ETSI TS 103 161-2 V1.1.1 (2011-10)

Technical Specification

Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 2: Architectural framework for the delivery of time critical services over Cable Television Networks using Cable Modems

Reference

DTS/ATTM-003011-2

Keywords

access, broadband, cable, IP, multimedia, PSTN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

The present document is part 2 of a multi-part IPCablecom 1.5 deliverable covering the Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services, as identified below:

Part 1: "Overview";

Part 2: "Architectural framework for the delivery of time critical services over Cable Television Networks using Cable Modems";

Part 3: "Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems";

Part 4: "Network Call Signalling Protocol";

Part 5: "Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems";

Part 6: "Event Message Specification";

Part 7: "Media Terminal Adapter (MTA Management Information Base (MIB)";

Part 8: "Network Call Signalling (NCS) MIB Requirements";

Part 9: "Security";

Part 10: "Management Information Base (MIB) Framework";

Part 11: "Media terminal adapter (MTA) device provisioning";

Part 12: "Management Event Mechanism";

Part 13: "Trunking Gateway Control Protocol - MGCP option";

Part 14: "Embedded MTA Analog Interface and Powering Specification"

Part 15: "Analog Trunking for PBX Specification";

Part 16: "Signalling for Call Management Server";

Part 17: "CMS Subscriber Provisioning Specification";

Part 18: "Media Terminal Adapter Extension MIB";

Part 19: "IPCablecom Audio Server Protocol Specification - MGCP option";

Part 20: "Management Event MIB Specification";

Part 21: "Signalling Extension MIB Specification".

NOTE 1: Additional parts may be proposed and will be added to the list in future versions.

NOTE 2: The choice of a multi-part format for this deliverable is to facilitate maintenance and future enhancements.

1 Scope

1.1 IPCablecom Overview

The IPCablecom project defines interface specifications that can be used to develop interoperable equipment capable of providing packet-based voice, video and other high-speed multimedia services over hybrid fibre coax (HFC) cable systems utilizing the DOCSIS® protocol [i.14]. Any reference to DOCSIS® in the present 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 clause 5.3.

1.2 IPCablecom Motivation

The emergence of the Internet Protocol (IP) as the standard transport for packet data networks has enabled a revolution in communications services and applications.

NOTE: IPCablecom 1.5 supports only IPv4 at the present time.

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 is to support the time-to-market business considerations for deploying packet-based services. Going forward, the IPCablecom architecture will 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.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 103 161-3: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 3: Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems".

[i.2] ETSI TS 103 161-5: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 5: Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems".

[i.3] ETSI TS 103 161-4: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 4: Network Call Signalling Protocol".

[i.4] ETSI TS 103 161-6: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 6: Event Message Specification".

[i.5] ETSI TS 103 161-7: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 7: Media Terminal Adapter (MTA) Management Information Base (MIB)".

[i.6] ETSI TS 103 161-8: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 8: Network Call Signalling (NCS) MIB Requirements".

[i.7] ETSI TS 103 161-10: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 10: Management Information Base (MIB) Framework".

[i.8] ETSI TS 103 161-13: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 13: Trunking Gateway Control Protocol - MGCP option".

[i.9] ETSI TS 103 161-11: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 11: Media Terminal Adapter (MTA) device provisioning".

[i.10] ETSI TS 103 161-9: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 9: Security".

[i.11] ETSI TS 103 161-16: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 16: Signalling for Call Management Server".

[i.12] ETSI TS 103 161-17: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 17: CMS Subscriber Provisioning Specification".

[i.13] ETSI TS 102 836-1 (V1.1.1): " Access, Terminals, Transmission and Multiplexing (ATTM); Lawful Interception (LI); Part 1: Interception of IP Telephony Service on Cable Operator's Broadband IP Network: Internal Network Interfaces".

[i.14] ETSI ES 201 488-2: "Access and Terminals (AT); Data Over Cable Systems; Part 2: Radio Frequency Interface Specification".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[i.34] ITU-T Recommendation V.152: "Procedures for supporting Voice-Band Data over IP Networks", January 2005.

[i.35] ETSI ES 201 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[i.36] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[i.37] ETSI TS 102 232: "Lawful Interception (LI); Handover specification for IP delivery".

[i.38] ETSI TS 103 161-1: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 1: Overview".

[i.39] ETSI TS 103 161-12: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 12: Management Event Mechanism".

[i.40] ETSI TS 103 161-14: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 14: Embedded MTA Analog Interface and Powering Specification".

[i.41] ETSI TS 103 161-18: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 18: Media Terminal Adapter Extension MIB".

[i.42] ETSI TS 103 161-19: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5 Part 19: IPCablecom Audio Server Protocol Specification - MGCP option".

[i.43] ETSI TS 103 161-20: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 20: Management Event MIB Specification".

[i.44] ETSI TS 103 161-21: "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 21: Signalling Extension MIB Specification".

[i.45] Telcordia GR-909: "Generic Criteria for Fiber in the Loop Systems", December 2004.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

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

admitted: allowed

asymmetric key: encryption key or decryption key used in a public key cryptography, where encryption and decryption keys are always distinct

authentication: process of verifying the claimed identity of an entity to another entity

authorization: act of giving access to a service or device if one has the permission to have the access

cipher: algorithm that transforms data between plaintext and ciphertext

ciphersuite: set which contains both an encryption algorithm and a message authentication algorithm (e.g. a MAC or an HMAC)

NOTE: In general, it may also contain a key management algorithm, which does not apply in the context of IPCablecom.

ciphertext: (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible

confidentiality: a way to ensure that information is not disclosed to anyone other than the intended parties; information is encrypted to provide confidentiality

cryptographic algorithm: algorithm used to transfer text between plaintext and ciphertext

decryption: procedure applied to ciphertext to translate it into plaintext

diffserv (also known as Differentiated Services)**:** IETF architecture for implementing scalable service differentiation in the Internet (see RFC 3260 [i.23])

digital certificate: 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: 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: direction from the head-end toward the subscriber location

encryption: method used to translate information in plaintext into ciphertext

endpoint: Terminal, Gateway or MCU.

event message: message capturing a single portion of a call connection

Exterior Border Proxy (EBP): proxy involved in inter-domain communication used to communicate between different domains

NOTE: Every non-isolated domain has interfaces with one or more other domains via one or more Exterior Border Proxies.

