were authorized as endpoints for the stream. The CMTS interacts with the CM portion of the MTA and the RKS. The responsibilities of the CMTS with respect to these elements are:

- CMTS to Record Keeping Server – The CMTS notifies the Record Keeping Server (RKS) each time that there is a change in the QoS between the CMTS and the MTA for a particular call.
- CMTS to MTA – The MTA makes dynamic requests for creation and modification of QoS traffic parameters associated with DOCSIS Dynamic Service Flows that carry the bearer traffic. When the CMTS receives a request, it checks whether the requested characteristics are within the authorized QoS envelope and also whether the media stream endpoints are authorized to carry this traffic. When the checks succeed, the CMTS creates or modifies the Dynamic Service Flow appropriately.

Record Keeping Server (RKS) – The RKS receives each event (in the form of an Event Message) sent by the CMTS. The RKS typically has an interface to one or more backend systems, and reformats and forwards the information received from the CMTS on to those other systems.

MTA – The MTA is the entity to which the Service Level Agreement is provided by the CMTS. The MTA is responsible for the proper use of the QoS link (and the CMTS is responsible for enforcing that proper use, since the MTA is an untrusted device). If the MTA attempts to exceed the traffic envelope authorized by the Service Level Agreement, then the CMTS ensures that the MTA will not receive the excess QoS that it has requested.

8.7 CMS Subscriber Provisioning

The CMS Subscriber Provisioning specification [12] provides a means for automated service activation by defining an interface between the Provisioning Server (or an authorized Back Office component) and the CMS. The CMS Subscriber Provisioning framework is represented in Figure 12.

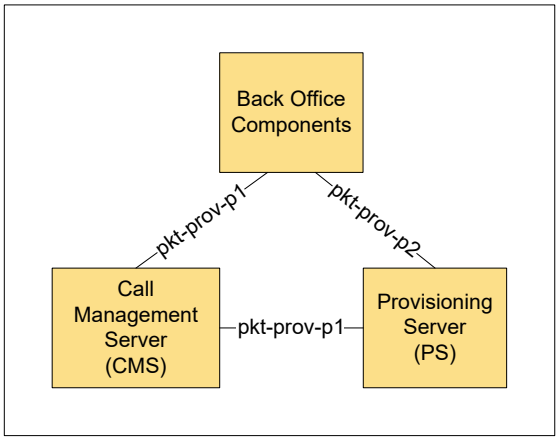

Figure 12. CMS Subscriber Provisioning Interfaces

The function of each CMS Subscriber Provisioning interface is further described in Table 8.

Table 8. CMS Subscriber Provisioning Interfaces

Interface	IPCablecom Functional Component	Description
pkt-prov-p1	PS-CMS Back Office-CMS	This is the CMS Subscriber Provisioning interface. Subscriber information can be delivered to the CMS by either the PS or an authorized Back Office component.
pkt-prov-p2	Back Office-PS	This interfaces allows the Back office components to exchange information with the Provisioning Server. This interface is not defined in IPCablecom 1.5.

Subscriber provisioning consists of:

- Customer record/billing support – Establishment of a customer record that contains the information needed to deliver service, bill, and collect payment from a customer. Customer record creation/billing is considered part of the back office OSS application and is currently out of scope for IPCablecom.
- Equipment setup/configuration – This may include physical installation and/or connection of equipment as well as any software and/or database updates necessary to actually deliver the service to the customer. With respect to the CMS Subscriber Provisioning interface, equipment setup affects the CMS. Provisioning of the CMS itself can be broken down into two main areas:
    - Basic Plain Old Telephone Service (POTS) Provisioning (BPP) – BPP provides the CMS with the minimal set of data necessary for routing of simple telephony service (POTS) in the IPCablecom network. This minimal set of data consists of a telephone number mapped to its associated MTA's FQDN and NCS endpoint identifier. This data will be used to setup translation tables enabling the CMS to route calls to the appropriate device/port given a specific telephone number. BPP provisioning for each customer is required before that customer can receive any calls in a IPCablecom network.
    - Call Feature Provisioning (CFP) – In addition to BPP, CFP is performed to provide call features to a customer. CFP is more complicated than BPP as the parameters passed may vary on a feature-by-feature basis and may also be dependent on vendor specific implementations.

