INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.160

(02/2002)

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 J-SERIES RECOMMENDATIONS

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

General Recommendations	J.1–J.9
General specifications for analogue sound-programme transmission	J.10–J.19
Performance characteristics of analogue sound-programme circuits	J.20–J.29
Equipment and lines used for analogue sound-programme circuits	J.30–J.39
Digital encoders for analogue sound-programme signals	J.40–J.49
Digital transmission of sound-programme signals	J.50–J.59
Circuits for analogue television transmission	J.60–J.69
Analogue television transmission over metallic lines and interconnection with radio-relay links	J.70–J.79
Digital transmission of television signals	J.80–J.89
Ancillary digital services for television transmission	J.90–J.99
Operational requirements and methods for television transmission	J.100–J.109
Interactive systems for digital television distribution	J.110–J.129
Transport of MPEG-2 signals on packetised networks	J.130–J.139
Measurement of the quality of service	J.140–J.149
Digital television distribution through local subscriber networks	J.150–J.159
IPCablecom	**J.160–J.179**
Miscellaneous	J.180–J.199
Application for Interactive Digital Television	J.200–J.209

For further details, please refer to the list of ITU-T Recommendations.

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

Source

ITU-T Recommendation J.160 was prepared by ITU-T Study Group 9 (2001-2004) and approved under the WTSA Resolution 1 procedure on 13 February 2002.

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.

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

ITU-T Recommendation J.160

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

1 Scope

This Recommendation is subject to further study to allow evolution of the architecture to meet additional requirements.

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; all 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.

– 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, *Transmission systems for interactive television services*, *Annexes A, B and C*.

– 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 (2001), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*.

– ITU-T Recommendation J.163 (2001), *Dynamic quality of service for the provision of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.164 (2001), *Event message requirements for the support of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.165 (2002), *IPCablecom signalling transport protocol*.

– ITU-T Recommendation J.166 (2001), *IPCablecom management information base (MIB) framework*.

– ITU-T Recommendation J.167 (2002), *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.168 (2001), *IPCablecom media terminal adapter (MTA) MIB requirements*.

– ITU-T Recommendation J.169 (2001), *IPCablecom network call signalling (NCS) MIB requirements*.

– ITU-T Recommendation J.170 (2002), *IPCablecom security specification*.

– ITU-T Recommendation J.171 (2002), *IPCablecom trunking gateway control protocol (TGCP)*.

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

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

3 Terms and definitions

This Recommendation defines the following terms:

3.1 access node: As used in this Recommendation, an Access Node is a layer two termination device that terminates the network end of the J.112 connection. It is technology specific. In J.112 Annex A it is called the INA while in Annex B it is the CMTS.

3.2 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.

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

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

3.5 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:

AN	Access Node
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	Operational 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 specification.

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 specification.

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

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

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

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

5 IPCablecom

5.1 IPCablecom architecture framework

At a very high level, the IPCablecom architecture contains three networks: the "J.112 HFC access network", the "Managed IP network" and the PSTN. The Access Node (AN) provides connectivity between the "J.112 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.

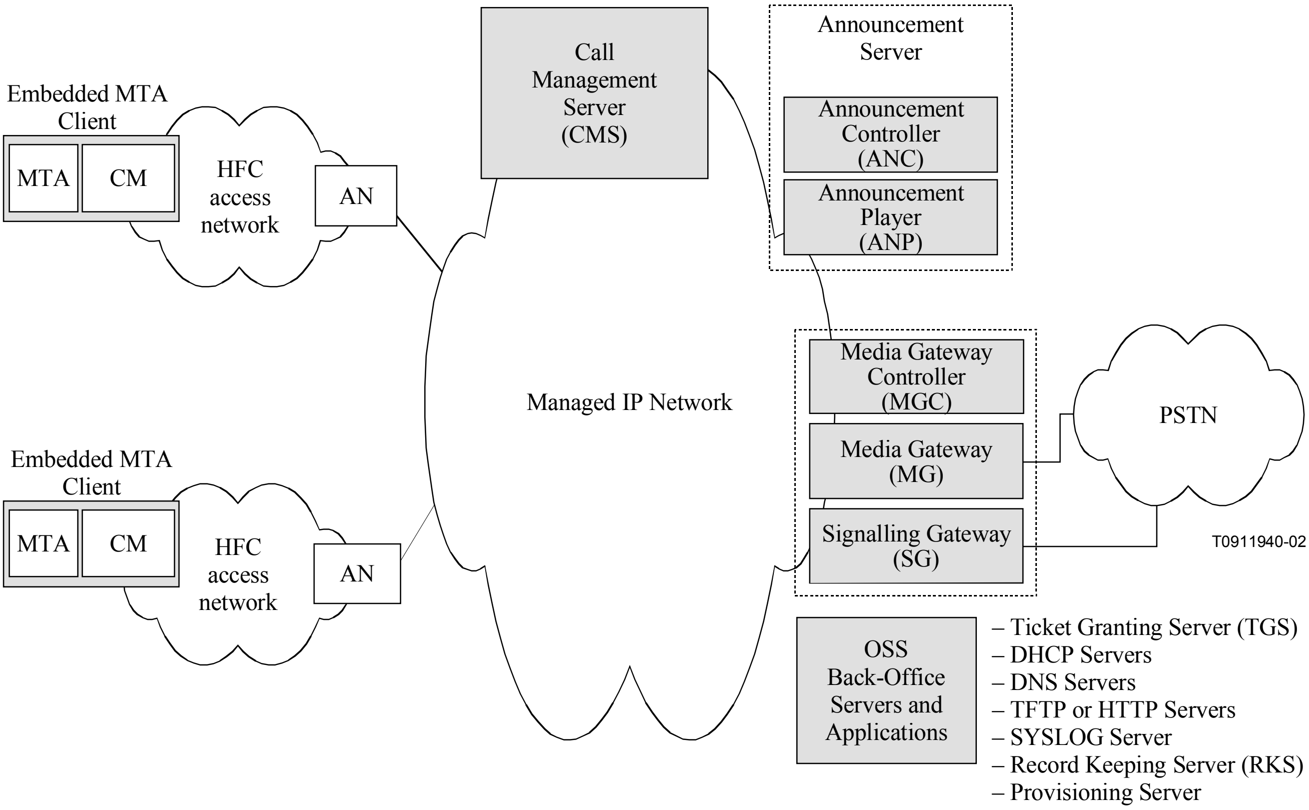


Figure 1/J.160 – IPCablecom reference architecture

The J.112 HFC access network provides high-speed, reliable, and secure transport between the customer premise and the cable headend. This access network may provide all J.112 capabilities including Quality of Service.

The Managed IP network serves several functions. First, it provides interconnection between the basic IPCablecom functional components responsible for signalling, media, provisioning, and quality of service establishment. In addition, the managed IP network provides long-haul IP connectivity between other Managed IP and J.112 HFC networks. The Managed IP network includes the following functional components: Call Management Server (CMS), Announcement Server (ANS), several Operational Support System (OSS) back-office servers, Signalling Gateway (SG), Media Gateway (MG), and Media Gateway Controller (MGC).

The individual network components that are shown in Figure 1 are described in detail in clause 6.

5.2 IPCablecom zones and domains

An IPCablecom zone consists of the set of MTAs in one or more J.112 HFC access networks that are managed by a single functional CMS as shown in Figure 2. Interfaces between functional components within a single zone are defined in the IPCablecom specifications. Interfaces between zones (e.g. CMS-CMS) have not been defined and will be addressed in future phases of the IPCablecom architecture.

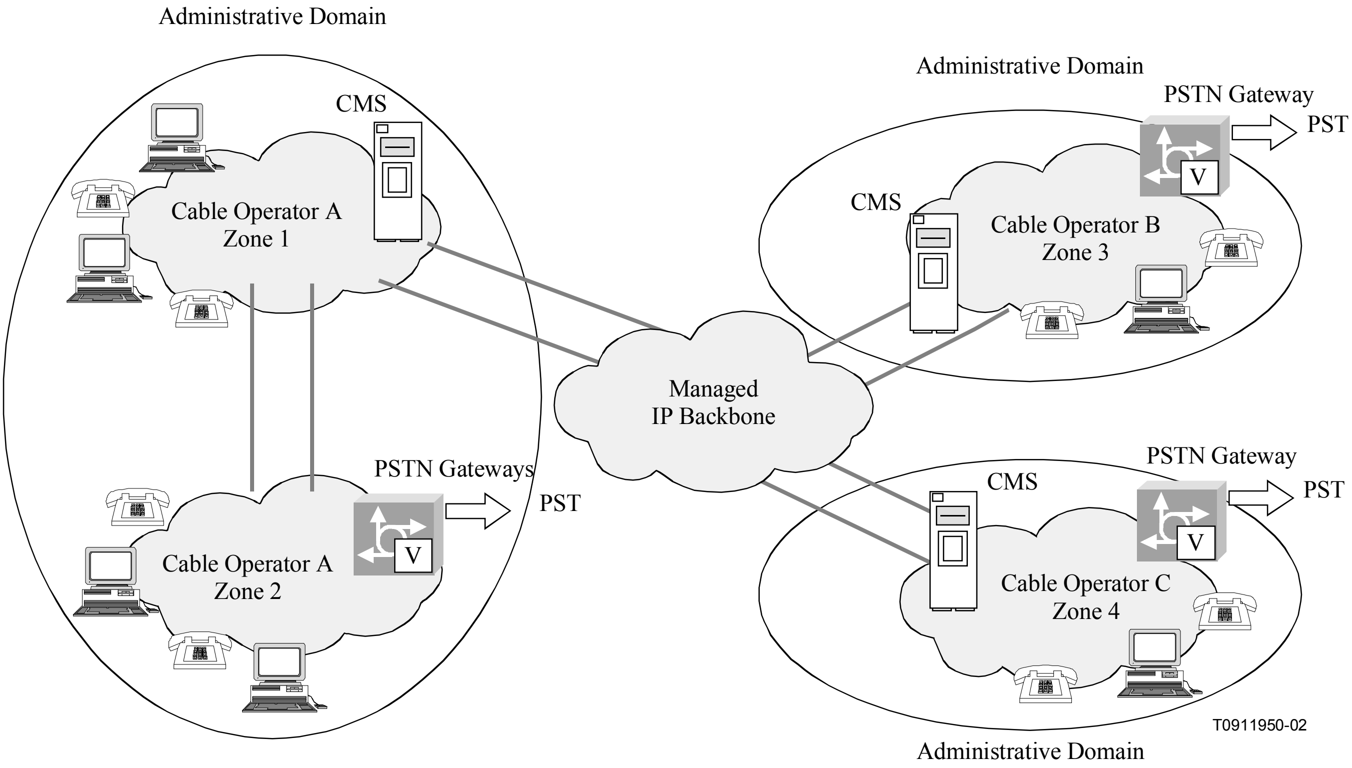


Figure 2/J.160 – Zones and administrative domains

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. Interfaces between domains have not been defined in IPCablecom and are for further study.