gateway: devices bridging between the IPCablecom IP Telephony world and the PSTN

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

jitter: variability in the delay of a stream of incoming packets making up a flow such as a voice call

Kerberos: secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication

key: mathematical value input into the selected cryptographic algorithm.

key exchange: swapping of public keys between entities to be used to encrypt communication between the entities

key management: process of distributing shared symmetric keys needed to run a security protocol

latency: time, expressed in quantity of symbols, taken for a signal element to pass through a device

Media Player (MP): device responsible for receiving and interpreting commands from the Media Player Controller and for delivering appropriate announcement(s) to the MTA

Media Player Controller (MPC): device that initiates and manages all announcement services provided by the media player.

network management: functions related to the management of data across the network

transit delays: 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

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ANC	Announcement Controller
ANP	Announcement Player

ANS	Announcement Server
ASP	Audio Server Protocol
BPI+	Baseline Privacy Interface Plus
CA	Call Agent
CDR	Call Detail Record
CIC	Circuit Identification Code
CLASS	Custom Local Area Signalling Services
CM	DOCSIS® Cable Modem
CMS	Call Management Server
CMTS	Cable Modem Termination System
CODEC	COder-DECoder
COPS	Common Open Policy Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS®	Data Over Cable System Interface Specification
DQoS	Dynamic Quality of Service
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi Frequency (tones)
E-MTA	Embedded MTA
FQDN	Fully Qualified Domain Name
GC	Gate Controller
HDBH	High Day Busy Hour
HFC	Hybrid Fibber/Coaxial cable
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange
IKE+	Internet Key Exchange Plus (requiring digital certificates for authentication)
IP	Internet Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
KDC	Key Distribution Centre
LATA	Local Access and Transport Area
LEA	Law Enforcement Agency
LNP	Local Number Portability
MAC	Media Access Control
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MSO	Multi-System Operator
MTA	Media Terminal Adapter
MTP	Message Transfer Part
NAT	Network Address Translation
NCS	Network-based Call Signalling
NTP	Network Time Protocol
OSS	Operations Systems Support
PCM	Pulse Code Modulation
PHY	Physical Layer
PKINIT	Public Key Cryptography Initial Authentication
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
PT	Payload Type
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RFC	Request for Comments
RFI	Radio Frequency Interface
RKS	Record Keeping Server
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
SCCP	Signalling Connection Control
SCP	A Service Control Point
SDP	Session Description Protocol

SG	Signalling Gateway
SID	Service ID
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SS7	Signalling System Number 7
TCAP	Transaction Capabilities Application Protocol
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Server used to grant Kerberos tickets
TOS	Type of Service
UDP	User Datagram Protocol
UTC	Universal Time Coordinated
VoIP	Voice over IP

4 Void

5 IPCablecom 1.5

IPCablecom 1.5 is a 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 clause 5.1 and subsequent subclauses for a description of these components);

- communication across IPCablecom zones and domains to enable end-to-end IP-based connections (refer to clause 5.2 and subsequent subclauses 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 signalling, QoS security, provisioning, billing and security protocols.

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

5.1 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 Signalling 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.

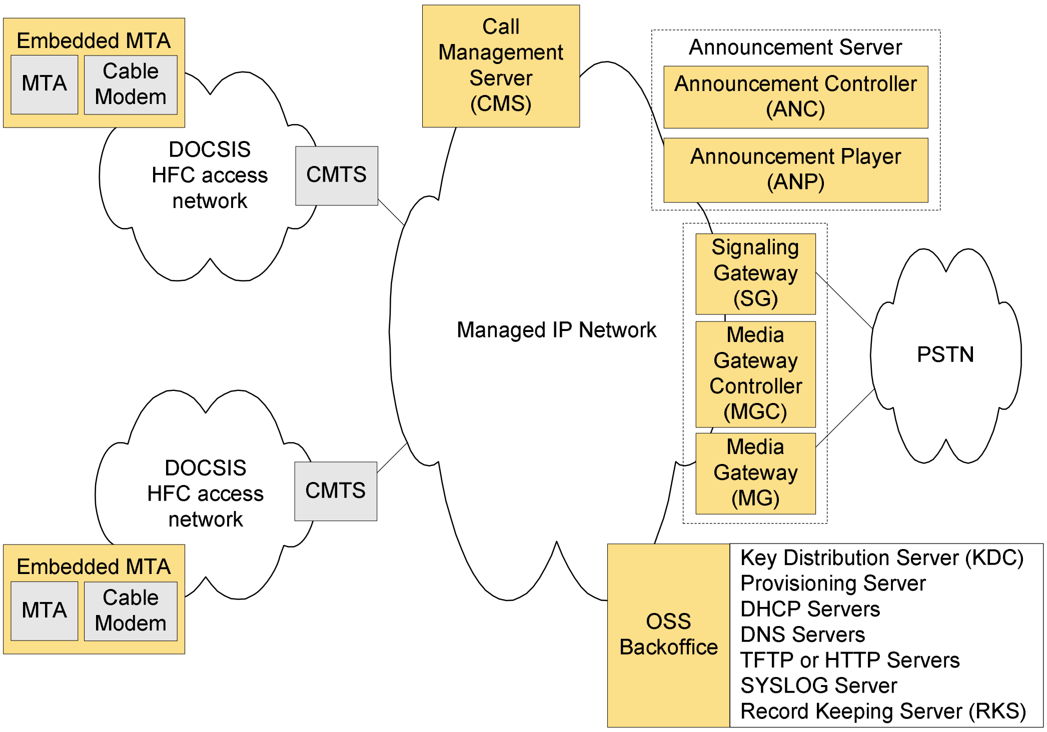


Figure 1: IPCablecom Reference Architecture

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 Media 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 signalling, 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, Signalling 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 clause 6.