8.8 Electronic Surveillance

The IPCablecom electronic surveillance framework enables Lawfully Authorized Electronic Surveillance (LAES) on IPCablecom networks. IPCablecom supports the delivery of call data and call content (refer to [13] for the definition of these terms) to Law Enforcement Agencies (LEAs). Call data and call content are delivered from different components in the network to a Delivery Function (DF). The DF is responsible for aggregating the call data and call content, and then delivering it to the appropriate LEA. The LEA operates a Collection Function, which is responsible for receiving the call data and call content from the DF.

IPCablecom only defines the mechanisms for performing electronic surveillance. It does not define how an electronic surveillance order is administered (i.e., accepted by the IPCablecom operator and provisioned in the network.

The IPCablecom electronic surveillance framework is represented in Figure 13.

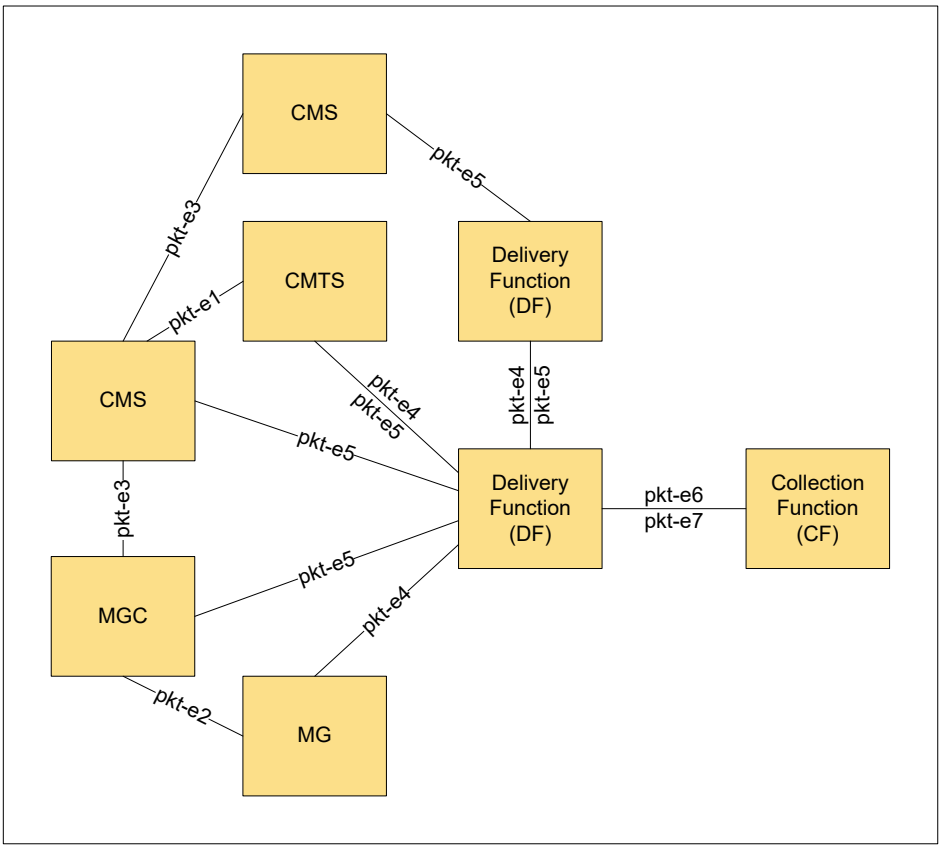

Figure 13. Electronic Surveillance Interfaces

The function of each electronic surveillance interface is further described in Table 9.

Table 9. Electronic Surveillance Interfaces

Interface	IPCablecom Functional Components	Description
pkt-e1	CMS-CMTS	This is the COPS DQoS interface, which allows a CMS to enable call data and call content surveillance.
pkt-e2	MGC-MG	This interface is TGCP, which allows a MGC to command the MG to perform electronic surveillance.
pkt-e3	CMS-CMS CMS-MGC	This interface is CMSS, which supports the ability to communicate electronic surveillance needs in the event of certain intradomain and interdomain call scenarios (e.g., subject forwards a call).
pkt-e4	CMS-DF MGC-DF CMTS-DF DF-DF	This interface is based on IPCablecom Event Messaging and is used to deliver call data from IPCablecom components to the DF, or from DF to DF.
pkt-e5	CMTS-DF MG-DF DF-DF	This interface used to deliver call content in the form of encapsulated RTP packets from IPCablecom components to the DF, or from DF to DF.
pkt-e6	DF-CF	This interface is used to deliver call data to the CF.
pkt-e7	DF-CF	This interface is used to deliver call content to the CF.

