International Telecommunication Union

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

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/.

CONTENTS

ITU-T Recommendation J.360

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 IPCablecom 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. IPCablecom2 defines enhancements to the IMS in order to ensure IPCablecom addresses requirements that are not already addressed by the IMS.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 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 IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

IPCablecom2 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), *IPCablecom security specification.*

[ITU-T J.171.1] ITU-T Recommendation J.171.1 (2005), *IPCablecom trunking gateway control protocol (TGCP): Profile 1*.

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

[ITU-T J.179 App.I] ITU-T Recommendation J.179 (2005), *IPCablecom support for multimedia*. Appendix I: *Background information*.

[ITU-T J.361] ITU-T Recommendation J.361 (2006), *IPCablecom2 codec media.*

[ITU-T J.362] ITU-T Recommendation J.362 (2006), *IPCablecom2 control point discovery*.

[ITU-T J.363] ITU-T Recommendation J.363 (2006), *IPCablecom2 data collection to support accounting.*

[ITU-T J.364] ITU-T Recommendation J.364 (2006), *IPCablecom2 provisioning, activation, configuration and management.*

[ITU-T J.365] ITU-T Recommendation J.365 (2006), *IPCablecom2 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*.

[TS 23.002] 3GPP 23.002 v6.10.0, *Network Architecture*, December 2005.

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 IPCablecom 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 IPCablecom.

3.5 IPCablecom 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 IPCablecom2

The IPCablecom2 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 IPCablecom2 architecture and specifications.
- A list of IPCablecom2 Recommendations.

5.1 Relationship with the 3GPP IMS

IPCablecom2 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 IPCablecom goal to leverage existing industry standards whenever possible is an objective to align with the IMS architecture and specifications being developed by 3GPP. Specifically, IPCablecom2 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 IPCablecom 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. IPCablecom2 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 IPCablecom 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 IPCablecom2 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 IPCablecom enhancements to the IMS include:

- Support for Quality of Service (QoS) for IMS-based applications on DOCSIS access networks, leveraging the IPCablecom 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.

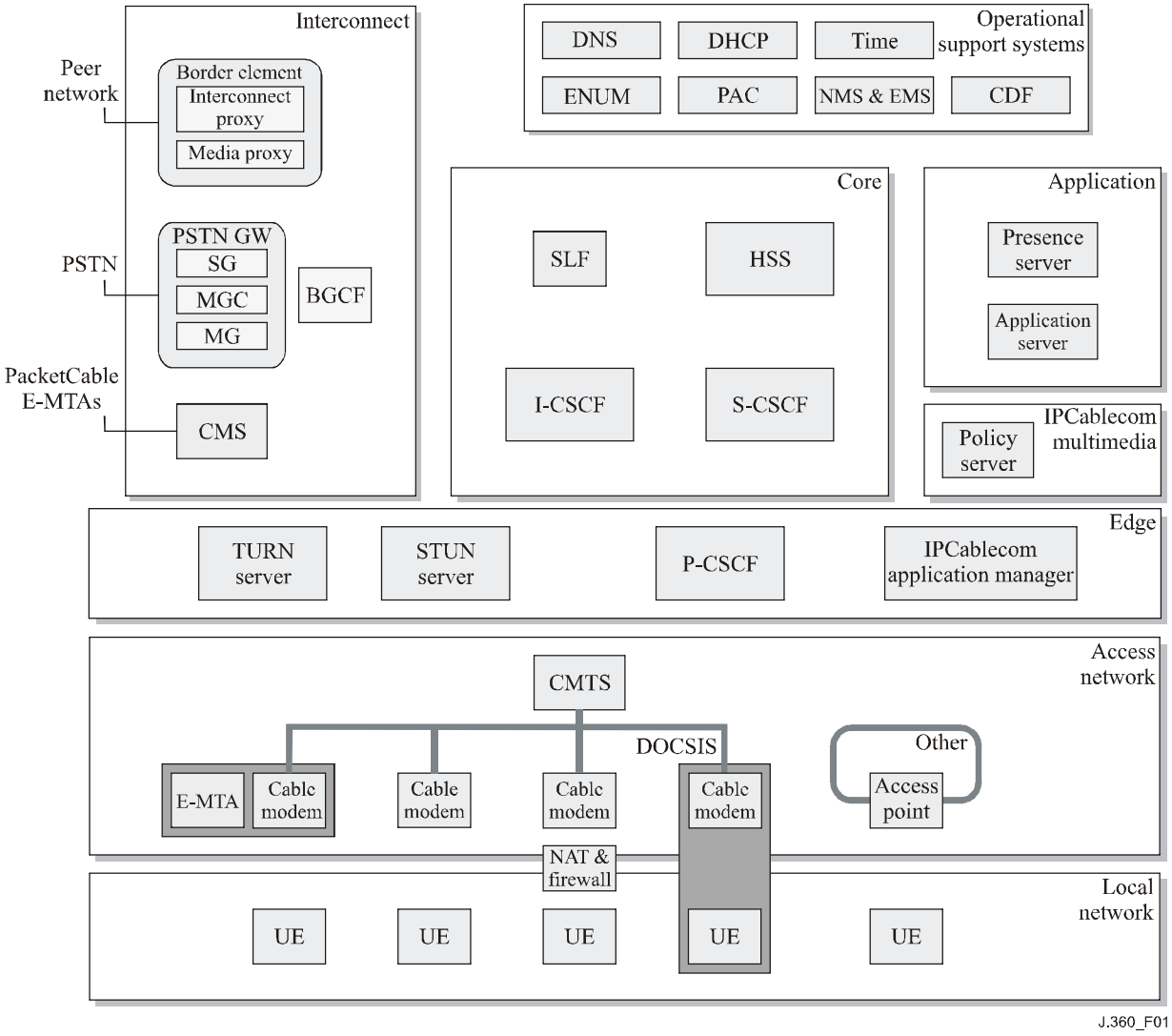


Figure 1 – IPCablecom reference architecture

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 IPCablecom 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 IPCablecom 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 IPCablecom releases and organization

5.3.1 IPCablecom releases

The IPCablecom 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 IPCablecom 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 IPCablecom 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.

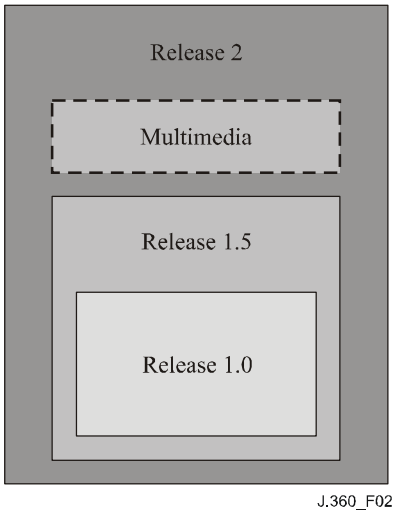


Figure 2 – IPCablecom releases

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.

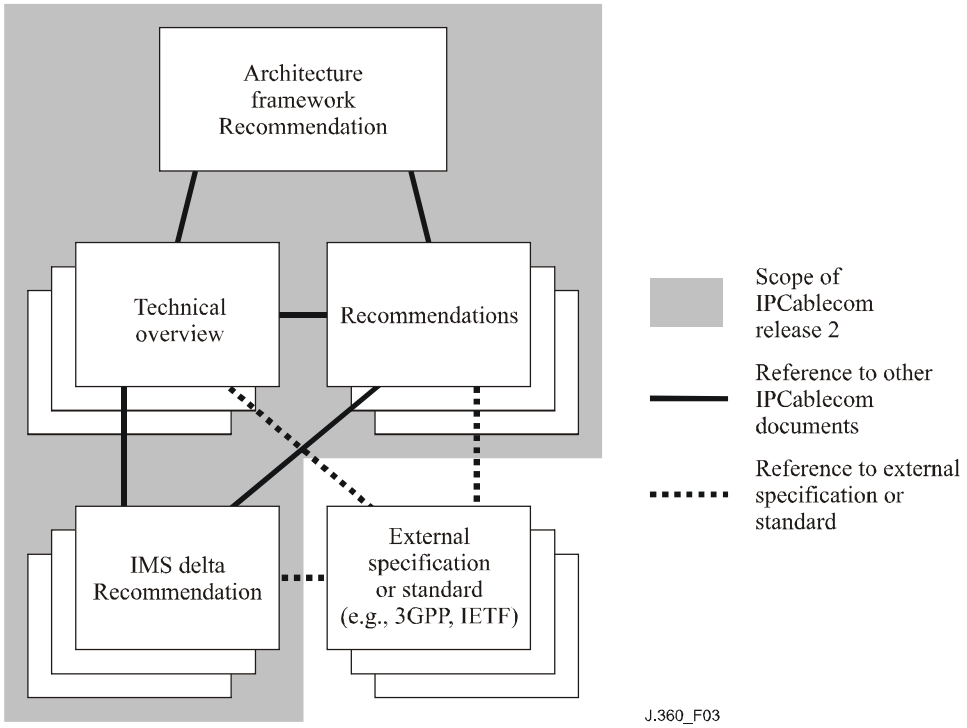


Figure 3 – IPCablecom2 organization

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 – IPCablecom2 Recommendations

IPCablecom2 Recommendations reference number	Document name
J.360	Architecture framework (this Recommendation)
Appendix I	IPCablecom2 SIP Signalling Overview
Appendix II	IPCablecom2 QoS Overview
Appendix III	IPCablecom2 Security Overview
Appendix IV	IPCablecom2 Home Subscriber Server (HSS) Overview
Appendix V	IPCablecom2 NAT and Firewall Traversal Overview
Appendix VI	IPCablecom2 IPv6 and IPv4 Strategy Overview
IPCablecom Recommendation reference number	**Recommendation name**
J.362	IPCablecom2 control point discovery
J.365	IPCablecom2 application manager interface
J.364	IPCablecom2 provisioning, activation, configuration and management
J.361	IPCablecom2 codec media
J.363	IPCablecom2 data collection to support accounting
IMS delta specification reference number	**Document name**
J.366.0	Overview of IPCablecom2 IMS Delta Recommendations
J.366.1	IPCablecom2 Organization of Subscriber Data Specification 3GPP TS 23.008
J.366.2	IPCablecom2 IP Multimedia Call Model Stage 2 Specification 3GPP TS 23.218
J.366.3	IPCablecom2 IP Multimedia Subsystem Stage 2 Specification 3GPP TS 23.228
J.366.4	IPCablecom2 SIP and SDP Stage 3 Specification 3GPP TS 24.229
J.366.5	IPCablecom2 Cx and Dx Interfaces Specification 3GPP TS 29.228
J.366.6	IPCablecom2 Cx and Dx Interfaces, Diameter Protocol Specification 3GPP TS 29.229
J.366.7	IPCablecom2 Access Security for IP-Based Services Specification 3GPP TS 33.203
J.366.8	IPCablecom2 Network Domain Security Specification 3GPP TS 33.210
J.366.9	IPCablecom2 Generic Authentication Architecture Specification 3GPP TS 33.220

As described in clause 1.2, this IPCablecom2 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 IPCablecom functional components

This clause provides additional detail on each of the functions in the IPCablecom architecture.

6.1 Local network

6.1.1 User equipment (UE)

IPCablecom supports NCS-based clients for telephony services. IPCablecom multimedia provides a service agnostic QoS and accounting framework. IPCablecom2 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, IPCablecom 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 IPCablecom 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 IPCablecom 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 IPCablecom 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. IPCablecom Multimedia defines a means for IP-enabled services to request QoS from the DOCSIS network. IPCablecom defines how QoS can be provided for SIP-based services via IPCablecom multimedia and DOCSIS.

6.2.3 Access point

IPCablecom 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 IPCablecom multimedia

IPCablecom 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 IPCablecom (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 IPCablecom CMS is customized for the delivery of residential telephony services, the IPCablecom multimedia components offer a general-purpose platform for cable operators to deliver a variety of IP-based multimedia services that require QoS treatment.

The IPCablecom 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. IPCablecom defines an IPCablecom application manager which is described in clause 6.3.3. The policy server, which is a unique IPCablecom 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 IPCablecom-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). IPCablecom 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 IPCablecom 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 IPCablecom elements deliver IPCablecom-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

IPCablecom2 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 IPCablecom2. These reference points are identified by their naming convention:

- IMS: Two or three letters (e.g., Gm, ISC);
- IPCablecom2 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 IPCablecom2 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

IPCablecom2 signalling and service control reference points are illustrated in Figure 4. Most reference points are IMS-defined, with appropriate deviations for IPCablecom as identified in various IPCablecom specifications. IPCablecom-specific reference points are also included.