5.2 IPCablecom Zones and Domains

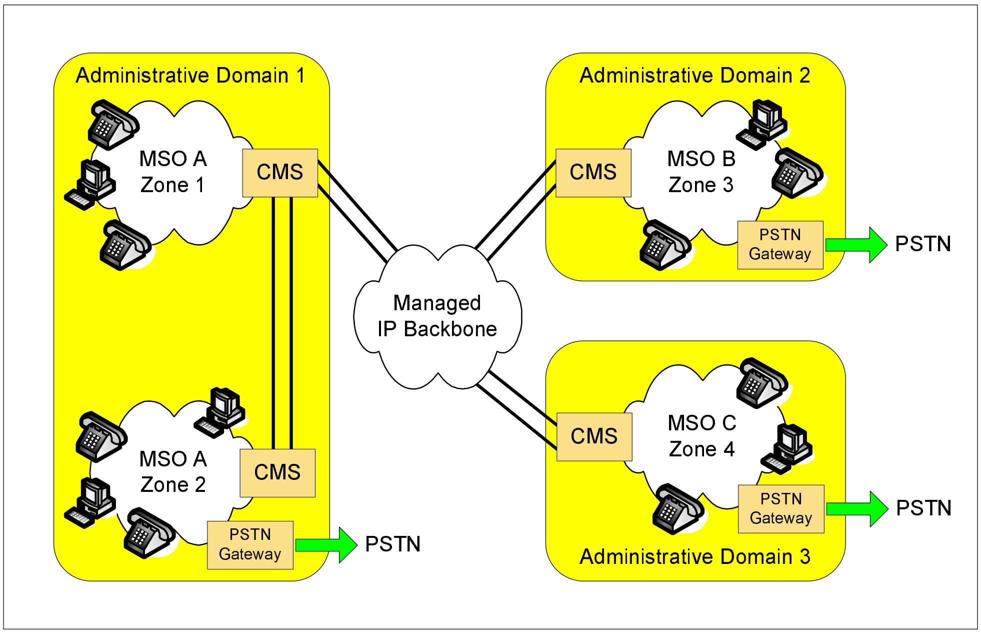


Figure 2: Zones and Administrative Domains

An 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).

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

5.3 IPCablecom 1.5 Analog Trunking Specifications

IPCablecom 1.5 consists of the twenty Technical Specifications shown in table 1.

Table 1: IPCablecom 1.5 Specifications and Reports

IPCablecom Technical Document Reference Number	Brief Document Description
TS 103 161-1 [i.38]	IPCablecom 1.5 Overview
TR 103 161-2	Architecture Framework (the present document)
TS 103 161-3 [i.1]	Audio/Video Codecs
TS 103 161-4 [i.3]	Network-based Call Signalling (NCS)
TS 103 161-5 [i.2]	Dynamic Quality-of-Service
TS 103 161-6 [i.4]	Event Messages
TS 103 161-7 [i.5]	MTA MIB
TS 103 161-8 [i.6]	MTA Signalling MIB
TS 103 161-9 [i.10]	Security
TS 103 161-10 [i.7]	MIB Framework
TS 103 161-11 [i.9]	MTA Device Provisioning
TS 103 161-12 [i.39]	Management Event Mechanism
TS 103 161-13 [i.8]	PSTN Gateway Call Signalling Protocol
TS 103 161-14 [i.40]	Analog Interface and Powering
TS 103 161-16 [i.11]	CMS to CMS Signalling
TS 103 161-17 [i.12]	CMS Subscriber Provisioning
TS 103 161-18 [i.41]	MTA MIB Extensions
TS 103 161-19 [i.42]	Audio Server Protocol
TS 103 161-20 [i.43]	MTA Event MIB
TS 103 161-21 [i.44]	MTA Signalling MIB Extensions
TS 102 836-1 [i.13]	Lawful Intercept

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

This clause 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.

5.4.1 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 45 ms.

- 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.

5.4.2 Call Signalling

- Define a network-based signalling architecture.
- Provide end-to-end call signalling 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 signalling 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 signalling to support Custom Local Area Signalling 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 signalling 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.

5.4.3 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 an 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 emergency and other priority-based signalling services.

5.4.4 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.

5.4.5 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).

5.4.6 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 cable operator from various denial of service, network disruption and theft-of-service attacks.
- Design considerations include confidentiality, authentication, integrity, and access control.

5.4.7 Lawful Interception

- Support the ability to perform lawful interception by reporting call data and call content.

6 IPCablecom Functional Components

This clause describes the functional components present in an 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: Specific product implementations may combine functional components as needed. Not all components are required to be present in a particular instance of an 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 cable operator's facility.

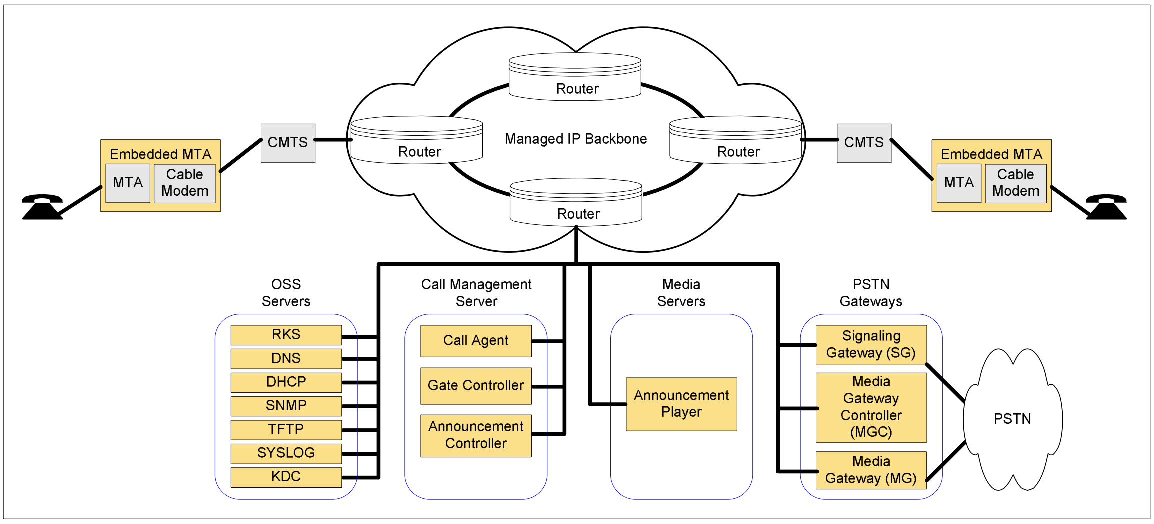


Figure 3: IPCablecom Component Reference Model

6.1 Media Terminal Adapter (MTA)

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

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 Signalling (NCS) protocol.

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

6.1.1 MTA Functional Requirements

An MTA is responsible for providing the following functionality:

- NCS call signalling with the CMS.
- QoS signalling 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 analogue line signalling for audio tones, voice transport, caller-id signalling, DTMF, and message waiting indicators.
- The G.711 audio codec [i.33] and low bit-rate audio codecs.
- One or more telephone interfaces (e.g. RJ11 analogue interface as defined by Telcordia (formerly Bellcore) GR-909 [i.45]).

