

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.360

(11/2006)

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

IPCablecom

IPCablecom2 architecture framework

ITU-T Recommendation J.360



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T Recommendation J.360

IPCablecom2 architecture framework

Summary

ITU-T Recommendation J.360 provides the architectural framework and technical overview for the expansion of IPCablecom into multimedia.

Source

ITU-T Recommendation J.360 was approved on 29 November 2006 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2007

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope and overview	1
1.1	Scope	1
1.2	IPCablecom2 overview	1
2	References.....	2
2.1	Normative references.....	2
2.2	Informative references.....	2
3	Terms and definitions	3
4	Abbreviations and acronyms	3
5	IPCablecom2	5
5.1	Relationship with the 3GPP IMS	5
5.2	Overview	6
5.3	IPCablecom releases and organization.....	10
5.4	IPCablecom2 design considerations.....	13
6	IPCablecom functional components.....	16
6.1	Local network.....	16
6.2	Access network.....	16
6.3	Edge	16
6.4	Core	17
6.5	IPCablecom multimedia	19
6.6	Application	19
6.7	Interconnect	20
6.8	Operational support systems.....	20
7	Protocol interfaces and reference points.....	22
7.1	Signalling and service control	22
7.2	Subscriber data	23
7.3	Quality of service	24
7.4	Network address translation (NAT) and firewall traversal	26
7.5	Media coding and transport	28
7.6	Provisioning, activation, configuration and management	28
7.7	Network accounting and usage.....	30
7.8	Security.....	32
7.9	Lawful intercept.....	34
7.10	Control point discovery	36
	Appendix I – SIP signalling overview	37
I.1	Introduction and purpose.....	37
I.2	References	38
I.3	Terms and definitions	39
I.4	Abbreviations and acronyms	40

	Page
I.5 IPCablecom2 SIP signalling.....	40
I.6 IPCablecom2 IMS requirements	46
Appendix II – Quality of service architecture technical overview	66
II.1 Introduction	66
II.2 References	66
II.3 Terms and definitions	67
II.4 Abbreviations and acronyms	67
II.5 QoS requirements and scope	67
II.6 QoS architecture framework.....	68
II.7 Architecture description	71
II.8 Example procedures	74
Appendix III – IPCablecom2 security overview.....	77
III.1 Introduction	77
III.2 References	77
III.3 Terms and definitions	78
III.4 Abbreviations and acronyms	78
III.5 IPCablecom2 security.....	78
III.6 IPCablecom security requirements.....	89
Appendix IV – IPCablecom2 home subscriber server (HSS) overview	105
Appendix V – IPCablecom2 NAT and firewall traversal overview	105
V.1 Introduction	105
V.2 References	105
V.3 Terms and definitions	105
V.4 Abbreviations and acronyms	106
V.5 IPCablecom2 NAT requirements and scope	106
V.6 NAT background	107
V.7 IPCablecom2 NAT architecture	110
V.8 Architecture description	112
Appendix VI – IPCablecom2 IPv6 and IPv4 strategy overview	117

IPCablecom2 architecture framework

1 Scope and overview

1.1 Scope

The initial release of IPCablecom [ITU-T J.160-J.178] provides for telephony. IPCablecom multimedia [ITU-T J.179] creates a bridge that allows for the expansion of IPCablecom into a full range of multimedia services. This Recommendation provides the architectural framework, technical background and project organization for the second release of the IPCablecom family of Recommendations providing for the extension into the multimedia domain.

1.2 IPCablecom2 overview

IPCablecom2 is a cable industry effort designed to support the convergence of voice, video, data and mobility technologies. There are tens of millions of cable broadband customers, and the capability of the network to provide innovative services beyond high-speed Internet access is ever-increasing. In particular, real-time communication services based on the IP protocols, such as Voice over Internet Protocol (VoIP), are rapidly evolving and consumers are embracing a wide-range of client devices and media types. It is expected that new technologies, such as Video over IP communications and the ability to display voice and video mail message notifications on a TV-set, will change the way communication and entertainment services are offered. These cutting edge technologies will present exciting new opportunities for cable operators to offer high-value services to consumers in a cost-effective manner.

IPCablecom2 defines an architecture and a set of open interfaces that leverage emerging communications technologies, such as the IETF session initiation protocol (SIP) [IETF RFC 3261], to support the rapid introduction of new IP-based services onto the cable network. A modular approach allows operators to flexibly deploy network capabilities as required by their specific service offerings, while maintaining interoperability across a variety of devices from multiple suppliers. Intentionally non service-specific, the platform should provide the basic capabilities necessary for operators to deploy services in areas such as:

- Enhanced Residential VoIP and IP Video Communications – Capabilities such as video telephony; call treatment based on presence, device capability, identity; and 'Click to dial' type of features.
- Cross Platform Feature Integration – Capabilities such as caller's name and number identification on the TV and call treatment from the TV.
- Mobility services and Integration with Cellular and Wireless Networks – Capabilities such as call handoff and roaming between IPCablecom VoIP over WiFi and wireless-cellular networks; voice-mail integration; and single E.164 number (e.g., telephone number).
- Multimedia Applications – Capabilities such as QoS-enabled audio and video streaming.
- Commercial Services Extensions – Capabilities such as PBX extension; IP Centrex Services to small to medium-sized businesses; and VoIP trunking for enterprise IP-PBXs.
- Residential SIP Telephony Extensions – Capabilities such as traditional telephony features (e.g., call waiting, caller ID), operator services, and emergency services.

As noted above, the architecture is designed to support a broad range of services. The IPCablecom2 set of Recommendations define a base architecture, and the components and generic requirements necessary to meet a large number of applications and services. Specific applications and services

rely on this base architecture, but are specified in separate releases. The base specifications should be able to accommodate different applications and services with very few, if any, changes.

This release of IP-Cablecom is based on Release 6 of the IP multimedia subsystem (IMS) as developed by the 3rd generation partnership project (3GPP). The IMS is a SIP-based architecture for providing multimedia services. IP-Cablecom2 defines enhancements to the IMS in order to ensure IP-Cablecom addresses requirements that are not already addressed by the IMS.

It is an important objective of this work that interoperability between IP-Cablecom 2.0 and 3GPP IMS is provided. IP-Cablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IP-Cablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IP-Cablecom 2.0.

IP-Cablecom2 leverages other open standards and specifications wherever possible.

2 References

2.1 Normative references

None.

2.2 Informative references

- [ITU-T J.160] ITU-T Recommendation J.160 (2005), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems.*
- [ITU-T J.170] ITU-T Recommendation J.170 (2005), *IP-Cablecom security specification.*
- [ITU-T J.171.1] ITU-T Recommendation J.171.1 (2005), *IP-Cablecom trunking gateway control protocol (TGCP): Profile 1.*
- [ITU-T J.178] ITU-T Recommendation J.178 (2005), *IP-Cablecom CMS to CMS signalling.*
- [ITU-T J.179 App.I] ITU-T Recommendation J.179 (2005), *IP-Cablecom support for multimedia. Appendix I: Background information.*
- [ITU-T J.361] ITU-T Recommendation J.361 (2006), *IP-Cablecom2 codec media.*
- [ITU-T J.362] ITU-T Recommendation J.362 (2006), *IP-Cablecom2 control point discovery.*
- [ITU-T J.363] ITU-T Recommendation J.363 (2006), *IP-Cablecom2 data collection to support accounting.*
- [ITU-T J.364] ITU-T Recommendation J.364 (2006), *IP-Cablecom2 provisioning, activation, configuration and management.*
- [ITU-T J.365] ITU-T Recommendation J.365 (2006), *IP-Cablecom2 application manager interface.*
- [ES-DCI] PacketCable Electronic Surveillance – *Delivery Function to Collection Function Interface Specification*, PKT-SP-ES-DCI-I01-060914 (2006), Cable Television Laboratories, Inc.
- [ES-INF] PacketCable Electronic Surveillance – *Intra-Network Functions Specification*, PKT-SP-ES-INF-I01-060406, 6 April 2006, Cable Television Laboratories, Inc.
- [IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*

3 Terms and definitions

This Recommendation uses the following terms and definitions:

3.1 contact address: The URI of a user agent on the network. Contact addresses, in the context of IP-Cablecom are often, but not always, addresses used to deliver requests to a specific user agent.

3.2 E.164: E.164 is an ITU-T Recommendation which defines the international public telecommunication numbering plan used in the PSTN and other data networks.

3.3 headend: The central location on the cable network that is responsible for injecting broadcast video and other signals in the downstream direction.

3.4 IMS delta specifications: Suite of 3GPP IMS specifications modified to reflect cable-specific deltas necessary to comply with IP-Cablecom.

3.5 IP-Cablecom multimedia: An application agnostic QoS architecture for services delivered over DOCSIS networks.

3.6 private identity: See private user identity.

3.7 private user identity: Used, for example, for registration, authorization, administration and accounting purposes. A private user identity is associated with one or more public user identities.

3.8 public identity: See public user identity.

3.9 public user identity: Used by any user for requesting communications to other users.

3.10 SIP user agent: Same as 'user agent'.

3.11 server: A network element that receives requests in order to service them and sends back responses to those requests. Examples of servers are proxies, user agent servers, redirect servers, and registrars.

3.12 subscriber: An entity (comprising one or more users) that is engaged in a subscription with a service provider.

3.13 subscription: A contract for service(s) between a user and a service provider.

3.14 user: A person who, in the context of this Recommendation, uses a defined service or invokes a feature on a UE.

3.15 user agent (UA): A SIP user agent as defined by [IETF RFC 3261].

3.16 multimedia session: A set of multimedia senders and receivers and the data streams flowing from senders to receivers. A multimedia conference is an example of a multimedia session.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
ALG	Application Layer Gateway
AM	Application Manager
AS	Application Server
BGCF	Breakout Gateway Control Function
CDF	Charging Data Function
CDR	Call Detail Record

CM	Cable Modem
CMS	Call Management Server
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS	Data-Over-Cable Service Interface Specification
EMS	Element Management System
E-MTA	Embedded Multimedia Terminal Adapter
ENUM	E.164 Number Mapping
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
FW	Firewall
GRUU	Globally Routable User Agent URI
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
ICE	Interactive Connectivity Establishment
I-CSCF	Interrogating Call Session Control Function
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
MG	Media Gateway
MGC	Media Gateway Controller
NA(P)T	Network Address and Port Translation; used interchangeably with NAT
NAT	Network Address Translation
NCS	Network-based Call Signalling
NMS	Network Management System
PAC	Provisioning, Activation and Configuration element (PAC element)
PACM	Provisioning, Activation, Configuration and Management
PAM	IPCablecom Application Manager
P-CSCF	Proxy Call Session Control Function
PDS	Profile Delivery Server
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
QoS	Quality of Service

RKS	Record Keeping Server
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SG	Signalling Gateway
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SS7	Signalling System No. 7
STUN	Simple Traversal of UDP Through NAT
TCP	Transmission Control Protocol
TGCP	Trunking Gateway Control Protocol
TLS	Transport Layer Security
TR	Technical Report
TURN	Traversal Using Relay NAT
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XDS	XCAP Data Server

5 IP-Cablecom2

The IP-Cablecom2 architecture describes a set of functional groups and logical entities, as well as a set of interfaces (called reference points) that support the information flows exchanged between entities.