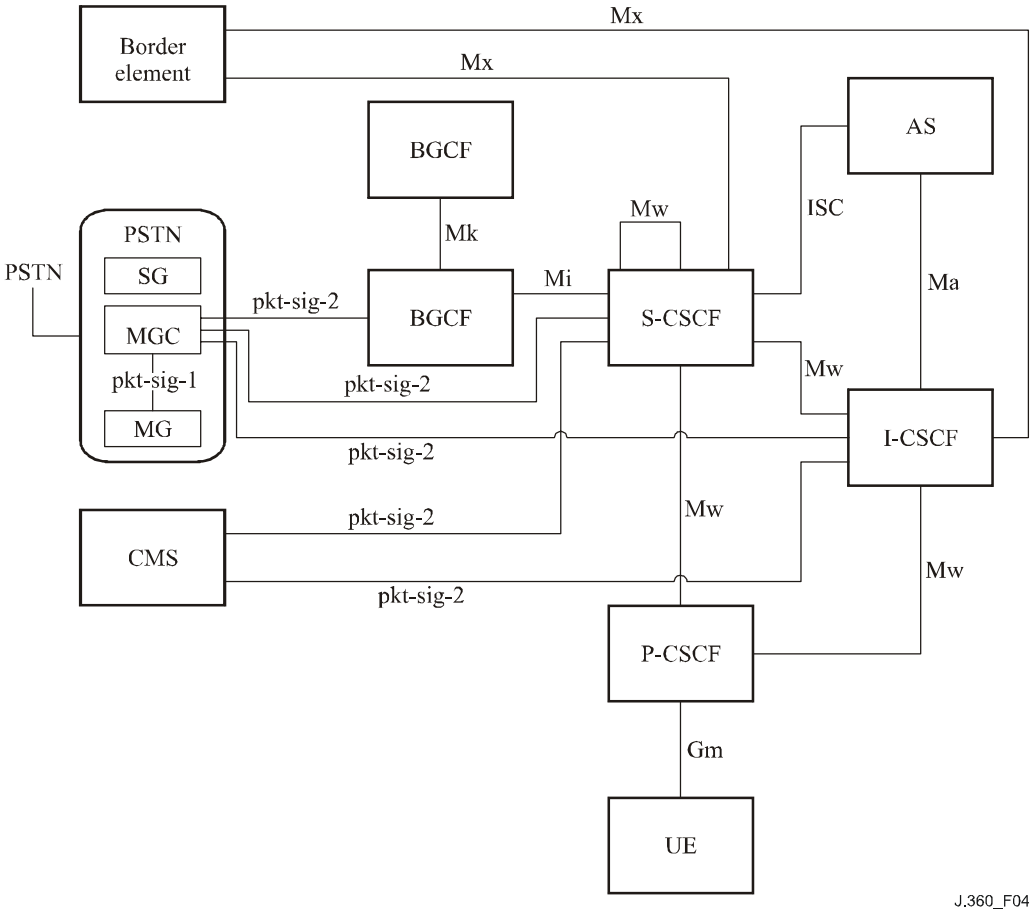


Figure 4 – Signalling reference points

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	IPCablecom 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 IPCablecom 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 IPCablecom CMS to CMS Signalling Specification [ITU-T J.178]. Allows IPCablecom E-MTAs to establish voice sessions with IPCablecom elements. Also allows the BGCF, I-CSCF, and S-CSCF to exchange session signalling with an IPCablecom MGC for the purpose of interworking with the PSTN.

Refer to the IPCablecom2 SIP signalling overview (Appendix I) for more information.

7.2 Subscriber data

IPCablecom 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.

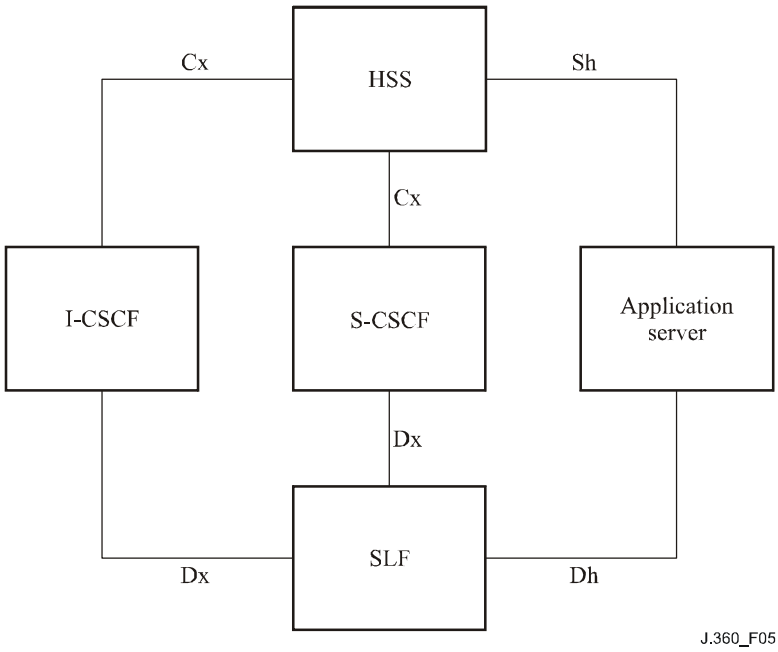


Figure 5 – Subscriber data reference points

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

Table 3 – Subscriber data reference point descriptions

Reference point	IPCablecom 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 IPCablecom HSS Overview (Appendix IV) for more information.

7.3 Quality of service

The quality of service approach for IPCablecom2 is based on IPCablecom multimedia. In the original IPCablecom 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 IPCablecom2 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 IPCablecom SIP architecture and the IPCablecom multimedia architecture. Its function is to receive QoS messages from the P-CSCF and to formulate appropriate messages to the IPCablecom multimedia policy server. While this AM function could be integrated into an IPCablecom 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.

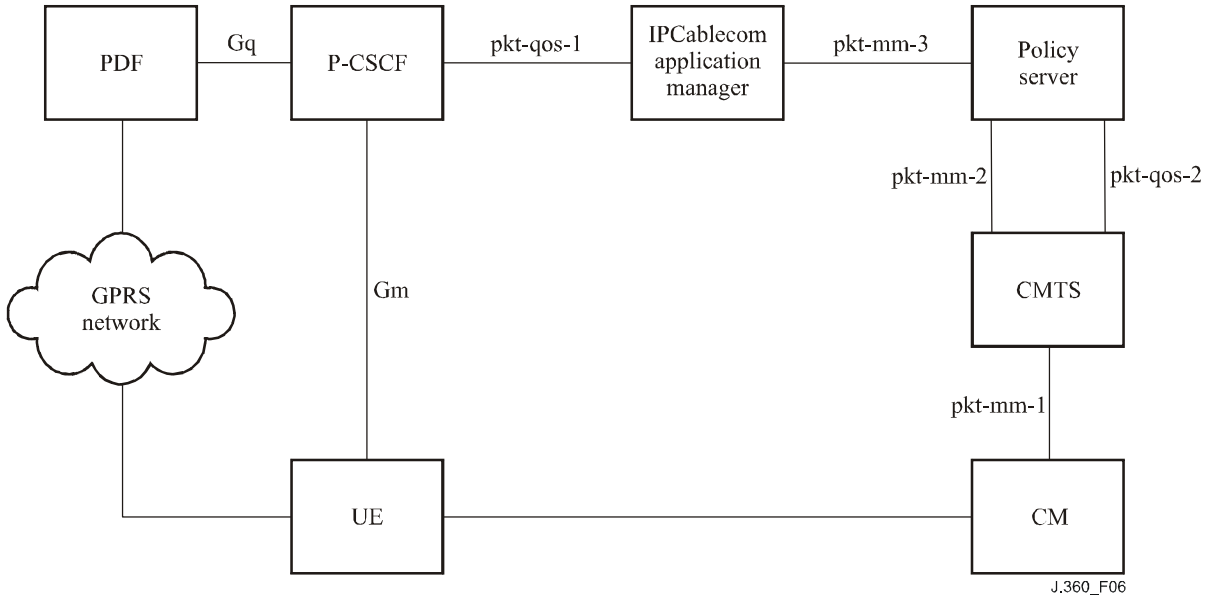


Figure 6 – QoS reference points

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.

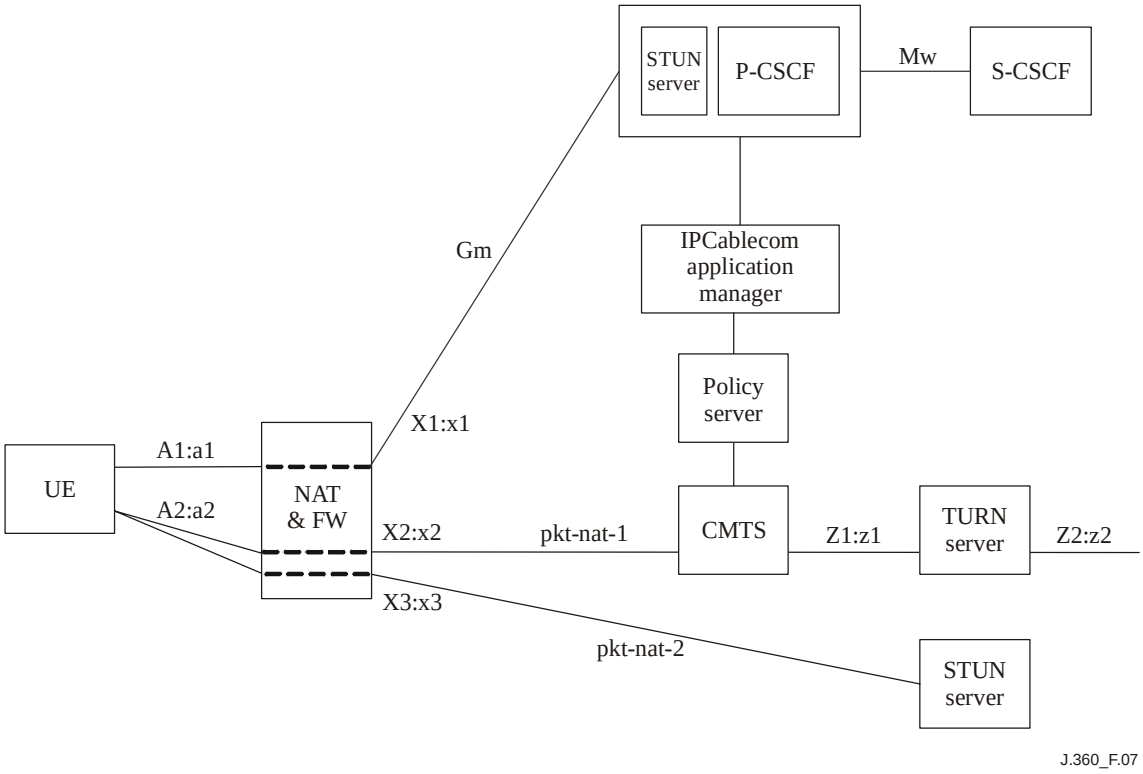


Figure 7 – NAT and FW traversal reference points

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

Table 5 – NAT and FW traversal reference point descriptions

Reference point	IPCablecom 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 IPCablecom 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.

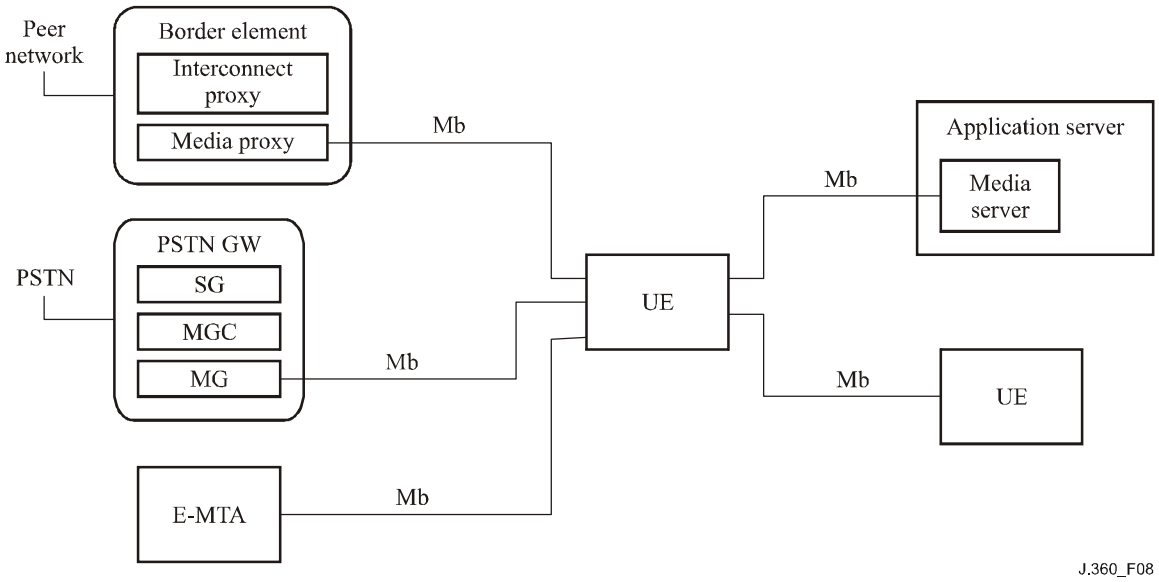


Figure 8 – Media stream reference points

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.