8.9 Security

8.9.1 Overview

Each of IPCablecom's protocol interfaces is subject to threats that could pose security risks to both the subscriber and service provider. The IPCablecom architecture addresses these threats by specifying, for each defined protocol interface, the underlying security mechanisms (such as IPsec) that provide the protocol interface with the security services it requires.

For most interfaces, IPCablecom requires that the defined security mechanism(s) be used; for some interfaces, the architecture allows operators to use unsecured links, although by doing so the operator will expose subscribers and the operator itself to attacks that are thwarted when the links are secured by the mechanisms defined in the IPCablecom security specification.

The security services available through IPCablecom's core service layer are: authentication, access control, integrity, and confidentiality. A IPCablecom protocol interface may employ any number of these services to address its particular security requirements.

IPCablecom security addresses the security requirements of each constituent protocol interface by:

- identifying the threat model specific to each constituent protocol interface;
- identifying the security services (authentication, authorization, confidentiality, integrity, and non-repudiation) required to address the identified threats;
- specifying the particular security mechanism providing the required security services.

The security mechanisms include both the security protocol (*e.g.*, IPsec, RTP-layer security, or SNMPv3 security) and the supporting key management protocol (*e.g.*, IKE or PKINIT/Kerberos).

Figure 14 provides a summary of all the IPCablecom 1.5 security interfaces.