This clause provides:

- An overview of the architecture, including a description of the main functional groupings (e.g., local network, access network, edge, core) and logical entities (e.g., UE, P-CSCF, S-CSCF, HSS) within those groupings.
- A set of design goals for the IP-Cablecom2 architecture and specifications.
- A list of IP-Cablecom2 Recommendations.

5.1 Relationship with the 3GPP IMS

IP-Cablecom2 is based on Release 6 of the IP multimedia subsystem (IMS) as defined by the 3rd generation partnership project (3GPP). 3GPP is a collaboration agreement between various standards bodies. The scope of 3GPP is to produce Technical Specifications and Technical Reports for GSM and 3rd generation (3G) mobile system networks.

The scope of 3GPP includes development of a SIP-based IP-communications architecture for mobile networks. The resulting architecture, dubbed the IP multimedia subsystem, defines how various protocols (e.g., SIP and DIAMETER) can be used in a system-level architecture to provide SIP-based communication services.

Within the overall IP-Cablecom goal to leverage existing industry standards whenever possible is an objective to align with the IMS architecture and specifications being developed by 3GPP. Specifically, IP-Cablecom2 reuses many of the basic functional entities and reference points defined in the IMS. The primary motivation behind this design objective is to align with a set of standards that are widely supported by vendor products, and therefore, minimize the product development effort required to deploy IP-Cablecom networks.

While many of the functional entities and reference points defined in the IMS have broad applicability in other industries, Release 6 of the IMS is a wireless-centric architecture designed to meet the business and operational needs of the wireless industry. Therefore, it does not meet all of the needs of the cable industry. IP-Cablecom2 enhances the IMS to support the unique technology requirements of the cable industry, and also addresses cable operator business and operating requirements.

3GPP is developing newer releases of the IMS specifications. Future updates to IP-Cablecom will align with these newer releases as necessary.

Refer to [TS 23.002] for additional information on the 3GPP IMS architecture.

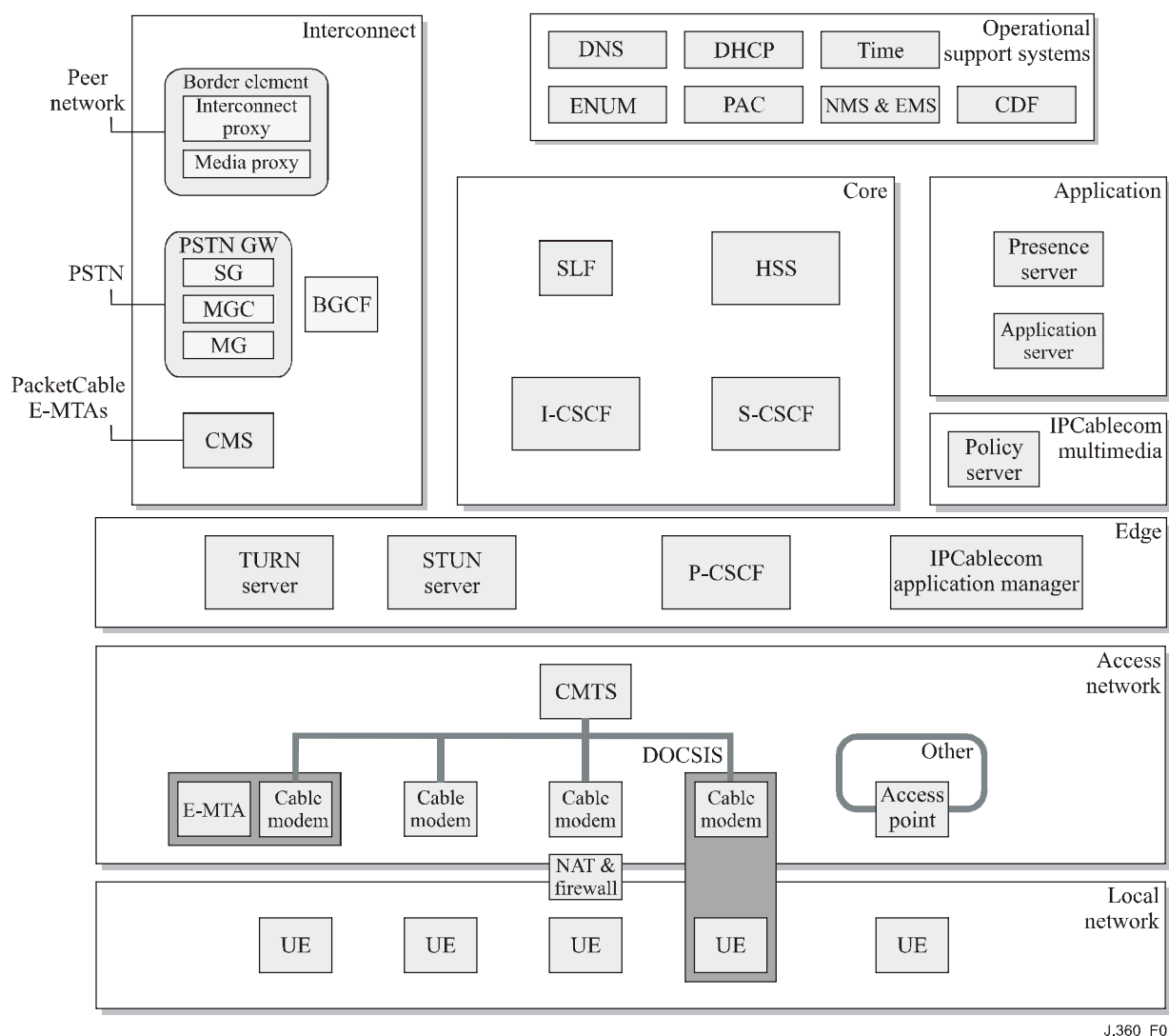
5.2 Overview

The IP-Cablecom2 architecture is based on the IMS architecture, with some incremental extensions as noted in clause 5.1. Extensions include use of additional or alternate functional components compared with the IMS architecture, as well as enhancements to capabilities provided by the IMS functional components.

Some of the major IP-Cablecom enhancements to the IMS include:

- Support for Quality of Service (QoS) for IMS-based applications on DOCSIS access networks, leveraging the IP-Cablecom Multimedia architecture [ITU-T J.179 App.I].
- Support for signalling and media traversal of network address translation (NAT) and firewall (FW) devices, based on IETF mechanisms.
- Support for the ability to uniquely identify and communicate with an individual when multiple UEs are registered under the same public identity.
- Support for additional access signalling security and UE authentication mechanisms.
- Support for provisioning, activation, configuration and management of UEs.

An overview of the IPcablecom2 architecture elements and functional groupings is illustrated in Figure 1.



J.360_F01

Figure 1 – IPcablecom reference architecture

The architecture provides a rich and modular platform upon which a variety of multimedia communication services can be built for a diverse set of UEs. Note the reference architecture depicts several different UE deployment scenarios (e.g., UE behind a CM, a NAT and firewall gateway between the UE and CM). These deployment scenarios are meant to illustrate the fact that UEs can be deployed in many different environments and configurations. The reference architecture does not provide an exhaustive set of deployment scenarios.

IPcablecom2 assumes a user model composed of users, public identities, UEs and devices. The potential relationships between users, public identities, UEs and devices are described in Appendix IV. For example, a user may have multiple user equipment (UE) devices, each of which may be registered to one or more public identities. A public identity can be an E.164 number or it can be an alphanumeric identifier that makes sense in the context of a SIP telephony service. Each public identity is generally associated with a user.

The architecture is divided into several logical areas or functional groupings:

- **Local network:** The local network is the network that the user equipment (UE) uses to connect to the access network. It may be Ethernet, WiFi, bluetooth, or any other technology

used to network or connect UEs. There may be a NAT and firewall gateway between the local network and the access network. In some instances, the UE may include an access network component. In such instances, the local network is an internal interface within the UE. This is the case with a UE that has an embedded DOCSIS cable modem.

A UE encompasses either a software-based application or a hardware-based device where service features are invoked, executed, or rendered for the subscriber. UEs all use the same basic SIP infrastructure to obtain real-time IP communication and multimedia services. An IPCablecom UE may be built in a modular fashion, and can contain varying levels of functionality based on the capabilities that it needs to support. For example, a UE may only support text-based instant messaging (IM), and thus will not need to support audio or video codecs. A NAT and firewall device may exist between a UE on a local network and the access network. As such, mechanisms are required to enable signalling and media traversal of NAT/FWs.

- Access network: A UE may reside on or be connected to the DOCSIS access network, or they may obtain services from other access networks (including other cable access networks not under the control of the cable operator owns the IPCablecom subscription); this is especially important for a mobile UE such as a laptop, WiFi-enabled phone, etc. When a UE is in the cable access network, it can obtain access network QoS by interacting with the cable networks SIP signalling infrastructure, which in turn interacts with the IPCablecom multimedia infrastructure via the IPCablecom application manager and policy server to reserve resources in the cable access network.

IPCablecom E-MTAs are included in the reference diagram for completeness.

- Edge: This functional grouping encompasses reference points that are provided to a UE and the access network. A UE obtains access to the SIP Infrastructure through the proxy call session control function (P-CSCF). The P-CSCF proxies SIP messages between the UE and the rest of the architecture and maintains security associations with the UE. The P-CSCF may request access network QoS resources upon session initiation on behalf of the UE via the IPCablecom application manager. The IPCablecom application manager interfaces with the IPCablecom multimedia policy server, which pushes QoS policy to the cable access network components. IETF STUN and TURN servers are used to enable media access through NAT & FW devices (the P-CSCF uses a separate STUN server for signalling access through NAT & FW devices). IPCablecom E-MTAs are served by their CMS as described in IPCablecom 1.5 architecture framework technical report [ITU-T J.160].
- Core: The core contains the basic components required to provide SIP services and subscriber data. The core functional grouping consists of the following functional components: Interrogating-CSCF (I-CSCF), Serving-CSCF (S-CSCF), subscription location function (SLF) and home subscriber server (HSS).
- The I-CSCF is the initial entry point into the core for SIP. The I-CSCF cooperates with the HSS to determine the S-CSCF to be assigned to a public identity, and routes requests originated by a UE to the S-CSCF assigned to the originating UE's public identity. The I-CSCF also routes terminating SIP requests received from within the network or from outside networks. In this case, the I-CSCF consults the HSS to determine the S-CSCF that is assigned to a terminating public identity, and route the SIP request to that S-CSCF for processing. The I-CSCF can also provide topology hiding when communicating with outside networks.
- The S-CSCF is responsible for SIP session processing. Calls or multimedia communication sessions initiated to and from public identities are sent to the assigned S-CSCF for authorization and processing. The S-CSCF has a service control framework that evaluates SIP requests against pre-defined filter criteria for a subscriber, or determines if the SIP request should be routed to an application server for processing. This enables an

extensible architecture for rapid introduction of value-added features and services. The S-CSCF may route SIP messages to application servers, presence servers, other CSCFs, or breakout gateway control functions (BGCFs) as appropriate. The S-CSCF also includes the SIP registrar function, which maps public identities to their registered SIP contact addresses, assigns globally routable user agent URIs (GRUUs), and stores any other parameters associated with the registration, e.g., SIP user agent capabilities. The S-CSCF obtains subscription data from the HSS.