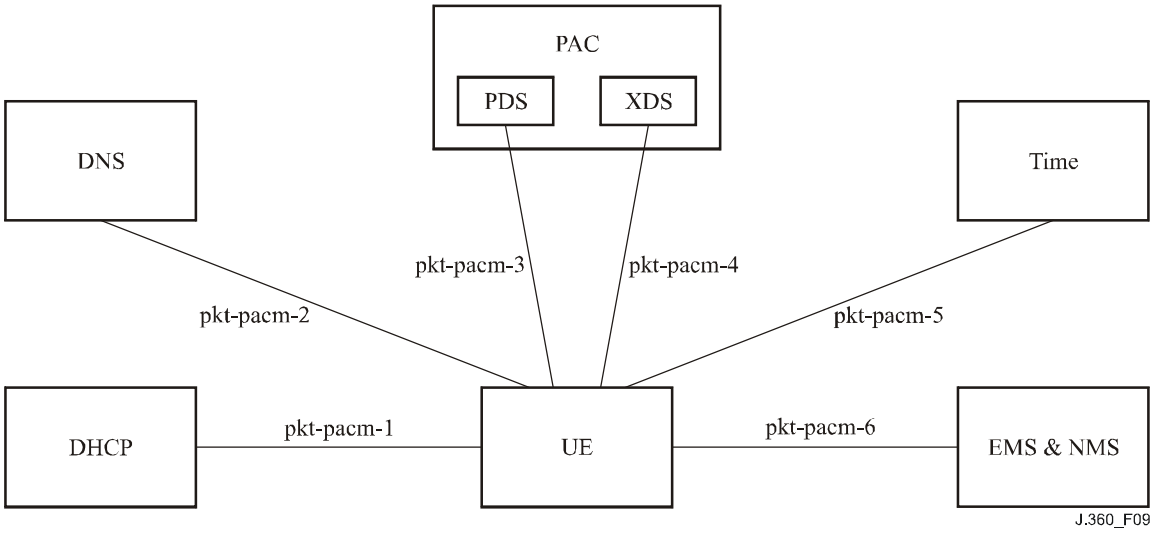


Figure 9 – PACM reference points

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.

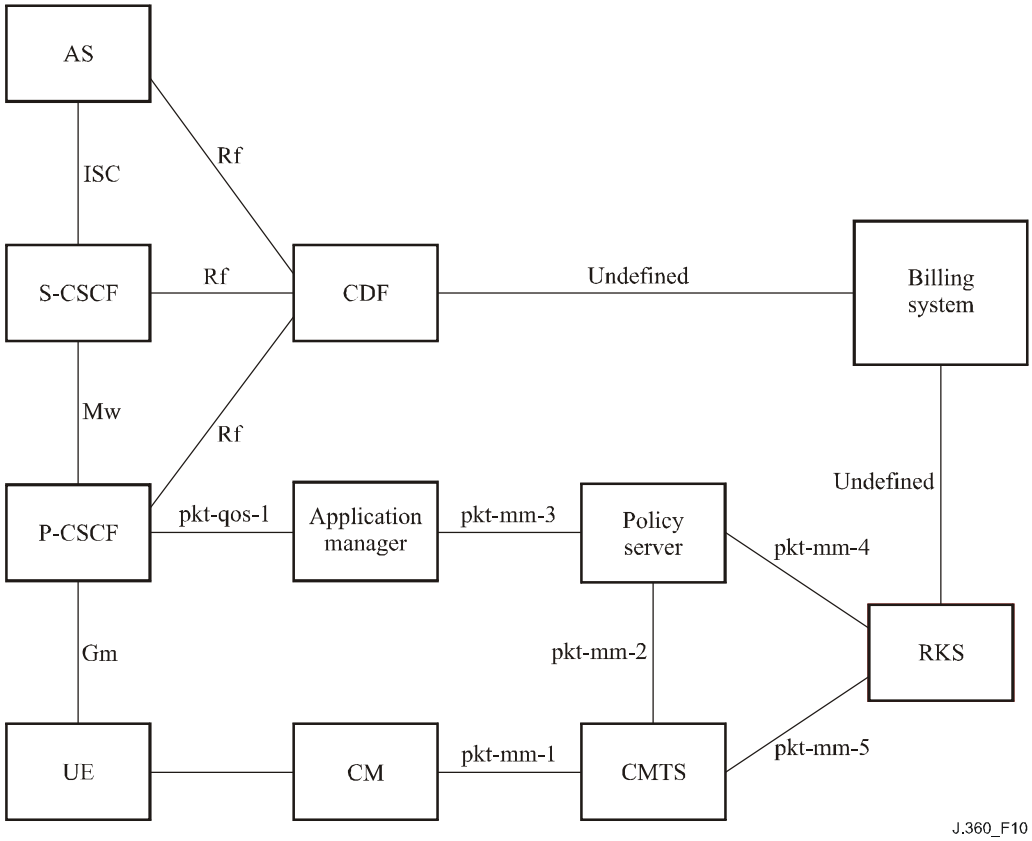


Figure 10 – Accounting reference points

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 IPCablecom accounting specification [ITU-T J.363] for more information.

7.8 Security

The IPCablecom2 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 IPCablecom architecture.

Refer to the IPCablecom2 Security Overview (Appendix III) for more information.

7.8.1 Access domain security

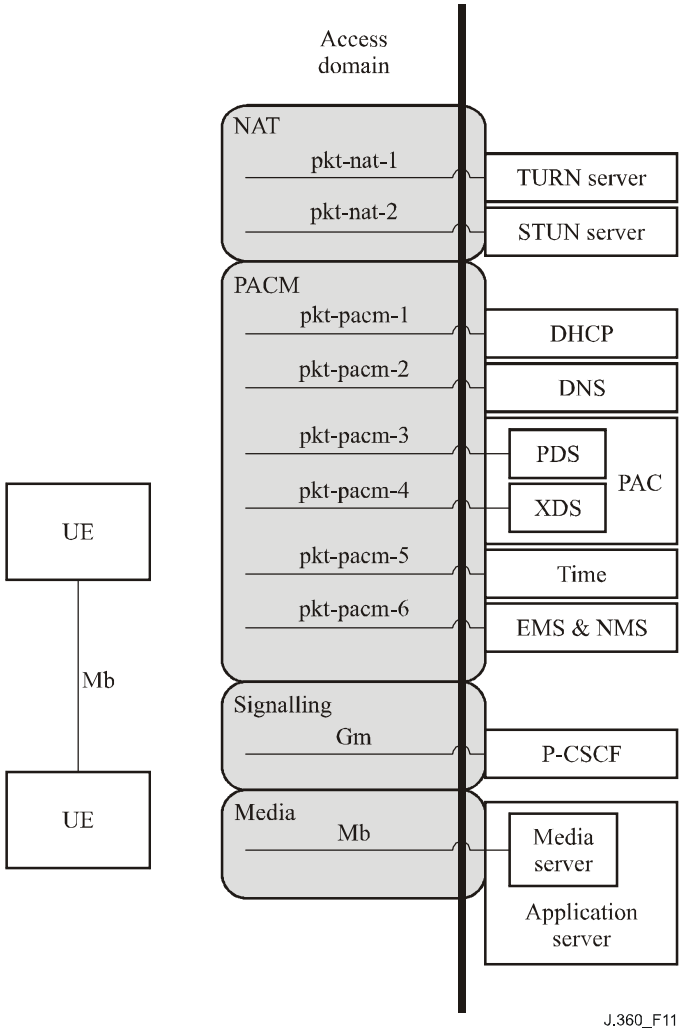


Figure 11 – Access domain reference points

UE interactions with the network occur in the access domain. Access methods are varied, and include DOCSIS and wireless. Due to these characteristics, the access domain is home to a multitude of threats, as described in Appendix III. Table 9 provides a high-level overview of how the access domain reference points are secured.

Table 9 – Access domain reference point descriptions

Reference point	IPCablecom network elements	Reference point description
pkt-nat-1	UE – TURN server	TURN: TURN requests are authenticated and authorized within the TURN protocol itself.
pkt-nat-2	UE – External STUN server	STUN: Message integrity is provided by STUN mechanisms.
pkt-pacm-1	UE – DHCP server	DHCP: IPCablecom does not define security for the DHCP protocol.
pkt-pacm-2	UE – DNS server	DNS: IPCablecom does not define security for the DNS protocol.
pkt-pacm-3	UE – PDS server	SIP: Message integrity and privacy via Internet Protocol Security (IPSec) or transport layer security (TLS).
pkt-pacm-4	UE – XDS server	XCAP: Message integrity and privacy via HTTP over TLS.
pkt-pacm-5	UE – Time server	SNTP: IPCablecom does not define security for the SNTP protocol.
pkt-pacm-6	UE – EMS & NMS server	Management interface security is out of scope for this Specification.
Gm	UE – P-CSCF	SIP: Message integrity and privacy via IPSec or TLS. STUN: Message integrity is provided by STUN mechanisms.
Mb	UE – UE UE – MG UE – Border element UE – AS UE – E-MTA	RTP: Media security is out of scope for this Specification. NOTE – Figure 11 only shows a few representative media flows.

7.8.2 Intra-network domain security

Intra-network domain reference points and components are contained within a service provider's network, and consequently, a holistic security policy. These reference points are generally secured using the Zb reference point. The Zb reference point uses IPSec encapsulating security payload (ESP). Zb reference points that support TCP may also use TLS.

The following Intra-domain reference points define additional security requirements that may be applied in addition to, or in place of, the Zb reference point:

- pkt-qos-2 – Cryptographic challenge mechanism defined by the control point discovery protocol.
- pkt-laes-4 – Cryptographic mechanisms defined by SNMPv3.
- pkt-laes-6 – Cryptographic challenge mechanism defined by the control point discovery protocol.

7.8.3 Inter-network domain security

The inter-network domain reference points consist of:

- Border element – Peer network – Secured using the Za reference point, which uses IPSec ESP. Inter-domain traffic in the IMS is required to pass through a security gateway (SEG). The SEG supports the Za reference point and enforces security policy on inter-domain traffic flows. It is assumed that the border element includes the SEG functionality, but the SEG may be a separate element.
- PSTN gateway – PSTN – PSTN security is not defined.
- CMS – Endpoints – Security for the CMS reference point is defined in the IPCablecom security specification [ITU-T J.170].

7.9 Lawful intercept

The IPCablecom2 lawful intercept architecture is illustrated in Figure 12. IPCablecom call control elements, such as the CSCFs, form the set of potential call related data intercept access points. IPCablecom bearer plane elements, such as the CMTS and MG, form the set of potential call content intercept access points. The delivery function (DF) receives intercepted call related events and call content from the IPCablecom intercept access points, correlates them to a target subscriber service, and then delivers the result to the law agency collection function (CF) over a standard reference point defined by [ES-DCI]. Note that the DF is not part of the IPCablecom architecture, although IPCablecom specifies reference points to the DF needed for the lawful interception with IPCablecom networks. Call control elements such as the S-CSCF and P-CSCF assigned to a target subscriber report call related events to the DF. These control elements also dynamically provision peer elements for intercept during call redirects and third party call control scenarios. Border elements, such as the BGCF, I-CSCF and MGC report interconnection carrier information to the DF. The DF provisions the call content intercept access points by first discovering the access points via the control point discovery protocol and then provisioning intercept on the content access points with SNMPv3. The call content provisioning process is initiated when the DF first receives a call initiation event from the call control elements.

The IPCablecom CMS is upgraded to interoperate with IPCablecom elements to support the interception of calls across NCS and SIP components. The IPCablecom MGC and MG elements may, as an option, be upgraded for the IPCablecom reference points in Figure 12.

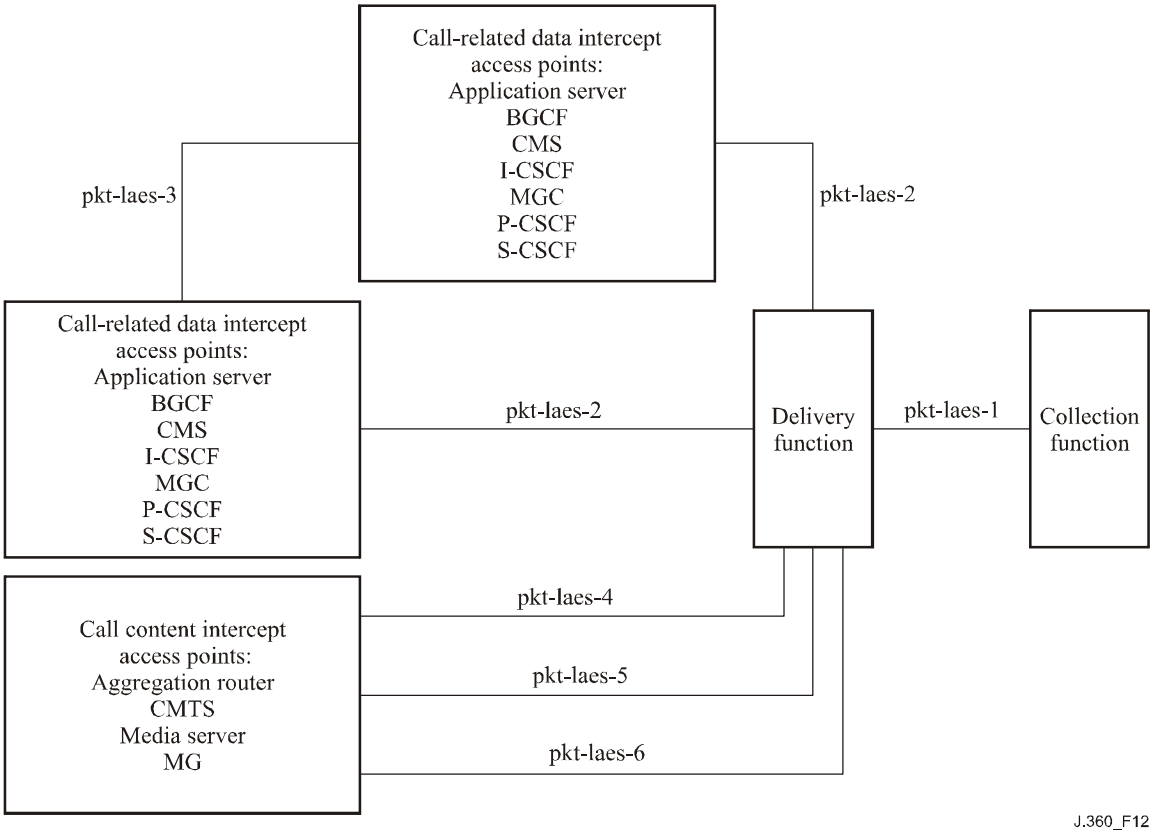


Figure 12 – Lawful intercept reference points

The reference points depicted in Figure 12 are described in Table 10.