Additional MTA functionality is defined in other IPCablecom specifications such as NCS Signalling [i.3], Dynamic Quality-of-Service [i.2], Audio-Video Codecs [i.1], MIBS [i.5], [i.6], Security [i.10], and MTA Device Provisioning [i.9].

NOTE: This is not an exhaustive list.

6.1.2 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.

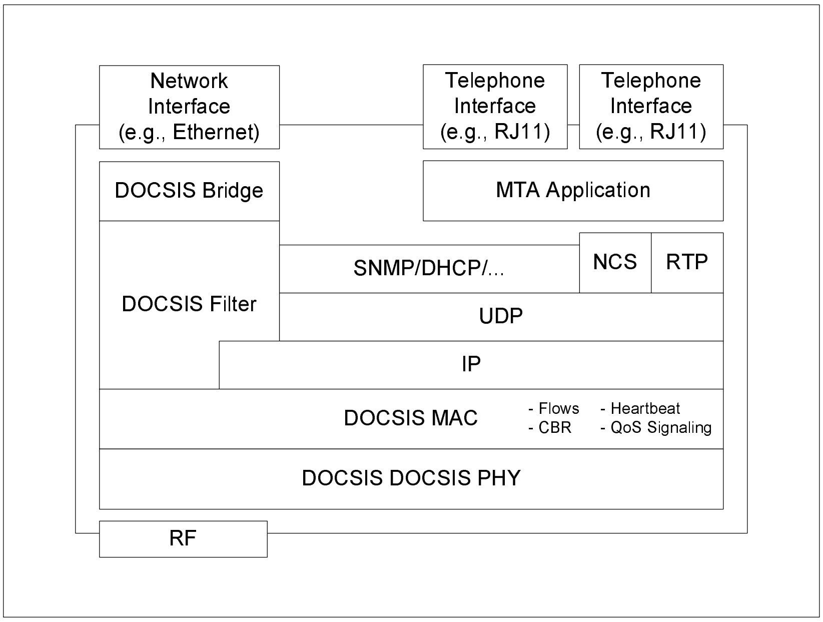


Figure 4: E-MTA Conceptual Functional Architecture

6.2 Cable Modem (CM)

The cable modem (CM) is a network element that is defined by DOCSIS® [i.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.

6.3 HFC Access Network

IPCablecom-based services are carried over the Hybrid fibre/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.

6.4 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.

6.4.1 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 an 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.

6.5 Call Management Server (CMS)

The Call Management Server provides call control and signalling 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.

An 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 signalling 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 dialled 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 [i.2].

The CMS may contain the following logical component:

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

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 the present document, 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.

6.6 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 behaviour of the PSTN gateway.

Signalling Gateway (SG) - The SG provides a signalling interconnection function between the PSTN SS7 signalling network and the IP network.

Media Gateway (MG) - The MG terminates the bearer paths and transcodes media between the PSTN and IP network.

6.6.1 Media Gateway Controller (MGC)

The Media Gateway Controller (MGC) receives and mediates call-signalling 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 Signalling - terminates and generates the call signalling 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.

6.6.2 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.

6.6.2.1 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.

6.6.3 Signalling Gateway (SG)

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

6.6.3.1 SS7 Signalling Gateway Functions

The following functions are performed by the Signalling Gateway function:

- Terminates physical SS7 signalling 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 signalling 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/Signalling 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 signalling information between the Signalling Gateway and the Media Gateway Controller.

6.7 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.

6.7.1 Security Server - Key Distribution Centre (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 [i.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 signalling 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.

6.7.2 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 RFC 2131 [i.17].

6.7.3 Domain Name System Server (DNS)

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

6.7.4 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.

6.7.5 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.

6.7.6 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.

6.8 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).

6.8.1 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.

6.8.2 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.

7 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 clause. 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.

7.1 Call Signalling Interfaces

Call signalling requires multiple interfaces within the IPCablecom architecture. These interfaces are identified in figure 5. Each interface in the diagram is labelled, and further described in the subsequent table 2.

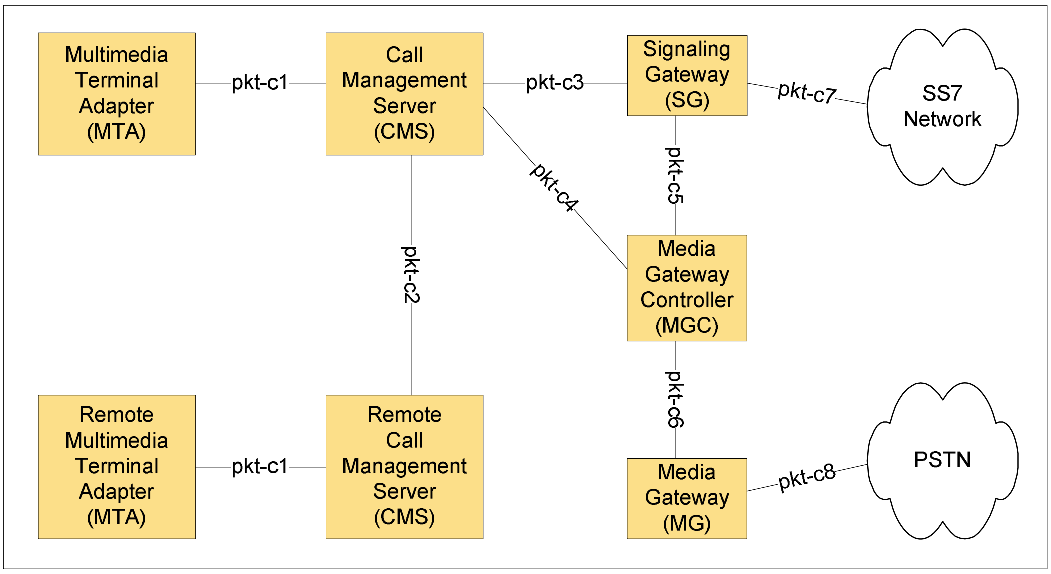

Multimedia Terminal Adapter (MTA)
pkt-c1
Call Management Server (CMS)
pkt-c3
Signaling Gateway (SG)
pkt-c7
SS7 Network
pkt-c4
pkt-c5
pkt-c2
Media Gateway Controller (MGC)
pkt-c6
Remote Multimedia Terminal Adapter (MTA)
pkt-c1
Remote Call Management Server (CMS)
Media Gateway (MG)
pkt-c8
PSTN

