International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.160

(11/2005)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

Architectural framework for the delivery of time-critical services over cable television networks using cable modems

ITU-T Recommendation J.160

ITU-T Recommendation J.160

Architectural framework for the delivery of time-critical services over cable television networks using cable modems

Summary

This Recommendation provides a high-level reference framework that identifies the functional components and defines the interfaces necessary to provide digital voice and telephony services. A family of Recommendations (ITU-T Recs J.161-J.178) has been developed to implement this architecture.

Source

ITU-T Recommendation J.160 was approved on 29 November 2005 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

		Page
1	Scope	1
2	References	1
3	Terms and definitions	2
4	Abbreviations and conventions	2
	4.1 Abbreviations	2
	4.2 Conventions	4
5	IPCablecom	4
	5.1 IPCablecom architecture framework	4
	5.2 IPCablecom zones and domains	5
	5.3 IPCablecom Recommendations	6
	5.4 IPCablecom design considerations	7
6	IPCablecom functional components	9
	6.1 Media Terminal Adapter (MTA)	10
	6.2 Cable Modem (CM)	12
	6.3 HFC access network	12
	6.4 Cable Modem Terminating System (CMTS)	12
	6.5 Call Management Server (CMS)	12
	6.6 PSTN gateway	13
	6.7 OSS back-office components	15
	6.8 Announcement Server (ANS)	16
7	Protocol interfaces	17
	7.1 Call signalling interfaces	17
	7.2 Media streams	19
	7.3 MTA device provisioning	21
	7.4 SNMP element management layer interfaces	22
	7.5 Event messages interfaces	23
	7.6 Quality of Service (QoS)	24
	7.7 CMS subscriber provisioning	27
	7.8 Electronic surveillance	28
	7.9 Security	29
8	Network design considerations	35
	8.1 Timekeeping and reporting issues	35
	8.2 Timing for playout buffer alignment with coding rate	35
	8.3 IP addressing	35
	8.4 Dynamic IP addressing assignment	36
	8.5 FQDN assignment	36
	8.6 Priority marking of signalling and media stream packets	36
	8.7 Fax support	37

Page

8.8 Analogue modem support 37

Appendix I – Glossary of terms 38

I.1 Definitions 38

I.2 Abbreviations 40

BIBLIOGRAPHY 43

ITU-T Recommendation J.160

Architectural framework for the delivery of time-critical services over cable television networks using cable modems

1 Scope

The IPCablecom project defines a family of Recommendations 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 cable modems per the DOCSIS family of Recommendations. Future work will extend this architecture to include multimedia applications.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

– ITU-T Recommendation G.711 (1988), *Pulse code modulation (PCM) of voice frequencies*.

– ITU-T Recommendation J.83 (1997), *Digital multi-programme systems for television, sound and data services for cable distribution*.

– ITU-T Recommendation J.112 (1998), *Transmission systems for interactive television services*, plus Annex A (2001), *Digital Video Broadcasting: DVB interaction channel for Cable TV (CATV distribution systems)*, Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification* and Annex C (2002), *Data-over-cable service interface specifications: Radio-frequency interface specification using QAM technique*.

– ITU-T Recommendation J.161 (2001), *Audio codec requirements for the provision of bidirectional audio service over cable television networks using cable modems*.

– ITU-T Recommendation J.162 (2005), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*.

– ITU-T Recommendation J.163 (2005), *Dynamic quality of service for the provision of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.164 (2005), *Event message requirements for the support of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.166 (2005), *IPCablecom management information base (MIB) framework*.

– ITU-T Recommendation J.167 (2005), *Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

– ITU-T Recommendation J.171.0 (2005), *IPCablecom trunking gateway control protocol (TGCP): Profiles overview*.

– ITU-T Recommendation J.178 (2005), *IPCablecom CMS to CMS signalling*.

– ITU-T Recommendation Q.704 (1996), *Signalling network functions and messages*.

– ITU-T Recommendation T.38 (2005), *Procedures for real-time Group 3 facsimile communication over IP networks*.

– IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

– IETF RFC 1119 (1989), *Network Time Protocol*.

– IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications*.

– IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal Control*.

– IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

– IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

– IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

– IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 IPCablecom: An ITU-T project that includes an architecture and a series of Recommendations that enable the delivery of real-time services over the cable television networks using cable modems.

3.2 cable modem: A cable modem is a layer two termination device that terminates the customer end of the DOCSIS connection.

3.3 managed IP network: An IP network, managed by a single entity for the purpose of transporting IPCablecom signalling and media packets.

3.4 managed IP backbone: A Managed IP network that is used for interconnecting IPCablecom domains.

4 Abbreviations and conventions

4.1 Abbreviations

This Recommendation uses the following abbreviations:

ANC Announcement Controller

ANP Announcement Player

ANS Announcement Server

CM Cable Modem

CMS Call Management Server
CPE Customer Premises Equipment
DHCP Dynamic Host Configuration Protocol
DNS Domain Name System
DTMF Dual Tone Multi-Frequency
FQDN Fully Qualified Domain Name
GC Gate Controller
HFC Hybrid Fibre/Coax
HTTP HyperText Transfer Protocol
IEEE Institute of Electrical and Electronic Engineers
IETF Internet Engineering Task Force
IP Internet Protocol
IPsec IP security
ISTP Internet Signalling Transport Protocol
ISUP Integrated Services Digital Network User Part
MAC Media Access Control
MF Multi-Frequency
MG Media Gateway
MGC Media Gateway Controller
MIB Management Information Base
MMH Multilinear Modular Hash
MTA Media Terminal Adapter
MTP Message Transfer Part
NAT Network Address Translator
NCS Network-Based Call Signalling
OSS Operations Support System
PSTN Public Switched Telephone Network
QoS Quality of Service
RKS Record Keeping Server
RTP Real-Time Transfer Protocol
SA Source Address
SCCP Signalling Connection Control Part
SG Signalling Gateway
SID System IDentification number
SNMP Simple Network Management Protocol
TCAP Transaction Capabilities Application Part
TFTP Trivial File Transfer Protocol

TGCP Trunking Gateway Control Protocol

TGS Ticket Granting Server

ToS Type of Service

UDP User Datagram Protocol

4.2 Conventions

If this Recommendation is implemented, the key words "MUST" and "SHALL" as well as "REQUIRED" are to be interpreted as indicating a mandatory aspect of this Recommendation.

The keywords indicating a certain level of significance of particular requirements that are used throughout this Recommendation are summarized.

"MUST" This word or the adjective "REQUIRED" means that the item is an absolute requirement of this Recommendation.

"MUST NOT" This phrase means that the item is an absolute prohibition of this Recommendation.

"SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that valid reasons may exist in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

"MAY" This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

5 IPCablecom

5.1 IPCablecom architecture framework

At a very high level, the IPCablecom 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 is shown in Figure 1.

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

The Managed IP network serves several functions. First, it provides interconnection between the basic IPCablecom functional components 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 Operations 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.