Table 10 – Lawful intercept reference point descriptions

Reference point	IPCablecom network elements	Reference point description
pkt-laes-1	DF – CF	Correlated call related data and call content are reported to the law agency collection function. Defined in [ES-DCI].
pkt-laes-2	Session control element – DF	Intercept call related events are reported to the DF. This reference point is DIAMETER based.
pkt-laes-3	Session control element – Session control element	Allows session control elements to dynamically provision intercept in peer elements for calls where the targeted subject's assigned control elements are no longer involved in the call. Call redirect is one example. This reference point is SIP based.
pkt-laes-4	DF to content access points	The DF dynamically provisions content intercept points. This reference point is SNMPv3 based.
pkt-laes-5	Content access point to DF	Intercepted call content is reported to the DF. This reference point is media over UDP based.
pkt-laes-6	DF to content access points	The DF, as the Requestor, uses the control point discovery protocol [ITU-T J.362] to determine the appropriate call content IAPs, acting as control points, in the network for call content intercept.

Refer to the IPCablecom electronic surveillance – Intra-network functions specification [ES-INF] and the IPCablecom electronic surveillance – Delivery function to collection function interface specification [ES-DCI] for more information.

7.10 Control point discovery

The control point discovery reference point, shown in Figure 13, defines a network-based protocol that can be used to find the IP address needed in order to make requests for QoS as well as for content tapping for the purposes of lawful intercept (LI).

For QoS requests, this applies to finding the IP address of the CMTS for DQoS and IPCablecom multimedia (PCMM). For LI it applies to discovering the IP address to use for content tapping at the CMTS as well as media gateways and aggregation routers/switches in front of media endpoints. In addition to providing the IP address, the response indicates the protocol to use and can also indicate the subnet that the requested destination address is contained within.

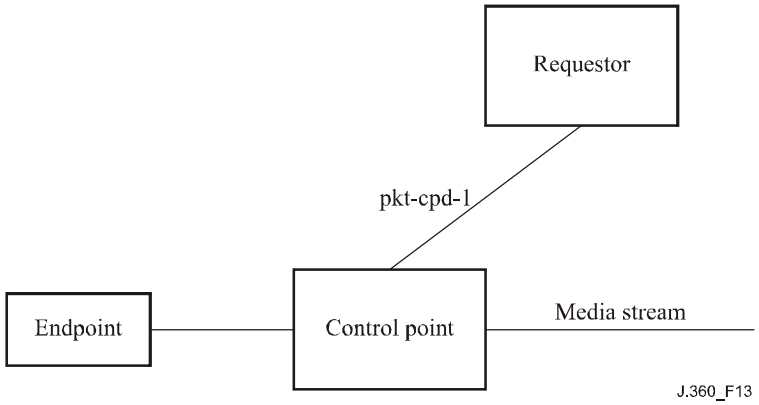


Figure 13 – Control point discovery reference point

The reference points depicted in Figure 13 are described in Table 11.

Table 11 – Control point discovery reference point description

Reference point	IPCablecom network elements	Reference point description
pkt-cpd-1	Requestor – Control point	The requestor uses the control point discovery protocol to determine the appropriate control point in the network for a given UE. Other reference points in the architecture are based on this reference point.

Refer to the IPCablecom2 Control Point Discovery Specification [ITU-T J.362] for more information.

Appendix I

SIP signalling overview

(This appendix does not form an integral part of this Recommendation)

I.1 Introduction and purpose

This appendix provides an overview of the SIP signalling architecture and describes the high-level requirements to support SIP communications within the IPCablecom2 architecture.

The primary focus of this appendix is to define how the IPCablecom2 functional elements involved in session signalling communicate based on the IETF SIP protocol and extensions, and to specify the enhancements made to 3GPP IMS.

Since IPCablecom2 SIP signalling is closely aligned with IMS, the IPCablecom2 SIP signalling normative requirements are defined in IMS Delta specifications, which are 3GPP specifications enhanced to accommodate cable-specific requirements. The IPCablecom2 SIP signalling requirements are documented in three IMS Delta specifications, ITU-T Recs J.366.2, J.366.3 and [ITU-T J.366.4].

I.1.1 Relationship to IPCablecom features and services

This appendix and its associated IMS Delta specifications serve as a SIP signalling foundation for support of a wide variety of IP-based communication services, ranging from legacy telephony features to new and enhanced communication applications and services. This SIP signalling base is service independent; and, therefore, requirements specific to each IPCablecom service and feature are out-of-scope for this appendix, and are defined separately. The relationship between this appendix, the base SIP signalling IMS Delta specifications, and the IPCablecom features and services is shown in Figure I.1.

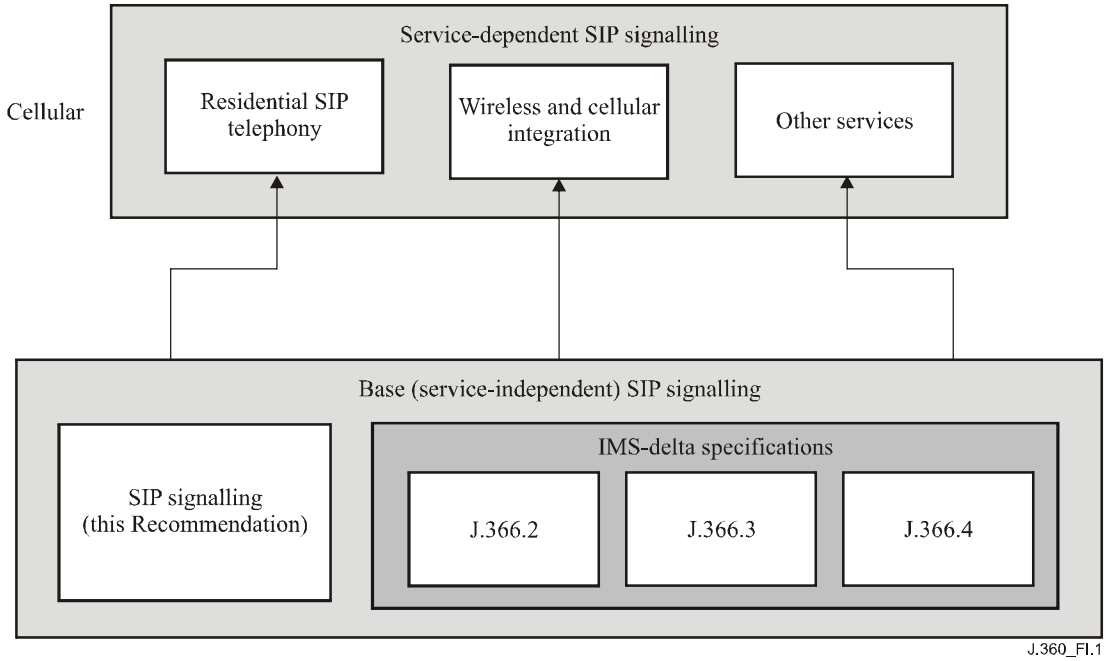


Figure I.1 – Relationship between base SIP signalling and services

I.1.2 Relationship to other IPCablecom2 specifications

The IPCablecom2 base SIP signalling specifications together define the signalling requirements for the following general capabilities:

- SIP message routing.
- Registration.
- Media session establishment.
- Event-Notification framework.
- Generic service control platform.
- Identity assertion.

Other IPCablecom2 specifications such as accounting, NAT traversal, and security, place additional requirements on SIP signalling; and therefore, impact the same IMS Delta specifications, specifically [ITU-T J.366.4]. Also, certain SIP signalling mechanisms impact non-SIP IMS Delta specifications such as [ITU-T J.366.5]. Finally, IPCablecom2 SIP signalling places requirements on [ITU-T J.178] to support IPCablecom2 UE to IPCablecom E-MTA interworking. The relationship among these various specifications is shown in Figure I.2.

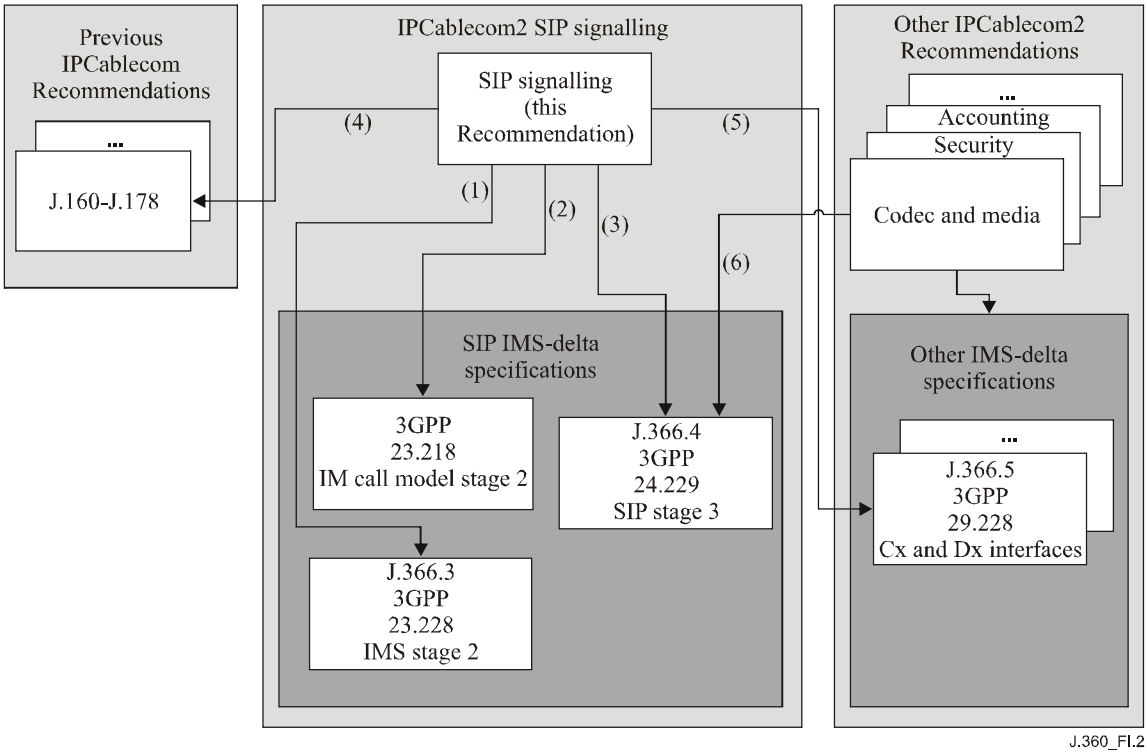


Figure I.2 – SIP signalling specification relationships

I.2 References

This appendix uses the following additional informative references.

[ITU-T J.366.4] ITU-T Recommendation J.366.4 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification.* (3GPP TS 24.229)

[ITU-T J.366.5] ITU-T Recommendation J.366.5 (2007), *IP multimedia (IM) subsystem Cx and Dx interfaces; signalling flows and message contents specification*. (3GPP TS 29.228)

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

[IETF RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).*

[IETF RFC 3311] IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method*.

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp).*

[IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).*

[IETF RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*

[IETF RFC 3486] IETF RFC 3486 (2003), *Compressing the Session Initiation Protocol (SIP).*

[IETF RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth*.

[IETF RFC 3680] IETF RFC 3680 (2004), *A Session Initiation Protocol (SIP) Event Package for Registrations*.

[IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

I.3 Terms and definitions

This appendix uses the following additional terms and definitions:

I.3.1 authorized identity: An instance of an 'Authorized Identity' in an IPCablecom2 network is a representation of an allowed pairing between a Private Identity and a Public Identity.

I.3.2 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 locator function (SLF), and home subscriber server (HSS).

I.3.3 identity credentials: A collection of the information needed to perform authentication of a private identity. The actual information depends on the authentication mechanism.

I.3.4 IPCablecom2 service provider: A network operator, operating one or more independent IPCablecom2 Administrative Domains.

I.3.5 IPCablecom2 service provider DNS domain: A DNS domain name that is owned and managed by an IPCablecom2 administrative domain. It is used to form SIP URIs that convey public identifiers.

I.3.6 proxy server: An intermediary SIP entity that acts as both a server and a UE for the purpose of making requests on behalf of other UEs. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.

I.3.7 public identifier: An identifier used to reference a public identity.

I.4 Abbreviations and acronyms

This appendix uses the following additional abbreviation:

SIP UE User equipment that contains a SIP user agent

I.5 IPCablecom2 SIP signalling

IPCablecom2 applications and services are controlled using session initiation protocol (SIP). IPCablecom2 aligns with a specific instance of the SIP architecture as defined by the IP multimedia subsystem (IMS) specifications being developed by the 3rd generation partnership project (3GPP). IPCablecom2 is based on Release 6 of IMS, and enhances IMS where necessary to support IPCablecom2 requirements.

I.5.1 IPCablecom2 SIP signalling architecture and reference points

IPCablecom2 signalling and service control reference points are illustrated in Figure I.3. Most reference points are IMS-standard, with appropriate deviations for IPCablecom2 as identified in various IPCablecom2 specifications. IPCablecom2-specific reference points are also included.