Figure 5: Call Signalling Interfaces

Table 2: Call Signalling Interfaces

Interface	IPCablecom Functional Components	Description
pkt-c1	MTA - CMS	Call signalling messages exchanged between the MTA and CMS using the NCS protocol, which is a profile of MGCP.
pkt-c2	CMS-CMS	Call signalling messages exchanged between CMSes. The protocol for this interface is CMSS.
pkt-c3	CMS - SG	Call signalling messages exchanged between the CMS and SG. The protocol for this interface is not defined in IPCablecom 1.5.
pkt-c4	CMS - MGC	Call signalling messages exchanged between the CMS and MGC. The protocol for this interface is CMSS.
pkt-c5	SG - MGC	Call signalling 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.
pkt-c7	SG - SS7	The SG terminates physical SS7 signalling links from the PSTN (A, F links). The following protocols are supported: • ISUP User Interface. Provides an SS7 ISUP signalling 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.

7.1.1 Network-based Call Signalling (NCS) Framework

The IPCablecom Network-based Call Signalling (NCS) protocol (pkt-c1) is a profile of the MGCP call signalling protocol defined in RFC 3435 [i.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 signalling 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.

7.1.2 PSTN Signalling Framework

PSTN signalling 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 signalling framework consists of a PSTN gateway that is divided into three functional components:

- Media Gateway Controller (MGC).
- Media Gateway (MG).
- Signalling 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 signalling 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) [i.8]. This includes creation, modification and deletion of connections. TGCP is a profile of the MGCP call signalling protocol defined in RFC 3435 [i.31] 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 signalling 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.

7.1.3 CMS to CMS Signalling Framework

IPCablecom 1.5 supports both inter-domain and intra-domain CMS-CMS and CMS-MGC signalling as defined in the IPCablecom CMSS specification [i.11]. The CMSS signalling architecture is based on the IETF Session Initiation Protocol (SIP) (RFC 3261 [i.26]). CMSS defines a call signalling 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 signalling from the MTA, e.g. by receiving an NCS message informing about dialled digits. A CMS includes a Gate Controller (GC) function. The User Agent part of the CMS participates in the CMSS signalling and the Gate Controller part participates in the D-QoS signalling. Together, they control the coordination of the signalling for call setup and resource management.

7.2 Media Streams

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

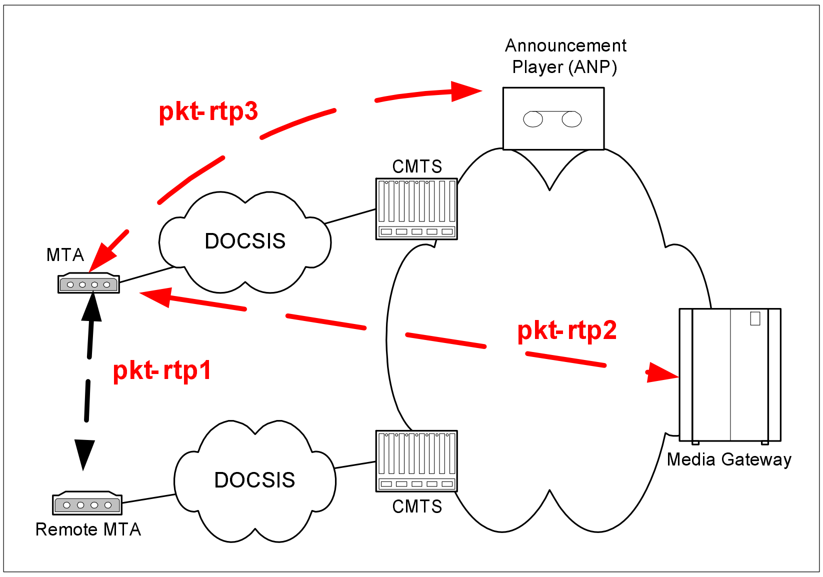


Figure 6: RTP Media Stream Flows in an IPCablecom Network

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

Table 3: RTP Media Stream Flows

Interface	IPCablecom Functional Components	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 signalling.

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

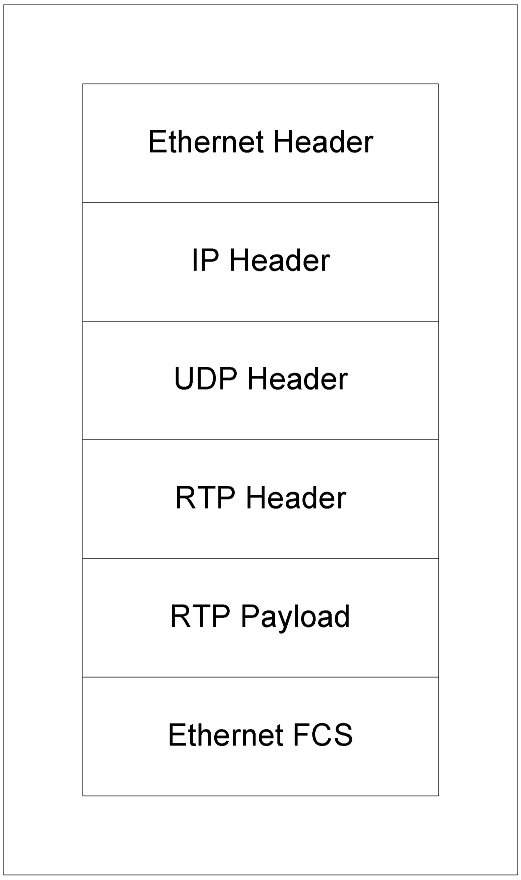


Figure 7: RTP Packet Format

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) [i.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 Recommendation T.38 [i.32] is also used to transport facsimile media in IPCablecom networks, refer to clause 8.7 of the present document for more details.

7.2.1 Real-time Transport Control Protocol (RTCP)

RTCP is defined in RFC 1889 [i.15]. 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 RFC 3611 [i.27]. RTCP XR contains many sets of metrics. IPCablecom 1.5 supports only the RTCP XR Voice Metrics on all endpoints.

7.3 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 [i.9] also includes attribute definitions required in the MTA configuration file.