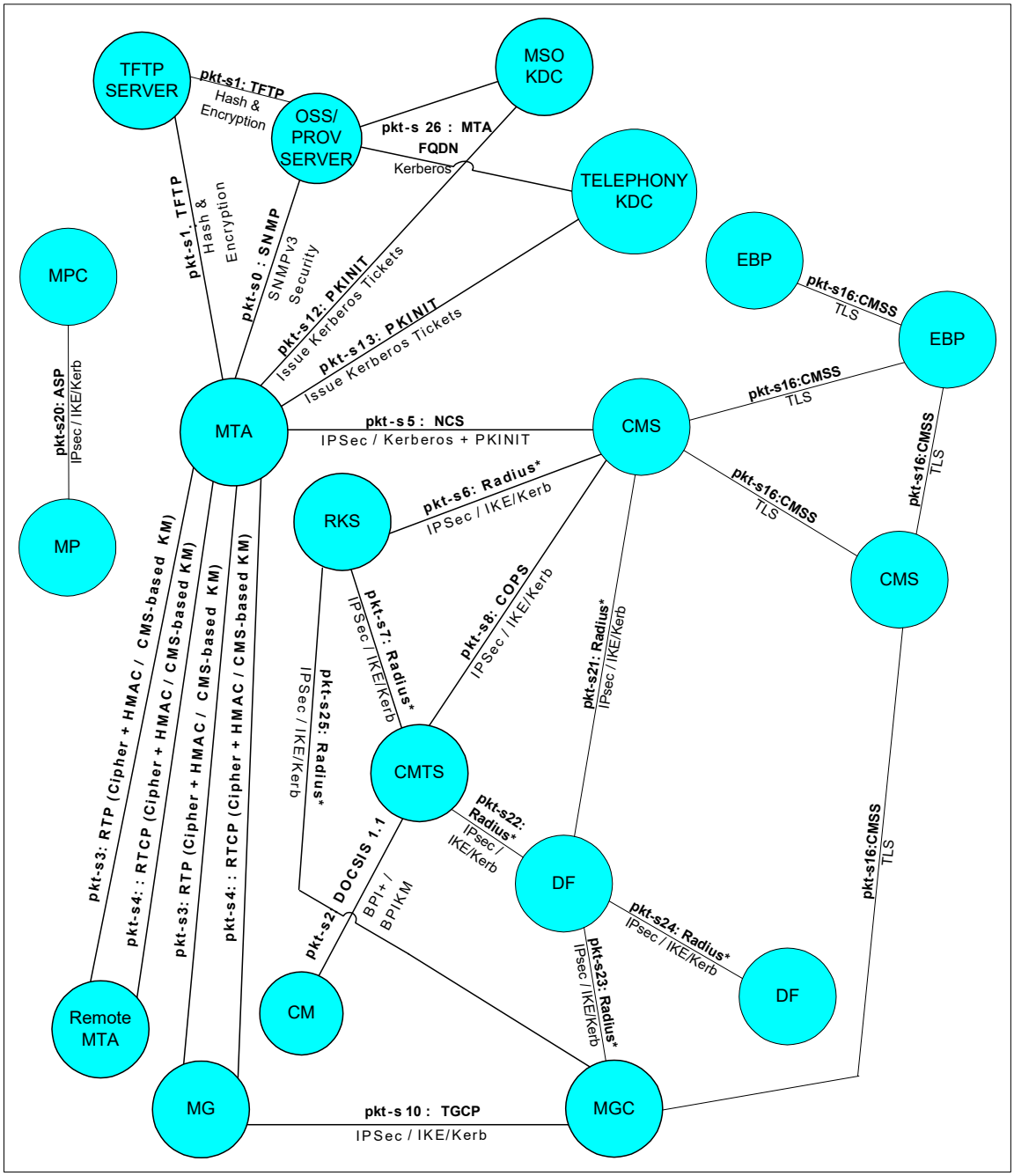

Figure 14. IPCablecom Security Interfaces

In Figure 14, each interface is labeled as:

```
<label>: <protocol> { <security protocol> / <key management protocol> }
```

If the key management protocol is missing, it means that it is not needed for that interface. IPCablecom interfaces that do not require security are not shown on this diagram. Devices compliant with the IPCablecom specifications are required to support security on all interfaces, even if the operator chooses not to use security on some of them.

Table 10 describes each of the interfaces shown in Figure 14.

Table 10. Security Interfaces

Interface	IPCablecom Functional Component	Description
pkt-s0	MTA – PS/OSS	Immediately after the DHCP sequence in the Secure Provisioning Flow, the MTA performs Kerberos-based key management with the Provisioning Server to establish SNMPv3 keys. The MTA bypasses Kerberized SNMPv3 and uses SNMPv2c in the Basic and Hybrid Flows.
pkt-s1	MTA – TFTP	MTA Configuration file download. When the Provisioning Server in the Secure Provisioning Flow sends an SNMP Set command to the MTA, it includes both the configuration name and the hash of the file. Later, when the MTA downloads the file, it authenticates the configuration file using the hash value. The configuration file may be optionally encrypted. HTTP may be used instead of TFTP.
pkt-s2	CM – CMTS	DOCSIS: This interface should be secured with BPI+ using BPI Key Management. BPI+ privacy is provided on the HFC link.
pkt-s3	MTA – MTA MTA – MG	RTP: End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with the chosen cipher. Message integrity is optionally provided by an MMH MAC. Keys are randomly generated, and exchanged by the two endpoints inside the signaling messages via the CMS or other application server.
pkt-s4	MTA – MTA MTA – MG	RTCP: RTCP control protocol for RTP. Message integrity and encryption by selected cipher. The RTCP keys are derived using the same secret negotiated during the RTP key management. No additional key management messages are needed or utilized.
pkt-s5	MTA – CMS	NCS: Message integrity and privacy via IPsec. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
pkt-s6	RKS – CMS	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s7	RKS – CMTS	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s8	CMS – CMTS	COPS: COPS protocol [20] between the GC and the CMTS, used to download QoS authorization to the CMTS. IPsec is used for message integrity, as well as privacy. Key management is IKE or Kerberos.
pkt-s10	MGC – MG	TGCP: IPCablecom interface to the PSTN Media Gateway. IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s12	MTA – MSO KDC	PKINIT: An AS-REQ message is sent to the KDC with public-key cryptography used for authentication. The KDC verifies the certificate and issues either a service ticket or a ticket granting ticket (TGT), depending on the contents of the AS Request. The AS Reply returned by the KDC contains a certificate chain and a digital signature that are used by the MTA to authenticate this message. In the case that the KDC returns a TGT, the MTA then sends a TGS Request to the KDC to which the KDC replies with a TGS Reply containing a service ticket. The TGS Request/Reply messages are authenticated using a symmetric session key inside the TGT.
pkt-s13	MTA – Telephony KDC	PKINIT: See pkt-s12. This interface is shown separately because a separate KDC can be used to provide authentication services for telephony service.