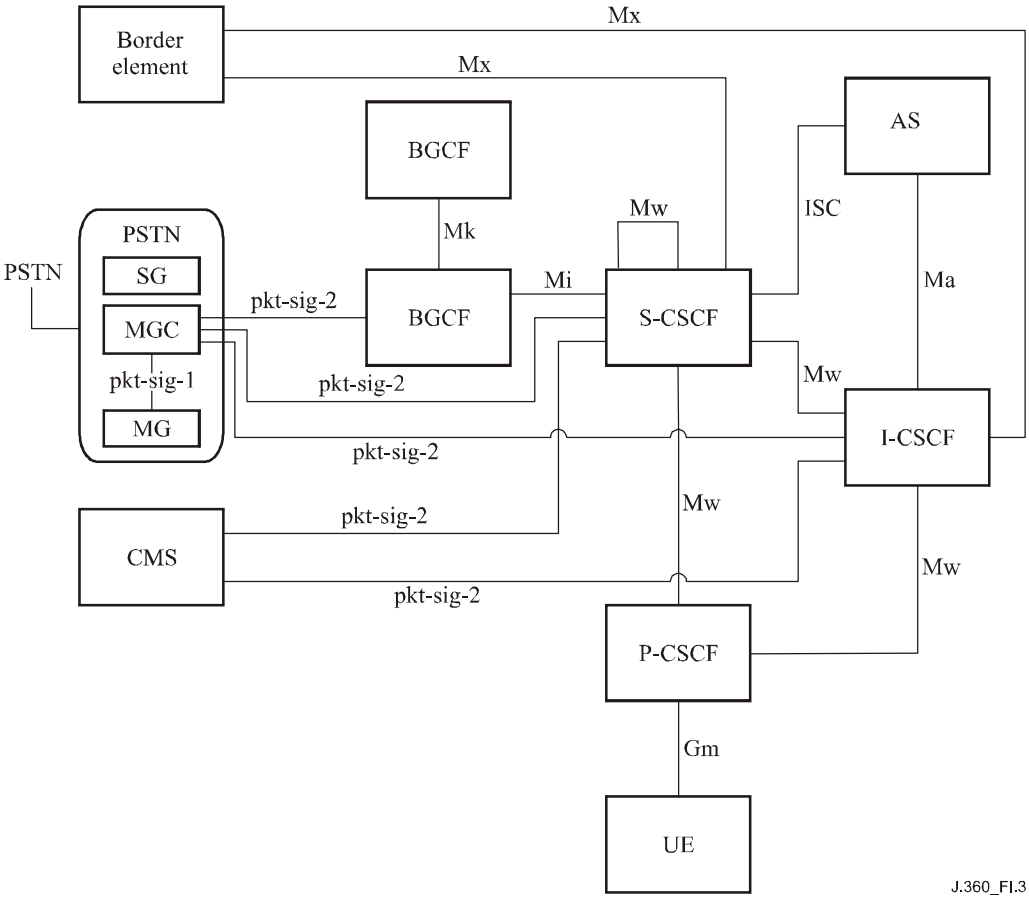


Figure I.3 – Call signalling reference points

I.5.1.1 SIP signalling functional components

I.5.1.1.1 User equipment (UE)

IPCablecom2 supports SIP clients with a variety of forms and capabilities, e.g., soft and hard phones, smart phones, wireless and wired phones, instant messaging applications, video communications terminals, etc. Consistent with IMS, IPCablecom2 clients are called user equipment (UE). All of the various UEs 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.

I.5.1.1.2 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 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). The P-CSCF provides the following functions:

- Routes SIP messages from the UE to the I-CSCF or S-CSCF and vice versa.
- Maintains security associations between itself and the UE and asserts the identity of authenticated public identities.
- Tracks the registration status of public identities, and removes security association with the UE when a public identity is deregistered by the network.
- Verifies the incoming messages data (e.g., verify the SIP route header).
- Blocks service (e.g., ignores certain incoming requests from unregistered public identities).
- Enforces policy (e.g., whether signalling security or compression is enabled or disabled).
- Generates accounting events.

I.5.1.1.3 Serving SCSF (S-CSCF)

The S-CSCF is responsible for providing services to UE-based subscribers. The S-CSCF does not, however, provide services to IPCablecom E-MTAs. Rather, E-MTAs are served by their CMS as described in [ITU-T J.160].

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

- SIP registrar function, which maintains data that dynamically binds registered public identifiers (AORs) to a set of contact addresses, assigns globally routable user agent URIs, 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, distributes user registration status to entities that subscribe to the Reg-Event package.
- SIP user authentication and authorization.
- Service control platform: Applies filter criteria to incoming dialog initiating requests, and based on service point triggers, routes requests to appropriate application servers to provide features and services.
- Routing of SIP messages to a P-CSCF for UEs served by the S-CSCF.
- Routing of SIP 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.
- Routing of messages to a peer I-CSCF for calls to a peer network.
- Routing of messages to the home I-CSCF THIG for topology hiding for calls to a peer network.
- 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 identifier 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 identifier.

- May query external routing databases such as ENUM, local number portability (LNP) and 800 number databases in order to determine where the call should be routed.
- Generation of accounting events.
- Monitoring the health of active sessions, and releasing sessions if a component in the signalling path fails (for example, the S-CSCF can release active sessions associated with, and on behalf of a failed UE).
- Network initiated release of sessions (e.g., due to administrative activity).

There may be multiple S-CSCFs in the IPCablecom core. At any one time, a subscription (and all the public identifiers associated with it) can only be handled by a single S-CSCF.

Public identifiers are assigned to an S-CSCF at registration time. Once a public identifier is assigned to an S-CSCF, all other registered instances of that public identifier must be assigned to the same S-CSCF. Also all public identifiers in the same subscription must be associated with the same S-CSCF. Subscription data is stored in one or more home subscriber server(s) (HSS). The S-CSCF interacts with 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.

Globally routable user agent URIs (GRUUs) are supported by the endpoints and the S-CSCF. This allows endpoints to be assigned a globally routable URI 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.

I.5.1.1.4 Interrogating CSCF (I-CSCF)

The I-CSCF is responsible for routing incoming requests to the correct terminating S-CSCF. It also provides a topology hiding interworking gateway function (THIG) that can be used to hide the internal topology of the home network from a peer network, or from a home UE.

- Routes incoming REGISTER messages received from the P-CSCF to the correct S-CSCF.
- Routes incoming dialog-initiating requests received from an originating S-CSCF in the home network or originating S-CSCF in a peer network to the correct terminating S-CSCF.
- Generation of accounting events.

The I-CSCF is the routing point in the network for external requests from other networks that are destined for users in the home network. It communicates with the HSS to determine the binding between a Subscription (and associated public identities) and an S-CSCF.

I.5.1.1.5 Application server (AS)

An AS provides value-added IPCablecom services and resides in either the user's home network or in a third party location, which could be another network or a stand-alone AS. An AS may influence a SIP session on behalf of its supported services and it may host and execute services. An AS may initiate services or terminate services on behalf of a user.

I.5.1.1.6 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. The border element can provide a variety of functions:

- 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 relay between peer networks (e.g., for media security or codec interworking).
- Address and topology hiding at the signalling level (e.g., acts as a signalling relay and provides obfuscation of address information in headers).

I.5.1.1.7 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. The BGCF may query external routing databases to determine where the call should be routed.

I.5.1.1.8 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 functional elements are defined in previous releases of IPCablecom, and are reused in this release of IPCablecom2, with the addition of an IPCablecom2 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.

I.5.1.1.9 Call management server (CMS)

An IPCablecom call management server (CMS) provides support for telephony services for NCS clients (i.e., E-MTAs). In IPCablecom2 the CMS provides most of the telephony features while, interacting directly with application servers (unified messaging servers, conference servers, etc.) to provide additional applications to NCS endpoints. It does not allow, however, for features to operate transparently across E-MTAs and UEs owned by the same user.

I.5.1.2 SIP signalling reference points

The reference points depicted in Figure I.3 are described in Table I.1. All reference points are SIP-based except where noted.

Table I.1 – Call signalling reference points

Reference point	IPCablecom2 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.

Table I.1 – Call signalling reference points

Reference point	IPCablecom2 network elements	Reference point description
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.
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 IPCablecom TGCP specification [ITU-T J.171.1].
pkt-sig-2	CMS – S-CSCF CMS – I-CSCF MGC – BGCF MGC – S-CSCF MGC – I-CSCF	Allows the S-CSCF and I-CSCF to exchange session signalling with the CMS to enable IPCablecom E-MTAs to establish voice sessions with UEs. Also allows the BGCF, I-CSCF and S-CSCF to exchange session signalling with the MGC for the purpose of interworking with the PSTN.

I.5.2 IPCablecom2 enhancements to IMS

While many of the components and interfaces defined in the IMS have broad applicability in other industries, Release 6 of the IMS is still 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. IPCablecom2 enhances 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 IPCablecom2 will align with these newer releases as necessary.

I.5.2.1 Cable broadband access

Radio access is typically limited by scarce resources and high latency. Therefore, IMS mandates support of special mechanisms and SIP extensions to mitigate these limitations. Since cable broadband access does not have the bandwidth resource or latency limitations typical of radio access, support of these capabilities is made optional for IPCablecom2.

UE support of the following SIP extensions, which is mandatory for IMS Release 6, is made optional for IPCablecom2.

I.5.2.1.1 Bandwidth modifiers for RTCP

[IETF RFC 3556] adds SDP attributes to enable a UE to explicitly specify the maximum RTCP bandwidth it wishes to receive from the remote UE. This enables an IMS UE to reduce its radio access resource usage by specifying a low (may be zero) RTCP bandwidth value. For IPCablecom2, support of the RTCP bandwidth modifiers is optional at the UE. If the UE supports this extension, then it must honour the RTCP bandwidth attributes when received in order to support interworking with IMS UEs that use these parameters. Also, the UE must be able to send the RTCP bandwidth modifiers based on a locally configured value (the configured value may be based on the type of access network).

I.5.2.1.2 P-Associated-URI

[IETF RFC 3455] defines a P-Associated-URI header that is used as part of implicit registration to inform the UE of the multiple public identities in the implicit registration set. This reduces the registration message traffic, since multiple public identities can be registered with a single transaction. For IPCablecom2, support of P-Associated-URI header is optional at the UE.

I.5.2.1.3 SIP compression

[IETF RFC 3486] provides a SIP message compression capability that reduces signalling bandwidth usage and latency on the radio access network. Support of SIP compression at the UE is optional for IPCablecom2. The P-CSCF controls whether SIP compression is enabled or not, based on locally configured data, or on the access network type reported in the P-network-access-info header.

I.5.2.1.4 SIP timers

IMS modifies (lengthens) the SIP message timing intervals to reduce the signalling load on the access network, and to tolerate the increased latency of radio access. For IPCablecom2, the UE must conform to the standard SIP timing intervals specified in [IETF RFC 3261].

I.5.2.2 Modularity

IPCablecom2 is required to support modularity at the UE, to promote interworking with non-3GPP SIP endpoints, and to enable operators to tune deployments to specific service offerings. Therefore, some of the SIP extensions that are mandated by IMS Release 6 are made optional for IPCablecom2.

I.5.2.2.1 Reliable provisional response

[IETF RFC 3262] defines a SIP request called PRACK that is used to enable early 2-way media and to ensure reliable delivery of provisional responses. For IPCablecom2, support of PRACK is mandatory at the UE, and its use must be configurable to one of the following two modes:

1) Required – The UE must include option tag "100rel" in SIP Require header of the INVITE request, so that it is able to establish sessions only with other UEs that also support PRACK.
2) Negotiated – The UE must include option tag "100rel" in the SIP Supported header of the INVITE request so that it can negotiate whether PRACK is actually used or not based on whether or not it is also supported by the remote UE.

I.5.2.2.2 Update

[IETF RFC 3311] defines a SIP request called UPDATE that is used to update media sessions before answer (primarily for preconditions). Support of UPDATE in IPCablecom2 is mandatory at the UE (i.e., UE must always advertise in Allow header), but optional to use. For example, the UE can choose not to send UPDATE if it knows the remote UE does not support it based on what was received in the incoming Allow header.

I.5.2.2.3 Reg event package

[IETF RFC 3680] defines a new event package called Reg-Event that is used by the network to inform the UE that it has been de-registered. The network can use this event package to block a UE from gaining access to network services, or to trigger a UE to re-register for S-CSCF re-assignment. For IPCablecom2, support of the Reg event package is optional at the UE. If supported, the UE must provide configuration controls to disable its use.

I.5.2.2.4 P-access-network-info header

[IETF RFC 3455] defines a SIP header called P-access-network-info which enables the UE to inform the network of the access technology (e.g., radio, 802.11, DOCSIS). For IPCablecom2,

support of the P-Access-Network-Info is optional at the UE. If this header is supported, then the UE will report P-Access-Network-Info only if it knows the type access technology that it is using. For example, an embedded MTA may know that its network access is over DOCSIS, while a soft client may not know whether its access is over DOCSIS or WiFi.

I.5.2.2.5 Disabling signalling security

IPCablecom2 mandates support of signalling security for both the UE and the P-CSCF. However, the P-CSCF must support configuration parameters that enable signalling security between the UE and P-CSCF to be disabled. The P-CSCF must support three modes that apply to all UE signalling associations with the P-PCSCF:

1) Signalling security off – Signalling security is always off across all UEs served by the P-CSCF.
2) Signalling security on – Signalling security is enabled for all UEs served by the P-CSCF.
3) Signalling security negotiated – Signalling security is on for UEs that support it (note that signalling security support is mandatory for IPCablecom2 UEs), and off for UEs that do not support it.