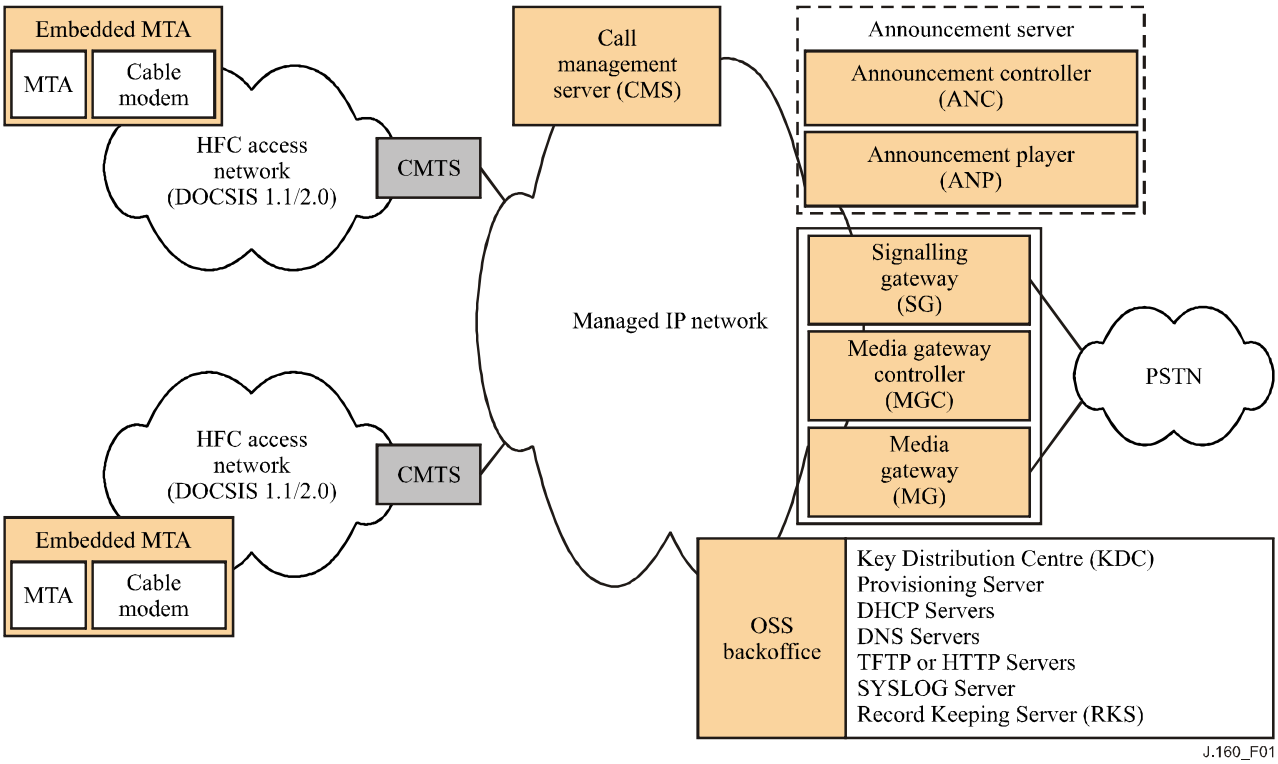


Figure 1/J.160 – IPCablecom reference architecture

5.2 IPCablecom zones and 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. Interfaces between functional components within a single zone and between zones (e.g., CMS ↔ CMS) are defined in the IPCablecom Recommendations.

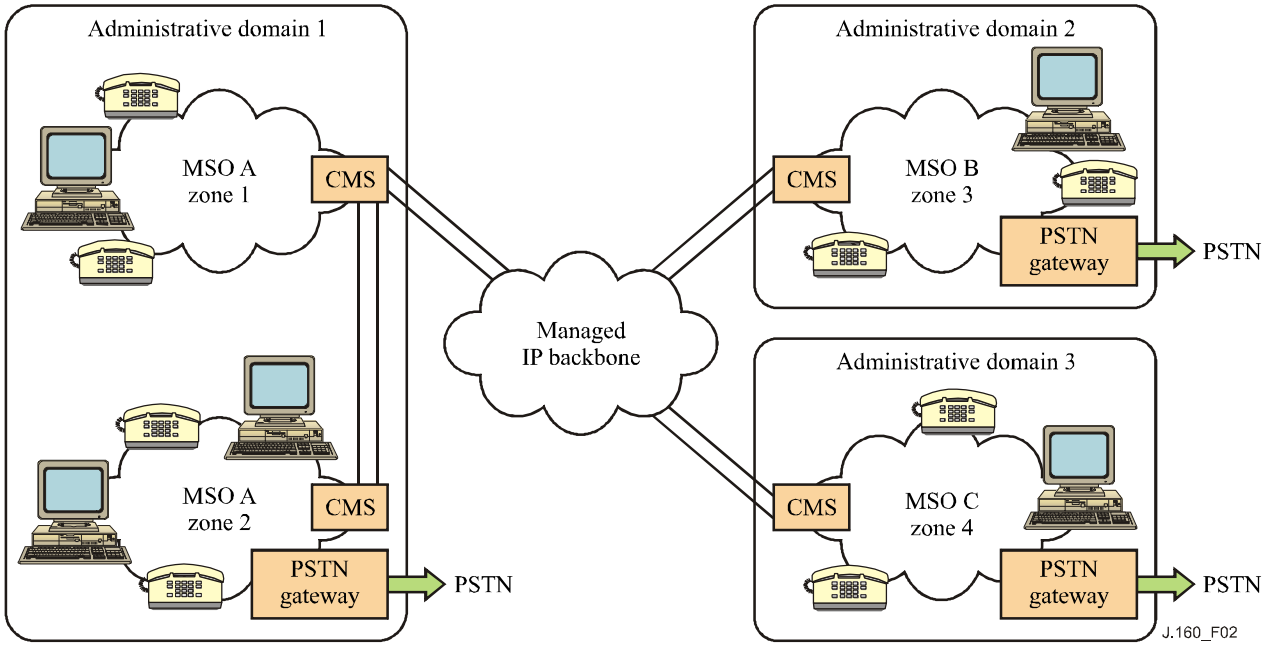


Figure 2/J.160 – Zones and administrative domains

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.

5.3 IPCablecom Recommendations

Table 1/J.160 – IPCablecom Recommendations

J.160	Architectural framework for the delivery of time-critical services over cable television networks using cable modems
J.161	Audio codec requirements for the provision of bidirectional audio service over cable television networks using cable modems
J.162	Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems
J.163	Dynamic quality of service for the provision of real-time services over cable television networks using cable modems
J.164	Event message requirements for the support of real-time services over cable television networks using cable modems
J.165	IPCablecom Internet signalling transport protocol (ISTP)
J.166	IPCablecom management information base (MIB) framework
J.167	Media Terminal Adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems
J.168	Vacant-Incorporated as Annex E/J.166
J.169	Vacant-Incorporated as Annex C/J.166
J.170	IPCablecom security specification
J.171.1	IPcablecom trunking gateway control protocol (TGCP): Profile1
J.171.2	IPcablecom trunking gateway control protocol (TGCP): Profile 2
J.172	IPCablecom management event mechanism

Table 1/J.160 – IPCablecom Recommendations

J.173	IPCablecom embedded MTA primary line support
J.174	IPCablecom interdomain quality of service
J.175	Audio server protocol
J.176	Vacant-Incorporated as Annex D/J.166
J.177	IPCablecom CMS subscriber provisioning specification
J.178	IPCablecom CMS to CMS signalling
J.179	IPCablecom support for multimedia

5.4 IPCablecom design considerations

In order to enable real-time multimedia communications across the cable network infrastructure, IPCablecom Recommendations 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 Recommendations that define the IPCablecom reference architecture. Individual IPCablecom Recommendations 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 standards. IPCablecom strives to specify open, approved industry standards that have been widely adopted in commercial communication networks. This includes standards approved by the ITU, IETF, IEEE, and other communications standards organizations.
- Leverage and build upon the data transport and Quality of Service capabilities enabled by the J.112 infrastructure.
- Define an architecture that allows multiple vendors to rapidly develop low-cost interoperable solutions to meet 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 cut-offs and call defects can be engineered to be less than 1 per 10 000 completed calls.