Interface	IPCablecom Functional Component	Description
pkt-s16	CMS – CMS CMS – MGC CMS – EBP EBP – EBP	SIP: TLS is used for both message integrity and privacy. Certificates are used for mutual authentication during the TLS handshake.
pkt-s20	MPC – MP	ASP: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s21	DF – CMS	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s22	DF – CMTS	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s23	DF – MGC	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s24	DF – DF	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE+.
pkt-s25	RKS – MGC	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s25	RKS – MGC	RADIUS: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s26	OSS/Prov Server – MSO KDC OSS/Prov Server – Telephony KDC	The KDC uses Kerberos to map the MTA's MAC address to its FQDN for the purpose of authenticating the MTA before issuing it a ticket.
pkt-s27	CMS-PS/OSS	HTTP: IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.

8.9.2 Device Provisioning Security

IPCablecom 1.5 allows device provisioning to occur in an unsecured mode, or in a secured mode. IPCablecom 1.5 also allows for insecure SNMPv2 management after the MTA has been securely provisioned. Since this section of this Technical Report is dedicated to security, we assume that the network is operating in secure mode.

The IPCablecom security architecture divides device provisioning into three distinct activities: subscriber enrollment, device provisioning and device authorization.

8.9.2.1 Subscriber Enrollment

The subscriber enrollment process establishes a permanent subscriber billing account that uniquely identifies the MTA to the CMS via the MTA's MAC address. The billing account is also used to identify the services to which the MTA has subscribed.

Subscriber enrollment may occur in-band or out-of-band. The specification of the subscriber enrollment process is out of scope for IPCablecom, and may be different for each Service Provider.

8.9.2.2 Device Provisioning

The MTA device authenticates itself to the KDC using the PKINIT extension to Kerberos. After checking the authentication credentials and ensuring that the MTA is known to the backend provisioning system, the KDC issues a ticket for the Provisioning Server. The MTA uses the ticket to exchange SNMPv3 keys in a secure manner with the Provisioning Server. Once a secured SNMPv3 session has been established, the MTA requests its configuration file (which is authenticated and may be encrypted) from a TFTP or HTTP server.

8.9.2.3 Dynamic Provisioning

SNMPv3 security will be used for dynamically provisioning and managing voice communications capabilities and other aspects of the MTA.

8.9.2.4 Device Authorization

Device authorization occurs when a provisioned MTA device authenticates itself to the Call Management Server, and establishes a security association with that server prior to becoming fully operational. Device authorization allows subsequent call signaling to be protected under the established security association.

The MTA device authenticates itself to the KDC using the PKINIT extension to Kerberos. After checking the authentication credentials and ensuring that the MTA is known to the backend provisioning system, the KDC issues a ticket for the CMS. The MTA uses the ticket to establish an IPsec pipe to the CMS in a secure manner. The IPsec pipe may use null encryption, in which case the NCS signaling messages travel unencrypted across this interface.

8.9.2.5 Signaling Security

All signaling traffic, which includes QoS signaling, call signaling, and signaling with the PSTN Gateway Interface, travels through IPsec pipes. IPsec security association management occurs using some combination of Kerberos and IKE. Kerberos with the PKINIT extension is used to exchange keys between MTA clients and their CMSs; IKE or, optionally, Kerberos, is used to manage all other signaling IPsec Security Associations.

8.9.2.6 Media Stream Security

During call setup, MTAs negotiate a particular encryption algorithm for the bearer stream. At a minimum, devices are required to support null encryption and AES encryption. Encryption is applied to the RTP packet's payload, but not to its header.

Each RTP packet may include an optional message authentication code (MAC) based on the MMH algorithm. The MAC computation spans the packet's unencrypted header and encrypted (or unencrypted) payload.

Keys for the encryption and MAC calculation are derived from a secret, which is exchanged between sending and receiving MTA as part of the call signaling at call setup time. Thus, the key exchanges for media stream security are themselves secured by the level of security offered by the IPsec transport that secures the call signaling.

8.9.2.7 OSS and Billing System Security

The SNMP agents in IPCablecom MTAs implement SNMPv3 when operated in secure mode. The SNMPv3 User Security Model (IETF RFC 3414 [28]) provides authentication and privacy services for SNMP traffic. SNMPv3 view-based access control (IETF RFC 3415 [29]) may be used for access control to MIB objects.