- The HSS provides access to user profiles and other provisioned subscriber data to the S-CSCF and application servers. The HSS also maintains the assignment of a public identities to an S-CSCF. A subscription may be associated with multiple public identities. An HSS maps a subscription to a S-CSCF; meaning that all the public identities will be assigned to the same HSS.
- S-CSCFs and application servers may store certain classes of data associated with subscriptions in the HSS.
- The SLF is used to locate an HSS instance for a given identity when multiple HSSs are present.
- Applications: The application server functional grouping defines application servers that may be invoked as part of originating or terminating request treatment on a S-CSCF for a given user, or they may be stand-alone application servers that can be invoked and operate independently. The presence server is a specialized application server that contains presence data for public identities. The presence data is obtained from a variety of sources in the network and provides a view of the willingness and availability of the user for communications. Privacy handling and subscription authorization of presence data is handled by the presence server as well.
- Interconnect: The interconnect functional grouping enables connections with other networks. Interconnect with the PSTN is handled via the breakout gateway control function (BGCF), which determines the media gateway controller (MGC) to utilize for PSTN interconnect. The MGC controls media gateways (MG) which provide transport layer and bearer interconnect to the PSTN. Signalling gateways (SG) provide SS7 connectivity. The IP-Cablecom MGC, SG and MG are used to interconnect to the PSTN. Interconnect with peer Voice over IP (VoIP) networks may be achieved through a border element. The Border Element contains Interconnect Proxy functionality and optionally Media Proxy functionality that may be on separate platforms. The Interconnect Proxy may perform a variety of tasks, including protocol profile enforcement and signalling conversion, as needed to interwork with other networks. The Media Relay may relay media for the purposes of topology hiding. The IP-Cablecom CMS is located in the Interconnect functional grouping to indicate that E-MTAs that it serves can communicate with UEs.
- Operational Support Systems: Operational Support Systems provide various functions like accounting and UE provisioning. The CDF collects accounting messages from various elements, DHCP helps with the distribution of IP addresses to UEs, ENUM and DNS aid in the resolution of URIs and FQDNs, PAC and XDS support provisioning and configuration of UEs, and EMSs and NMSs assist with monitoring and management functions.

Note that the functional components described above are logical functions, which may be combined on common platforms.

5.3 IP-Cablecom releases and organization

5.3.1 IP-Cablecom releases

The IP-Cablecom architecture continues to evolve as new capabilities are added, and as such is comprised of several releases.

- Release 1.0 – This release provides support for a telephony application using E-MTAs; it is specified in the initial release of ITU-T Recs J.160-J.178.
- Release 1.5 – This release provides incremental new capabilities and adds SIP for session management within and among IP-Cablecom networks; it is specified in the revisions to ITU-T Recs J.160-J.178.
- Multimedia – This release separates out the QoS capabilities and defines a generic QoS architecture; it is specified in [ITU-T J.179].
- Release 2 – This release adds support for SIP-based endpoints, and a SIP-based service platform that may be used to support a variety of services.

Figure 2 illustrates the IP-Cablecom releases. Applications that make use of the SIP service platform will be defined in separate stand-alone releases and are not depicted in Figure 2.

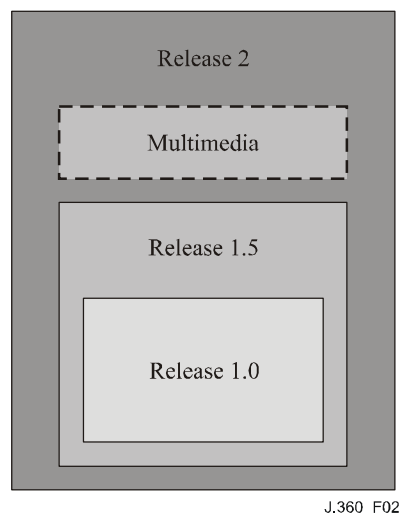


Figure 2 – IP-Cablecom releases

5.3.2 IPCablecom organization

The organization of this IPCablecom2 release is based upon the need to both align with and extend the IMS. Figure 3 illustrates the scope of the IPCablecom2 release.

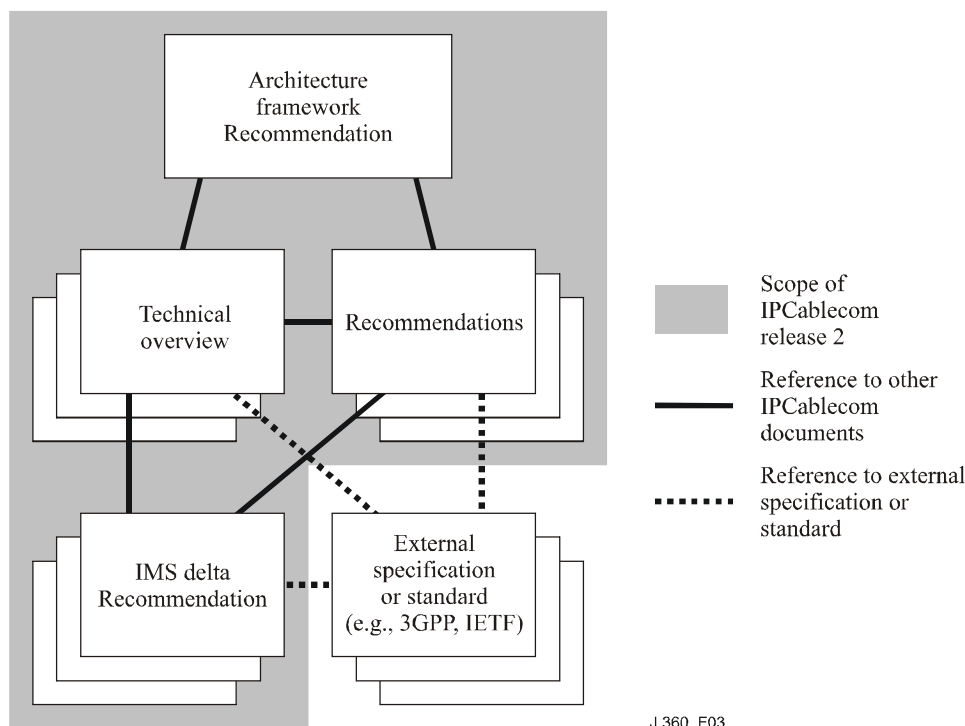


Figure 3 – IPCablecom2 organization

This architecture framework Recommendation describes the IPCablecom2 architecture at a high level. Individual functional areas (e.g., SIP, NAT and FW traversal, security, etc.) have dedicated appendices or Recommendations. The purpose of these documents is to capture architecture issues and expected usage of the IMS for cable. A document may be a specification if it documents normative requirements and defines reference points that are specific to IPCablecom, or if it includes a very small number of changes to an IMS specification (i.e., the number of changes made to an IMS specification was not sufficient to warrant releasing an IMS Delta specification).

In some cases, these documents do not draw on any IMS architectural components or reference points. However, in general these documents are based upon the IMS and in some cases enhance the IMS. Documents that are based upon the IMS simply refer to IMS documents in the same way any other document is normatively referenced. Enhancements to the IMS are contained in IMS Delta specifications. IMS Delta specifications are republished IMS specifications that contain changes based upon cable-specific requirements. Depending on the way the IMS documents are organized, an IMS Delta specification may contain changes to accommodate a number of different IPCablecom specifications or TRs. For example, the IMS Delta Specification for 3GPP TS 24.229 contains changes for the functional areas of SIP, NAT & FW traversal, security and QoS.

The goal is to introduce the IPCablecom enhancements to the IMS into the actual 3GPP specifications. As this occurs, IMS Delta specifications may be withdrawn and replaced with direct references to 3GPP IMS specifications.

Table 1 contains a list of Recommendations.

Table 1 – IP_Cablecom2 Recommendations

IP_Cablecom2 Recommendations reference number	Document name
J.360	Architecture framework (this Recommendation)
Appendix I	IP_Cablecom2 SIP Signalling Overview
Appendix II	IP_Cablecom2 QoS Overview
Appendix III	IP_Cablecom2 Security Overview
Appendix IV	IP_Cablecom2 Home Subscriber Server (HSS) Overview
Appendix V	IP_Cablecom2 NAT and Firewall Traversal Overview
Appendix VI	IP_Cablecom2 IPv6 and IPv4 Strategy Overview
IP_Cablecom Recommendation reference number	Recommendation name
J.362	IP_Cablecom2 control point discovery
J.365	IP_Cablecom2 application manager interface
J.364	IP_Cablecom2 provisioning, activation, configuration and management
J.361	IP_Cablecom2 codec media
J.363	IP_Cablecom2 data collection to support accounting
IMS delta specification reference number	Document name
J.366.0	Overview of IP_Cablecom2 IMS Delta Recommendations
J.366.1	IP_Cablecom2 Organization of Subscriber Data Specification 3GPP TS 23.008
J.366.2	IP_Cablecom2 IP Multimedia Call Model Stage 2 Specification 3GPP TS 23.218
J.366.3	IP_Cablecom2 IP Multimedia Subsystem Stage 2 Specification 3GPP TS 23.228
J.366.4	IP_Cablecom2 SIP and SDP Stage 3 Specification 3GPP TS 24.229
J.366.5	IP_Cablecom2 Cx and Dx Interfaces Specification 3GPP TS 29.228
J.366.6	IP_Cablecom2 Cx and Dx Interfaces, Diameter Protocol Specification 3GPP TS 29.229
J.366.7	IP_Cablecom2 Access Security for IP-Based Services Specification 3GPP TS 33.203
J.366.8	IP_Cablecom2 Network Domain Security Specification 3GPP TS 33.210
J.366.9	IP_Cablecom2 Generic Authentication Architecture Specification 3GPP TS 33.220

As described in clause 1.2, this IP_Cablecom2 release defines a base architecture upon which applications can be built. While these applications rely on the base architecture, they are independent of the base architecture and are specified in separate releases.

5.4 IPCablecom2 design considerations

In order to enable real-time IP communications across the cable network infrastructure, IPCablecom2 specifications define technical requirements and specify reference points in the following areas:

- Signalling and service control.
- Subscriber data.
- Network address translation (NAT) and firewall traversal.
- Quality of service.
- Media stream transport and encoding.
- Provisioning, activation, configuration and management.
- Network accounting and usage.
- Security.
- Lawful intercept.