- Support modems (up to V.90 56 kbit/s) and fax (up to 14.4 kbit/s).
- Ensure that frame slips due to unsynchronized sampling clocks or due to lost packets occur less than 0.25 per minute Call Signalling.

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 calling features such as:
  - Call Waiting;
  - Cancel Call Waiting;
  - Call Forwarding (no-answer, busy, variable);
  - Three-way Calling;
  - Voice mail Message Waiting Indicator;
  - 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.
- Ability to direct dial any domestic or international telephone number (ITU-T Rec. E.164 address).
- Ability to receive a call from any domestic or international telephone number supported by the PSTN.
- Ensure that a new subscriber is able to retain current phone number via Local Number Portability (LNP).
- Ability to use the carrier of choice for long distance calls. This includes pre-subscription and per call selection.
- Support Call Blocking/Call Blocking Toll restrictions (e.g., blocking calls to specific prefixes).

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 in the middle of IPCablecom calls.

- Minimize and prevent 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 that delay, packet loss, and jitter have 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 wideband codec technologies.
- Specify echo cancellation and voice activity detection mechanisms.
- Support for transparent, error-free 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 calculation and reporting of VoIP Metrics to monitor voice quality.

5.4.5 Device provisioning and OSS

- Support dynamic and static provisioning of customer premises equipment (MTA and CM).
- 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 premises 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 Electronic surveillance

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

6 IPCablecom functional components

This clause describes the functional components present in an IPCablecom network (see Figure 3). Component descriptions are not intended to define or imply product implementation requirements but instead to describe the functional role of each of these components in the reference architecture. Note that specific product implementations may combine functional components as needed. Not all components are required to be present in an IPCablecom network.

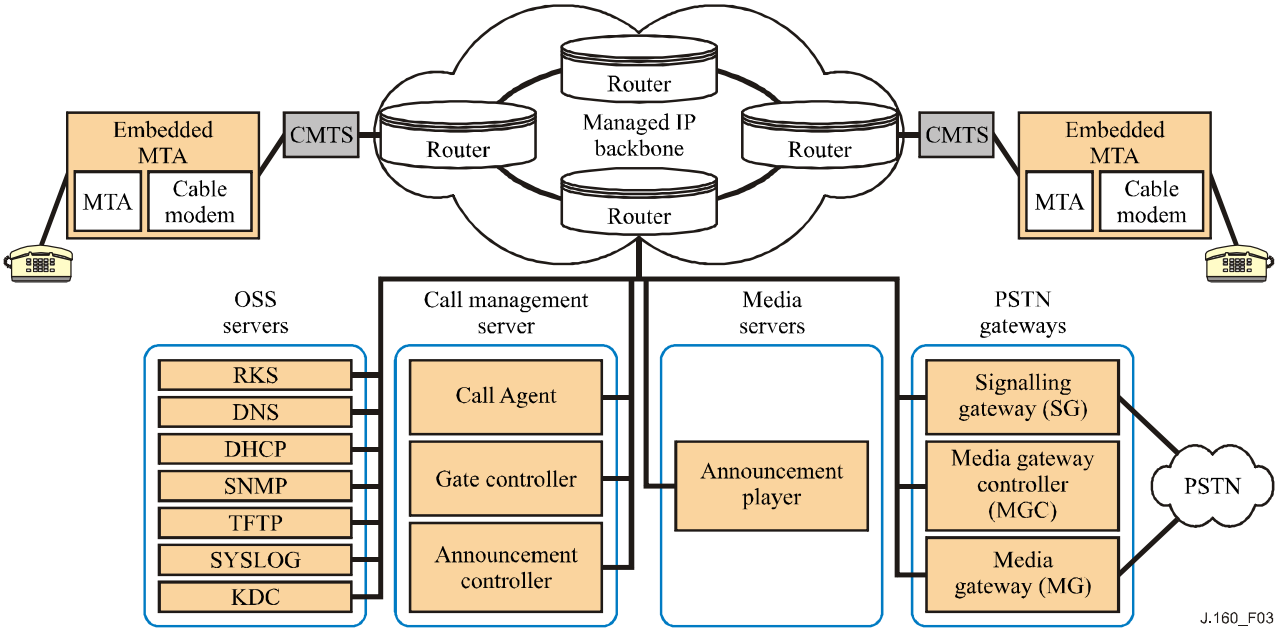


Figure 3/J.160 – IPCablecom component reference model

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 CM and MTA, are typically located within the subscriber's home and outside of the Cable Operator's facility.

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 (ITU-T Rec. J.112). IPCablecom MTAs are required to support the Network Call Signalling (NCS) protocol (ITU-T Rec. J.162).

An embedded MTA (E-MTA) is a single hardware device that incorporates a cable modem as well as an IPCablecom MTA component. Figure 4 shows a representative functional diagram of an E-MTA.

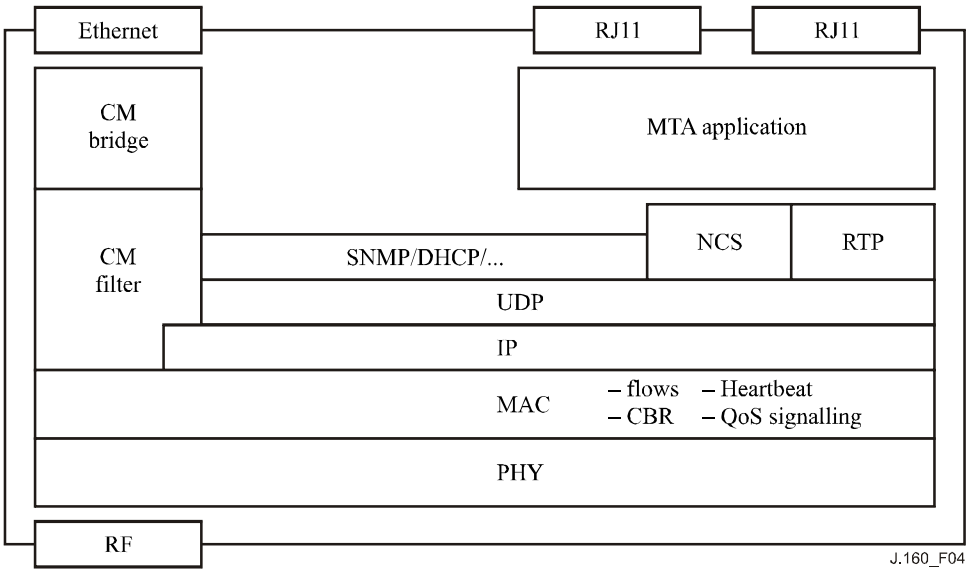


Figure 4/J.160 – E-MTA conceptual functional architecture

6.1.1 MTA functional requirements

An MTA is responsible for the following functionalities:

- NCS call signalling with the CMS.
- QoS signalling with the CMS and 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 and low bit rate codecs.
- One or more analogue and/or ISDN BRI interface(s).

Additional MTA functionality is defined in other IPCablecom Recommendations.

6.1.2 MTA Attributes

The following attributes characterize the E-MTA:

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

6.2 Cable Modem (CM)

The CM is a modulator/demodulator residing in 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 bidirectional, shared-media system that consists of the CM, the CMTS, and the DOCSIS MAC and PHY access layers.