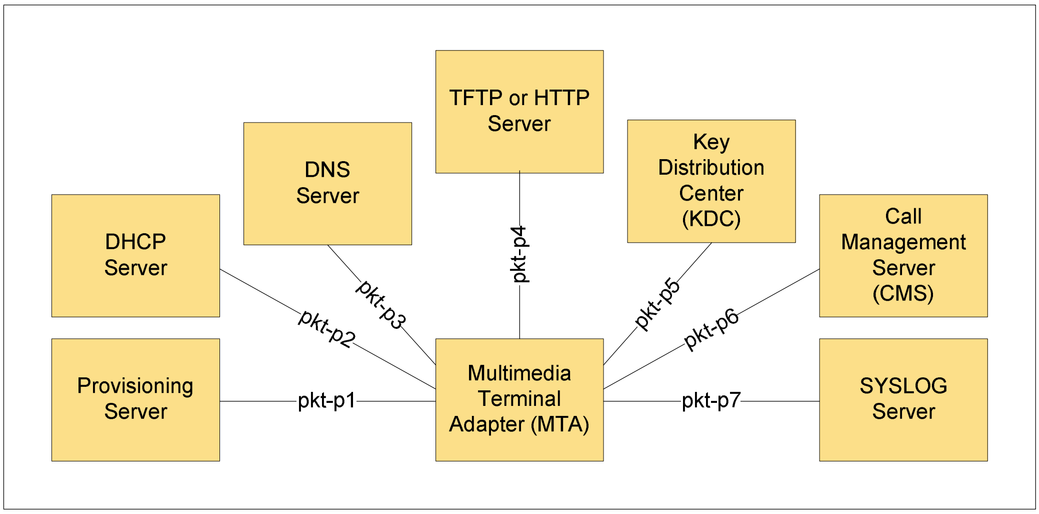


Figure 8: IPCablecom Provisioning Interfaces

Table 4 describes the provisioning interfaces shown in figure 8.

Table 4: Device Provisioning Interfaces

Interface	IPCablecom Functional Components	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 an 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 Centre 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.

7.4 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 [i.7] and defined in the IPCablecom 1.5 MTA MIB specification [i.5] and the IPCablecom 1.5 Signalling MIB specification [i.6].

The IPCablecom 1.5 Signalling MIB module contains Network-based Call Signalling 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.

7.5 Event Messages Interfaces

7.5.1 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 [i.4] defines the structure of the Event Message data record and defines RADIUS (RFCs 2865 [i.21] and 2866 [i.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.

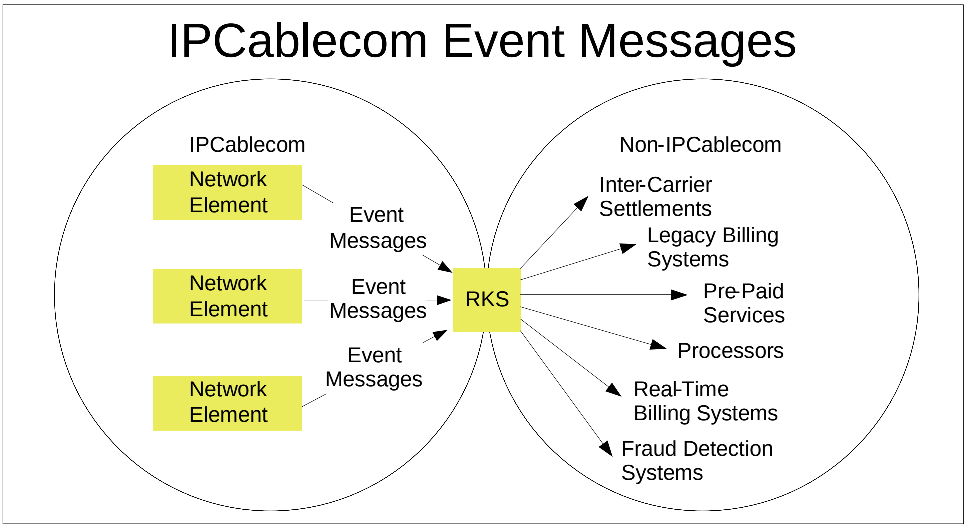
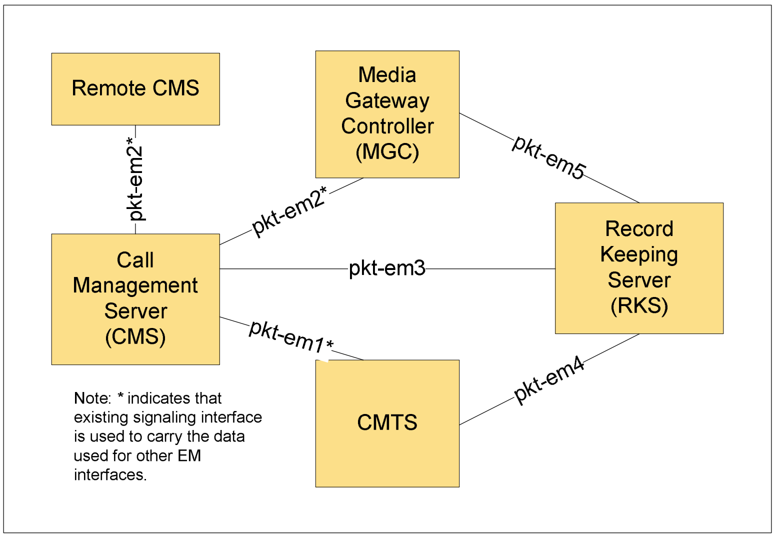


Figure 9: Representative Event Messages Architecture


Remote CMS
Media Gateway Controller (MGC)
pkt-em5
pkt-em2*
pkt-em2*
Call Management Server (CMS)
pkt-em3
Record Keeping Server (RKS)
pkt-em1*
pkt-em4
CMTS

Note: * indicates that existing signaling interface is used to carry the data used for other EM interfaces.

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.
pkt-em4	CMTS-RKS	RADIUS protocol carrying IPCablecom Event Messages.
pkt-em5	MGC-RKS	RADIUS protocol carrying IPCablecom Event Messages.

7.6 Quality of Service (QoS)

7.6.1 QoS Framework

The IPCablecom QoS Framework is represented in figure 11.