5.4.1 Generic architecture goals

The design goals of the IPCablecom2 architecture include:

- Provide a service-independent architecture that allows new services to be added without impacting the underlying service control platform.
- Provide a modular architecture, where architectural components can be combined in a variety of ways to support a wide range of features. For example, a UE could be built from a mix of basic building blocks such as SIP user agents, media endpoints, presence watchers, and event subscribers.
- Support many-to-many relationships between users, endpoint devices and sessions.
- Support a wide variety of UE devices, including soft or hard UEs, smart UEs, wired or wireless UEs.
- Support IPv4 and IPv6 operation.
- Support interworking with previous releases of IPCablecom.
- Support UE mobility so that a UE can access services from any access network, not just the cable access network. In general, mobility within the context of IPCablecom means that a UE with IP connectivity can access IPCablecom services. While this is different than 3GPP-style roaming (i.e., the P-CSCF may be located in the visited network), the IPCablecom enhancements should not break the 3GPP roaming model.
- Leverage existing standards and open protocols whenever possible. Most importantly, adopt the IMS architecture and define incremental extensions as necessary.

5.4.2 Signalling and service control

IPCablecom2 signalling and service control design goals include:

- Support multiple service control models. These models include: control in the UE, control in the network, and shared control. It is up to each specific application that uses IPCablecom to define the service control model.
- Support ability for users to establish communication sessions with other users in the same network, with users in peering networks, or with the PSTN.
- Support unregistered UEs for emergency services and UE configuration.

5.4.3 Subscriber data

IPCablecom2 subscriber data design goals include:

- Define a logical entity which is the central repository for end user or subscription information needed for the invocation or execution of services by CSCFs and application servers.
- Allow for the centralized storage and distribution of persistent and semi-persistent data.

5.4.4 Network address and port translation (NA(P)T) and firewall traversal

IPCablecom2 NAT (NAT and NAPT are used interchangeably) and firewall traversal design goals include:

- Not imposing any requirements on the NAT devices nor require the network to be aware of the presence of a NAT.
- Support for multiple UEs behind a single NAT.
- Ability to support both inbound requests from and outbound requests to UEs through NATs.
- Ability to maintain bindings to multiple P-CSCFs to provide reliable inbound message delivery in the face of a P-CSCF failure.
- Support the traversal of NATs between the UE and network (home NAT, visited network NAT).
- Be application independent, meaning the solution should employ mechanisms that can be used by non-SIP-based applications. However, these solutions may require application support in order to use the defined mechanism.
- Avoid unnecessarily long media paths due to media pinning.
- Ability to re-establish communications in failure situations (e.g., the NAT/FW device re-boots and NAT bindings are lost).

5.4.5 Quality of service

IPCablecom2 QoS design goals include:

- Leverage the IPCablecom Multimedia specification in order to provide QoS when a subscriber is accessing service through the DOCSIS network.
- Support packet marking and classification from the access network such that a QoS mechanism like Differentiated Services (DiffServ) can be used in the backbone.
- Provide a mechanism that does not require applications to be aware of access network topology.

5.4.6 Media stream transport and encoding

IPCablecom2 media stream transport and encoding design goals include:

- Minimize the effects of latency, packet loss and jitter on sensitive media streams (e.g., voice and video) to ensure a quality level in the target environments (including audio/video telephony, IP video streaming and wireless).
- Define a set of audio and video codecs and associated media transmission protocols that may be supported.
- Accommodate emerging narrow-band and wideband voice codec technologies.
- Accommodate emerging video codec technologies to provide support for applications like video telephony, IP video streaming, etc.
- Specify minimum requirements for echo cancellation and voice activity detection.

- Support transparent, error-free dual-tone multi frequency (DTMF) transmission.
- Support for fax relay, modem relay, DTMF relay, and TTY.
- Support calculation and reporting of voice quality metrics.

5.4.7 Provisioning, activation, configuration and management (PACM)

IPCablecom2 PACM design goals include:

- Support lightweight static and dynamic PACM models, considering both controlled (UE's local network under service provider's control) and uncontrolled environments (UE's local network not under service provider's control).
- Support a non-DHCP based P-CSCF discovery mechanism.
- Support a multi-layered PACM framework for UEs, services and users; allowing for separate PACM definitions for each layer.
- Support for software upgrade methods for UEs.
- Support multiple operational models (i.e., branded and unbranded).

5.4.8 Network accounting and usage

IPCablecom2 network accounting and usage design goals include:

- Enable the ability to account for network usage and activities in both real-time.
In this case, real-time is relative to when the events are sent to the central repository and does not imply when the final bill may be available to the customer nor that events are sent to indicate incremental usage of network resources (i.e., on-line charging).
- Allow for multiple network elements to generate events which can be correlated to a given session or subscriber.
- Support the correlation of accounting events across the signalling and bearer planes.
- Facilitate the rapid introduction of features and services by minimizing the impact to other network elements and their need to signal feature and service related information.

5.4.9 Security

IPCablecom2 security design goals include:

- Support for confidentiality, authentication, integrity and access control mechanisms.
- Protection of the network from various denial of service, network disruption, theft-of-service attacks.
- Protection of the UEs from denial of service attacks, security vulnerabilities, unauthorized access (from network).
- Support for end-user privacy through encryption and mechanisms that control access to subscriber data such as presence information.
- Mechanisms for UE authentication, secure provisioning, secure signalling, secure media and secure software download.

5.4.10 Lawful intercept

IPCablecom2 lawful intercept design goals include:

- Support a service independent intercept architecture that is not tightly coupled to basic IPCablecom service capabilities.
- Maximize transparency of the surveillance within the network.
- Ensure the surveillance architecture does not constrain the design of applications.
- Support for interception of calls that are executed across NCS and SIP.

6 IP-Cablecom functional components

This clause provides additional detail on each of the functions in the IP-Cablecom architecture.

6.1 Local network

6.1.1 User equipment (UE)

IP-Cablecom supports NCS-based clients for telephony services. IP-Cablecom multimedia provides a service agnostic QoS and accounting framework. IP-Cablecom2 adds support for SIP-based clients with a variety of capabilities, e.g., soft and hard phones, smart phones, wireless and wired phones, instant messaging UEs, video communications terminals, etc. Consistent with IMS, IP-Cablecom clients are called user equipment (UE). All of the various UEs described previously use the same basic infrastructure to obtain multimedia services. UEs may be fixed or mobile devices such as laptops or WiFi-enabled phones. They may reside on the cable access network, or they may obtain services from other access networks. When UEs are in the cable access network, they can obtain access network QoS by interacting with the signalling infrastructure, which in turn interacts with the IP-Cablecom multimedia policy server.

6.1.2 NAT and firewall

A NA(P)T (network address and port translation) and a firewall may be present between the local network and the access network. Since NAT may modify IP addresses and ports, and a firewall restricts access, the signalling and bearer planes need to behave differently when these elements are inserted between the UE and the P-CSCF.

6.2 Access network

The UE connects to the Edge via the existing cable access network or via other available access networks (e.g., public WiFi access point, 3G cellular data network). The access network elements provide the IP connectivity and QoS resources needed by the UE to perform the IP-Cablecom services.

6.2.1 Cable modem (CM)

The CM is the customer premises equipment (CPE) used in conjunction with the CMTS to provide broadband Internet access service. An E-MTA is an IP-Cablecom NCS-based client with an embedded cable modem. While the E-MTA does not communicate directly with the network, it is important to note that a NCS-based telephony service and SIP-based service may be provided through the same CM.

6.2.2 Cable modem termination system (CMTS)

The CMTS resides in the cable operators headend, and, in conjunction with the CM, it is used to provide broadband Internet access service. Beginning with ITU-T Rec. J.112, DOCSIS defines a means to provide QoS on the access network. IP-Cablecom Multimedia defines a means for IP-enabled services to request QoS from the DOCSIS network. IP-Cablecom defines how QoS can be provided for SIP-based services via IP-Cablecom multimedia and DOCSIS.

6.2.3 Access point

IP-Cablecom may be used to provide service to UEs that receive IP connectivity through other kinds of access networks.

6.3 Edge

6.3.1 Proxy call session control function (P-CSCF)

A UE accesses the SIP Infrastructure through a P-CSCF. The P-CSCF shields the SIP network from access network specific protocol details and provides scaling for the infrastructure by handling

certain resource intensive tasks when interacting with the UE. It also represents the trust boundary for SIP between untrusted parts of the network (Access Network, Local Network) and trusted parts of the network (core, application, interconnect, operational support systems). The functions performed by the P-CSCF are:

- Routing SIP messages from the UE to the I-CSCF or S-CSCF and vice versa.
- Maintaining security associations between itself and the UE and asserting the identity of authenticated public identities.
- Interacting with the IPCablecom application manager for QoS management.
- Providing functionality to allow the UE to traverse NATs and maintain NAT bindings for SIP signalling.
- Generation of accounting correlation IDs and accounting events.

6.3.2 STUN and TURN servers

A STUN server is an entity that receives STUN requests, and sends STUN responses. STUN requests are typically binding requests which are used to determine the bindings allocated by NATs. The UE sends a Binding Request to the server, over UDP. The server examines the source IP address and port of the request, and copies them into a response that is sent back to the UE.

Two STUN servers are employed by the IPCablecom network, one employed as a functional component of the P-CSCF (not shown in Figure 1) and one as a stand-alone STUN server:

- The STUN server as a functional component within the P-CSCF is used by SIP UEs in order to maintain the NAT bindings for signalling. These STUN messages may also act as a keep-alives, allowing the UE to determine P-CSCF availability and detect NAT reboots.
- The external STUN server shown in Figure 1 is used to determine one of several possible candidate media addresses using the STUN protocol.

In addition to the STUN servers, the architecture also contains a TURN server. A TURN server is an entity that receives TURN requests, and sends TURN responses. The server is capable of acting as a data relay, receiving data on the address it provides to UEs, and forwarding it to the UEs. This data relay functionality allows media to traverse NATs in cases when other NAT traversal techniques are insufficient.

6.3.3 IPCablecom application manager

The IPCablecom application manager is responsible for a variety of tasks. Most importantly it is responsible for determining the QoS resources needed for a session based on the received session descriptors and managing the QoS resources allocated for a session.

Determining the QoS resources for a session involves interpreting the session descriptor and calculating the bandwidth necessary, determining the traffic scheduling type and populating the traffic classifiers. This also involves determining the number of flows necessary for the session (voice only vs voice and video) and managing the association of the flows to the session.

6.4 Core

6.4.1 Serving CSCF (S-CSCF)

All SIP messages outside of a dialog that go to and from a given subscriber pass through the S-CSCF serving that subscriber. At a high level, the S-CSCF supports the following capabilities:

- SIP registrar function, which provides a database that dynamically binds registered public identities (AORs) to a set of contact addresses, assigns GRUUs, as well as stores any other parameters associated with the registration, e.g., user agent capabilities and the address(es) of the P-CSCF which can be used to reach the contacts.