6.4 Cable Modem Terminating System (CMTS)

The CMTS provides data connectivity and complimentary functionality to CMs over the HFC access network. 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 network-side interface and assigning it to a QoS level based on defined filter specifications.
- Policing the TOS field in received packets from the cable network to enforce TOS field settings per network operator policy.
- Altering the TOS field in the downstream IP headers based on the network operator's policy.
- Performing traffic shaping and policing as required by the flow specification.
- Forwarding downstream packets to the DOCSIS network using the assigned QoS.
- Forwarding upstream packets to the backbone network devices using the assigned QoS.
- Converting QoS Gate parameters into DOCSIS QoS parameters.
- Recording usage of 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 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. In an IPCablecom, the Call Agent (CA) refers to the control component of the CMS that is responsible for providing signalling services using the NCS protocol (ITU-T Rec. J.162) to the MTA. In this context, Call Agent responsibilities include but are not limited to:
  - implementing call features;
  - maintaining call progress state;
  - the use of codecs within the subscriber MTA device;
  - collecting and pre-processing dialled digits;
  - collecting and classifying user actions;
  - controlling 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 Dynamic Quality of Service Recommendation.

The CMS may also 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 the following functions:

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

For the purposes of this Recommendation, 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 behavior 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 is a list of functions 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 connections.
  - Connection Control instructs the MG on the basic handling of connections from and to 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 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 is a list of functions 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, e.g., continuity tests, as instructed by the MGC.
- 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 upon 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, the Signalling Gateway function only supports non-facility-associated signalling in the form of SS7.

6.6.3.1 SS7 signalling gateway functions

The following is a list of functions performed by the Signalling Gateway:

- 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) levels 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/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 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.

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 where 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 (DHCP) server

The DHCP server is a back office network element used during the MTA device provisioning process to dynamically allocate IP addresses and other client configuration information.

6.7.3 Domain Name System (DNS) server

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 instead of a TFTP server to download configuration files to the MTA.

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 is a network component that manages and plays informational tones and messages in response to events that occur in the network. An Announcement Server (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 architecture. An overview of each protocol interface is provided within this clause. The individual IPCablecom Recommendations 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 Table 2.

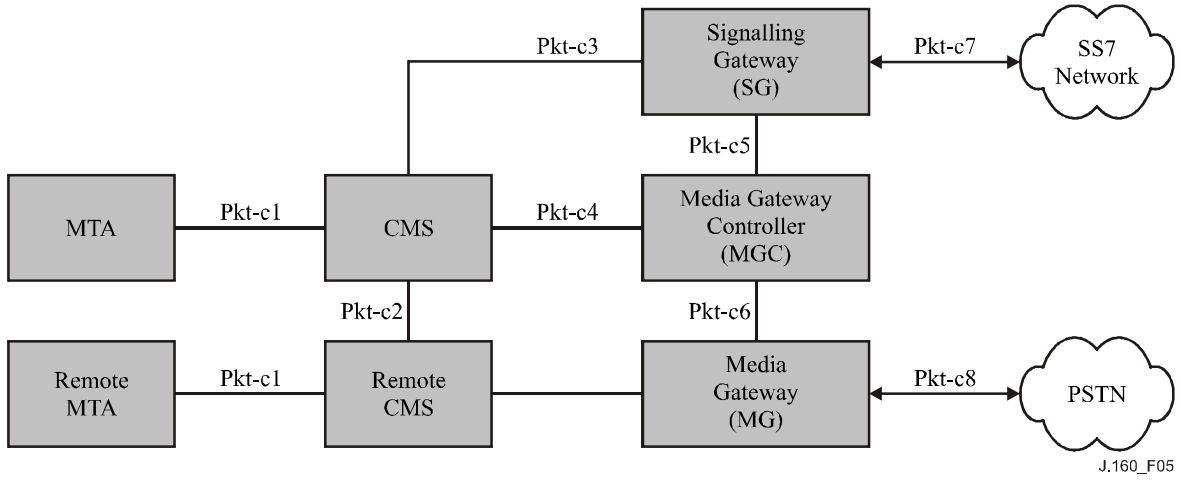


Figure 5/J.160 – Call signalling interfaces

Table 2/J.160 – 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 CMSs. The protocol for this interface is CMSS (ITU-T Rec. J.178).
Pkt-c3	CMS ↔ SG	Call signalling messages exchanged between the CMS and SG.
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.
Pkt-c6	MGC ↔ MG	Interface for control of the media gateway using the TGCP protocol, which is a profile of MGCP, similar to NCS.

Table 2/J.160 – Call signalling interfaces

Interface	IPCablecom functional components	Description
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 an extended variant of the IETF's MGCP call signalling protocol. 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 advanced services (enhanced calling features), performing call authorization, and generating billing event records, etc.

Examples of the partition of function would be for the CMS to instruct the MTA to inform the CMS when the phone goes off hook, and the appropriate number of DTMF digits have been entered. When this sequence of events occurs, the MTA notifies the CMS. The CMS may then instruct 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 an answer from the far end, it instructs the MTA to stop the ringback tone, to activate the media connection between the MTA and the far-end MTA, and to 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 centrally manage the reliability of the service provided. In addition, the service provider gains full access to all software and hardware in the event that a defect that impacts subscriber services occurs. Software can be centrally controlled, and updated in quick debugging and resolution cycles that do not require deployment of field personnel to the customer premises. Additionally, the service provider has direct control over the services introduced and the associated revenue streams associated with such services.

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 subdivided into three functional components:

- Media Gateway Controller (MGC);
- Media Gateway (MG);

- Signalling Gateway (SG).

The Media Gateway Controller and 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 (J.171) protocol (Pkt-c6). This includes creation, modification and deletion of connections. TGCP is an extended variant of the IETF's MGCP call signalling protocol. The TGCP variant is closely aligned with NCS.

The CMS and the MGC may each send routing queries (e.g., freephone 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.

7.1.3 CMS-to-CMS signalling framework

IPCablecom supports both inter-domain and intra-domain CMS-CMS and CMS-MGC signalling as defined in the CMSS Recommendation, ITU-T Rec. J.178. The CMSS signalling architecture is based on the IETF Session Initiation Protocol (SIP) (IETF RFC 3261). 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 DQoS signalling. Together, they control the coordination of the signalling for call setup and resource management.

7.2 Media streams

The IETF standard RTP (RFC 1889, *RTP: A Transport Protocol for Real-Time Applications)* is used to transport all media streams in the IPCablecom network. IPCablecom utilizes the RTP profile for audio and video streams as defined in IETF RFC 1890 (*RTP Profile for Audio and Video Conferences with Minimal Control*).

The primary media flow paths in the IPCablecom network architecture are shown in Figure 6 and are further described below.

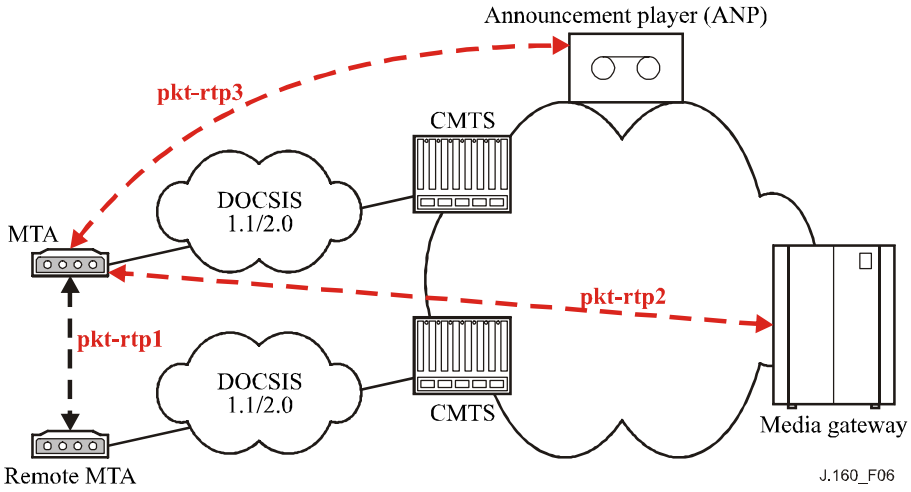


Figure 6/J.160 – RTP media stream flows in an IPCablecom network

Table 3/J.160 – 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 packet. Most of the common audio algorithms are assigned to particular payload type 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.