I.5.2.3 Services

The base IPCablecom2 architecture needs to support some additional basic capabilities required by services such as residential SIP telephony and wireless and cellular integration that are not supported in IMS Release 6.

I.5.2.3.1 Tel URI number portability and carrier routing

For IPCablecom2, support of number portability is optional for the S-CSCF and mandatory for the MGC. The BGCF may support addition of a network-wide pre-subscribed carrier. Support of these parameters is optional for the UE. Note that a UE that supports the Tel URI must support these parameters as well.

I.5.2.3.2 Globally routable user agent URI (GRUU)

GRUU defines a mechanism whereby a registrar can provide a globally routable contact address to a registering user agent. This is required by certain features such as call-transfer that require the ability to route a dialog-initiating request to a specific registered instance of an AOR, when multiple registered instances exist. For IPCablecom2, support of GRUU is optional at the UE, but mandatory for the network components that are impacted by GRUU (e.g., S-CSCF). A UE that supports GRUU must resort to using the AOR as a contact address when interworking with remote UEs that do not support GRUU.

I.5.2.3.3 Internet-draft – GRUU Reg-event package

Implicit registration enables multiple public identities to register under a single REGISTER transaction. The response to REGISTER can carry only a single GRUU URI. Therefore, when both GRUU and implicit registration are supported, there needs to be a way to communicate multiple GRUUs to the UE. This is accomplished using an extension to the Reg event package that enables multiple GRUU URIs to be communicated in a NOTIFY to the Reg event package.

I.6 IPCablecom2 IMS requirements

This clause describes the requirements that are currently not supported in IMS Release 6, but that are needed in the IPCablecom2 SIP signalling architecture.

I.6.1 SIP secure signalling

IPCablecom2 allows signalling security to be disabled between the UE and the P-CSCF. This clause first outlines the signalling security model defined in 3GPP for IMS communications and then

describes the impacts to IMS for allowing access to IMS-services without secure SIP signalling between the UE and P-CSCF.

I.6.1.1 Description

The IMS security architecture [ITU-T J.366.7] is based on several mandatory security relationships, two of which are closely coupled with IMS registration procedures:

1) Mutual authentication between the user and network.

2) Security association between the UE and P-CSCF, which provides integrity protection and optional confidentiality protection of SIP signalling (i.e., signalling security).

According to IMS registration procedures, the UE first sends an initial REGISTER request to the P-CSCF which routes the request to the S-CSCF serving the user. Since a security association has not yet been established between the UE and P-CSCF, the initial REGISTER request is sent unprotected. The S-CSCF determines that the received REGISTER request was sent unprotected by checking the "integrity-protected" parameter in the SIP authorization header. Because the REGISTER request was sent unprotected and the user is not already registered, the S-CSCF initiates the mutual authentication procedures by generating a 401 (Unauthorized) response to the unprotected REGISTER request, and the S-CSCF starts a reg-await-auth timer.

After receiving the 401 (Unauthorized) response, the UE establishes a set of security associations with the P-CSCF. The UE then sends a second REGISTER request containing the authentication challenge response, which is sent protected over the newly established security association and routed to the same S-CSCF. Because the REGISTER request was sent protected and an authorization procedure is ongoing for this user (i.e., a reg-await-auth timer is running for this particular user), the S-CSCF authenticates the user by verifying the authentication challenge response. Once the S-CSCF successfully completes registration procedures, a 200 (OK) response is sent to the UE.

With the exception of an initial REGISTER request, IMS requires all SIP messages to and from the UE to be sent protected over the security association. The security association also provides data origin authentication, which enables the P-CSCF to assert the identity of the UE.

Signalling security is a mandatory capability of the UE in the IPCablecom2 SIP architecture. However, IPCablecom2 allows signalling security to be disabled in the following ways:

1) the UE may be configured [ITU-T J.364] to have signalling security disabled; or

2) the P-CSCF may be configured to have signalling security disabled for all UEs that access IMS services through that P-CSCF.

In addition, there are certain requests that may not require signalling security. In IPCablecom2 IMS, the only such request is subscription to the ua-profile event package.

I.6.1.2 Impacted components

This clause describes the IMS components impacted by allowing access to IMS-services without secure SIP signalling between the UE and P-CSCF, as well as the nature of the impact on the component.

NOTE – Additional security considerations for disabling signalling security are documented in Appendix III.

I.6.1.2.1 UE

An IPCablecom2 UE must support the negotiation and establishment of security associations as described in IMS. However, while disabling security is not recommended, an IPCablecom2 UE must be flexible to be able to interoperate in an operator environment where signalling security procedures have been disabled.

In IPCablecom2, a security association is not initiated by the UE in the following scenarios:

- The UE receives an indication from the P-CSCF during initial registration that signalling security is disabled.
- The UE is configured to have signalling security disabled as described in [ITU-T J.364], and the UE has not received an indication from the P-CSCF during initial registration that signalling security is required.

If the UE includes the "sec-agree" option tag in the Require header as defined in [IETF RFC 3329] when sending an initial REGISTER request and a 420 (Bad Extension) response is received with the "sec-agree" option tag value in the Unsupported header, the UE should resend the REGISTER request and not follow the procedures defined in [IETF RFC 3329].

If the UE is configured to have signalling security disabled and the UE has not received a 494 (Security Agreement Required) response, the UE must not follow the procedures described in [IETF RFC 3329].

If the UE successfully registers without having established a security association, then the following applies for any initial request or stand-alone transaction (excluding REGISTER):

- If the UE supports the P-Preferred-Identity header, the UE must insert it and set its value to a registered public user identity of the user.
- If the UE does not support the P-Preferred-Identity header, the UE shall ensure that the From header field is set to a registered public user identity of the user. In this case, privacy may not be supported.

Subscription requests to the ua-profile event package may be allowed prior to registration, based on local policy. If the UE is not registered, then the following applies for SUBSCRIBE requests to the ua-profile event package:

- The UE must include the From header and set its value to the public user identity derived as described in clause I.6.13: "Routing SUBSCRIBEs for configuration information".
- If the UE supports the P-Preferred-Identity header, the UE must insert it and set its value to the same public user identity included in the From header field.

I.6.1.2.2 P-CSCF

In IPCablecom2, the P-CSCF must support signalling security requirements as defined in Appendix III.

The P-CSCF may be configured to have signalling security "disabled" or "required" for all UEs that access IMS-services through that P-CSCF. The P-CSCF may also be configured to have signalling security "optional"; in this case, the P-CSCF determines whether signalling security is disabled for a particular UE based on an indication received from the UE during initial registration.

If the P-CSCF is configured to have signalling security "optional" or "disabled", then the following applies:

- The P-CSCF must accept REGISTER requests that do not contain the "sec-agree" option tag in the Require header as defined in [IETF RFC 3329]. In this case, the P-CSCF must ignore the security mechanism agreement related procedures specified in [ITU-T J.364].
- The P-CSCF should allow unprotected non-REGISTER requests.

If the P-CSCF is configured to have signalling security "disabled", then the following applies:

- The P-CSCF must accept REGISTER requests that do not contain the "sec-agree" option tag in the Require header as defined in [IETF RFC 3329]. In this case, the P-CSCF must ignore the security mechanism agreement related procedures specified in [ITU-T J.366.4].
- If the P-CSCF receives a REGISTER request from a UE that includes the "sec-agree" option tag in the Require header as defined in [IETF RFC 3329], the P-CSCF must reject the request with a 420 (Bad Extension) response and include the "sec-agree" option tag in the Unsupported header.
- The P-CSCF should allow unprotected non-REGISTER requests.

If the P-CSCF is configured to have signalling security "required", then the following applies:

- If the P-CSCF receives a REGISTER request from a UE that does not contain the "sec-agree" option tag in the Require header as defined in [IETF RFC 3329], the P-CSCF shall reject the request with a 494 (Security Agreement Required) response.

The P-CSCF should assert the identity of the request originator (i.e., insert a P-Asserted-Identity header), and remove the P-Preferred-Identity header, if present, only for non-REGISTER requests received over a security association.

If the P-CSCF receives a non-REGISTER request that does not contain a Route header (i.e., a request from an unregistered user), the P-CSCF shall forward the request to the I-CSCF of the served user.

I.6.1.2.3 I-CSCF

In IPCablecom2, the I-CSCF must support signalling security requirements as defined in Appendix III.

I.6.1.2.4 S-CSCF

In IPCablecom2, the S-CSCF must support signalling security requirements as defined in Appendix III.

The S-CSCF may be configured to have signalling security "required" for all UEs that access IMS-services through that S-CSCF. The S-CSCF may also be configured to have signalling security "optional"; in this case, the S-CSCF accepts unprotected REGISTER requests that are authenticated. The configuration of the S-CSCF and P-CSCF must be coordinated by the operator.

If the S-CSCF and P-CSCF are configured to allow access to IMS-services without secure SIP signalling for one or more UE, then the following applies:

- If the S-CSCF receives a REGISTER request and authentication is currently ongoing for this user (i.e., the timer reg-await-auth is running), then the S-CSCF shall perform the registration procedures specified in [ITU-T J.366.4] as if the "integrity-protected" parameter in the Authorization header was set to "yes".
- While performing origination processing for a registered public user identity, if the S-CSCF receives a request that is missing a P-Asserted-Identity header that is otherwise required by [ITU-T J.366.4], then:
  - The S-CSCF shall identify the originator based on the value contained in the P-Preferred-Identity header, if present, or the From header, if the P-Preferred-Identity header is absent.
  - If the request contains a valid authentication response, the S-CSCF shall insert a P-Asserted-Identity header and remove the P-Preferred-Identity header, if present.
  - If the request does not contain a valid authentication response, the S-CSCF should challenge the request by generating a 401 (Unauthorized) response.

If the S-CSCF receives a SUBSCRIBE request to the ua-profile event package from an unregistered but known public user identity, the S-CSCF should perform origination processing as if the user was registered.

I.6.1.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for SIP secure signalling: [ITU-T J.366.4].

I.6.2 Support of IPv4 and IPv6

I.6.2.1 Description

[ITU-T J.366.4] specifies that UEs and IMS subsystem entities are assigned IPv6 addresses. As part of the 3GPP IMS Release 7 support for "Fixed Broadband", this is being extended to allow UEs and IMS subsystems to be assigned IPv4 addresses, IPv6 addresses, or both. IPCablecom2 requires IPv4 support and both types of addresses must be supported by IPCablecom2 UEs and IMS components.

Some procedures in [ITU-T J.366.4] are explicitly described as specific to IPv6. Such procedures are not applicable to IPv4 clients (i.e., "Change of IPv6 address due to privacy").

I.6.2.2 Impacted components

Changes required for support of IPv4 are incorporated into [ITU-T J.366.4]. This 3GPP change request includes the following relevant changes:

- Changes for URI and address assignments, to allow IPv4, IPv6, or both to be assigned to IMS subsystem entities and UEs (clause 4.2 of [ITU-T J.366.4]).
  - Use of IPv6 in IPCablecom2 is planned for further study. Use of IPv4 only is initially assumed. The change is included per the 3GPP changes.
- Modifications of the S-CSCF procedures, by generalizing a procedure that checks for an IP address type in SDP, in an error scenario where the far end indicates the address type is not supported (clause 5.4.3.2 of [ITU-T J.366.4]).
  - Interworking between an IPv4-based IPCablecom2 network and IPv6-based networks is planned for further study, but this change is included to incorporate all related changes from the 3GPP R7 CR.
  - Modifications of the UE procedures for P-CSCF discovery to references relevant to IPv4 DHCP procedures (clause 9.2.1 of [ITU-T J.366.4]).
  - This particular change is not relevant to IPCablecom2 since alternate procedures are used for P-CSCF discovery, but it is included to incorporate all related changes from the 3GPP R7 CR.

I.6.2.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for Support of IPv4 and IPv6: clauses 4.2, 5.4.3.2 and 9.2.1 of [ITU-T J.366.4].

I.6.3 SIP compression

I.6.3.1 Description

3GPP IMS Release 6 [ITU-T J.366.4] mandates the UE and P-CSCF to support signalling compression (SigComp) as defined in [IETF RFC 3320] and SIP compression as defined in [IETF RFC 3486]. SIP compression is mandated to minimize delays over low bandwidth 3GPP access. For the cable broadband access part of IPCablecom2, this set of considerations does not apply. Note that, as part of the 3GPP IMS Release 7 support for "Fixed Broadband", the support and use of SIP compression is made optional for UEs using broadband access technology, and use

of SIP compression by the P-CSCF (e.g., when supported by the client) is not required if the UE is using broadband access technology.

IPCablecom2 incorporates these 3GPP IMS Release 7 changes for SIP compression: Support for signalling compression (SigComp) as defined in [IETF RFC 3320] and SIP compression as defined in [IETF RFC 3486] is optional for IPCablecom2 UE to implement and for P-CSCF to use.

The implementation of the above requirement is dependent upon the knowledge that the UE is on a cable broadband network using a new value for the access type for the P-Access-Network-Info header, representing DOCSIS broadband access network technology. Refer to clause I.6.12.1.2 for further details.

NOTE – The 3GPP IMS Release 7 solution may be subject to further study within 3GPP to determine if there are better ways to determine access delays and whether SIP compression should be utilized. As such, IPCablecom2 may re-align with any future changes made in this area.

I.6.3.2 Impacted components

The required changes are identified and incorporated into Release 7.