- SIP user authentication and authorization.
- Service selection and filtering.
- Routing of messages to the P-CSCF of UEs serviced by the S-CSCF.
- Routing of messages to an I-CSCF for Public User Identities not serviced by the S-CSCF.
- Routing of messages to a BGCF for calls to the PSTN.
- Origination Processing: processing of incoming dialog-initiating requests from SIP UAs contained in UEs or Application Servers served by the S-CSCF.
- Terminating Processing: processing of outgoing SIP messages terminating to a Public Identity served by the S-CSCF. This includes support for forking of SIP messages for the case in which multiple contact addresses are registered for that Public Identity.
- External routing queries to databases such as ENUM in order to determine where the call should be routed.
- Network initiated release of sessions.
- Generation of Accounting Events.

There may be multiple S-CSCFs in the Core. At any one time, a Subscription (and all the Public Identities associated with it) can only be handled by a single S-CSCF.

Subscriptions are associated with S-CSCFs. Subscription data is stored in one or more home subscriber servers (HSSs). The S-CSCF interacts with the SLF to identify the relevant HSSs to obtain user data for the users it serves. The S-CSCF may also interact with the HSS to store certain types of user data for the users it serves.

GRUUs are supported by the endpoints and the S-CSCF. This allows endpoints to be assigned a GRUU during the registration process, which in turn enables endpoints to initiate a request to a specific contact instead of an AOR. This is important for various features such as call transfer and conferencing.

6.4.2 Interrogating CSCF (I-CSCF)

The I-CSCF supports:

- Interacting with the HSS to determine the binding between a subscription (and associated public identities) and a S-CSCF.
- Querying the HSS to obtain the S-CSCF and then routing SIP requests from another network operator to the correct S-CSCF.
- Routing of messages to ASs using public service identities (PSIs).
- Routing of messages to a border element for VoIP peering.

6.4.3 Home subscriber server (HSS)

The HSS is responsible for storing the following subscription-related information:

- Association between a subscription and S-CSCF.
- Subscription profile information (filter criteria).
- Subscription security information.
- Transparent or opaque data for usage by application servers.

The HSS provides information storage, retrieval, and processing support to components of the network. It supports the following capabilities:

- Session establishment – The HSS supports the session establishment procedures. For terminating traffic, it provides information on which S-CSCF is assigned to handle a public identity.

- Security – The HSS supports various authentication schemes by storing security-related data and providing this data as required to support UE security procedures.
- Service Provisioning – The HSS provides access to the service profile data for use by the S-CSCF. The HSS may also store application-specific data for application server.

6.4.4 Subscription locator function (SLF)

The SLF provides the name of the HSS containing the required subscriber specific data. The SLF is not needed in a single HSS environment.

6.5 IP-Cablecom multimedia

IP-Cablecom multimedia defines an IP-based platform for delivering QoS-enhanced multimedia services over DOCSIS 1.1 (this Recommendation uses DOCSIS and assumes DOCSIS 1.1 or greater) access networks. This platform allows the core capabilities of IP-Cablecom (e.g., QoS authorization and admission control, event messages for billing and other back-office functions, and security) to support a wide range of IP-based services beyond telephony. That is, while the IP-Cablecom CMS is customized for the delivery of residential telephony services, the IP-Cablecom multimedia components offer a general-purpose platform for cable operators to deliver a variety of IP-based multimedia services that require QoS treatment.

The IP-Cablecom multimedia architecture defines the interaction between a CMTS, policy server, and application manager. The CMTS is included as part of the access network and is described in clause 6.2.2. The application manager is specific to each application. IP-Cablecom defines an IP-Cablecom application manager which is described in clause 6.3.3. The policy server, which is a unique IP-Cablecom multimedia element that may communicate with a variety of application managers, is described below.

6.5.1 Policy server

The policy server primarily acts as an intermediary between application manager(s) and CMTS(s). It applies network policies to application manager requests and proxies messages between the application manager and CMTS.

6.6 Application

6.6.1 Application server (AS)

An application server (AS) provides application-specific services. An AS may influence a SIP session based on its supported services. It may also host and execute services. An AS may initiate services or terminate services on behalf of a user.

6.6.2 Presence server

The presence server is a specialized application server. It acts as the focal point for connecting sources of presence information and interested parties.

The presence server can obtain presence information in multiple ways, e.g.:

- Using the SIP PUBLISH method: The PUBLISH request is addressed to a public identity, and then forwarded by the S-CSCF to the presence server in accordance with normal routing rules.
- Using the SIP SUBSCRIBE method: the presence server may also act as a Watcher, using the SIP SUBSCRIBE method to subscribe to presence information that is available elsewhere, e.g., from a Registrar.

Presence subscriptions by Watchers are addressed to a public identity and delivered by the S-CSCF to the presence server. The presence server manages the dialog for each subscription, and sends a

SIP NOTIFY message to the Watcher(s) each time there is a change in the presence status for which the Watcher is subscribed and authorized.

6.7 Interconnect

6.7.1 Border element

Interconnect with peer networks may be supported through a border element. The border element contains an interconnect proxy function, and may contain a media proxy function.

Interconnect proxy functionality includes:

- Protocol interworking.
- SIP profile enforcement (translation, adaptation, or normalization).
- Security-related services (e.g., maintaining a security association with the peer).
- IP address management (peer networks with the same private IP address space).
- Interworking between IPv6 and IPv4 networks.
- Media proxies relay media between peer networks.

IPcablecom does not define specific functional requirements that border elements must support. Instead, it is left to each operator to determine the need for and requirements on a border element.

6.7.2 Breakout gateway control function (BGCF)

The BGCF provides network selection for routing to the PSTN and within its own network determines which MGC is used to connect to the PSTN.

6.7.3 Public switched telephone network gateway (PSTN GW)

The PSTN GW consists of the signalling gateway (SG), media gateway controller (MGC) and the media gateway (MG). The SG, MGC and MG are defined in previous releases of IPcablecom, and are reused in this release of IPcablecom, with the addition of an IPcablecom reference point to the MGC. The SG, MGC and MG are logical components that may exist on separate platforms, or may be combined together onto a single platform.

The SG performs signalling conversion at a transport layer between SS7-based transport and the IP-based transport used in the IPcablecom network. The SG does not interpret the application layer, but does interpret the layers needed for routing signalling messages.

The MGC performs protocol conversion between SS7 ISUP messages and the IPcablecom call control protocols and provides connection control of the media channels in the MG.

The MG provides bearer channel conversion between the circuit switched network and the IP RTP media streams in the IPcablecom network. The MG may introduce codecs and echo cancellers, etc. as needed to provide the bearer channel conversions.

6.7.4 Call management server (CMS)

An IPcablecom call management server (CMS) provides support for telephony services for NCS clients (i.e., E-MTAs). The CMS provides most of the telephony features while interacting directly with application servers (e.g., unified messaging servers and conference servers) to provide additional applications to E-MTAs. It may not allow for features to operate transparently across E-MTAs and UEs owned by the same user.

The IPcablecom CMS communicates with the CSCFs as a peer.

6.8 Operational support systems

The IPcablecom network is expected to have the following servers as part of the operational support system.

6.8.1 Dynamic host configuration protocol (DHCP) server

A DHCP server is used when the UE's local network is under the control of the service provider. It provides IP network participation information (e.g., IP address and DNS server information). UEs in environments that are not under the control of the service provider may not be able to use the services of the service provider's DHCP server. In such cases, it is assumed that the UE receives IP network participation information from the local network.

6.8.2 Domain name system (DNS) server

A DNS server is used to resolve DNS entities (e.g., FQDNs, SRV records) into network addresses and vice versa. A service provider's DNS service is expected to be utilized by UEs and network components alike, for locating entities or routing of messages.

6.8.3 ENUM server

An ENUM server is used to store and translate E.164 numbers to SIP URIs or name server (NS) records pointing to the name server for the operator with delegation for that particular E.164 number. More specifically, an ENUM server uses DNS to identify the owner (service provider or end user) of an E.164 number.

6.8.4 Provisioning, activation and configuration (PAC) element

The PAC element is an IP-Cablecom-defined component responsible for the provisioning, activation and configuration of UEs. It is responsible for maintaining UE configuration information. The configuration data contains the information necessary for a UE to provide services. It is also the element that conveys runtime configuration changes from the network to the user or vice versa.

The PAC element contains the logical components profile delivery server (PDS) and XCAP data server (XDS) and implements the associated reference points:

- A PDS is the logical collection of the notifier and the server responsible for handling configuration subscription requests.
- An XDS is as an XCAP server that stores, modifies and retrieves data between UEs and network elements, or between network elements.

6.8.5 Element management and network management systems

An Element management system (EMS) or network management system (NMS) relates to one or more entities associated with monitoring and management of specific network elements or an entire network, respectively.

While EMSs vary in functionality and may differ between network elements, they usually have interfaces to NMSs which are responsible for tracking and maintaining the health of a network.

EMSs and NMSs require management reference points to various elements (e.g., UEs, PAC, application servers, S-CSCF). IP-Cablecom only defines monitoring and management reference points for UEs.

6.8.6 Time server

A time server is used by UEs to obtain the time.

6.8.7 Charging data function (CDF)

The charging data function (CDF) receives charging events from the various IP-Cablecom network elements via the IMS defined Rf reference point. It can then use the information contained in the charging events to construct call detail records (CDRs).

Some IP-Cablecom elements deliver IP-Cablecom-defined event messages (EMs) to a record keeping server (RKS). The RKS may be used to support a CMS, CMTS, MGC and policy server. However, the RKS is not included in the reference architecture.

7 Protocol interfaces and reference points

IP-Cablecom2 defines a set of protocol interfaces, or reference points, in a number of areas. Many of these reference points are taken directly from the IMS and are enhanced as necessary. Some of the reference points are defined within IP-Cablecom2. These reference points are identified by their naming convention:

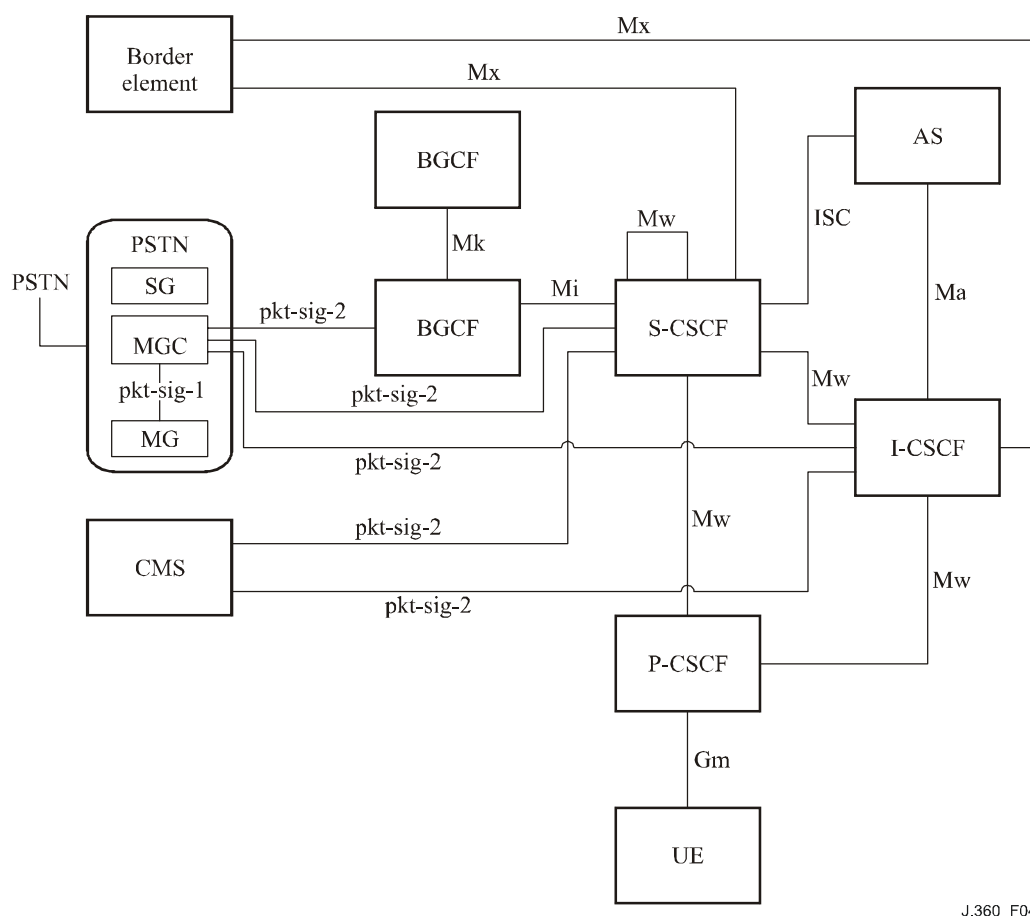
- IMS: Two or three letters (e.g., Gm, ISC);
- IP-Cablecom2 defined reference points: pkt-<functional area>-<reference point number>.