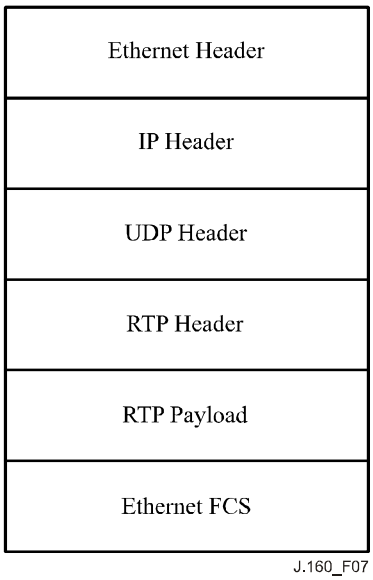


Figure 7/J.160 – RTP packet format

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) 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 10 bytes for packetized voice. The DOCSIS Recommendations address this issue with a Payload Header Suppression feature for abbreviating common headers.

ITU-T Rec. T.38 is also used to transport facsimile media in IPCablecom networks, refer to clause 8.7 for more details.

7.2.1 Real-time Transport Control Protocol (RTCP)

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

Extensions to RTCP exist in order to better assess the quality of a voice call and diagnose problems on the network more effectively. These extensions are called RTCP Extended Reports (RTCP XR), and are defined in IETF RFC 3611. RTCP XR contains many sets of metrics. IPCablecom 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 provisioning Recommendation also includes attribute definitions required in the MTA configuration file. (See Figure 8.)

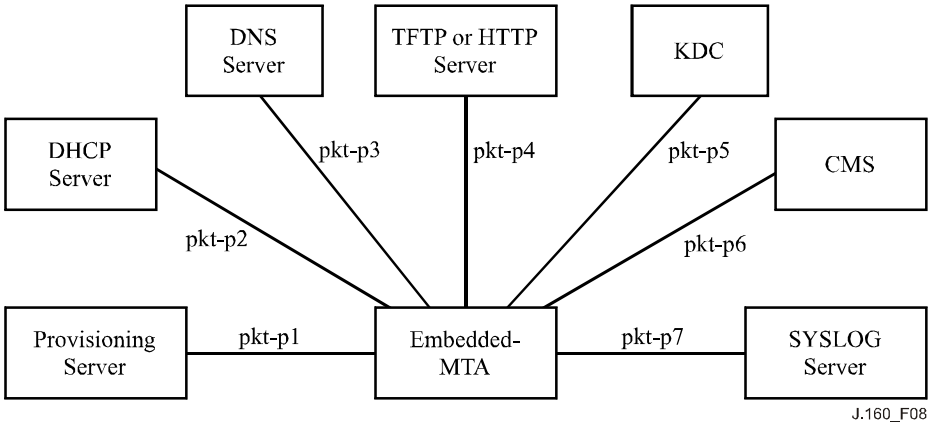


Figure 8/J.160 – IPCablecom provisioning interfaces

Table 4 describes the provisioning interfaces shown in Figure 8.

Table 4/J.160 – 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 sends 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	MTA configuration file is downloaded to the MTA from the TFTP Server or HTTP Server.
Pkt-p5	MTA ↔ KDC	MTA obtains a Kerberos ticket from the Key Distribution Centre using the Kerberos protocol.
Pkt-p6	MTA ↔ CMS	MTA establishes an IPsec Security Association with the CMS 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. SNMPv3 "traps" and "informs" are supported for event handling, as well as "sets" and "gets" for provisioning. The IPCablecom NCS MIB contains Network Call Signalling information for provisioning on both a device and a per-endpoint basis. The MTA MIB contains data for device provisioning and for supporting provisioned functions such as event logging. More detailed information on the MIBs can be found in the IPCablecom MIBs framework Recommendation (ITU-T Rec. J.166).

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 with 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.

This IPCablecom Event Messages Recommendation (ITU-T Rec. J.164) defines the structure of the Event Message data record and defines RADIUS 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.

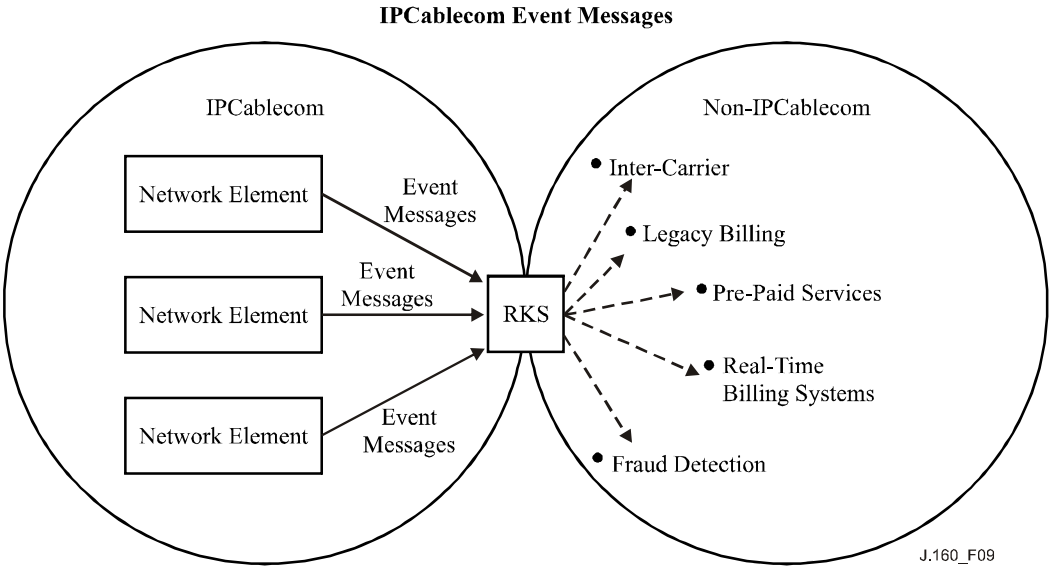
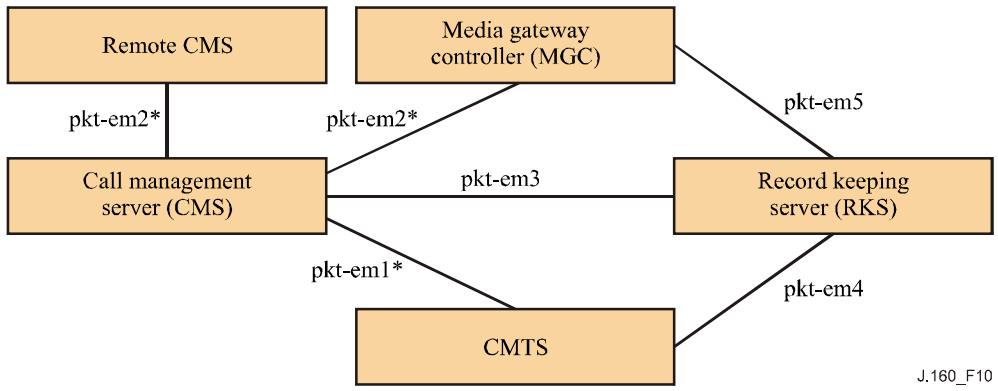


Figure 9/J.160 – Representative Event Messages architecture

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

Table 5/J.160 – 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 ↔ MGC CMS ↔ CMS	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.