The IKE or Kerberos key management protocol is used to establish encryption and authentication keys between the Record Keeping Server (RKS) and each IPCablecom network element that generates Event Messages. Devices that conform to the IPCablecom security specification are required to implement IKE with pre-shared keys; they may also implement either IKE with certificates or Kerberos, which allow vendors to implement fully automatic key-change mechanisms. The Event Messages are sent from the CMS and CMTS to the RKS using the RADIUS transport protocol, which is in turn secured by IPsec.

9 NETWORK DESIGN CONSIDERATIONS

9.1 Time Keeping and Reporting Issues

In order to maintain service quality, it is highly recommended that all network equipment clocks be maintained to within 200 milliseconds of Universal Time Coordinated (UTC). Devices that send Event Messages are required to maintain time synchronization with the Network Time Protocol (NTP) [19].

It is recommended that IPCablecom networks maintain an NTP server that is accurate to within a specified interval of Universal Time Coordinated (UTC).

9.2 Timing for Playout Buffer Alignment with Coding Rate

Equipment that generates and/or processes packets generally operates with a free-running clock. Problems may arise when offering isochronous services with such equipment due to the plesiochronous nature of these clocks. The difference in clock speed between these plesiochronous entities is generally exhibited as overrun or underrun of playout buffers.

In order to minimize the occurrence of these conditions, all CMTSes should lock their downstream transmission rate to a clock derived from a source that reflects a Stratum-3 clock. MTAs should use the downstream transmission rate to derive the clock that is used to determine packetization period. MTAs should also use this clock to determine the rate of playout from the receive buffer.

9.3 IP Addressing

An MTA is a multi-function entity with one function required for CM administration and the second function being the MTA function itself.

IPCablecom 1.5 MTAs are required to have two IP addresses (one for the CM and one for the MTA) and two MAC addresses (also one for the CM and one for the MTA). IPCablecom 1.5 supports only IPv4 IP addresses.

By using two IP addresses per device, IPCablecom allows the following modes of operation:

- The IPCablecom operator can assign a private IP address for the CM host function, in the case where NAT is not provided elsewhere in the IPCablecom network.
- The operator can route bearer voice packets over a voice backbone and all other packets (data) over a data backbone. In such a case, the routing backbone must be configured such that different paths are followed for the two IP addresses.
- The operator can simplify network-side administration and management functions by using separate IP addresses. For example, policy filters can be installed to either block or permit traffic from the MTA component of the device. In addition, network service providers can provide source address screening services, and network traffic statistics and diagnostics can be collected based upon the IP address of the MTA.

Dual IP addresses result in special considerations that affect the following:

- IP protocol stack implementation of the MTA;
- Implementation of IPCablecom OSS and device provisioning protocols;
- Network routing implementations.

9.4 Dynamic IP Address Assignment

An operational requirement exists to dynamically assign IP addresses to MTAs for both device provisioning and management and the various protocol operations. The call signaling model specified in the IPCablecom 1.5 NCS specification is based on the ability for a Call Management Server to map a subscriber's service to an endpoint identifier and an MTA Fully Qualified Domain Name (FQDN). Call processing operations would be affected if the address assigned to the MTA is changed during an active call (which may occur if the DHCP lease expires during an active call). DHCP does not allow an IP address to change across renewals; a change can only be administered by forcing the MTA to reinitialize (either explicitly or by denying a renewal). It is recommended that the continuity of

the MTA's IP address be maintained via DHCP renewals. Operations such as 'IP address renumbering' should consider such impacts.

9.5 Fully Qualified Domain Name (FQDN) Assignment

It is assumed that the OSS back office systems will generate the FQDNs for IPCablecom devices and pass this data to the appropriate IPCablecom devices and other network elements. These interfaces are not defined in IPCablecom 1.5.

9.6 Priority Marking of Signaling and Media Stream Packets

The media and signaling streams for IPCablecom-based services require methods for properly marking and transporting packets at a sufficiently high level of Quality of Service, both in the DOCSIS access network and in the managed IP backbone.

The mechanism for providing low-latency Quality of Service for media streams in the access network is the DOCSIS flow classification service. This service classifies packets into specific flows based upon packet fields such as the IP source and destination addresses and the UDP port numbers. In the upstream, such classified packets are transported via an appropriate constant bit rate service (for currently supported codecs) as dynamically scheduled by the CMTS. In the downstream, the packets are transported via an appropriate high-priority queuing and scheduling mechanism. DQoS (between CMS and CMTS) and DOCSIS (between CMTS and CM) signaling mechanisms are used to dynamically configure the media stream flow classification rules and service flow QoS traffic parameters.