5.3 IPCablecom Recommendations

Refer to clause 2 for a list of IPCablecom Recommendations. Should a technical detail in one of these Recommendations conflict with this Recommendation, the IPCablecom Recommendations in clause 2 take precedence.

5.4 IPCablecom design considerations

This clause provides an overview of the high-level design goals and concepts used in developing the specifications that define the IPCablecom reference architecture.

5.4.1 General architectural goals

- Enable voice quality capabilities comparable 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) can meet the delay requirements for all IPCablecom real-time services, including voice.
- Ensure the packet loss rate, jitter, and latency (delay) for the Managed IP Network can meet the requirements for all IPCablecom real-time services, including voice.
- Support primary and/or secondary line residential voice communications capabilities.
- 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 meet the service provider's requirements.
- 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.
- Define a network-based signalling paradigm.
- 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 within a single IPCablecom zone;
  - calls that originate from the cable network and terminate on the PSTN;
  - calls that originate within one IPCablecom zone and terminate in another IPCablecom zone are for further study;
  - calls that originate on the PSTN, transit the IPCablecom network, and terminate on the PSTN are not specifically considered in this architecture.
- 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 a signalling paradigm 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).

5.4.2 Quality of Service

- Provide a rich set of policy mechanisms to provide 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.
- Enable transparent access to all of the QoS mechanisms defined in ITU-T Rec. J.112. IPCablecom clients need not be aware of specific J.112 QoS primitives and parameters.
- Minimize and prevent abusive QoS usage including theft-of 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.

5.4.3 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). Evaluation criteria for mandatory codecs are selected as those most efficient with respect to voice quality, bandwidth utilization, and implementation complexity.
- Accommodate evolving narrow-band and wide-band codec technologies.
- Specify echo cancellation and voice activity detection mechanisms.
- Support for transparent, error-free DTMF transmission and detection.
- Support terminal devices for the deaf and hearing impaired.

- Provide mechanisms for codec switching when fax and modem services are required.

5.4.4 Device provisioning and OSS

- Support dynamic and static provisioning of customer premises equipment (MTA and CM).
- 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 SNMP MIBs for managing customer premises equipment (MTA).

5.4.5 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, non-repudiation and access control.

5.4.6 Managed IP network

The network needs to have bounds on the QoS performance parameters, e.g. packet loss, for packets traversing the network.

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.

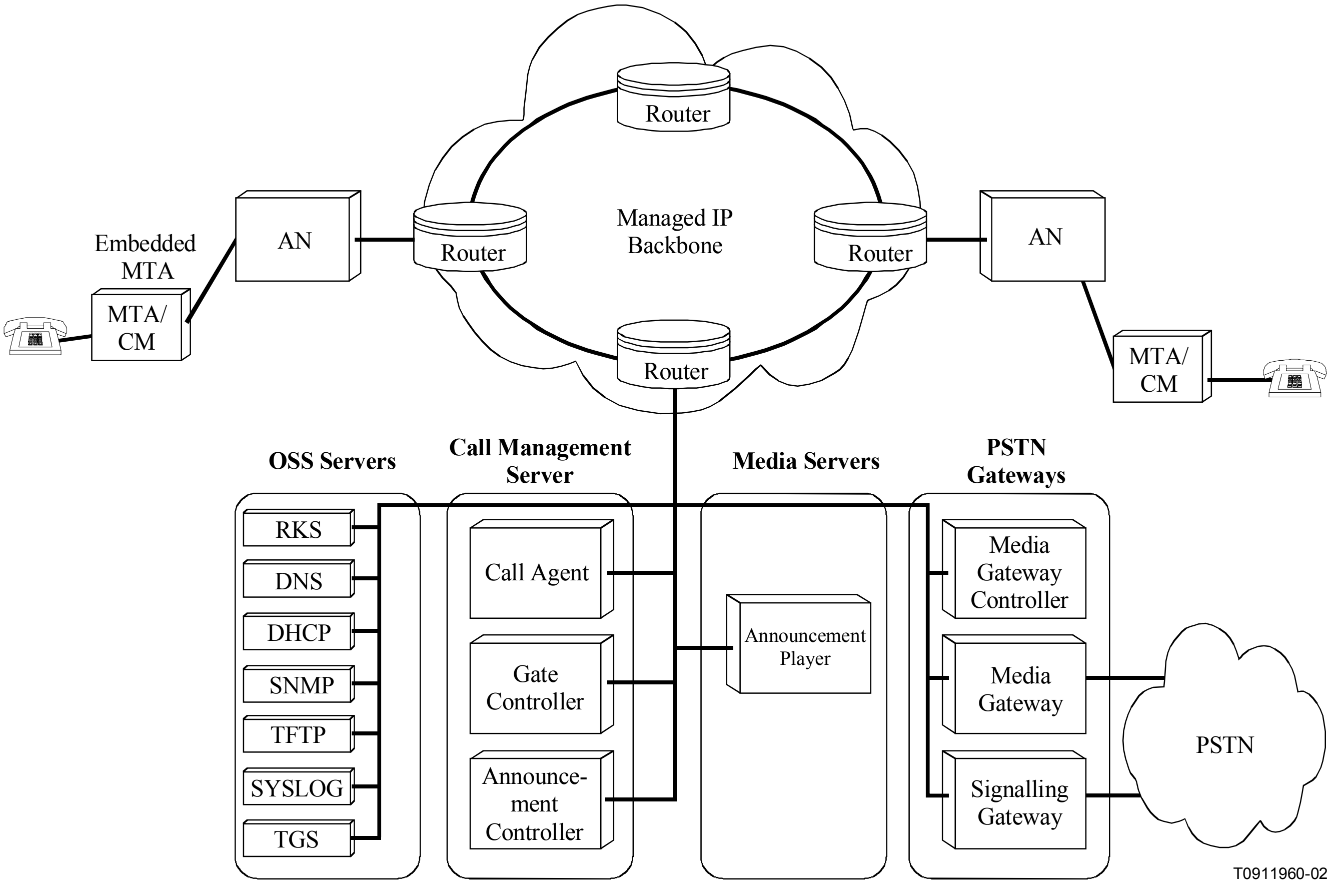


Figure 3/J.160 – IPCablecom component reference model

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 (J.112). IPCablecom MTAs are required to support the Network Call Signalling (NCS) protocol.

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.

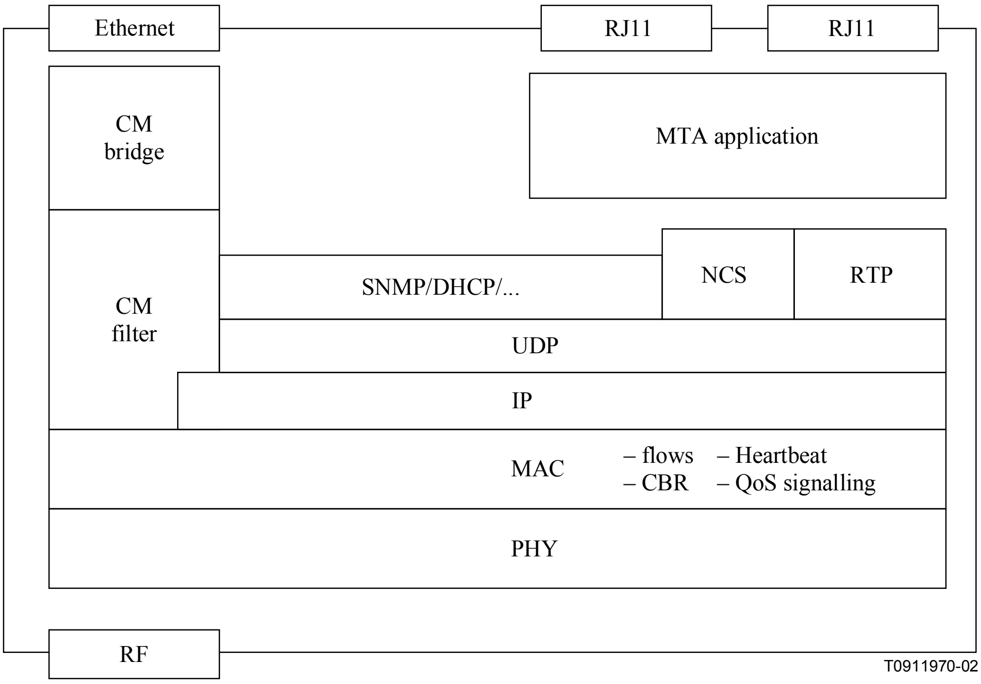


Figure 4/J.160 – E-MTA conceptual functional architecture

IPCablecom specifications only require support for embedded MTAs. Throughout this Recommendation, unless otherwise noted, the term "MTA" refers to an embedded MTA.