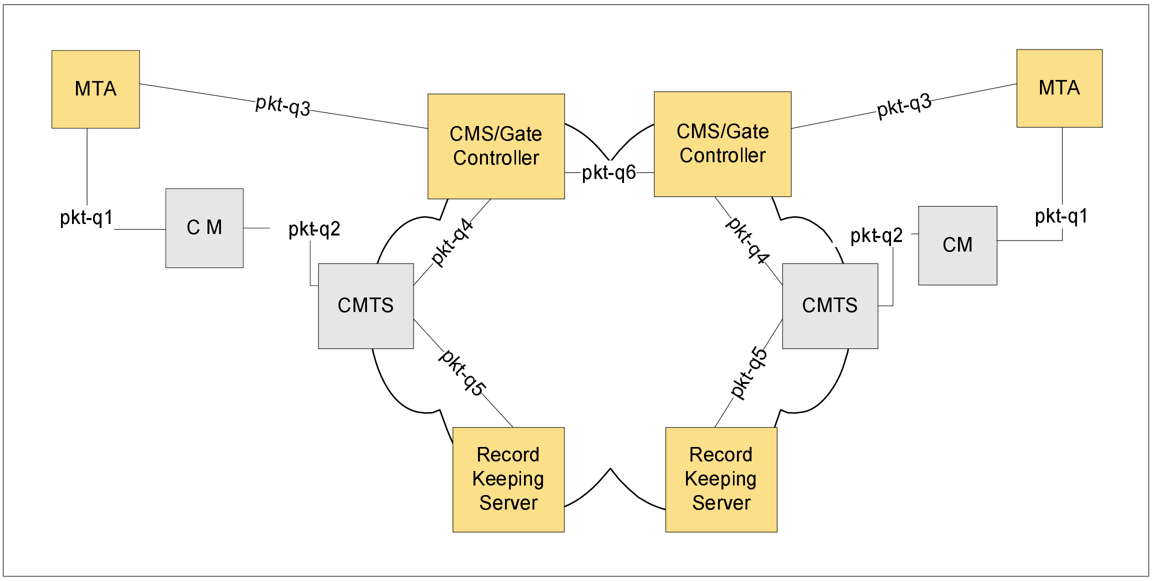


Figure 11: IPCablecom QoS Interfaces

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

Table 6: QoS Interfaces

Interface	IPCablecom Functional Components	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 Interface Descriptions

Interface	IPCablecom Functional Components	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 [i.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 signalling between IPCablecom MTA and DOCSIS®. This interface is further defined in the DOCSIS® RFI specification [i.14].
pkt-q3	MTA -CMS	Signalling interface between the MTA and CMS. Many parameters are signalled 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.

7.6.2 Dynamic Quality of Service

IPCablecom Dynamic QoS (DQoS) utilizes the call signalling 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 signalling 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.

7.7 CMS Subscriber Provisioning

The CMS Subscriber Provisioning specification [i.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.

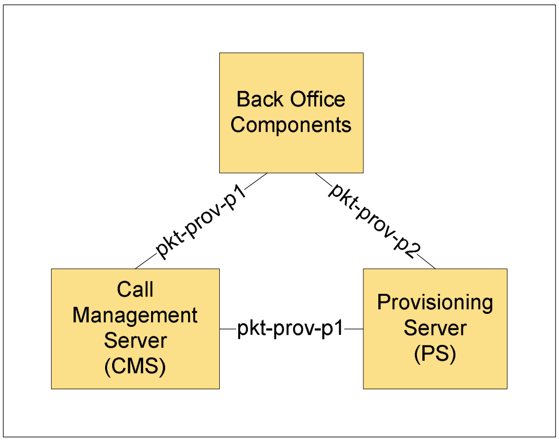


Figure 12: CMS Subscriber Provisioning Interfaces

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

Table 8: CMS Subscriber Provisioning Interfaces

Interface	IPCablecom Functional Components	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 interface 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 an 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.

7.8 Lawful Interception

The IPCablecom lawful interception framework for Law Enforcement Authorities (LEA) to lawfully intercept the IP Telephony services over cable operators' broadband IP networks is in accordance with TS 102 836-1 [i.13]. The delivery of the intercepted call data and contents is in accordance with the delivery requirements specified by ETSI Technical Committee Lawful Intercept (TC LI), ES 201 671 [i.35], TS 101 671 [i.36] and TS 102 232 [i.37].

7.9 Security

7.9.1 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 [i.10].

The security services available through IPCablecom's core service layer are: authentication, access control, integrity, and confidentiality. An 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 13 provides a summary of all the IPCablecom 1.5 security interfaces.