In addition to flow classification, it is useful to mark media stream packets with appropriate priority markings. Such priority markings can be used within CMTS/CM queuing systems and also within Diffserv managed QoS backbones in order to provide high priority QoS treatment of such packets. IPCablecom 1.5 does not define how QoS policies are applied managed backbone but provides the protocol mechanisms to create special classes of services.

Signaling packets may also benefit from prioritized QoS services. In particular, as an access network becomes loaded to capacity it may be important to forward signaling packets at a higher priority than data packets in order to avoid excessive signaling latency. If signaling prioritization is desired, then the method for providing prioritized QoS is based upon two mechanisms: 1) Mark all signaling packets with a high priority marking; 2) provide a DOCSIS Classifier that classifies such packets to be transported on a higher priority service flow. The Classifier can be as simple as mapping all upstream packets with this priority to the high priority SID, or can be more complex and also identify the IP address of the MTA(s) which originate the signaling. The higher priority service flow may be either statically provisioned or dynamically created by the administrator of the CMTS. It should be noted that if the administrator is concerned about theft of service of the high priority service flow, then he may configure the service flow for high priority (*i.e.*, low latency) but low bandwidth.

The IPCablecom Architecture enables the use of the Differentiated Services framework (IETF RFC 3260 [23]) to differentiate IPCablecom media and signaling from high-speed data packets. Marking of packets for the media streams (RTP and RTCP) and the signaling stream (NCS, TGCP) is performed by the MTA/MG and/or the CMS/MGC. The packet marking may be performed at the IP layer using the Diffserv Code Point (DSCP). Note that the IETF RFC 2474 [24] attempts to rename the TOS octet of the IPv4 header, and Traffic Class octet of the IPV6 header, respectively, to the DS field. The DS Field has a six-bit Diffserv Codepoint and two "currently unused" bits. IETF RFC 2474 was updated by IETF RFC 3168 [25] which defined the two "unused" bits as "explicit congestion notification (ECN)" bits. It is strongly recommended to use the DSCP field rather than the IPv4 TOS byte.

The configuration of the DSCP values for the media and signaling streams is performed via the IPCablecom MIB modules for the MTA. It should be noted that in NCS the signaled SDP parameters may contain values that override the configured media stream priority marking value on a connection-by-connection basis.

9.7 Fax Support

IPCablecom supports real-time fax transmission. In IPCablecom 1.5, fax is best accomplished using the ITU-T T.38 recommendation [32] for fax relay over IP networks (i.e., local termination of fax and translating the fax stream to an IP fax-relay data stream). If a call is established using an audio codec, the MTA is instructed to look for fax tones. If fax tones are detected, the CMS is then notified and the MTA is instructed to switch the bearer stream to T.38. IPCablecom 1.5 also supports fax pass-through, where the fax tones are passed through the IP network as a G.711 encoded audio stream. Echo cancellation is also supported for fax pass-through.

Support for switching over to fax from a voice call is required in IPCablecom 1.5. In the case of fax relay, switching from fax back to voice is also supported.

9.8 Analog Modem Support

Analog modems may be supported in one of two ways: pass-through or modem relay via V.152 [35].

Similar to fax pass-through – an MTA will be asked to detect modem tones and, when such tones are detected, the CMS will instruct the MTA to switch over to the G.711 codec if it is not already in use. Echo cancellation is also supported for modem pass-through. Switching from a low-bandwidth codec to G.711 to support analog modem signaling from a voice call is supported. Returning to a low-bandwidth codec after modem signaling is complete is also supported.

A more robust solution for supporting analog modems is to employ voice band data transmission using the method described in ITU-T standard V.152 [35]. V.152 involves quickly switching to a codec that can accurately relay modem signals over an IP network.

9.9 DTMF Relay

DTMF is the use of dual-tone multiple frequency signals either by an autodialing system or through manual entry of tones. In order for DTMF tones to be captured correctly by the receiving device, tonal integrity (frequency accuracy and signal duration) must be maintained even through compression and transcoding.

IPCablecom 1.5 supports the relay of DTMF tone transmissions via IETF RFC 2833 [30] telephone events. IPCablecom 1.5 also supports DTMF pass-through, where the DTMF tones are passed through the IP network as an encoded audio stream.