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 AN.
- Authentication, confidentiality and integrity of some messages between the MTA and other IPCablecom network elements.
- Mapping media streams to the MAC services of the J.112 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.
- One or more analogue and/or ISDN BRI interface(s).

Additional MTA functionality is defined in other IPCablecom specifications.

6.1.2 MTA identifiers

The following identifiers 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 J.112 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 AN, and the J.112 MAC and PHY access layers.

6.4 Access Node (AN)

The AN provides data connectivity and complimentary functionality to CMs over the HFC access network. It also provides connectivity to wide-area networks. The AN is located at the cable television system head-end or distribution hub.

The AN is responsible for the following functions:

- Providing the required QoS to the CM based upon policy configuration.
- 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 J.112 network using the assigned QoS.
- Forwarding upstream packets to the backbone network devices using the assigned QoS.
- Converting and classifying QoS Gate parameters into J.112 QoS parameters.
- Signalling and reserving any backbone QoS necessary to complete the service reservation.
- Recording usage of resources per call using IPCablecom Event Messages.

6.4.1 AN Gate

The AN Gate is a functional component of the AN that performs traffic classification and enforces QoS policy on media streams as directed by the Gate Controller (GC).

6.5 Call Management Server (CMS)

The Call Management Server provides call control and signalling-related services for the MTA, AN, 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 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.

– **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 specification.

The CMS may also contain the following logical components:

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

– **Announcement Controller** – The ANC is a logical signalling management component used to control network announcement servers. The ANC function is defined in detail in 6.8.

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;
- Zone-to-Zone call signalling (for further study) and QoS admission control.

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 inter-operate 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 C7 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, or MF signalling for MF 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 interfaces 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 and seizure state, on the endpoint and possibly 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 connectivity between the PSTN and the IPCablecom IP network. Each bearer is represented as an endpoint and the MGC instructs the MG to set up and control media connections to other endpoints on the IPCablecom network. The MGC also instructs the MG to detect and generate events and signals relevant to the call state known to the MGC.

6.6.2.1 Media Gateway functions

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

- Terminates and controls physical circuits in the form of bearer channels from the PSTN.
- Discriminates between media and Channel Associated In-band signalling information from the PSTN circuit.
- Detects events on endpoints and connections as requested by the MGC. This includes events needed to support in-band signalling, e.g. MF.
- Generates signals on endpoints and connections, e.g. continuity tests, alerting, etc., as instructed by the MGC. This includes signals needed to support in-band signalling.
- 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 a general request 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 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 C7. Facility-associated signalling in the form of MF is supported by the MG function directly.

6.6.3.1 C7 Signalling Gateway functions

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

- Terminates physical C7 signalling links from the PSTN (A, F links).
- Implements security features, to ensure that the Gateway security is consistent with IPCablecom and C7 network security requirements.
- Terminates Message Transfer Part (MTP) levels 1, 2 and 3.
- Implements MTP network management functions as required for any C7 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 C7 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 C7 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 C7 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. These topics will be covered in detail in a future IPCablecom OSS framework Recommendation.

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 TGS

For IPCablecom, the term "TGS" (Ticket Granting Server) is utilized for a Kerberos server. The Kerberos protocol with the public key PKINIT extension is used for key management on the MTA-CMS interface.

The TGS grants Kerberos tickets to the MTA. A ticket contains information used to set up authentication, privacy, integrity and access control for the call signalling between the MTA and the CMS. This ticket is issued in three different scenarios.

- During device provisioning, the MTA requests a ticket from the TGS. It is strongly recommended that the MTA save Kerberos tickets in persistent storage. In the case when the MTA reboots, if the saved ticket is still valid, then the MTA will not need to execute the PKINIT to request a new ticket from the TGS.
- In normal operation, each time a ticket expires, the MTA will request a new ticket during the grace period from the TGS. Note that in the case of power failure in the CMS, the MTA will no longer be associated with this CMS. When this CMS restarts it will request "wake up" information from the MTA. If the ticket the MTA currently holds is beyond the expiration time, often referred to as a stale ticket, the MTA will request a new ticket from the TGS. If the MTA is still holding a valid ticket, then it should send this ticket to the CMS without requesting a new one from the TGS.
- When the TGS is not available on the network and the MTA can not get a new ticket during the grace period, the MTA must hold on to the current, but stale ticket until a TGS is available to grant a new ticket. The request from the MTA during this condition will be specified in a future IPCablecom Security Recommendation.

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 ASCII 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 configuration files 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 a back office network element used to collect events such as traps and errors from an MTA.

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, AN, and MGC. The RKS also, at a minimum, is a short-term repository for IPCablecom Event Messages. The RKS may assemble the Event Messages into coherent sets or Call Detail Records (CDRs), which are then made available to other back office systems such as billing, fraud detection, and other systems.

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 specifications should be consulted for the complete protocol requirements.

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

7.1 Call signalling interfaces

Call signalling requires multiple interfaces within the IPCablecom architecture. These interfaces are identified in Figure 5. Each interface in the diagram is labelled, and further described in the subsequent Table 1.

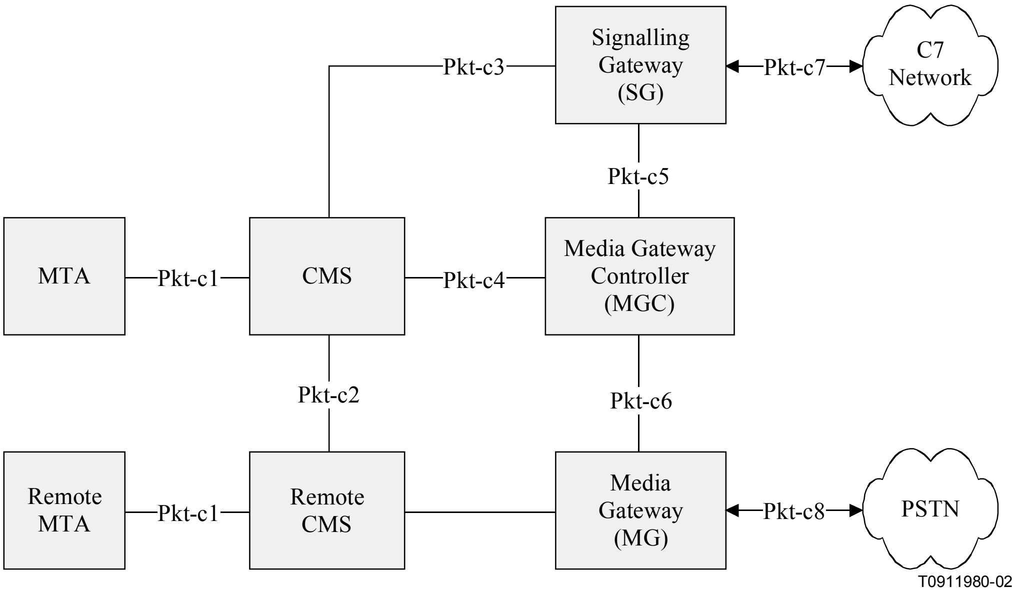


Figure 5/J.160 – Call signalling interfaces

Table 1/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 undefined.
Pkt-c3	CMS ⟷ SG	Call signalling messages exchanged between CMS and SG using the ISTP/TCAP protocol.
Pkt-c4	CMS ⟷ MGC	Call signalling messages exchanged between the CMS and MGC. The protocol for this interface is undefined.
Pkt-c5	SG ⟷ MGC	Call signalling messages exchanged between the MGC and SG using the ISTP/ISUP and ISTP/TCAP protocol.
Pkt-c6	MGC ⟷ MG	Interface for media control of the media gateway and possibly in-band signalling using the TGCP protocol, which is a profile of MGCP, similar to NCS.
Pkt-c7	SG ⟷ C7	The SG terminates physical C7 signalling links from the PSTN (A, F links). The following protocols are supported: • ISUP User Interface: Provides an C7 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 C7 network.
Pkt-c8	MG ⟷ PSTN	This interface defines bearer channel connectivity from the Media Gateway to the PSTN and supports the following call signalling protocols: • In-Band MF Signalling. A future version of IPCablecom may support ISDN PRI. NOTE – This function may be viewed as belonging in the Signalling Gateway function.

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 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 1 (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 protocol (Pkt-c6). This includes creation, modification and deletion of connections as well as in-band signalling information to and from the MG. 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 C7 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 C7 entities for trunk management and control. The ISTP provides the signalling interconnection service between the IPCablecom network call control elements (Call Management Server and Media Gateway Controller) and the PSTN C7 Signalling network through the C7 Signalling Gateway. The ISTP contains features for initialization; address mapping from the C7 domain to the IP domain; message delivery for C7 ISUP and TCAP; congestion management, fault management, maintenance operations; and redundant configuration support. The ISTP bridges the gap between basic IP transport mechanisms and application-level signalling. Although not a translation of the C7 MTP3 and SCCP protocols, the ISTP implements analogues to some of the MTP3 and SCCP functions in a fashion appropriate to distributed systems communicating over an IP network. These capabilities allow the IP network to interact with and receive all the services of the PSTN. As service capabilities evolve over time, these same signalling capabilities may be used to support PSTN access to the IPCablecom network's own routing and service databases.

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.