Refer to the relevant TRs and specifications for a more complete description and protocol definition.

It is possible that some of these reference points may not exist in a given vendor's product implementation. For example, if several functional IP-Cablecom2 components are integrated, then it is possible that some of these reference points are internal to the integrated device.

7.1 Signalling and service control

IP-Cablecom2 signalling and service control reference points are illustrated in Figure 4. Most reference points are IMS-defined, with appropriate deviations for IP-Cablecom as identified in various IP-Cablecom specifications. IP-Cablecom-specific reference points are also included.



J.360_F04

Figure 4 – Signalling reference points

The reference points depicted in Figure 4 are described in Table 2. All reference points are SIP-based except where noted.

Table 2 – Signalling reference point descriptions

Reference point	IP-Cablecom network elements	Reference point description
Mx	I-CSCF – Border element S-CSCF – Border element	Allows an S-CSCF or I-CSCF to communicate with a border element when interworking with another network. For example, a session between the home and peer network could be routed via an IMS ALG function within the border element in order to provide interworking between IPv6 and IPv4 SIP networks.
Mi	S-CSCF – BGCF	Allows the S-CSCF to forward the session signalling to the BGCF for the purpose of interworking with the PSTN networks.
Mk	BGCF – BGCF	Allows one BGCF to forward the session signalling to another BGCF.
Mw	P-CSCF – I-CSCF P-CSCF – S-CSCF I-CSCF – S-CSCF S-CSCF – S-CSCF	Allows the communication and forwarding of signalling messaging among CSCFs in support of registration and session control. It also allows the CMS to exchange SIP messages with the S-CSCF and I-CSCF for calls between E-MTAs and UEs.
Ma	I-CSCF – AS	Allows the I-CSCF to forward SIP requests destined to a public service identity hosted by an application server directly to the application server.
ISC	S-CSCF – AS	Allows an S-CSCF to communicate with an AS in support of various applications.
Gm	UE – P-CSCF	Allows the UE to communicate with the P-CSCF for registration and session control.
pkt-sig-1	MGC – MG	Trunking gateway control protocol (TGCP) interface as defined in the IP-Cablecom TGCP Specification [ITU-T J.171.1].
pkt-sig-2	CMS – S-CSCF CMS – I-CSCF MGC – BGCF MGC – S-CSCF MGC – I-CSCF	CMSS protocol as defined in the IP-Cablecom CMS to CMS Signalling Specification [ITU-T J.178]. Allows IP-Cablecom E-MTAs to establish voice sessions with IP-Cablecom elements. Also allows the BGCF, I-CSCF, and S-CSCF to exchange session signalling with an IP-Cablecom MGC for the purpose of interworking with the PSTN.

Refer to the IP-Cablecom2 SIP signalling overview (Appendix I) for more information.

7.2 Subscriber data

IP-Cablecom subscriber data is stored in the HSS located within the home network. The HSS serves the S-CSCF, I-CSCF, and various application servers including the presence server. The appropriate HSS for a given subscriber can be located by querying the SLF.

Figure 5 illustrates the reference points related to subscriber data services.

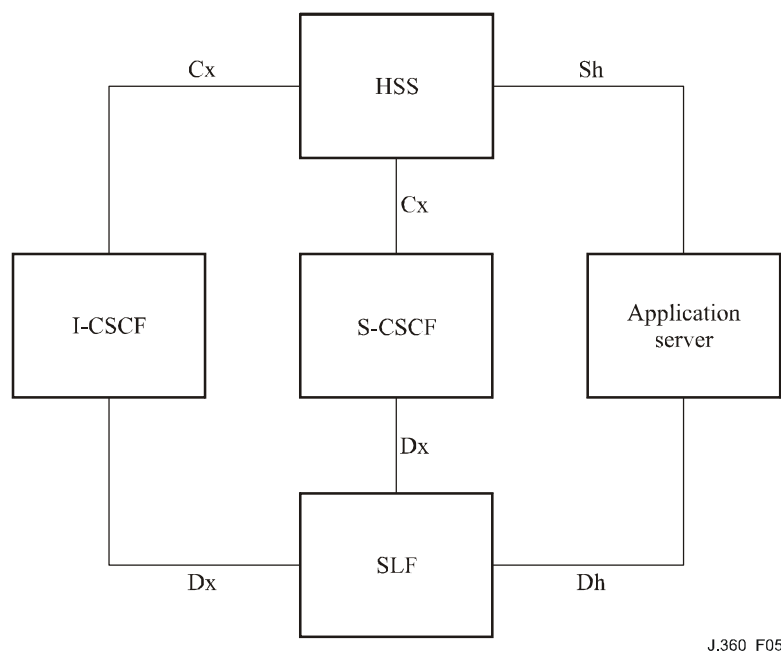


Figure 5 – Subscriber data reference points

The reference points depicted in Figure 5 are described in Table 3.

Table 3 – Subscriber data reference point descriptions

Reference point	IP-Cablecom network elements	Reference point description
Cx	I-CSCF – HSS S-CSCF – HSS	Allows an I-CSCF and S-CSCF to fetch from the HSS information related to routing, authorization and authentication, subscriber profile and S-CSCF assignment.
Sh	AS – HSS	Allows an AS to communicate with the HSS in support of various applications.
Dx	I-CSCF – SLF S-CSCF – SLF	Allows an I-CSCF and S-CSCF to fetch the address of the HSS which hosts the subscription data for a given user. This reference point is not required in a single HSS environment.
Dh	AS – SLF	Allows an AS to fetch the address of the HSS which hosts the subscription data for a given user. This reference point is not required in a single HSS environment.

Refer to the IP-Cablecom HSS Overview (Appendix IV) for more information.

7.3 Quality of service

The quality of service approach for IP-Cablecom2 is based on IP-Cablecom multimedia. In the original IP-Cablecom multimedia architecture, all service control domain functions were lumped into a single entity called the application manager (AM), of which there can be many. The IP-Cablecom2 architecture resolves this domain into more discrete elements with defined reference points. For the purposes of providing quality of service, an application manager (AM) serves as the interface between the IP-Cablecom SIP architecture and the IP-Cablecom multimedia architecture. Its function is to receive QoS messages from the P-CSCF and to formulate appropriate messages to the IP-Cablecom multimedia policy server. While this AM function could be integrated into an IP-Cablecom multimedia policy server, it should be considered as a separate function since it has

unique requirements separate from those of the policy server, such as the resolution of a single session based QoS request into a series of individual QoS requests for each IP flow. The IPCablecom version of the AM is the IPCablecom application manager (PAM).

Figure 6 illustrates the relationship between the application manager, the P-CSCF and the IPCablecom multimedia policy server. Note also that the application manager shown here as a distinct function may be packaged along with an IPCablecom multimedia policy server or, alternatively, with a P-CSCF.

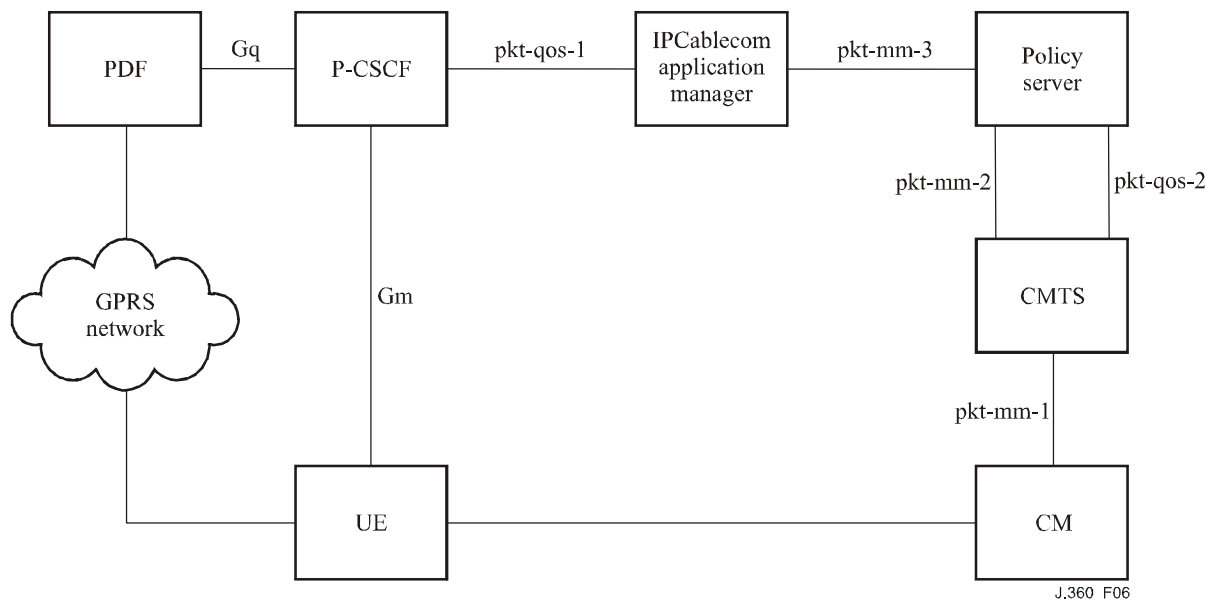


Figure 6 – QoS reference points

As illustrated in Figure 6, the AM function provides the mapping between the session or dialog QoS requirements as indicated by the SIP signalling and the QoS state of each of the associated IP service flows in the cable access network.

The reference points shown in Figure 6 are described in Table 4.