I.6.3.2.1 UE

Support of SigComp and SIP compression is optional for UEs that are intended for use on a broadband access network.

If SigComp and SIP compression are supported by the UE, SigComp and SIP compression should not be utilized by the UE if the UE is on a broadband access network (based on access type in P-Access-Network-Info), or the UE is unaware of the access type.

I.6.3.2.2 P-CSCF

Support of SigComp and SIP compression is required for the P-CSCF deployed in a cable broadband access network but its actual use is optional.

If SigComp is supported by the UE, the use of SIP compression should not be proposed by the P-CSCF if the UE is on a cable broadband access network (based on access type in P-Access-Network-Info), or if the access type is unknown.

I.6.3.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for SIP compression: Clause 8 of [ITU-T J.366.4].

I.6.4 Reliability of SIP provisional responses

I.6.4.1 Description

The reliability of provisional response in the SIP protocol is an extension defined in [IETF RFC 3262] in support of multiple applications. First, it is necessary when establishing sessions using the SIP preconditions extension. Secondly, it enables an SDP offer/answer exchange as part of an INVITE request and initial provisional response, which is required to support early media (for example, in certain PSTN interworking scenarios). Finally, it guarantees that the action taken by a UE on receiving a provisional response does in fact occur (e.g., guarantees that an originating UE applies ring-back tone on receiving a 180 response to INVITE).

3GPP IMS Release 6 mandates support of the reliability of provisional responses for the UE when initiating sessions, in support of the SIP preconditions extension. IPCablecom2 will update these requirements to enable the UE, based on configuration data, to interwork with non-3GPP UEs that do not support this SIP extension.

I.6.4.2 Impacted components

The impacts to enable a UE to interwork with endpoints that do not support the reliable provisional response SIP extension are localized to the UE itself.

I.6.4.2.1 UE

A UE that supports sessions must support the reliable provisional response extension as defined in [IETF RFC 3262].

A UE can be configured to require support of the reliable provisional response extension. In this case, session establishment with another UE that does not support the same extension will fail.

Alternatively, a UE can be configured to negotiate support of the reliable provisional response extension, so that the extension is used only if it is supported by both the initiating and terminating UE.

I.6.4.3 Impacted IMS Delta specifications

The following IPCablecom2 IMS Delta specification contains the necessary requirements for reliability of SIP provisional responses:

See clause 5.1 and Table A.4 of [ITU-T J.366.4].

I.6.5 SIP UPDATE

I.6.5.1 Description

The SIP UPDATE extension method defined in [IETF RFC 3311] allows a SIP client to update the parameters of a session. In particular, it is used in support of SIP preconditions [IETF RFC 3312].

3GPP IMS Release 6 mandates support of the UPDATE method as part of the preconditions extension. IPCablecom2 extends these requirements to enable optional use of UPDATE outside of preconditions. Specifically, an IPCablecom2 UE must support UPDATE, but should adopt procedures to maximize interworking with UEs that do not support UPDATE (e.g., substitute re-INVITE).

I.6.5.2 Impacted components

The impacts to enable a UE to interwork with endpoints that do not support the SIP UPDATE extension are localized to the UE itself.

I.6.5.2.1 UE

A UE must support UPDATE for sessions that are established using preconditions.

A UE can also require support of UPDATE for sessions that are established without preconditions. In this case, session establishment with another UE that does not support UPDATE will fail.

Alternatively, a UE can negotiate support of UPDATE for sessions that are established without preconditions, so that the extension is used only if it is supported by both the initiating and terminating UE.

I.6.5.3 IPCablecom2 impacted IMS Delta specifications

The following IPCablecom2 IMS Delta specification contains the necessary requirements for SIP UPDATE: See clause 5.1 and Table A.4 of [ITU-T J.366.4].

I.6.6 SIP preconditions

I.6.6.1 description

The support for preconditions in SIP, as defined in [IETF RFC 3312] and updated by [IETF RFC 4032], is an optional feature of the IPCablecom2 signalling architecture. Originally

mandated by IMS, the requirements for SIP preconditions have been relaxed. SIP Preconditions are not mandatory anymore in 3GPP IMS Release 6. The changes will be incorporated in the next version of the IMS Release 6 specifications.

I.6.6.2 Impacted components

This clause describes the component impacts for optional UE support of the SIP preconditions extension.

I.6.6.2.1 UE

IPCablecom2 UEs may support SIP preconditions. If supported, the UE must comply with [IETF RFC 3312] and [IETF RFC 4032].

The IPCablecom2 UE should negotiate the use of SIP pre-conditions. The UE should indicate its support for SIP preconditions in the appropriate SIP headers (Supported or Require) and it should be flexible in allowing the establishment of sessions with UEs that do not support preconditions. For example, a UE terminating a SIP dialog should include the "precondition" option tag in the Require header if the dialog-initiating request received from the originating UE contained an indication that SIP preconditions is supported with the "preconditions" option tag in the Supported header.

I.6.6.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for SIP preconditions: See clauses 5.1.3, 5.1.4 and 6.1 of [ITU-T J.366.4].

I.6.7 SDP bandwidth modifiers for RTCP

I.6.7.1 Description

Standard SDP does not provide a mechanism to explicitly control RTCP bandwidth. Instead, RTCP bandwidth is implicitly fixed at 5% of the session bandwidth. [IETF RFC 3556] introduces two new SDP bandwidth modifiers for RTCP that can be used to explicitly set the RTCP bandwidth to any value independent of the RTP session bandwidth. IMS uses this mechanism to limit the RTCP bandwidth to a value less than 5% (possibly zero) in deployments where radio access is scarce and expensive.

Since cable broadband access does not have the bandwidth resource restrictions of radio, there is no need to limit the RTCP bandwidth below the 5% default within the IPCablecom access network. However, there is value in having an IPCablecom2 UE support these bandwidth modifiers when received from an IMS UE, in order to avoid overrunning the RTCP bandwidth allocation in the IMS radio access network. Therefore, support of the RTCP bandwidth modifiers is made optional for IPCablecom2 UEs.

I.6.7.2 Impacted components

This clause describes the component impacts for optional UE support of the RTCP bandwidth modifiers.

I.6.7.2.1 UE

Support of [IETF RFC 3556] is optional for IPCablecom2 UEs deployed in a cable broadband access network.

I.6.7.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for SDP bandwidth modifiers for RTCP:

See clause 6 of [ITU-T J.366.4].

I.6.8 Registration state event package

The SIP event package for registration-state is an optional function of the IPCablecom2 UE.

I.6.8.1 Description

When a UE successfully performs initial registration, registration state is created in a SIP registrar (i.e., S-CSCF) for a list of URIs associated with the public user identity that was registered. The list of URIs includes the public user identity that was explicitly registered (unless it is barred), the associated set of implicitly registered public user identities, and possibly other associated public user identities.

The registration state of a URI in the list can change dynamically, for reasons such as:

- Network-initiated deregistration: According to local administrator policy, the network may deregister a public user identity. This might occur, for example, due to non-payment of bills.
- Network-initiated re-authentication: According to local administrator policy, the network may reduce the expiry time for a current registration, in order to force the UE to re-authenticate. This might occur, for example, when fraud is detected.
- Registration from multiple devices: The contact addresses bound to any URI in the list can change, due to registrations from other devices.

According to IMS registration procedures, the UE is required to subscribe to registration-state information after successful initial registration, and to maintain the subscription until all URIs in the list become deregistered. This subscription enables the SIP registrar to notify the UE of events such as changes to registration state (i.e., "active" to "terminated"), shortening of registration expiry timers, and modifications to contact address bindings.

I.6.8.2 Impacted components

This clause describes the component impacts for optional UE support of the Reg Event package.

I.6.8.2.1 UE

Support of "A SIP Event Package for Registrations" [IETF RFC 3680] is optional for the IPCablecom2 UE. If the UE does not support the registration-state event package described in [IETF RFC 3680], it does not perform procedures in [ITU-T J.366.4] related to subscription and notification of registration-state information.

The primary implications of non-support for [IETF RFC 3680] are:

- The UE does not receive explicit indication that additional AORs are implicitly registered, unless it supports the optional P-Associated-URI header (see clause I.6.12).
- The UE may become unregistered without its knowledge. If this occurs, the UE will be unable to receive requests, and most non-REGISTER requests sent by the UE will either be dropped or rejected by the P-CSCF depending on whether a security association did or did not exist (see clause I.6.1).

If the UE determines that it has been deregistered (e.g., a request is sent that times out or is rejected with an appropriate error code), the UE should attempt to recover using implementation specific procedures. As an example, the UE might perform network-initiated deregistration procedures as described in [ITU-T J.366.4].

If the UE supports the registration-state event package, it should also support the P-Associated-URI header in order to determine if the public user identity used for registration is barred (see clause I.6.12.2.1).

I.6.8.2.2 P-CSCF

There is no impact to the P-CSCF. In IMS, it is already possible (e.g., as an abnormal case) that the P-CSCF receive requests from UE that have unknowingly become deregistered. Such requests may increase if the IPCablecom2 network performs network-initiated deregistration or re-authentication, and there are UEs which do not support the registration-state event package.

I.6.9 Number portability

I.6.9.1 Description

IPCablecom supports local number portability and equal access carrier routing. This clause describes how number portability and carrier routing data is obtained and used in an IPCablecom2 network.

To support local number portability, the IPCablecom2 network should determine, when appropriate, whether or not the called number is ported. If the called number is ported to a PSTN destination, then the IPCablecom2 network should apply routing policy based on the LNP routing number, and also must pass the routing number and the LNP database dip indicator to the PSTN. The mechanism for obtaining the LNP data is out-of-scope and may vary based on the IPCablecom2 component that obtains the LNP data.

Existing IMS procedures define that the S-CSCF resolves a Tel URI containing an E.164 address to a SIP URI using an ENUM/DNS mechanism. IPCablecom2 assumes that when such a Tel URI resolves to a SIP URI, an LNP Query is not required by the IPCablecom2 network. In this case, the request may be routed based on the SIP URI. As such, it is assumed that the ENUM/DNS Server containing the E.164 address to SIP URI mapping is synchronized with LNP porting procedures. The procedures/mechanisms for such synchronization are out of scope of this appendix.

When a Tel URI containing an E.164 number cannot be resolved to a SIP URI, the IPCablecom2 network will obtain LNP data for the called number, where appropriate (for example, if the request is to be routed to an Inter-Exchange Carrier, the IPCablecom2 network is not required to perform the query. Rather, the "N – 1" carrier should typically perform the query).

As a default, the LNP query, when required, is performed by the MGC, if an LNP query had not already occurred for the request (Note that since only "Local" porting is supported, it is reasonable that the request will be normally routed to an MGC that would be able to route appropriately based on the results of a query).

The S-CSCF may also support LNP capabilities. If the S-CSCF supports LNP capabilities, the S-CSCF should be configurable to control whether or not these capabilities are to be utilized, to provide flexibility as to where the LNP query is performed. The mechanisms by which an S-CSCF obtains LNP data is out of scope of this appendix. (Mechanisms could include ENUM based mechanisms, including mechanisms by which LNP data is obtained from the E.164 to SIP URI resolution request.) Such mechanisms are the subject of currently evolving IEFT Internet Drafts. Routing policies to handle the case where the S-CSCF resolves a Tel URI to a SIP URI, and also obtains LNP data associated with the Tel URI, are out of scope of this appendix.

To support equal access carrier routing, the IPCablecom2 network selects the route to the PSTN based on the dialled or presubscribed carrier, and passes the carrier ID and the dial-around indicator to the PSTN. This implies that the Tel URI should support the "cic" and "dai" parameters, so the MGC can select the correct trunk group, and also pass the carrier id and dial-around-indicator to the PSTN.

Note that current IPCablecom2 requirements do not call for support of a presubscribed carrier on a subscriber basis. Rather, a carrier may be presubscribed for all subscribers on a network basis. The BGCF may support addition of the network assigned carrier to the Tel URI via the "cic" parameter and also update the "dai" parameter. If supported, the BGCF adds these parameters based on routing

policy/configuration. Note these parameters may have already been added by a prior network component, and hence should not be overwritten by the BGCF.

The following responsibilities related to equal access are in the scope of an application server:

- Setting/policing the dial around indicator for a carrier ID provided by a UE in a request.
- Obtaining the carrier id for freephone calls.
- Populating the carrier and dial around indicator for a presubscribed carrier, for the case where a presubscribed carrier has been configured for an individual subscriber.

  NOTE – As discussed previously, this is not a requirement currently, but should it be required, it could be supported in this fashion.

IPCablecom2 supports the number portability and carrier routing requirements using the Tel URI LNP and carrier routing parameters and the dial-around-indicator parameter defined in [ITU-T J.178].

I.6.9.2 Impacted components

In order to support number portability and carrier routing, the number portability information must be carried in the SIP signalling. Specifically, the Tel URI needs to support the "rn", "cic", and the "npdi" parameters, and the "dai" parameter defined in [ITU-T J.178]. This information is used by the routing proxies (e.g., BGCF) to select the correct hop-off point to the PSTN, and by the PSTN gateway to communicate the correct routing information to the PSTN. These parameters can be carried in a native Tel URI, or the SIP equivalent of a Tel URI where user=phone.

I.6.9.2.1 UE

The only responsibility of the UE in support of carrier routing is to identify a user-dialled carrier to the network on an originating call. The UE does this by recognizing user-dialled carrier digits provisioned via a digit map, and identifying the carrier in the Tel URI "cic" parameter of the originating INVITE.