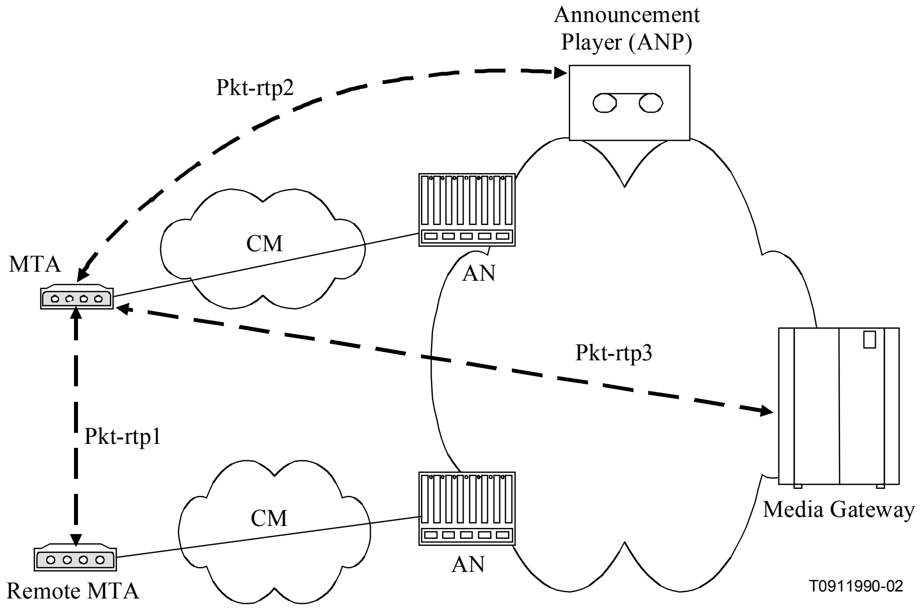


Figure 6/J.160 – RTP media stream flows in an IPCablecom network

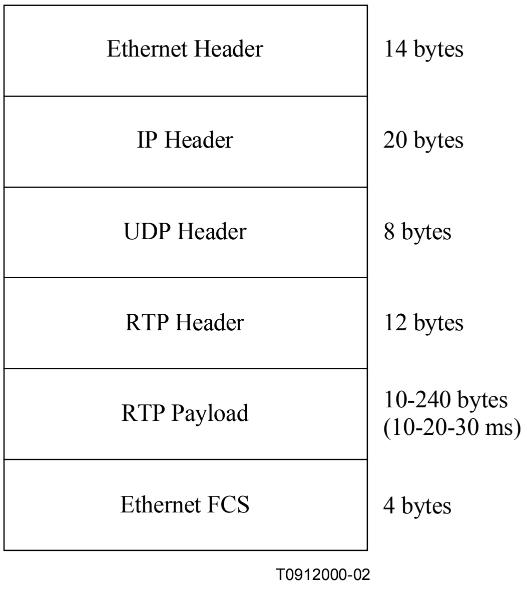
Pkt-rtp1: Media flow between MTAs. Includes, for example, encoded voice, video, and fax.

Pkt-rtp2: Media flow between the ANP and the MTA. Includes, for example, tones and announcements sent to the MTA by the Announcement Player.

Pkt-rtp3: Media flow between the MG and the MTA. Includes, for example, tones, announcements, and PSTN media flow sent to the MTA from the Media Gateway.

RTP encodes a single channel of multimedia information in a single direction. The standard calls for an 8-byte header with each packet. An 8-bit RTP "Payload Type" is defined to indicate which encoding algorithm is used. Most of the standard audio and video 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. The range 128 through 255 is reserved for private administration.

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



Ethernet Header	14 bytes
IP Header	20 bytes
UDP Header	8 bytes
RTP Header	12 bytes
RTP Payload	10-240 bytes (10-20-30 ms)
Ethernet FCS	4 bytes

T0912000-02

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 algorithm as defined by the Payload Type field.

RTP sessions are established dynamically by the endpoints involved, so there is no "well-known" UDP port number. The Session Description Protocol (SDP) was developed by the IETF to communicate the particular IP address and UDP port an RTP session is using.

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. J.112 addresses this issue with a Payload Header Suppression feature for abbreviating common headers.

7.3 MTA device provisioning

The scope of MTA device provisioning is to enable a MTA to register and provide subscriber services over the HFC network. Provisioning covers initialization, authentication, and registration functions required for MTA device provisioning. The provisioning specification also includes attribute definitions required in the MTA configuration file. (See Figure 8.)

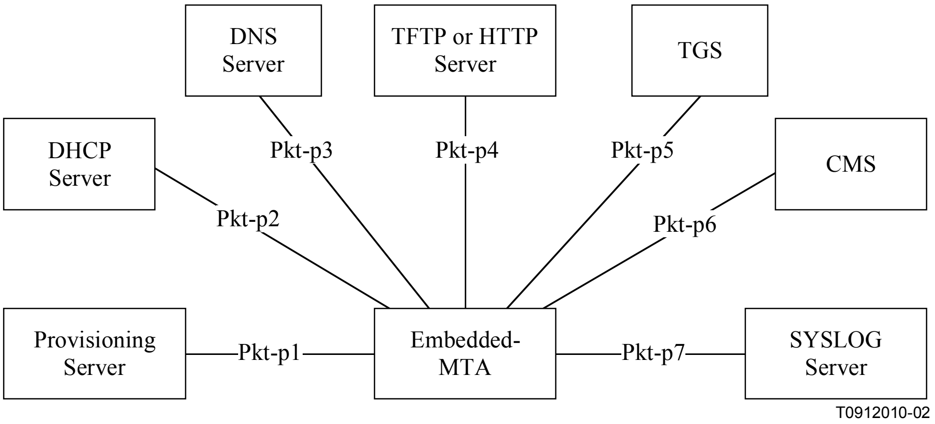


Figure 8/J.160 – IPCablecom provisioning interfaces

Table 2 describes the provisioning interfaces shown in Figure 8.

Table 2/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. If a DNS server is required during provisioning, then the address of this server is also included.
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 ⟷ TGS	MTA obtains a Kerberos ticket from the Ticket Granting Server 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	MTA sends notification that provisioning has completed along with a pass/fail status to the SYSLOG server via UDP.

7.4 SNMP Element Management Layer Interfaces

IPCablecom requires SNMPv3 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. IPCablecom MIBs will be defined in a future MTA MIB Recommendation.

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 framework can be found in the IPCablecom MIBs framework specification.

7.5 Event Messages interfaces

7.5.1 Event Message framework

An Event Message is a data record containing information about network usage and activities. A single Event Message may contain a complete set of data regarding usage or it may only contain part of the total usage information. When correlated by the Record Keeping System (RKS), information contained in multiple Event Messages provides a complete record of the service. 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 specification defines the structure of the Event Message data record and defines RADIUS as the transport protocol. Event Message data record is designed to be flexible and extensible in order to carry information about network usage for a wide variety of services. Additional transport protocols may be recommended in future releases of this Recommendation. Although the scope of the Recommendation is limited to defining Event Messages for basic residential voice capabilities, it is expected that this Recommendation will be expanded to support additional IPCablecom-based services. Figure 9 shows a representative Event Message architecture.

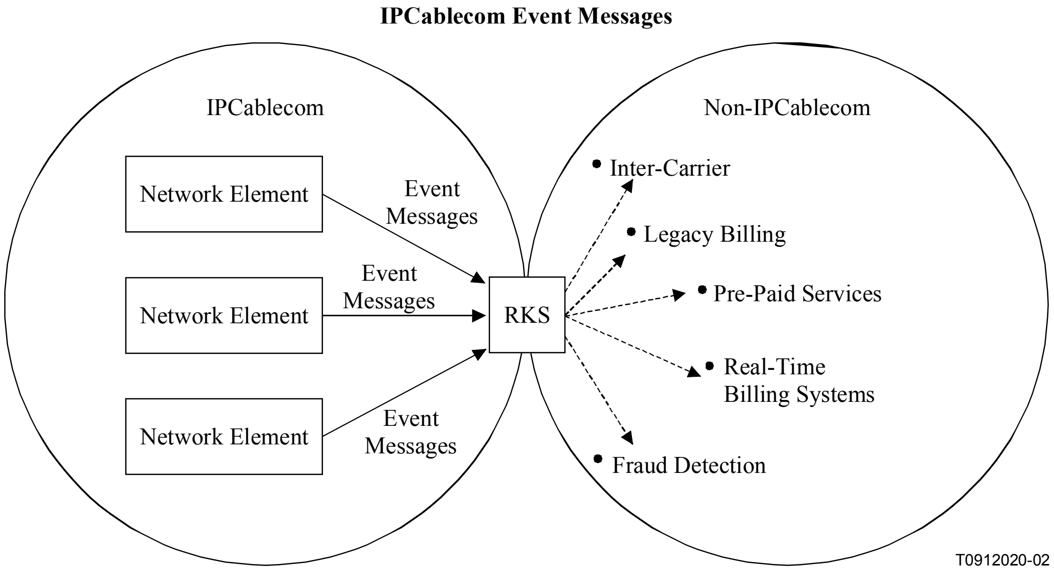
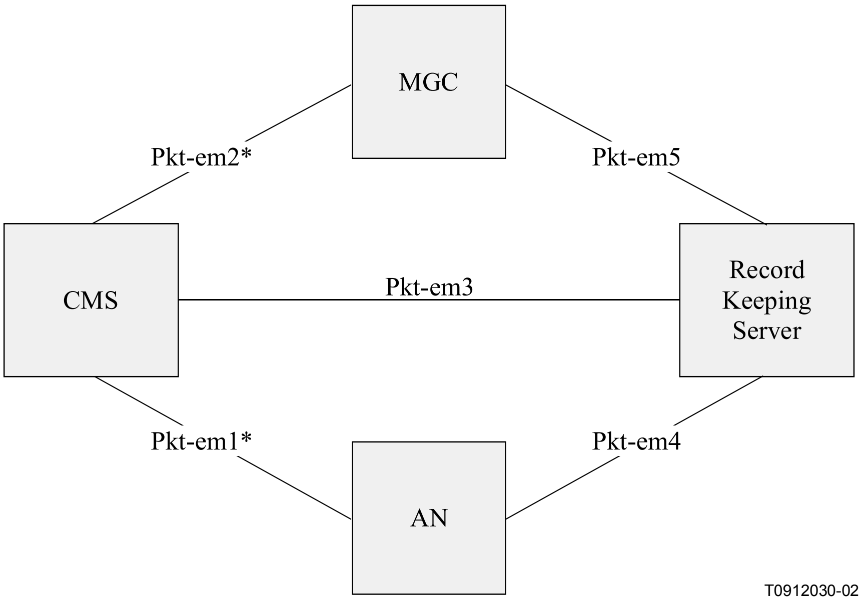


Figure 9/J.160 – Representative Event Messages architecture

Table 3 describes the Event Message interfaces shown in Figure 10.