Table 4 – QoS reference point descriptions

Reference point	IPCablecom network elements	Reference point description
Gm	UE – P-CSCF	Refer to Table 2.
pkt-qos-1	P-CSCF – Application manager	This is the IPCablecom multimedia web service interface, which enables the P-CSCF to make QoS-related service requests to the application manager, which in turn maps these service requests to policy requests via the pkt-mm-3 reference point. The QoS-related service requests are derived by the P-CSCF from the SIP messages carrying appropriate session descriptions. This reference point is defined in the IPCablecom application manager interface specification [ITU-T J.365].
pkt-qos-2	Policy server – CMTS	The policy server uses the control point discovery protocol [ITU-T J.362] to determine the serving CMTS in the network for a given UE.

Table 4 – QoS reference point descriptions

Reference point	IPCablecom network elements	Reference point description
pkt-mm-1	CM – CMTS	The CMTS instructs the CM to set up, tear down or change a DOCSIS service flow via DSx signalling. This reference point is defined in IPCablecom Multimedia [ITU-T J.179 App.I].
pkt-mm-2	Policy server – CMTS	Policy decisions are pushed by the policy server onto the CMTS, and the CMTS provides responses. This reference point is defined in IPCablecom multimedia [ITU-T J.179 App.I].
pkt-mm-3	Application manager – Policy server	Allows the application manager to request the policy server to install policy decisions on the CMTS. This reference point is defined in IPCablecom multimedia [ITU-T J.179 App.I].

Refer to the IPCablecom2 QoS Overview (Appendix II) for more information.

7.4 Network address translation (NAT) and firewall traversal

Network address translators (NATs) manipulate address and port information in the IP and transport header. This causes challenges to UEs in communicating with each other using SIP:

- The UE advertises addresses required for media communications in SIP signalling (i.e., SDP). However, the local address available to the UE located behind a NAT may not be reachable by other UEs and network components.
- NAT/firewall devices contain rules that may vary in terms of how the firewall can be traversed as well as how the NAT bindings are created (i.e., address independent mapping/filtering, address dependent mapping/filtering, or address and port dependent mapping/filtering).
- Once communication is established, the NAT/firewall maintains state (i.e., firewall pin-holes and NAT bindings) based on timeouts. If the timeout expires, pin-holes are closed and NAT bindings are removed. Mechanisms have to be in place in order to maintain NAT bindings and keep pin-holes open for both signalling and media communications.

The objectives of the NAT/firewall traversal solution are to provide a mechanism by which a UE can:

- Obtain and advertise (e.g., via SDP) a reachable address. For cases, where multiple reachable addresses are possible, a "best" reachable address should be agreed upon.
- Provide a means to open and maintain pin-holes and NAT bindings for both media and signalling.

IPCablecom2 uses the ICE methodology to obtain and advertise the "best" reachable address and meet the design goals. This methodology makes use of STUN and TURN in order to obtain candidate addresses. These candidate addresses are then advertised by the UE using SDP attributes described in the ICE methodology. The UE then uses STUN to perform reachability tests, allowing it to pick the best address that uses the least network resources and results in the least network delay while maintaining the state in the UE (rather than in the network). It also allows for interworking with E-MTAs, since the address advertised in the media or connection lines of the SDP will always be a reachable address.

The IPCablecom2 NAT and Firewall Traversal Overview (Appendix V) provides additional details on the ICE methodology including a description of how UEs locate STUN and TURN servers. It also describes how NAT bindings are opened and maintained.

Note that one of the design goals is to provide a NAT and firewall traversal mechanism that works regardless of where NATs are located and whether or not they are nested. However, this may not be possible in all cases.

Figure 7 shows the reference points related to NAT/firewall traversal.

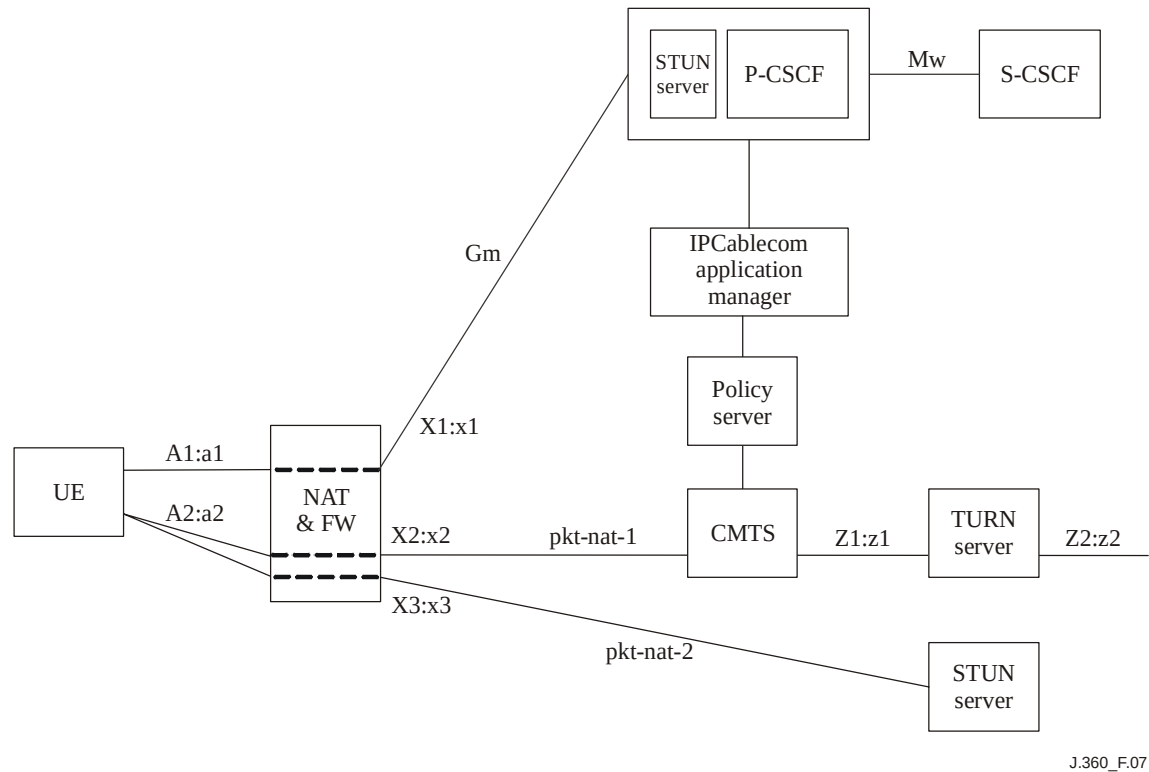


Figure 7 – NAT and FW traversal reference points

The reference points depicted in Figure 7 are described in Table 5.

Table 5 – NAT and FW traversal reference point descriptions

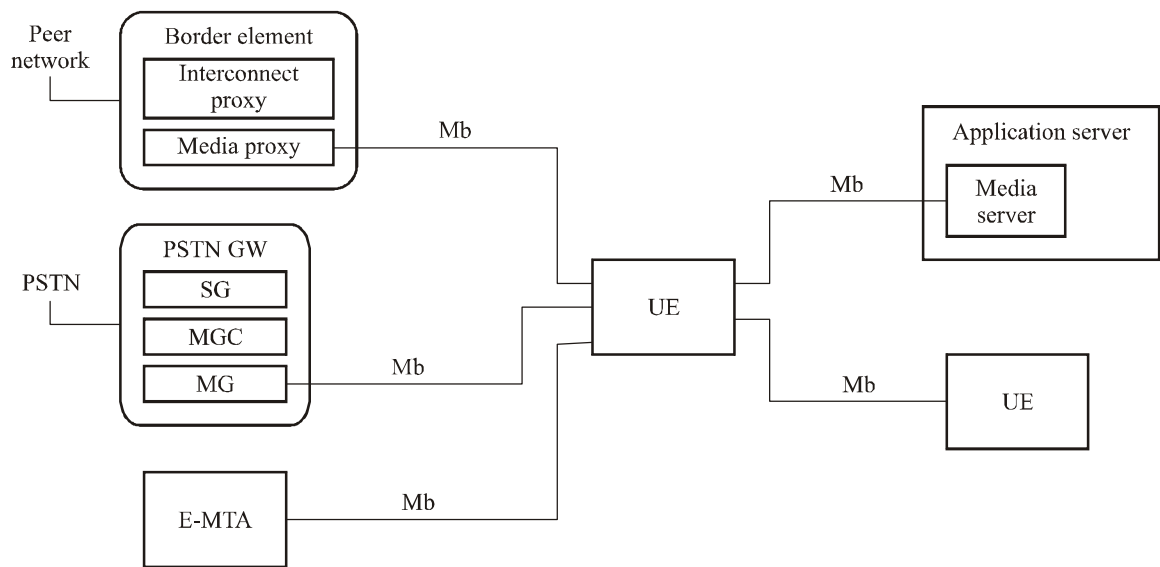
Reference point	IP-Cablecom network elements	Reference point description
Gm	UE – P-CSCF	Refer to Table 2.
Mw	P-CSCF – S-CSCF	Refer to Table 2.
pkt-nat-1	UE – TURN server	Allows the UE to access a TURN server in order to support the traversal of the NAT that does not perform Address Independent Mapping.
pkt-nat-2	UE – External STUN server	Enables the UE to determine one of several possible candidate media addresses using STUN, in support of the ICE methodology.

Refer to the IP-Cablecom NAT and firewall traversal overview (Appendix V) for more information.

7.5 Media coding and transport

IPCablecom2 uses RTP to transport most communication services (primarily voice and video).

The primary media flows in the IPCablecom2 architecture are shown in Figure 8.



J.360_F08

Figure 8 – Media stream reference points

The reference points depicted in Figure 8 are described in Table 6.

Table 6 – Media stream reference point descriptions

Reference point	IPCablecom network elements	Reference point description
Mb	UE – UE UE – MG UE – Border element UE – AS UE – E-MTA	Allows media-capable components to send and receive media data packets. Specifically, a UE can exchange media with another UE, a MG, an application server, a border element and an E-MTA.

The media that travels across the Mb reference point can be the audio traffic encoded narrow-band or wideband audio codecs, the video traffic encoded by video codecs, or the combination of both traffic types. The media may also be data in support of fax relay, modem relay, and DTMF relay.

Audio quality monitoring on the Mb reference points is supported by RTCP. Metrics for video streams are not specified.

Refer to the IPCablecom audio/video codecs specification [ITU-T J.361] for more information.

7.6 Provisioning, activation, configuration and management

IPCablecom2 defines a provisioning, activation, configuration and management (PACM) framework to aid the core business processes. The framework includes standard elements (e.g., DHCP), protocols (e.g., XCAP) and IPCablecom specific network elements (e.g., PAC).

Further, the PACM framework is separated into the following areas and sub-areas:

- Provisioning.
- IP network participation (connectivity to the local network).
- Service provider identification.
- Provisioning flows.
- Support for branded (i.e., tied to a specific operator) and unbranded (i.e., will work with any operator) models.
- UE Activation, Configuration and Management Framework.
- UE, Subscriber and Service Activation.
- UE Configuration and Management Framework.
- Data model.
- Transport protocols.