NOTE – * Indicates that existing signalling interface is used to carry the data used for other EM interfaces

Figure 10/J.160 – Event Message interfaces

7.6 Quality of Service (QoS)

7.6.1 QoS framework

The IPCablecom QoS Framework is represented in Figure 11:

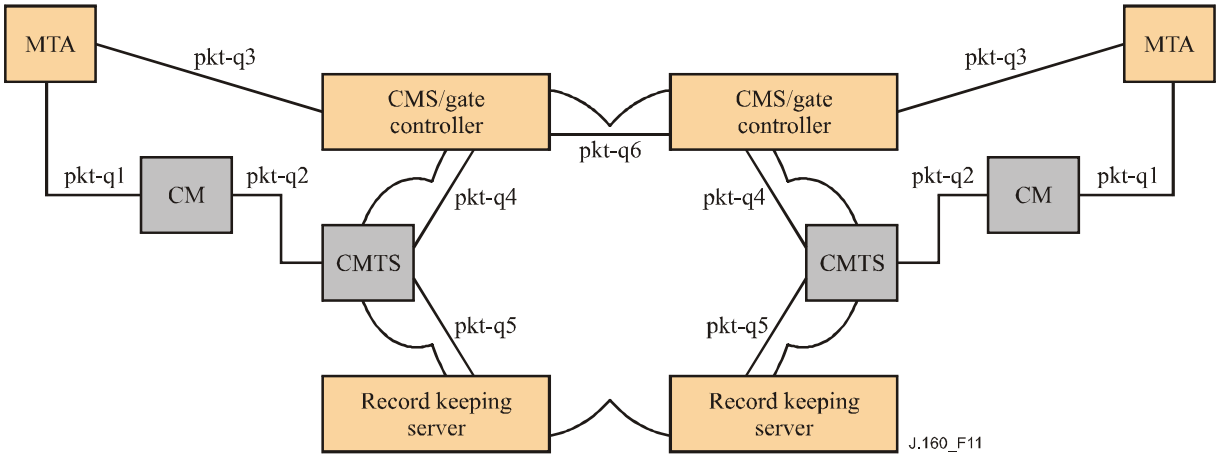


Figure 11/J.160 – IPCablecom QoS signalling interfaces

Table 6 briefly identifies each interface and how each interface is used in the Dynamic QoS Recommendation (DQoS/ITU-T Rec. J.163).

Table 6/J.160 – QoS interfaces

Interface	IPCablecom functional components	DQoS description
Pkt-q1	MTA ↔ CM	E-MTA, MAC Control Service Interface
Pkt-q2	CM ↔ CMTS	J.112, 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/J.160 – QoS interfaces

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 delay 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 ITU-T Rec. J.112.
Pkt-q2	CM ↔ CMTS	This is the DOCSIS QoS interface (control, scheduling, and transport). It should be noted that, architecturally, control functions can be initiated only by the CM. The CMTS 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 bit rate 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 delay and jitter. • Internal sublayer signalling between IPCablecom MTA and the CM (embedded MTA). This interface is further defined in ITU-T Rec. J.112.

Table 7/J.160 – QoS interfaces

Interface	IPCablecom functional components	Description
Pkt-q3	MTA ↔ CMS	Signalling interface between the MTA and CMS. Many parameters are signalled across this interface such as media stream, IP addresses, port numbers, and the selection of Codec and packetization.
Pkt-q4	CMS ↔ 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 Recommendation.
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 dynamically authorize resources for the call. Dynamic QoS 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 10 ms") 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, the request will be 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 data stream is destined to and originated from the parties that are authorized.

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 CMTS with respect to each of 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 Recommendation 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.

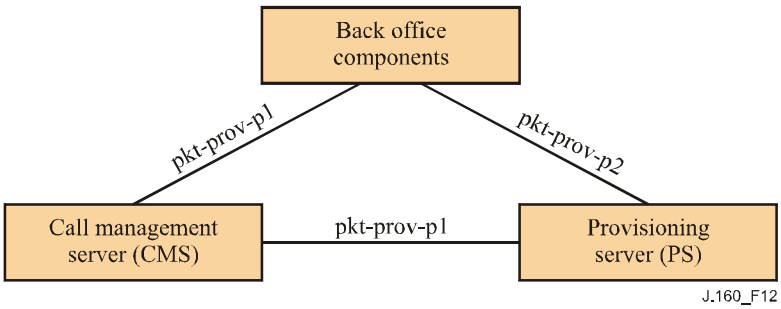


Figure 12/J.160 – CMS subscriber provisioning interfaces

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

Table 8/J.160 – CMS subscriber provisioning interfaces

Interface	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 interfaces allows the Back office components to exchange information with the Provisioning Server. This interface is not defined in IPCablecom.

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 beyond the scope of 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 set up 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 Electronic surveillance

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

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

The IPCablecom electronic surveillance framework is represented in Figure 13.

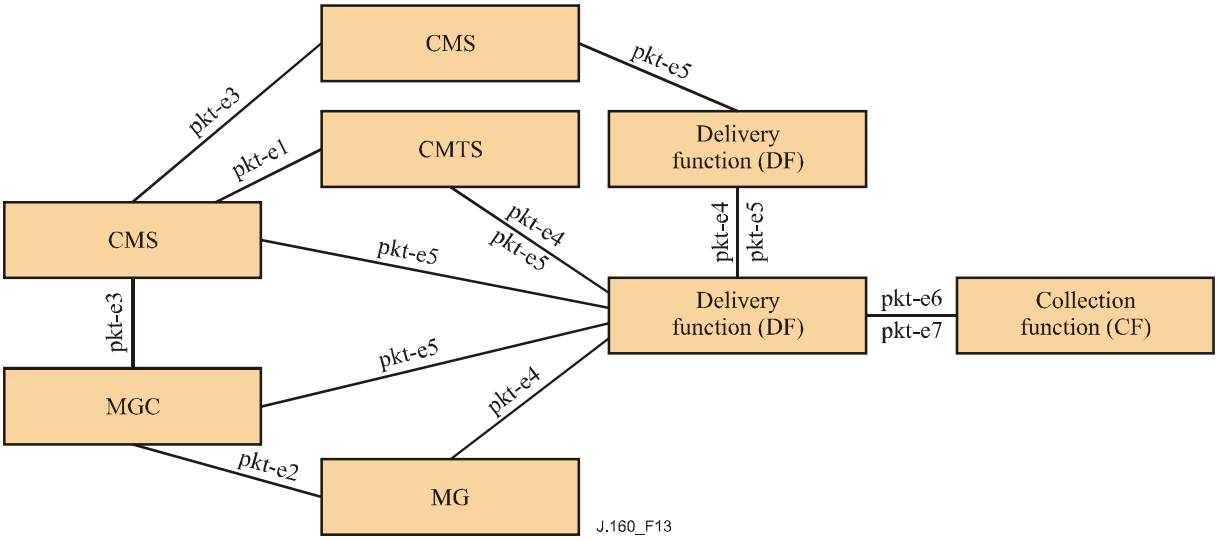


Figure 13/J.160 – Electronic surveillance interfaces

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

Table 9/J.160 – Electronic surveillance interfaces

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

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 Recommendation (ITU-T Rec. J.170).