Table 3/J.160 – Event Message interfaces

Interface	IPCablecom Functional Component	Description
Pkt-em1	CMS ⟷ AN	DQoS Gate-Set message carrying Billing Correlation ID and other data required for AN to send Event Messages to an RKS.
Pkt-em2	CMS ⟷ MGC	Vendor-proprietary interface carrying Billing Correlation ID and other data required billing data. Either the CMS or MGC may originate a call and therefore need to create the Billing Correlation ID and send this data to the other.
Pkt-em3	CMS ⟷ RKS	RADIUS protocol carrying IPCablecom Event Messages.
Pkt-em4	AN ⟷ RKS	RADIUS protocol carrying IPCablecom Event Messages.
Pkt-em5	MGC ⟷ RKS	RADIUS protocol carrying IPCablecom Event Messages.



NOTE – * indicates that the Billing Correlation ID and other billing data is carried on an existing signalling interface.

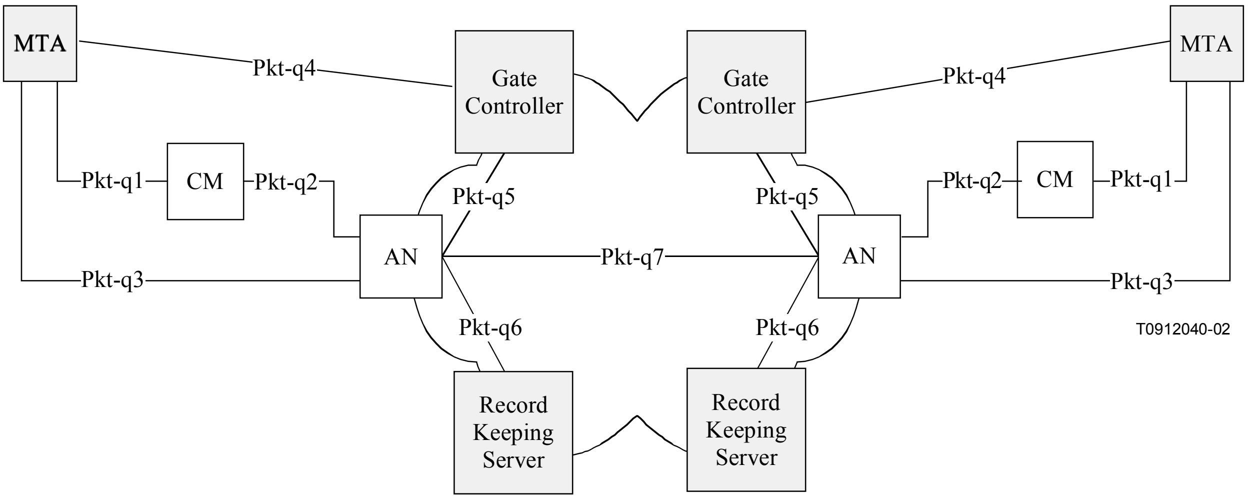
Figure 10/J.160 – Event Message interfaces

7.6 Quality of Service (QoS)

7.6.1 QoS Framework

Quality of Service signalling interfaces are defined between many of the components of the IPCablecom network. Signalling may be handled at the application layer (e.g. SDP parameters), network layer (e.g. RSVP), or the data-link layer (e.g. J.112 QoS).

From the perspective of the MTA and its access network, the IPCablecom QoS Framework is represented in Figure 11:



NOTE – Gate Controller is a function contained within a CMS node.

Figure 11/J.160 – IPCablecom QoS signalling interfaces

Table 4 briefly identifies each interface and how each interface is used in the Dynamic QoS Specification (DQoS). Two alternatives are shown for this specification: first, a general interface that is applicable to either embedded or standalone MTAs; and second, an optional interface that is available only to embedded MTAs.

Table 4/J.160 – QoS interfaces for standalone and embedded MTAs

Interface	IPCablecom functional components	DQoS embedded/ standalone MTA	D-QoS embedded MTA
Pkt-q1	MTA ⟷ CM	N/A	E-MTA, MAC Control Service Interface
Pkt-q2	CM ⟷ AN	J.112, AN-initiated	J.112, CM-initiated
Pkt-q3	MTA ⟷ AN	RSVP+[a)]	N/A
Pkt-q4	MTA ⟷ GC/CMS	NCS/DCS	NCS
Pkt-q5	GC ⟷ AN	Gate Management	Gate Management
Pkt-q6	AN ⟷ RKS	Billing	Billing
Pkt-q7	AN ⟷ AN	Gate Management	Gate Management
[a)] For IPCablecom, only the embedded MTA interfaces as defined in clause 7 of the Dynamic Quality of Service specification are required. The CMTS is not required to support RSVP across the MTA-CMTS interface as defined in DQoS clause 6.			

The function of each QoS interface is further described in Table 5.

Table 5/J.160 – QoS interfaces

Interface	IPCablecom functional components	Description
Pkt-q1	MTA ⟷ CM	This interface is only defined for the embedded MTA. The interface decomposes into three sub-interfaces: *Control*: used to manage J.112 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.

Interface	IPCablecom functional components	Description
Pkt-q2	CM ⟷ AN	This is the J.112 QoS interface (control, scheduling, and transport). It should be noted that, architecturally, control functions can be initiated from either the CM or the AN. However, the AN is the final policy arbiter and granter of admission into the J.112 access network. The following capabilities of the J.112 MAC are used within IPCablecom: • Multiple service flows, each with its own class of upstream traffic, both single and multiple voice connections per J.112 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). • J.112 packet header suppression for increased call density. • J.112 classification of voice flows to service flow. • J.112 synchronization of CODEC to AN 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.
Pkt-q3	MTA ⟷ AN	The interface is used for request of bandwidth and QoS resources related to the bandwidth. The interface runs on top of layer 4 protocols that bypass the CM. As a result of message exchanges between the MTA and AN, service flows are activated using AN-originated signalling on interface Pkt-q2. An enhanced version of RSVP is utilized for this signalling.
Pkt-q4	MTA ⟷ CMS/GC	Signalling interface between the MTA and CMS/GC. Many parameters are signalled across this interface such as media stream, IP addresses, and Codec selection, but it is possible for certain protocols to either derive QoS semantics from the signalling, or to extend the application layer signalling protocol to contain explicit QoS signalling parameters.
Pkt-q5	CMS/GC ⟷ AN	This interface is used to manage the dynamic Gates for media stream bearer channels. This interface enables the IPCablecom network to request and authorize QoS changes without requiring any layer two J.112 access network QoS control functions in MTA. When supporting standalone MTAs, no new client-side QoS signalling protocol needs to be designed. The GC/CMS takes responsibility for requesting policy, and the AN takes responsibility for access control and quickly setting up QoS on the J.112 access link.
Pkt-q6	AN ⟷ RKS	This interface is used by the AN to signal to the RKS all changes in call authorization and usage. This interface is defined in the Event Messages specification.

Interface	IPCablecom functional components	Description
Pkt-q7	AN ⟷ AN	This interface is used for coordination of resources between the AN of the local MTA and the AN of the remote MTA. The AN is responsible for the allocation and policing of local QoS resources.

7.6.2 Layer two vs. Layer three MTA QoS signalling

QoS signalling from the MTA can be performed either at layer two (J.112) or layer three (RSVP). Layer two signalling is accessible to CM and AN devices that exist at the RF boundary of the J.112 access network. Layer three signalling is required for devices that are one or more hops removed from the RF boundary of the J.112 access network.

If layer two QoS signalling is initiated by the MTA, the MTA must be an embedded MTA. The MTA utilizes the implicit interface for controlling the J.112 MAC service flows as suggested by ITU-T Rec. J.112.

Layer three QoS signalling is initiated by the MTA; the MTA may be either an embedded MTA or standalone MTA. Enhanced RSVP is used for this signalling and is intercepted by the AN. The AN utilizes layer two QoS signalling to communicate QoS signalling changes to the CM.

7.6.3 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 function within the AN that performs traffic classification and enforces QoS policy on media streams is called a Gate. The Gate Controller element manages Gates for IPCablecom media streams. The following key information is included in signalling between the GC and the AN:

Maximum Allowed QoS Envelope – The maximum allowed QoS envelope enumerates the maximum QoS resource (e.g. "2 grants of 160 bytes per 10 ms") the MTA is allowed to admit 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 AN can police the data stream to ensure that the data stream is destined to and originated from the parties that are authorized.

Billing Information – The GC/CMS creates opaque billing information that the AN does not have to decode. The information might be as simple as billing identity or the nature of the call. The AN forwards this billing information to the RKS as the call is activated or terminated.

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.

AN – Using information supplied by the GC/CMS, the AN performs admission control on the QoS requests and at the same time polices the data stream to make sure that the data stream is originated from and sent to authorized media stream parties. The AN interacts with CM, RKS, MTA, and Terminating AN. The responsibilities of AN with respect to each of these elements are:

- **AN to CM** – The AN is responsible for setting up and tearing down service flows in such a way that the service level agreement it made with the MTA is met. Inasmuch as the AN does not trust the CM, it polices the traffic from the CM such that the CM works in the way AN requested.