Figure 9 illustrates reference points associated with PACM.

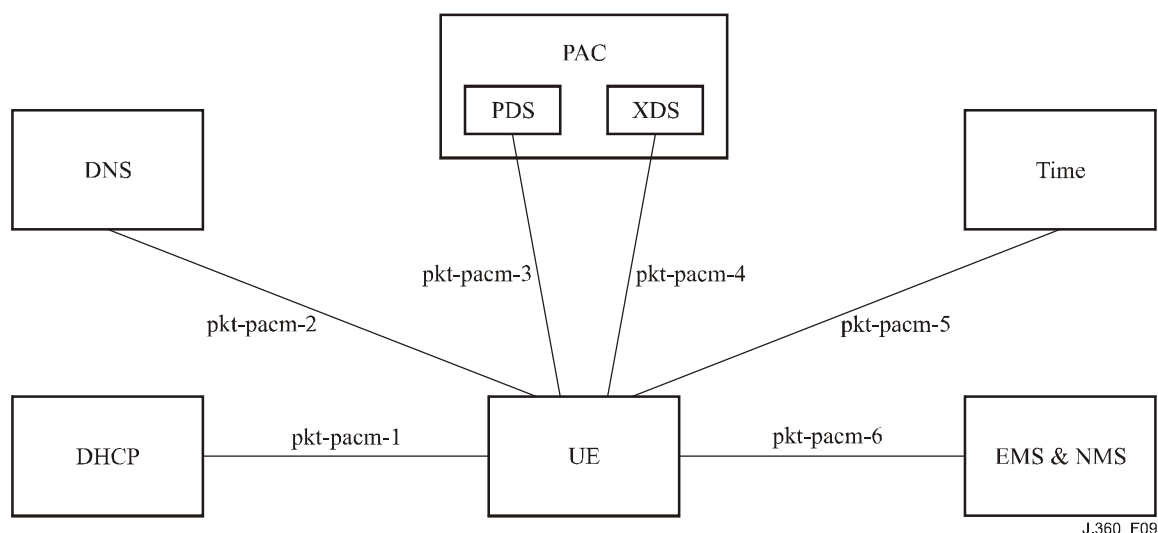


Figure 9 – PACM reference points

The reference points depicted in Figure 9 are described in Table 7.

Table 7 – PACM reference point descriptions

Reference point	IPCablecom network elements	Reference point description
pkt-pacm-1	UE – DHCP	Provides network participation information (e.g., IP address, DNS server addresses). This reference point may be provided by the local network, or by an access network not operated by the IPCablecom service provider.
pkt-pacm-2	UE – DNS	Allows the UE to resolve DNS names for location of network elements or routing of messages.

Table 7 – PACM reference point descriptions

Reference point	IPCablecom network elements	Reference point description
pkt-pacm-3	UE – PDS	Through the use of SIP, this reference point enables UEs to subscribe to the status of configuration and feature data. This is a generic reference point that describes the interaction between the UE and the XDS. However, in reality, the PDS interacts with the rest of the SIP components as an application server. Therefore, PACM SIP messages will traverse the Gm, Ma, Mw and ISC interfaces. NOTE 1 – The PDS described here is used specifically for PACM. However, as a logical component it may be defined for use in other applications as well.
pkt-pacm-4	UE – XDS	This reference point is used to distribute and manage configuration and feature data. NOTE 2 – The XDS described here is used specifically for PACM. However, as a logical component it may be defined for use in other applications as well.
pkt-pacm-5	UE-Time	Allows UEs to obtain the time.
pkt-pacm-6	UE – EMS & NMS	Enables EMSs and NMSs to monitor and manage UEs.

Refer to the IPCablecom2 provisioning, activation, configuration and management specification [ITU-T J.364] for more information.

7.7 Network accounting and usage

The IMS defines reference points that allow it to support different types of IMS connectivity access networks (CANs). IPCablecom2 Accounting assumes the Cable HFC access network along with the IPCablecom multimedia subsystem define a new type of IP-CAN for incorporation into the overall IMS architecture.

Figure 10 shows the main IPCablecom components involved with offline charging and the reference points between each of the components.

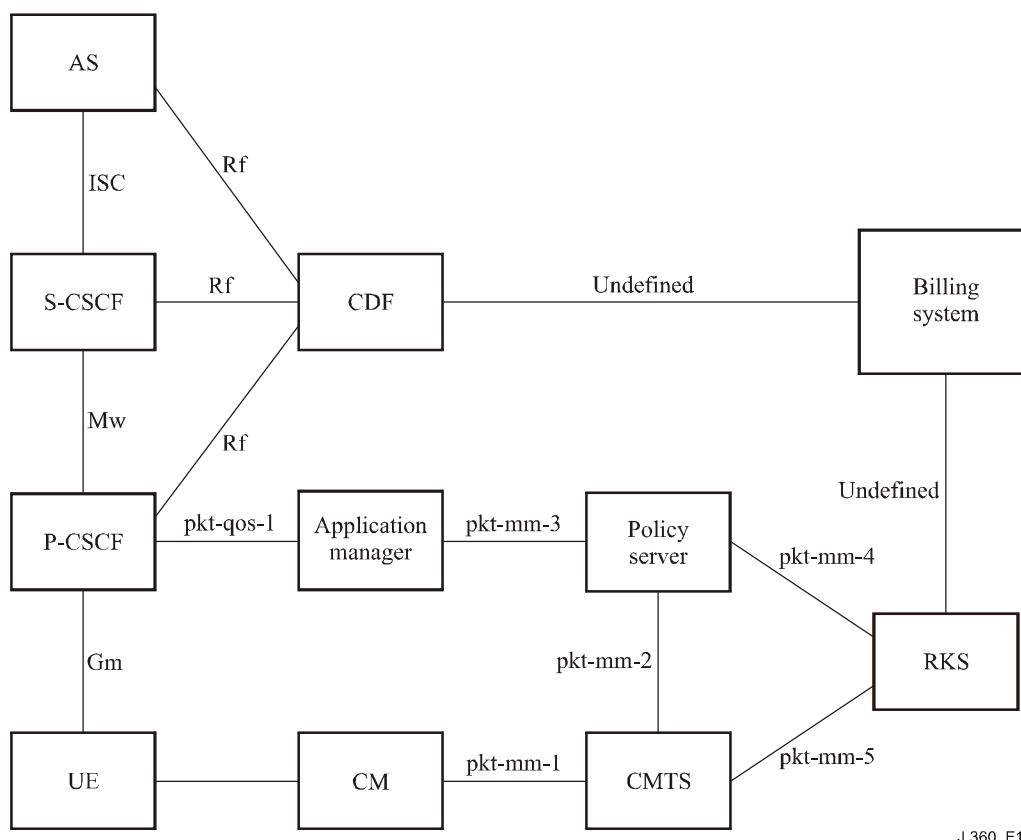


Figure 10 – Accounting reference points

The reference points depicted in Figure 10 are described in Table 8.

Table 8 – Accounting reference point descriptions

Reference point	IPCablecom network elements	Reference point description
Gm	UE – P-CSCF	Refer to Table 2.
Mw	P-CSCF – S-CSCF	Refer to Table 2.
ISC	S-CSCF – AS	Refer to Table 2.
Rf	CSCF – CDF	DIAMETER-based reference point from between the IMS nodes (P-CSCF, S-CSCF, and AS) to the charging data function (CDF).
pkt-qos-1	P-CSCF – Application manager	Refer to Table 4.
pkt-mm-1	CM – CMTS	Refer to Table 4.
pkt-mm-2	Policy server – CMTS	Refer to Table 4.
pkt-mm-3	Application manager – Policy server	Refer to Table 4.
pkt-mm-4	PS – RKS	RADIUS-based reference point between the PS and the record keeping server (RKS). This reference point is defined in IPCablecom multimedia [ITU-T J.179 App.I].
pkt-mm-5	CMTS – RKS	RADIUS-based reference point between the CMTS and the RKS. This reference point is defined in IPCablecom multimedia [ITU-T J.179 App.I].

Refer to the IP-Cablecom accounting specification [ITU-T J.363] for more information.

7.8 Security

The IP-Cablecom2 security architecture documents the security requirements reference points across the entire architecture. For the purpose of organizing the security reference points, three different trust domains have been defined.

- Intra-Network Domain – Reference points in this domain connect network elements within a service provider's domain.
- Inter-Network Domain – Reference points in this domain connect two domains. The domains can be different service providers, or the same provider.
- Access Domain – Reference points in this domain allow UEs to connect to a service provider.

These trust domains are used to decompose the IP-Cablecom architecture.

Refer to the IP-Cablecom2 Security Overview (Appendix III) for more information.

7.8.1 Access domain security

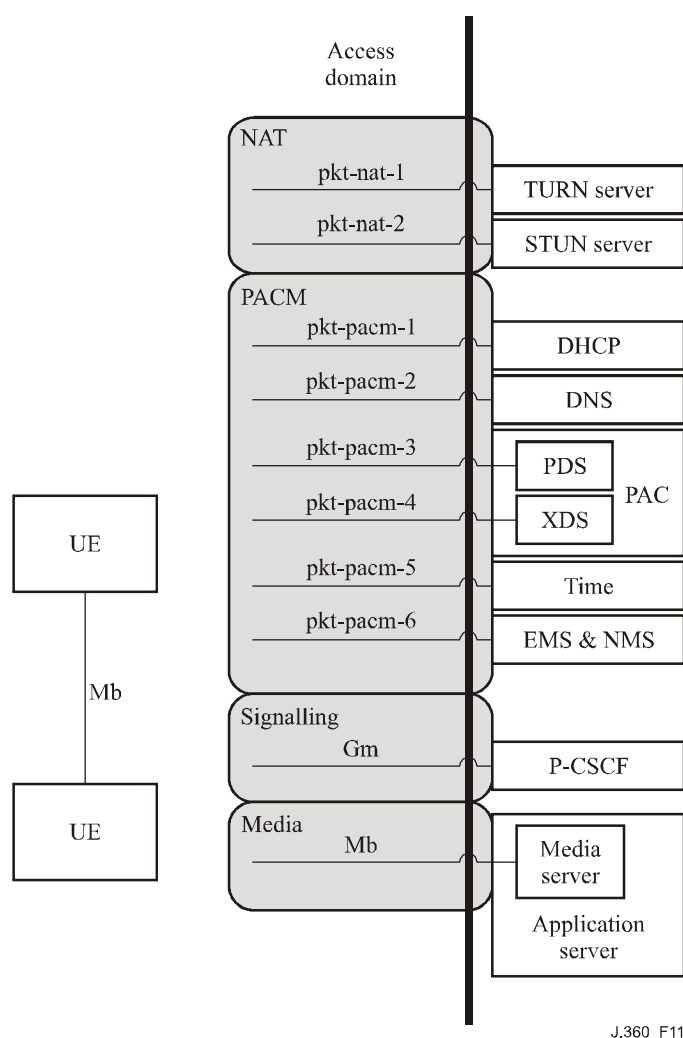


Figure 11 – Access domain reference points