The security services available through IPCablecom's core service layer are authentication, access control, integrity, and confidentiality. An IPCablecom protocol interface may employ zero, one or more of these services to address its particular security requirements.

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

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

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

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

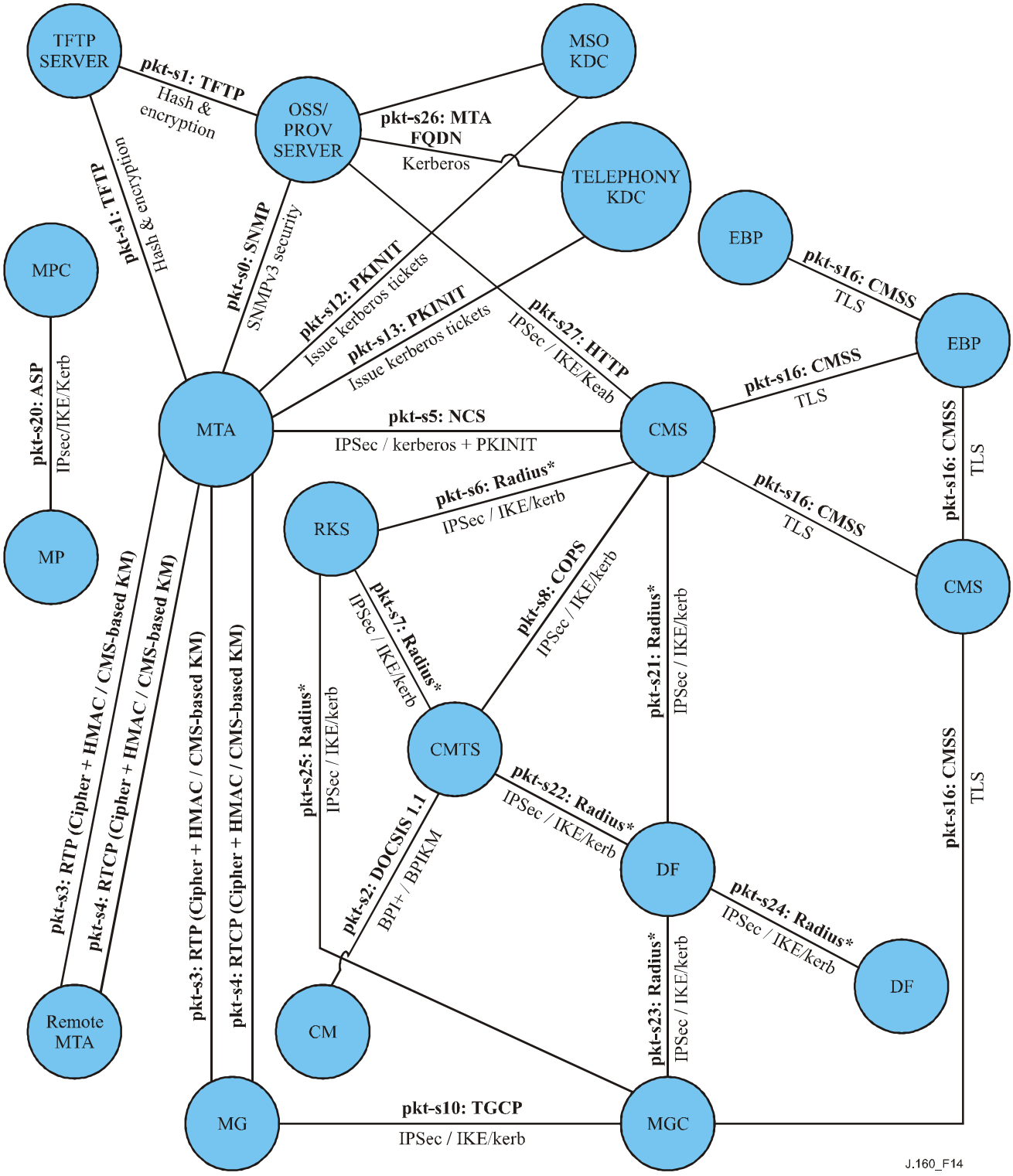


Figure 14/J.160 – IPCablecom security interfaces

In Figure 14, 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 in Figure 14.

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

Table 10/J.160 – 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 or PS/OSS	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	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 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	CMTS ↔ RKS	Radius, IPsec is used for both message integrity as well as privacy. Key management is IKE– or Kerberos.
Pkt-s8	CMS ↔ CMTS	COPS protocol between the GC and the CMTS, used to download QoS authorization to the CMTS. Message integrity and privacy provided with IPsec. 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 where 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.

Table 10/J.160 – Security interfaces

Interface	IPCablecom functional components	Description
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+.
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 allows device provisioning to occur in an unsecured mode, or in a secured mode. IPCablecom also allows for insecure SNMPv2 management after the MTA has been securely provisioned. Since this section of this Recommendation 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 subscribed to by the subscriber for the MTA.

Subscriber enrolment may occur in-band or out-of-band. The actual specification of the subscriber enrolment process is beyond the scope of 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 extensions, is used to exchange keys between MTA clients and their CMS server; IKE or, optionally, Kerberos, will be used to manage all other signalling IPsec SAs.

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 operating in secure mode. The SNMPv3 User Security Model (RFC 3414) provides authentication and privacy services for SNMP traffic. SNMPv3 view-based access control (RFC 3415) 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 PacketCable security Recommendation 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 Timekeeping 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) (per RFC 1119).

It is recommended that IPCablecom networks maintain a 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

Packet generating and packet handing equipment generally operate with free-running clocks. Problems may arise in the offering of isochronous services 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 the playout buffers.

In order to minimize the occurrence of these conditions, all CMTSs 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 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.

All IPCablecom MTAs are required to have two IP addresses – one for the CM and one for the MTA. All IPCablecom embedded MTAs are required to have 2 MAC addresses – one for the CM and one for the MTA. IPCablecom supports only IPv4 addresses.

The following requirements can be met using the dual IP address configuration:

- 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.
- With two IP addresses per MTA, the IPCablecom operator can route the voice service 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 each of the two destination IP addresses.
- The IPCablecom 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 addressing 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 NCS Recommendation (ITU-T Rec. J.162) 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 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 (phase 1).

8.6 Priority marking of signalling and media stream packets

Both the media stream and the signalling stream 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 primary mechanism for providing low-delay 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 number. 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 utilized within CMTS/CM queuing systems and also within Diffserv managed QoS backbones in order to provide high priority QoS treatment of such packets. IPCablecom does not define how QoS policies are applied in the 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 delay. If signalling prioritization is desired, then the method for providing prioritized QoS is based upon two mechanisms. First, mark all signalling packets with a high priority marking, and second, 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 (low delay) but low bandwidth.

The IPCablecom Architecture enables the use of the Differentiated Services framework (IETF RFC 3260) 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 IETF RFC 2474 attempts to rename the TOS octet of the IPv4 header, and Traffic Class octet of the IPv6 header, respectively, to the DS field. The DS Field has a six-bit Diffserv Codepoint and two "currently unused" bits. IETF RFC 2474 was updated by IETF RFC 3168 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, fax is best accomplished using ITU-T Rec. T.38 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 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 the case of fax relay, switching from fax back to voice is also supported.

8.8 Analogue modem support

Analogue modems are supported in a similar fashion 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.

Local termination of modems and translating the modem stream to an IP modem relay data stream is not required.

Appendix I

Glossary of terms

This appendix contains the complete list of terms, definitions, acronyms and abbreviations used in the suite of IPCablecom Recommendations.