- **AN to Record Keeping Server** – The AN updates the Record Keeping Server (RKS) each time there is a change in the QoS Service Level Agreement between AN and MTA. It uses the Billing Information that is given by GC/CMS to identify each authorized QoS link. The AN puts timing information in the message it sends and also buffers the messages if the connection to RKS is severed.
- **AN to MTA** – The MTA makes dynamic requests for modification of QoS traffic parameters. When the AN receives the request, it makes an authorization check to find out whether the requested characteristics are within the authorized QoS envelope and also whether the media stream endpoints are authorized. Then, it provisions the QoS attributes for the RFI link on the AN and activates the appropriate QoS traffic parameters via signalling with the CM. When all the provisioning and authorization checks succeed, the AN sends a success message to the GC/CMS indicating that MTA and AN are engaged in a Service Level Agreement.
- **AN to terminating AN** – The AN sends messages to the terminating end AN (or other terminating access networking device) to ensure that the committed bandwidth on both sides is the same. If the committed bandwidth is not the same, then both sides close the connection.

Cable Modem (CM) – Even though the CM is an untrusted entity, the CM is responsible for the correct operation of the QoS link between itself and the AN. The AN makes sure that the CM cannot abuse the RFI link, but it is the responsibility of the CM to utilize the RFI link to provide services that are defined by ITU-T Rec. J.112.

Record Keeping Server (RKS) – The RKS acts as a database and stores each event as sent by the AN. The RKS stores the messages by attaching received time and network element information. The RKS has to have sufficient interface and/or processing power to allow additional processing to be done.

MTA – The MTA is the entity to which the Service Level Agreement is provided by the access network. The MTA is responsible for the proper use of the QoS link. If it exceeds the traffic authorized by the SLA, then the MTA will not receive the QoS characteristics that it requested. The MTA uses two-stage QoS bandwidth allocation – while the call origination is proceeding the QoS resources are admitted; then, when the call is answered, the resources are activated.

7.7 Announcement Services

Announcements are typically needed for calls that do not complete. Additionally, they may be used to provide enhanced information services to the caller. The signalling interfaces to support IPCablecom Announcement Services are shown in Figure 12 and are summarized in Table 6.

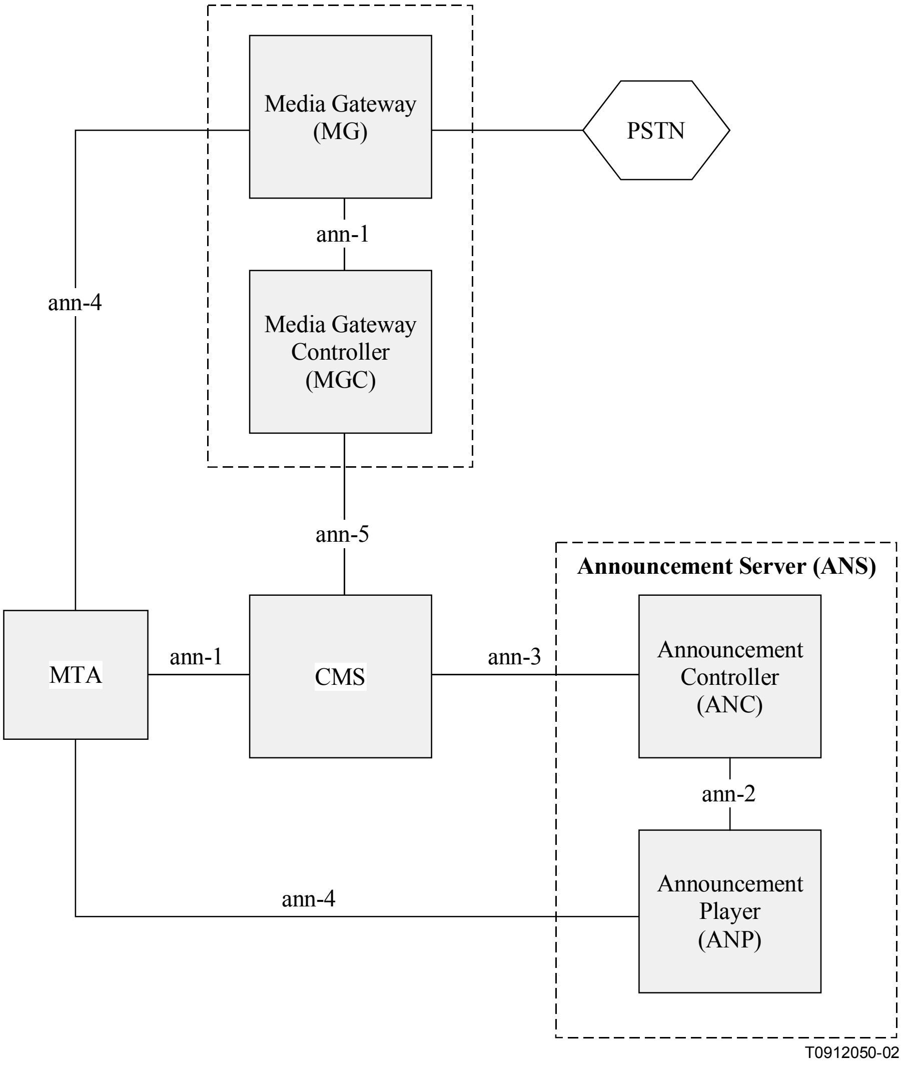

Media Gateway (MG)
PSTN
ann-1
ann-4
Media Gateway Controller (MGC)
ann-5
Announcement Server (ANS)
MTA
ann-1
CMS
ann-3
Announcement Controller (ANC)
ann-2
ann-4
Announcement Player (ANP)
T0912050-02

Figure 12/J.160 – Announcement Services components and interfaces

Table 6/J.160 – Announcement interfaces

Interface	IPCablecom functional components	Protocol
Pkt-ann1	MTA ⟷ CMS MGC ⟷ MG	The CMS to MTA interface provides a mechanism for the CMS to signal the MTA to play locally stored announcements. Storing announcements in the MTA allows for providing informative progress tones to the end user independently of the network state (e.g. congestion). An NCS-based announcement package has been defined that can be used for both the CMS-MTA and MGC-MG interfaces. Simple, fixed-content announcements (e.g. all-lines-busy) may also be stored at the Media Gateway to provide announcements to PSTN users. The MGC to MG interface provides a mechanism for the MG to play fixed-content announcements to PSTN end-users involved in off-net to on-net calls.
Pkt-ann2	ANC ⟷ ANP	The signalling protocol for the ANC to ANP interface is NCS with an announcement package. When the CMS identifies a need for an ANS-based announcement, it sends a request to the ANC over interface Pkt-ann-3. Upon receiving a request from the CMS, the ANC opens a session with the Announcement Player using the NCS package.
Pkt-ann3	CMS ⟷ ANC	The protocol for the Pkt-ann-3 interface is undefined for IPCablecom.
Pkt-ann4	ANP ⟷ MTA	Defines the media stream format (RTP) for delivery of the announcement from the Announcement Player to the MTA using the RTP protocol.
Pkt-ann5	CMS ⟷ MGC	The Pkt-ann-5 protocol interface is undefined for IPCablecom.

7.7.1 ANS Physical vs. Logical configuration

The ANC and ANP are logical components that may reside in the same physical entities. When logical components reside in the same physical entity, interfaces between these components become optional. In addition, standalone components using the Pkt-ann-2 and Pkt-ann-3 interfaces may be shared by many network entities.

7.8 Security

7.8.1 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, e.g. authentication, integrity, confidentiality.

For example, the media stream path may traverse a large number of potentially unknown Internet service and backbone service providers' wires. As a result, the media stream may be vulnerable to malicious eavesdropping, resulting in a loss of communications privacy. IPCablecom core security services include a mechanism for providing end-to-end encryption of RTP media streams, thus substantially reducing the threat to privacy.

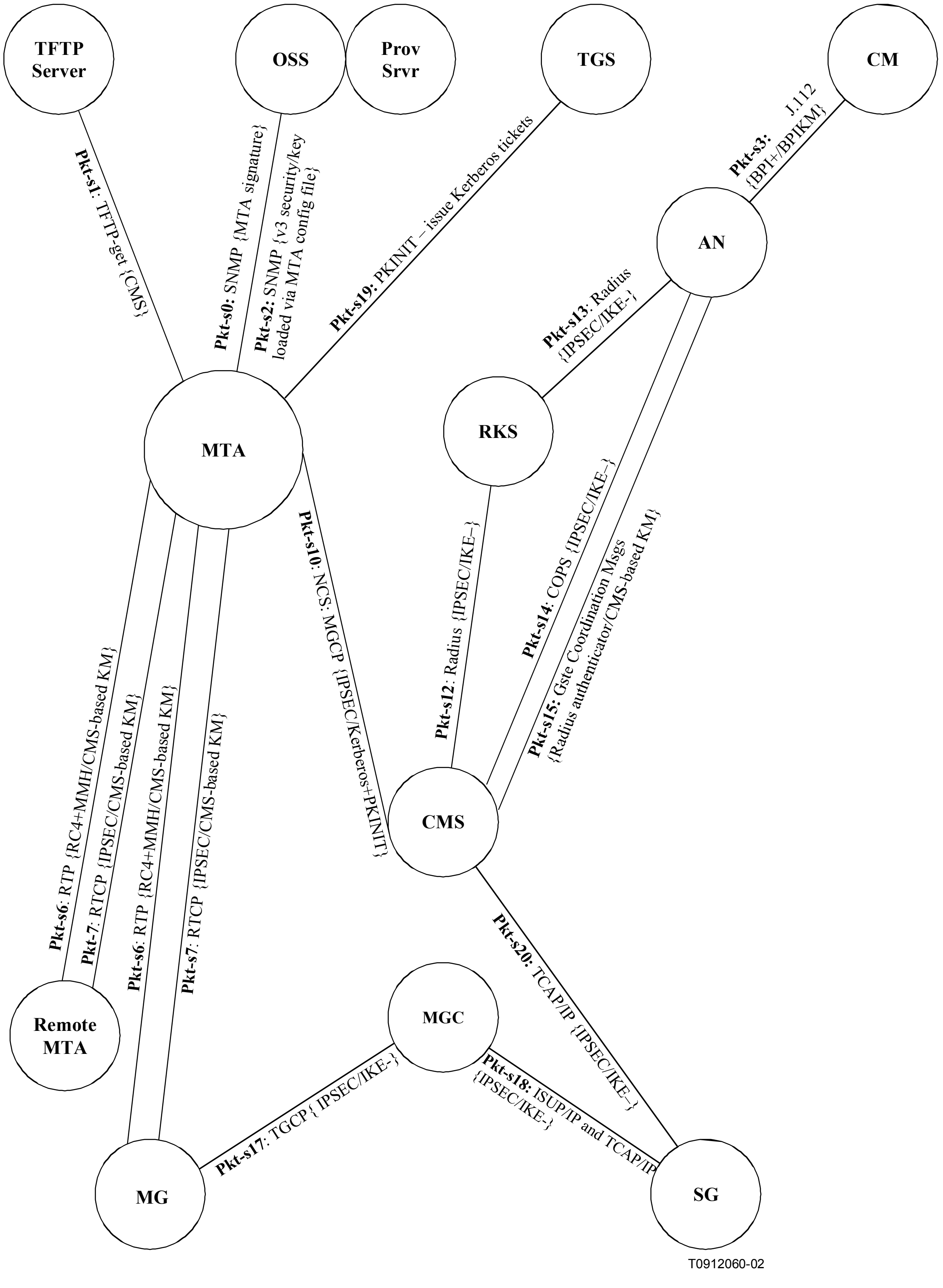
The security services available through IPCablecom's core service layer are authentication, access control, integrity, confidentiality and non-repudiation. An IPCablecom protocol interface may employ zero, one or more of these services to address its particular security requirements.