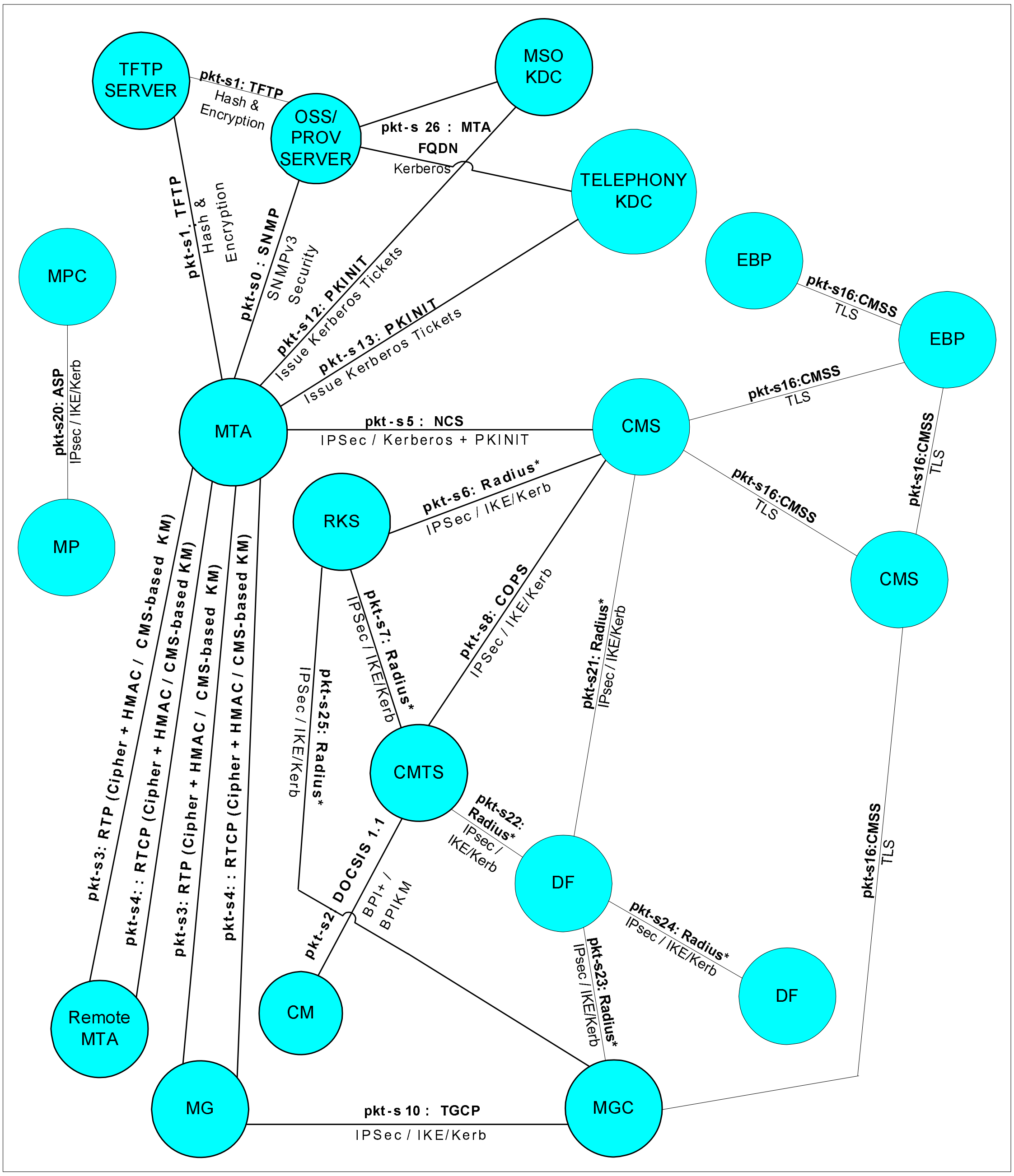

TFTP SERVER
pkt-s1: TFTP Hash & Encryption
OSS/ PROV SERVER
MSO KDC
pkt-s 26 : MTA FQDN Kerberos
TELEPHONY KDC
pkt-s1, TFTP Hash & Encryption
pkt-s0 : SNMP SNMPv3 Security
pkt-s12: PKINIT Issue Kerberos Tickets
pkt-s13: PKINIT Issue Kerberos Tickets
MPC
pkt-s20: ASP IPsec / IKE/Kerb
MP
EBP
pkt-s16:CMSS TLS
EBP
MTA
pkt-s5 : NCS IPSec / Kerberos + PKINIT
CMS
pkt-s16:CMSS TLS
pkt-s16:CMSS TLS
pkt-s16:CMSS TLS
CMS
RKS
pkt-s6: Radius* IPSec / IKE/Kerb
pkt-s3: RTP (Cipher + HMAC / CMS-based KM)
pkt-s4: : RTCP (Cipher + HMAC / CMS-based KM)
pkt-s3: RTP (Cipher + HMAC / CMS-based KM)
pkt-s4: : RTCP (Cipher + HMAC / CMS-based KM)
pkt-s25: Radius* IPSec / IKE/Kerb
pkt-s7: Radius* IPSec / IKE/Kerb
pkt-s8: COPS IPSec / IKE/Kerb
pkt-s21: Radius* IPSec / IKE/Kerb
CMTS
pkt-s22: Radius* IPSec / IKE/Kerb
DOCSIS 1.1 BPI+ / BPIKM
pkt-s2
DF
pkt-s24: Radius* IPSec / IKE/Kerb
DF
pkt-s23: Radius* IPSec / IKE/Kerb
pkt-s16:CMSS TLS
Remote MTA
CM
MG
pkt-s 10 : TGCP IPSec / IKE/Kerb
MGC

Figure 13: IPCablecom Security Interfaces

In figure 13, each interface is labelled 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 9 describes each of the interfaces shown in figure 13.

Table 9: Security Interfaces

Interface	IPCablecom Functional Components	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 signalling 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 [i.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.
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+.

Interface	IPCablecom Functional Components	Description
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.

7.9.2 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 clause 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 enrolment, device provisioning and device authorization.

7.9.2.1 Subscriber Enrolment

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

7.9.2.2 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.

7.9.2.3 Dynamic Provisioning

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

7.9.2.4 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 signalling 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 signalling messages travel unencrypted across this interface.

7.9.2.5 Signalling Security

All signalling traffic, which includes QoS signalling, call signalling, and signalling 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 signalling IPsec Security Associations.

7.9.2.6 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 signalling 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 signalling.

7.9.2.7 OSS and Billing System Security

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

8 Network Design Considerations

8.1 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) [i.19].

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

8.2 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.

8.3 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.

8.4 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 signalling 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.

8.5 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.

8.6 Priority Marking of Signalling and Media Stream Packets

The media and signalling 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) signalling 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.

Signalling packets may also benefit from prioritized QoS services. In particular, as an access network becomes loaded to capacity it may be important to forward signalling packets at a higher priority than data packets in order to avoid excessive signalling latency. If signalling prioritization is desired, then the method for providing prioritized QoS is based upon two mechanisms:

1) mark all signalling 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 signalling. 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 (RFC 3260 [i.23]) to differentiate IPCablecom media and signalling from high-speed data packets. Marking of packets for the media streams (RTP and RTCP) and the signalling 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 RFC 2474 [i.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. RFC 2474 [i.24] was updated by RFC 3168 [i.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 signalling streams is performed via the IPCablecom MIB modules for the MTA. It should be noted that in NCS the signalled SDP parameters may contain values that override the configured media stream priority marking value on a connection-by-connection basis.

8.7 Fax Support

IPCablecom supports real-time fax transmission. In IPCablecom 1.5, fax is best accomplished using the ITU-T Recommendation T.38 [i.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.

8.8 Analog Modem Support

Analog modems may be supported in one of two ways: pass-through or modem relay via V.152 [i.34].

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 analogue modem signalling from a voice call is supported. Returning to a low-bandwidth codec after modem signalling is complete is also supported.

A more robust solution for supporting analogue modems is to employ voice band data transmission using the method described in ITU-T Recommendation V.152 [i.34]. V.152 involves quickly switching to a codec that can accurately relay modem signals over an IP network.

8.9 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 RFC 2833 [i.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.

History

Document history		
V1.1.1	October 2011	Publication