I.1 Definitions

I.1.1 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.

I.1.2 active: A J.112 Flow is said to be "active" when it is permitted to forward data packets. A J.112 Flow must first be admitted before it is active.

I.1.3 authentication: The process of verifying the claimed identity of an entity to another entity.

I.1.4 authenticity: The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.

I.1.5 authorization: The act of giving access to a service or device if one has the permission to have the access.

I.1.6 cable modem: A cable modem is a layer-two termination device that terminates the customer end of the J.112 connection.

I.1.7 call: A call is an instance of user-initiated voice communication capabilities. In traditional telephony, a call is generally considered as the establishment of connectivity directly between two points: originating party and terminating party. In the IPCablecom context, as noted above, the communication between the parties is "connectionless" in the traditional sense.

I.1.8 cipher: An algorithm that transforms data between plaintext and ciphertext.

I.1.9 ciphersuite: A set which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of IPCablecom.

I.1.10 confidentiality: A way to ensure that information is not disclosed to any one, other than the intended parties. Information is encrypted to provide confidentiality. Also known as "privacy".

I.1.11 downstream: The direction from the head-end toward the subscriber location.

I.1.12 encryption: A method used to translate information in plaintext into ciphertext.

I.1.13 endpoint: A Terminal, Gateway or MCU.

I.1.14 event message: An Event Message is a set of data, representative of an event in the IPCablecom architecture that could be indicative of usage of one or more billable IPCablecom capabilities. An Event Message by itself may not be fully indicative of a customer's billable activities, but an Event Message correlated with other Event Messages builds the basis of a billable Usage Detail Record.

I.1.15 event message attribute: An Event Message Attribute is a predefined data element described by an attribute definition and attribute type.

I.1.16 gateway: Bridging devices between the IPCablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signalling Gateway which sends and receives circuit switched network signalling to the edge of the IPCablecom network.

I.1.17 header: Protocol control information located at the beginning of a protocol data unit.

I.1.18 integrity: A way to ensure that information is not modified except by those who are authorized to do so.

I.1.19 IPCablecom: An ITU-T project that includes an architecture and a series of Recommendations that enable the delivery of real-time services over the cable television networks using cable modems.

I.1.20 IPCablecom transaction: An IPCablecom transaction is a collection of events on the IPCablecom network when delivering a service to a subscriber. Event Messages for the same transaction are identified by one unique Billing Correlation ID. For some services, multiple transactions may be required to provide information that is necessary to collect the total usage for the service. Multiple Event Messages may be required to track resources for each individual service used. A Transaction may persist over time.

I.1.21 J.112 flow: A unidirectional or bidirectional flow of data packets that is subject to MAC-layer signalling and QoS assignment compliant with ITU-T Rec. J.112.

I.1.22 Kerberos: A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.

I.1.23 key: A mathematical value input into the selected cryptographic algorithm.

I.1.24 key exchange: The swapping of public keys between entities to be used to encrypt communication between the entities.

I.1.25 key management: The process of distributing shared symmetric keys needed to run a security protocol.

I.1.26 Management Information Base (MIB): The specification of information in a manner that allows standard access through a network management protocol.

I.1.27 non-repudiation: The ability to prevent a sender from denying later that he or she sent a message or performed an action.

I.1.28 privacy: A way to ensure that information is not disclosed to any one, other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as "confidentiality".

I.1.29 private key: The key used in public key cryptography that belongs to an individual entity and must be kept secret.

I.1.30 proxy: A facility that indirectly provides some service or acts as a representative in delivering information, thereby relieving a host from having to support the services itself.

I.1.31 public key: The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.

I.1.32 public key certificate: A binding between an entity's public key and one or more attributes relating to its identity. Also known as a "digital certificate".

I.1.33 public key cryptography: A procedure that uses a pair of keys, a public key and a private key, for encryption and decryption; also known as a asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key which can decrypt messages sent encrypted by the user's public key.

I.1.34 root private key: The private signing key of the highest level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.

I.1.35 root public key: The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.

I.1.36 service: A service is an individual or package of communications features a subscriber may select. A service is identified by a set of one or more "calls" or transactions that deliver the desired functionality to the subscriber. Examples of a service include: a voice communication between two local IPCablecom subscribers, a 3-way call, pay-per-view movie, and a web-surfing session. A service may be instantaneous or persist over time.

I.1.37 Signalling Gateway (SG): An SG is a signalling agent that receives/sends SCN native signalling at the edge of the IP network. In particular, the SS7 SG function translates variants ISUP and TCAP in a SS7-Internet Gateway to a common version of ISUP and TCAP.

I.1.38 X.509 certificate: A public key certificate specification developed as part of the ITU-T Rec. X.500-series standards directory.

I.2 Abbreviations

AH	Authentication Header
AMA	Automated Message Accounting
AN	Access Node
ANC	Announcement Controller
ANP	Announcement Player
ANS	Announcement Server
API	Application Programming Interface
BPI+	Baseline Privacy Interface Plus
CA	Call Agent
CBC	Cipher Block Chaining (mode)
CDR	Call Detail Record
CIC	Circuit Identification Code
CID	Circuit ID
CM	Cable Modem
CMS	Call Management Server
CMS	Cryptographic Message Syntax
CMTS	Cable Modem Termination System
COPS	Common Open Policy Service
CPE	Customer Premises Equipment
DCS	Distributed Call Signalling
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPC	Destination Point Code
DQoS	Dynamic Quality of Service
DTMF	Dual Tone Multi-Frequency
ESP	IPsec Encapsulation Security
FID	Flow Identifier

FQDN	Fully Qualified Domain Name
GC	Gate Controller
HFC	Hybrid Fibre/Coaxial (cable)
HMAC	Hashed Message Authentication Code
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKE–	IKE with pre-shared keys for authentication
IKE+	A notation defined to refer to the use of IKE, which requires digital certificates for authentication
INA	Interactive Network Adapter
IP	Internet Protocol
IPsec	IP security
ISTP	Internet Signalling Transport Protocol
ISUP	Integrated Services Digital Network User Part
LNP	Local Number Portability
MAC	Message Authentication Code
MAC	Media Access Control
MD5	Message Digest 5
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MGCI	Media Gateway Controller Interface
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MMH	Multilinear Modular Hash
MTA	Media Terminal Adapter
MTP	Message Transfer Part
MWD	Maximum Waiting Delay
NCS	Network Call Signalling
NTP	Network Time Protocol
OSS	Operations Support System
PHS	Payload Header Suppression
PKI	Public Key Infrastructure
PKINIT	Public Key Cryptography Initial Authentication

PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAP	Resource Allocation Protocol
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in IPCablecom
RFC	Request for Comments
RFI	Radio Frequency Interface
RKS	Record Keeping Server
RSVP	Resource reSerVation Protocol
RTCP	Real-Time Control Protocol
RTO	Retransmission Timeout
RTP	Real-Time Transfer Protocol
SA	Source Address
SA	Security Association
SCCP	Signalling Connection Control Part
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SG	Signalling Gateway
SHA-1	Secure Hash Algorithm 1
SID	System IDentification number
SIP	Session Initiation Protocol
SIP+	Session Initiation Protocol Plus
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SS7	Signalling System No. 7
SSP	Signal Switching Point
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TGS	Ticket Granting Server
TLV	Type-Length-Value
ToS	Type of Service
UDP	User Datagram Protocol
VAD	Voice Activity Detection
VoIP	Voice Over IP

BIBLIOGRAPHY

– IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

– IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.

– IETF RFC 2274 (1998), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).* (Obsoletes RFC 2275).

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006