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, and SNMPv3 security) and the supporting key management protocol (e.g. IKE, PKINIT/Kerberos).

Figure 13 provides a summary of all the IPCablecom security interfaces.


TFTP Server
OSS
Prov Srvr
TGS
CM
AN
RKS
MTA
CMS
MGC
Remote MTA
MG
SG
Pkt-s1: TFTP-get {CMS}
Pkt-s0: SNMP {MTA signature}
Pkt-s2: SNMP {v3 security/key loaded via MTA config file}
Pkt-s19: PKINIT – issue Kerberos tickets
Pkt-s3: J.112 {BPI+/BPIKM}
Pkt-s13: Radius {IPSEC/IKE-}
Pkt-s12: Radius {IPSEC/IKE–}
Pkt-s14: COPS {IPSEC/IKE–}
Pkt-s15: Gste Coordination Msgs {Radius authenticator/CMS-based KM}
Pkt-s10: NCS: MGCP {IPSEC/Kerberos+PKINIT}
Pkt-s6: RTP {RC4+MMH/CMS-based KM}
Pkt-7: RTCP {IPSEC/CMS-based KM}
Pkt-s6: RTP {RC4+MMH/CMS-based KM}
Pkt-s7: RTCP {IPSEC/CMS-based KM}
Pkt-s20: TCAP/IP {IPSEC/IKE–}
Pkt-s18: ISUP/IP and TCAP/IP {IPSEC/IKE-}
Pkt-s17: TGCP{ IPSEC/IKE-}
T0912060-02

IKE –	IKE with pre-shared keys
IKE+	IKE requires public key certificates
CMS-based KM	Keys randomly generated and distributed by CMS

Figure 13/J.160 – IPCablecom security interfaces

In Figure 13, each interface is labelled as:

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

If the key management protocol is missing, it means that it is not needed for that interface. IPCablecom interfaces that do not require security are not shown in Figure 13.

Table 7 describes each of the interfaces shown in the Figure 7.

Table 7/J.160 – Security interfaces

Interface	IPCablecom functional components	Description
Pkt-s0	MTA ⟷ Provisioning app	SNMPv3 INFORM from the MTA to the SNMP Manager, followed by optional SNMP GET(s) by the SNMP Manager are used to query MTA device capabilities. This occurs at the time where SNMPv3 keys may not be available, and security is provided with an RSA signature, formatted according to CMS (Cryptographic Message Syntax).
Pkt-s1	MTA ⟷ TFTP or HTTP server	MTA Configuration file download. The MTA downloads a configuration file (with TFTP-get) that is signed by the TFTP server and sealed with the MTA public key, with a CMS (Cryptographic Message Syntax) wrapper. This flow occurs right after an SNMPv3 INFORM followed by an optional SNMP GET(s), see flow Pkt-s0.
Pkt-s2	MTA ⟷ Provisioning app	Standard SNMPv3 security. The SNMPv3 keys are downloaded with the MTA configuration file, using interface Pkt-s1.
Pkt-s3	CM ⟷ AN	BPI+ privacy layer on the HFC link. Both security and key management are defined by ITU-T Rec. J.112.
Pkt-s6	MTA ⟷ MTA	End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with RC4, without any additional security layers. An MMH-based MAC (Message Authentication Code) optionally provides message integrity. Keys are distributed by the CMS to the two endpoints.
Pkt-s7	MTA ⟷ MTA	RTCP control protocol for RTP, defined above. Message integrity and encryption provided with IPsec. Key management is same as for RTP; keys are distributed by CMS.
Pkt-s10	MTA ⟷ CMS	MTA-CMS signalling for NCS. Message integrity and privacy via IPsec. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
Pkt-s12	CMS ⟷ RKS	Radius billing events sent by the CMS to the RKS. Radius authentication keys are hardcoded to 0. Instead, IPsec is used for message integrity as well as privacy. Key management is IKE–.
Pkt-s13	AN ⟷ RKS	Radius events sent by the AN to the RKS. Radius authentication keys are hardcoded to 0. Instead, IPsec is used for message integrity, as well as privacy. Key management is IKE–.
Pkt-s14	CMS ⟷ AN	COPS protocol between the GC and the AN, used to download QoS authorization to the AN. Message integrity and privacy provided with IPsec. Key management is IKE–.

Interface	IPCablecom functional components	Description
Pkt-s15	CMS ⟷ AN	Gate Coordination messages for DQoS. Message integrity is provided with an application-layer (Radius) authenticator. Keys are distributed by local CMS over COPS.
Pkt-s16	N/A	N/A
Pkt-s17	MGC ⟷ MG	IPCablecom interface to the PSTN Media Gateway. IPsec is used for both message integrity and privacy. Key management is IKE–.
Pkt-s18	MGC ⟷ SG	IPCablecom interface to the PSTN Signalling Gateway. IPsec is used for both message integrity and privacy. Key management is IKE–.
Pkt-s19	MTA ⟷ TGS	Kerberos/PKINIT key management protocol, where the TGS issues CMS tickets to the MTAs.
Pkt-s20	CMS ⟷ SG	CMS queries the PSTN Gateway for LNP (Local Number Portability) and other telephony services. IPsec is used for both message integrity and privacy. Key management is IKE–.

7.8.2 Device provisioning security

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

7.8.2.1 Subscriber enrolment

The subscriber enrolment process establishes a permanent subscriber billing account that uniquely identifies the MTA to the CMS via the MTA's serial number or 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 out of scope for IPCablecom and may be different for each service provider.

7.8.2.2 Device provisioning

The MTA device verifies the authenticity of the configuration file it downloads from the boot server. Privacy of the configuration data is also provided. The configuration data will be "signed and sealed" by packaging it into a PKCS #7 sealed object.

7.8.2.3 Dynamic provisioning

SNMPv3 security will be used for dynamically provisioning voice communications capabilities on an embedded MTA.

7.8.2.4 Device authorization

Device authorization is 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.

7.8.2.5 Signalling security

All signalling traffic, which includes QoS signalling, call signalling, and signalling with the PSTN Gateway Interface, will be secured via IPsec. IPsec security association management will be done through the use of two key management protocols: Kerberos/PKINIT and IKE. Kerberos/PKINIT will be used to exchange keys between MTA clients and their CMS server; IKE will be used to manage all other signalling IPsec SAs.

7.8.2.6 Media stream security

Each media RTP packet is encrypted for privacy. The MTAs have an ability to negotiate a particular encryption algorithm, although the only one that is currently specified is RC4. Encryption is applied to the packet's payload but not to its header.

Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. The MAC computation spans the packet's unencrypted header and encrypted payload.

Keys for the encryption and MAC calculation are derived from the End-End secret, which is exchanged between sending and receiving MTA as part of the call signalling. Thus, the key exchanges for media stream security are secured themselves by the call signalling security.

7.8.2.7 OSS and billing system security

The SNMP agents in IPCablecom devices implement SNMPv3. The SNMPv3 User Security Model [RFC 2274] provides authentication and privacy services for SNMP traffic. SNMPv3 view-based access control [RFC 2275] may be used for access control to MIB objects.

The IKE 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. When the network IPsec Security Associations are established, these keys must be created between each RKS (primary, secondary, etc.) and every CMS and AN. The key exchange between the MGC and RKS may exist and is left to vendor implementation in IPCablecom Phase 1. The Event Messages are sent from the CMS and AN 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).

It is recommended that IPCablecom networks maintain a timeserver that is accurate to within a specified interval of Universal Time Coordinated (UTC). It is recommended that the server be able to exchange time information with other network equipment such that the receiving equipment is able to be synchronized to the time server clock at the completion of the synchronization protocol exchange.

Network Time Protocol (NTP) is the recommended protocol for IPCablecom time synchronization.

All systems that generate billing event messages must synchronize their clocks to a network clock source. Synchronization should be done to ensure that the reporting device's own clock remains within ±100 milliseconds of the last synchronization value.

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 are generally exhibited as overrun or underrun of the playout buffers.

In order to minimize the occurrence of these conditions, all ANs should lock their downstream transmission rate to a clock derived from a source that reflects a Stratum-3 clock. Embedded 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. Non-embedded MTAs should use the average packet arrival interval[1] as the basis for determining their packetization and playout clock.

8.3 IP addressing

An embedded MTA is a multi-function entity with one function required for CM administration and the second function being the MTA function itself. All IP addresses in an IPCablecom network are IPV4.

All IPCablecom embedded 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.

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

- An embedded MTA containing a dual IP address can assign a private IP address for the CM host function, in the case where NAT translation 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. Essentially the routing backbone must be configured such that different routing paths are followed for each of the two destination IP addresses.
- The IPCablecom operator can simplify network side administration and management functions using separate IP addresses. For example, policy filters can be instantiated that block or permit traffic from the MTA component of the node. 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 issue exists regarding the dynamic IP addresses assignment for MTAs. The NCS model specified in IPCablecom is based on a Call Management Server mapping a subscriber's service to an endpoint identifier and an IP address. Therefore, call-processing operations would be affected if the MTA's IP address changed during an active call. However, there are some recommendations that network operators and MTA vendors can employ to eliminate this situation.

1) When configuring DHCP options for an MTA, the network operator should configure the IP Address Lease Time (Option Code 51) to specify a very long lease time. This option is detailed in "Dynamic Host Configuration Protocol" [RFC 2131] and "DHCP Options and BOOTP Vendor Extensions" [RFC 2132]. Per paragraph 3.3 of RFC 2131, a lease time setting of "0xffffffff" represents an infinite lease. Use of long lease times will minimize the possibility that an active MTA would be unable to renew its assigned IP address lease.

[1] I.e., the interval from arrival of the first bit of packet N to the arrival of the first bit of packet N+1, ignoring intervals where a packet does not arrive within 5 ms of the expected periodicity.

2) Network operators should also configure an MTA's DHCP Timer T1 and T2 values (Option Codes 58 and 59, respectively) to be no more than the default values specified in paragraph 4.4.5 of RFC 2131. Configuring an MTA to begin its IP address lease time renewal process at no more than 50% of the assigned lease time, combined with the use of very long lease time values, will further ensure that an MTA will be able to renew its IP address lease.

3) MTA vendors should implement mechanisms to prevent an MTA from entering the RENEWING state (as specified in RFC 2131) while call processing is active. It is left to vendor implementation to determine exactly how this capability might best be implemented in their product.

8.5 FQDN assignment

The following are potential operational issues that are expected to be resolved through vendor-specific implementations:

It is assumed that the OSS back office will generate the appropriate FQDNs for all IPCablecom devices, and pass this data to the appropriate IPCablecom devices and other network elements. These interfaces are not defined in IPCablecom (phase 1).

An operational issue exists regarding synchronization of databases within the provisioning domain. Specifically the DHCP database, and the DNS table's require concurrent updates when a subscriber record changes (this includes creation). RFC 2131 provides a mechanism by which a host (a DHCP client) could acquire certain configuration information, specifically its IP address(es). However, DHCP does not provide any mechanisms to update the DNS Resource Records that contain the information about mapping between the host's FQDN and its IP address(es) (i.e. the Address and Pointer Resource Records). Thus, the information maintained by DNS for a DHCP client may be incorrect – a host (the client) could acquire its address by using DHCP, but the Address Resource Record for the host's FQDN wouldn't reflect the address that the host acquired, and the Pointer Resource Record for the acquired address wouldn't reflect the host's FQDN.

The problem has two main issues: first, how do you update the DNS system when a new IP address is dispensed, and second, how long do you make timeout values for RRs. Both of these issues are vendor implementation issues and therefore lie outside of the scope of IPCablecom specifications. However, some recommendations on 'best practices' are outlined in RFC 2131.

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 J.112 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 J.112 flow classification service. This service classifies packets into specific flows based upon packet fields such as IP source and destination addresses and UDP port number parameters. In the upstream such classified packets are transported via an appropriate constant bit rate service (for current codecs) as dynamically scheduled by the AN. In the downstream the packets are transported via an appropriate high priority queuing and scheduling mechanism. DQoS (between CMS and AN) and J.112 (between AN and CM) signalling mechanisms are used to dynamically setup 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 AN/CM queuing systems and also within Diff-serv managed QoS backbones (which may not contain flow classification mechanisms) in order to provide high priority QoS treatment of such packets. It should be noted that while no definition is provided as to how QoS is managed in the Managed IP backbone in the current architecture, it is expected that the mechanisms defined for IPCablecom QoS will be usable within such a managed backbone.

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. It should be noted that, from a network traffic-engineering point of view, it has not yet been determined whether high priority treatment of signalling packets is required. 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 J.112 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 AN. 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.

Marking of packets for both the media stream and the signalling stream (NCS) is performed by the MTA and the CMS. The marking is performed at the IP layer using a field that has alternately been called the TOS byte or the Diff-serv Code Point (DSCP). The TOS byte was the original definition of the byte while DSCP is the new definition of the byte as used by the IETF Diff-serv architecture. Because two formats for this byte exist, the configuration of the values should be done in a format and type independent way (in the MIBs for the MTA and Call Agent).

Management Information Bases (MIBs) are defined in IPCablecom for assigning the provisioned and default values for media stream priority marking and signalling stream priority marking (e.g. a value of "3" for signalling and a value of "5" for media). It should be noted that in NCS the signalled SDP parameters may contain overrides for the configured media stream priority marking value on a connection by connection basis. No mechanism currently exists for dynamically overriding the provisioned priority marking value of the signalling stream on a call by call basis.

8.7 Fax support

IPCablecom supports real-time fax transmission. Fax is "best" accomplished using the G.711 standard for audio encoding/decoding. If a call is established using a compressed codec, the embedded MTA will have to be instructed to look for fax tones. If fax tones are detected, the CMS will have to be notified and the MTA will be instructed to switch to using G.711. Note that this places a requirement on the embedded device to monitor the media stream and detect fax tones.

Support for switching over to fax from a voice call is required; however, switching back to voice from fax is not required (i.e. monitoring the fax media stream for an ending signal and then switching back to a low bandwidth codec).

Local termination of fax and translating the fax stream to an IP fax relay data stream is not required in this version of the architecture.

8.8 Analogue modem support

Analogue modems are supported in a similar fashion to fax – a 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. Note that this places a requirement on the embedded device to monitor the voice stream and to detect analogue modem tones.

Switching over to G.711 to support analogue modem signalling from a voice call will be supported; however, switching back to voice from modem signalling will not be required to be supported (i.e., monitoring the modem media stream for an ending signal and then switching back to a low-bandwidth codec).

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

APPENDIX I

Bibliography

- IETF RFC 1899 (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 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 2275 (1998), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* (Obsoleted by RFC 2575).
- IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).* (Obsoletes RFC 2275).

APPENDIX II

Glossary of terms

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

II.1 Definitions

II.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.

II.1.2 access node: As used in this Recommendation, an Access Node is a layer two termination device that terminates the network end of the J.112 connection. It is technology specific. In J.112 Annex A it is called the INA while in Annex B it is the CMTS.

II.1.3 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.

II.1.4 authentication: The process of verifying the claimed identity of an entity to another entity.

II.1.5 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.

II.1.6 authorization: The act of giving access to a service or device if one has the permission to have the access.

II.1.7 cable modem: A cable modem is a layer two termination device that terminates the customer end of the J.112 connection.

II.1.8 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.

II.1.9 cipher: An algorithm that transforms data between plaintext and ciphertext.

II.1.10 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.

II.1.11 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".

II.1.12 downstream: The direction from the head-end toward the subscriber location.

II.1.13 encryption: A method used to translate information in plaintext into ciphertext.

II.1.14 endpoint: A Terminal, Gateway or MCU.

II.1.15 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.

II.1.16 event message attribute: An Event Message Attribute is a predefined data element described by an attribute definition and attribute type.

II.1.17 gateway: Devices bridging between the IPCablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signalling Gateway which sends and receives circuit switched network signalling to the edge of the IPCablecom network.

II.1.18 header: Protocol control information located at the beginning of a protocol data unit.

II.1.19 integrity: A way to ensure that information is not modified except by those who are authorized to do so.

II.1.20 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.

II.1.21 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.

II.1.22 J.112 flow: A unidirectional or bidirectional flow of data packets that is subject to MAC-layer signalling and QoS assignment compliant to ITU-T Rec. J.112.

II.1.23 Kerberos: A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.

II.1.24 key: A mathematical value input into the selected cryptographic algorithm.

II.1.25 key exchange: The swapping of public keys between entities to be used to encrypt communication between the entities.

II.1.26 key management: The process of distributing shared symmetric keys needed to run a security protocol.

II.1.27 MIB: Management Information Base The specification of information in a manner that allows standard access through a network management protocol.

II.1.28 non-repudiation: The ability to prevent a sender from denying later that he or she sent a message or performed an action.

II.1.29 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".

II.1.30 private key: The key used in public key cryptography that belongs to an individual entity and must be kept secret.

II.1.31 proxy: A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.

II.1.32 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.

II.1.33 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".

II.1.34 public key cryptography: A procedure that uses a pair of keys, a public key and a private key for encryption and decryption; also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key which can decrypt messages sent encrypted by the user's public key.

II.1.35 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.

II.1.36 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.

II.1.37 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.

II.1.38 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 C7 SG function translates variants ISUP and TCAP in a C7-Internet Gateway to a common version of ISUP and TCAP.

II.1.39 X.509 certificate: A public key certificate specification developed as part of the ITU-T Rec. X.500 standards directory.

II.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

C7	Signalling System No. 7
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
F ID	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	Operational 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 Parameters Index
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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
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	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
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 and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

21842

Printed in Switzerland
Geneva, 2002