Alternately, the digit map may specify that the UE must report all dialled digits, including the dialled carrier digits, in a SIP URI with user parameter of "user=dialstring". With this approach, an AS would be required to extract the CIC and normalize the Tel URI.

Mechanisms to configure the digit map to control the UE behaviour are out of scope of this appendix.

The UE does not play any other role in support of number portability.

I.6.9.2.2 S-CSCF

As specified in [ITU-T J.366.4], when the originating S-CSCF receives an originating request with a Request-URI of the Tel URI form, then it must attempt to resolve the E.164 address to a globally routable SIP URI using ENUM. If the resolution fails, then the S-CSCF assumes that the call is destined for the PSTN, and forwards the INVITE to the BGCF for further routing.

IPCablecom2 enhances these requirements to support number portability. The S-CSCF may support number portability capabilities. If so, the S-CSCF should provide configuration controls that allow the operator to enable or disable the number-portability procedures. This will enable the operator to choose whether the LNP query is done by the S-CSCF, or by a downstream entity such as the MGC, or PSTN.

If the S-CSCF has been configured to support number portability, then once it has determined that a call is destined for the PSTN, the originating S-CSCF must determine whether or not the called number is ported, and, if it is ported, then the actual routing number. How the S-CSCF gets this information is not specified (for example, it could be via an ENUM query). If the number is ported, then the originating S-CSCF must add an "rn" parameter to the request Tel URI to identify the

routing number, and add an "npdi" parameter to indicate that the LNP database dip has been performed.

If the S-CSCF is configured to not support number portability, then it will forward requests destined for the PSTN to the BGCF without populating the Tel URI number-portability parameters.

Policies and procedures for handling scenarios where both a SIP URI, and Tel URI with number portability information, are obtained from an attempt to resolve an E.164 address to a SIP URI, (should this be possible with some mechanisms), are out of scope of this appendix.

I.6.9.2.3 BGCF

The BGCF receives INVITE requests from the S-CSCF and selects the best route to the PSTN based on locally configured routing policy. As specified in [ITU-T J.366.4], the input to the routing decision is the called telephone number identified in the Tel URI of the INVITE request URI. IPCablecom2 enhances the routing requirements to include the Tel URI "cic" and "rn" parameters, and as a result the BGCF may support use of these parameters in routing decision. How these parameters affect routing is not specified.

The BGCF may support addition of the "cic" and "dai" parameters to the Tel URI, to support a network-wide presubscribed carrier. Addition of these parameters is based on routing policy. The attributes of the request being routed may determine whether a "cic" parameter is added. The BGCF shall allow for these parameters to have already been added to the request by another network component, and hence not overwrite the parameters if already provided.

I.6.9.2.4 MGC

The MGC receives requests from the BGCF for routing to the PSTN or from the PSTN for routing into the IPCablecom network.

Requests from the BGCF may have a Tel URI that contains the carrier ("cic") and/or number portability ("npdi", "rn") parameters. Requests from the PSTN may also contain number portability parameters.

The MGC will determine whether to make an LNP query based on local configuration, and the contents of the request, including the received number portability parameters.

MGC routing policy includes routing based on carrier and number portability parameters. The details of MGC routing policy are outside the scope of this appendix.

I.6.10 Globally routable user agent URI (GRUU)

I.6.10.1 Description

The support of SIP globally routable user agent URI (GRUU) is optional for the UE in the IPCablecom2 SIP architecture. GRUU benefits IPCablecom2 by permitting certain call features, such as call transfer, to accurately target SIP requests to a particular SIP user agent instance of a UE. It also permits features to be defined to apply appropriately to requests that are intended for a particular SIP user agent instance of a UE rather than generally to a public user identity. For instance, when a request is targeted to a particular UE via a GRUU, it may be desirable to abstain from retargeting the request to voicemail.

I.6.10.2 Impacted components

This clause describes the component impacts for support of GRUU.

I.6.10.2.1 UE

An IPCablecom2 UE supporting GRUU will need to comply with the user agent requirements and guidelines under development.

- The UE must request a GRUU when registering, and retrieve and retain the GRUU provided in the registration response.
- If the registered public user identity is part of an implicit registration set, the UE must also obtain and retain the GRUU for each implicitly registered public user identity. (See clause I.6.10.3 for more information.)

When sending SIP requests or responses that require a contact address, the UE should use a GRUU rather than the contact URI it registered.

- In particular, the UE must use the corresponding retained GRUU as a contact address when sending SIP requests with a "From" header containing a registered public user identity.
- The UE must also use the corresponding retained GRUU as a contact address when responding to SIP requests where the P-called-party is an implicitly registered public user identity.

I.6.10.2.2 S-CSCF

The S-CSCF needs to be capable of responding to registration requests that ask for GRUU URIs to be returned. In this case, it needs to construct and return a GRUU that is linked to the provided public user identity and instance ID.

In addition to servicing requests addressed to public user identities it is responsible for, an S-CSCF must also service requests addressed to any GRUU that was previously assigned to a public user identity it is responsible for. This remains the case even when responsibility for a public user identity is transferred from one S-CSCF to another.

To meet this need, by convention, the GRUU format for IPCablecom2 is defined as follows:

- The GRUU associated with a public user identity in SIP or SIPS format is the same URI as the public user identity with the addition of a 'gruu' URI parameter and an 'opaque' parameter.
- For a URI that contains a telephone number, a GRUU may be requested by using a SIP URI that includes a properly formatted telephone number in the user part of the SIP URI, together with the domain name of the provider and a 'user=phone' parameter. Indeed, a GRUU may not be requested for a public user identity in TEL URI because a URI following the tel format may not be registered. The resulting GRUU may be used for both the SIP and TEL forms of the public user identity.
- The 'opaque' parameter of the GRUU returned by the S-CSCF consists of an "opaque=" parameter name followed by a value identical to the value of the 'sip.instance' parameter provided by the UE in the REGISTER request.

When a request is addressed to a GRUU, the user profile must be able to differentiate which services are to be applied to the request based on the target of the request being a GRUU, or a public user identity. This may be achieved via a service point trigger (SPT) which tests the Request URI of the current request for the presence of a 'gruu' URI parameter.

As described in the GRUU specification, when a SIP request is made to a URI with the GRUU property, the routing logic is dictated by the GRUU property. Therefore, the S-CSCF logic for translating the Request URI of a terminating request is different for a GRUU than a public user identity. For a GRUU, the only possible target is a contact registered with the public user identity and instance ID associated with the GRUU.

I.6.10.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specifications contain the necessary requirements for globally routable user agent URI (GRUU): ITU-T Recs J.366.2, J.366.3, [ITU-T J.366.4] and [ITU-T J.366.5].

I.6.11 Registration state event package extension for GRUU

I.6.11.1 Description

Additional extensions are defined to support the conveyance of GRUU URIs in the SIP registration event package. The registration-event package extension for GRUU must be supported if GRUU is supported by the IPCablecom2 elements (UE, S-CSCF and HSS). The support of registration-event package extension for GRUU is otherwise optional in the IPCablecom2 SIP signalling architecture.

Reg-event package extension for GRUU support is optional in the IPCablecom2 SIP signalling architecture. It enhances the information provided by the reg event package to include a GRUU if one is assigned for a registered contact.

This functionality is included in IPCablecom2 because it allows a UE to obtain all the GRUUs associated with an implicit registration set. Indeed, when a UE registers and requests the assignment of a GRUU, the response will contain the corresponding GRUU for the public user identity that was registered. However, if the public user identity is part of an implicit registration set, then registrations of the same contact are made to each of those public user identities. Each results in the assignment of a distinct GRUU, but there is no way to obtain those GRUUs in the response to the REGISTER. If the UE has a subscription to the registration event package, then the inclusion of the registration event package extension for GRUU means that the UE will receive the GRUUs associated with an implicit registration set in a notification.

I.6.11.2 Impacted components

This clause describes the component impacts for optional UE support of the Reg Event GRUU extension.

I.6.11.2.1 UE

If a UE has subscribed to the reg event package, and subsequently receives a notification indicating that an implicit registration has occurred for a contact the UE has registered, then the UE must retain the GRUU from the notification for future use. The manner in which this is used is covered by clause I.6.10.

I.6.11.2.2 S-CSCF

When sending notification for the reg event package, the S-CSCF must use the reg event package to include the GRUU for each registered Contact that has been assigned a GRUU.

I.6.11.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for Registration state event package extension for GRUU: [ITU-T J.366.4].

I.6.12 Private 3GPP headers

A set of private SIP headers for use by 3GPP is described in [IETF RFC 3455]. Of these, there are two p-headers whose requirements in IPCablecom2 differ from those of IMS.

NOTE – P-headers described in [IETF RFC 3455] which are not identified in this clause are supported by IPCablecom2 without change.

I.6.12.1 Description

I.6.12.1.1 P-Associated-URI header

The P-Associated-URI header is received by the UE in the 200 (OK) response to a REGISTER request. According to [ITU-T J.366.4], it contains the registered public user identity and its associated set of implicitly registered public user identities.

NOTE – This differs from the description in [IETF RFC 3455].

According to IMS registration procedures, the UE is required to support this header, which indicates to the UE the following information:

- The set of implicitly registered public user identities.
- The default public user identity, which will be asserted by the P-CSCF in the P-Asserted-Identity procedures if the UE does not include a P-Preferred-Identity header, or does not include a registered public user identity in the P-Preferred-Identity header.
- Whether or not the public user identity used for registration is barred, since barred identities are not included in the P-Associated-URI header.

In IPCablecom2, support for the P-Associated-URI header is optional for the UE.

I.6.12.1.2 P-Access-Network-Info header

According to IMS, the P-Access-Network-Info header must be included by the UE in any SIP message (with some exceptions) sent integrity protected. It identifies the access technology being used for IP-connectivity (i.e., IP-CAN), and is passed by the S-CSCF to trusted application servers as part of 3rd party registration.

Its potential usages include:

- emergency services, as described in clause 5.2.10 of [ITU-T J.366.4];
- determination of whether SIP compression is needed between the UE and P-CSCF, as described in clause I.6.3;
- optimization of the values of SIP timers, as described in clause I.6.14; and
- optimization of services based on access network type.

In IPCablecom2, the P-Access-Network-Info header is included by the UE only if the access technology is known.

NOTE – New access-type value(s) for IPCablecom2 must be registered with the appropriate standards body.

I.6.12.2 Impacted components

This clause describes the component impacts for optional support of the P-Associated-URI and P-Access-Network-Info headers.

I.6.12.2.1 UE

If the P-Associated-URI header is not supported by the UE, the UE has no ways of knowing whether or not the user identity it used during registration is barred. Therefore, care must be taken that UEs not supporting the P-Associated-URI header do not register using a barred identity. Barred identities are not bound to the contact information, and cannot be used for identity assertion. The primary implications of non-support for the P-Associated-URI header are:

- The UE does not receive explicit indication that additional AORs are implicitly registered unless it supports the optional registration-state event package (see clause I.6.8).
- If the public user identity used for registration is barred, the UE will not be able to successfully subscribe to the registration-state event package, if there is no security association.

- If a request is issued with a P-Preferred-Identity containing a barred public user identity, the P-CSCF will ignore it and insert a P-Asserted-Identity with a known default public user identity instead.

The UE shall support the P-Access-Network-Info header procedures described in [ITU-T J.366.4], with the following clarification:

- The P-Access-Network-Info header is inserted by the UE, only if the access network technology is known.

I.6.12.2.2 P-CSCF

If the P-CSCF receives a REGISTER request that does not contain a P-Access-Network-Info header and the P-CSCF has knowledge of the access technology being used at the UE, the P-CSCF shall insert the P-Access-Network-Info header.

NOTE – Since the P-Access-Network-Info header may not be inserted by either the UE or P-CSCF (i.e., when neither have knowledge of the access technology), features and services that make use of the P-Access-Network-Info must appropriately handle its absence.

I.6.12.2.3 S-CSCF

If the P-Associated-URI header is not supported by the UE and signalling security is disabled or optional, the originating S-CSCF may receive non-REGISTER requests that contain a barred public user identity in the P-Preferred-Identity and/or From header. In this case, the S-CSCF shall reject the request by generating a 403 (Forbidden) response.

I.6.13 Routing SUBSCRIBEs for configuration information

I.6.13.1 Description

IPCablecom2 UEs obtain configuration information using the SIP protocol by subscribing to the ua-profile event package. The initial subscription for configuration is addressed to a special Request-URI that is device specific. The Request-URI is constructed by the UE from a UE-specific device identifier, combined with the domain name of the provider. The initial subscription request for configuration must be routed to an IPCablecom2 PAC element that is capable of providing a suitable device profile for the UE.

It is important to differentiate between two classes of UEs for which the SUBSCRIBE requests for configuration information must be processed:

1) UEs whose device URI is known to the system.

2) UEs whose device URI is unknown to the system.

The procedures described below allow the SUBSCRIBE requests for configuration information to be properly routed in either case.

A UE may or may not be aware whether its device URI is known or unknown by the network. If it is unknown then it will not be able to register. The procedure it follows will work in either case. It sends a subscribe request for its profile before registering. This request is addressed to the device-specific URI. It includes a From header containing the device-specific URI, and should include a P-Preferred-Identity header also containing the device-specific URI. This follows the procedures of clause I.6.1.2.1 that apply when there is no security association between the UE and the P-CSCF and the UE has not registered.

Because the UE has not registered, the P-CSCF has no basis for authenticating the request. Instead, it leaves the P-Preferred-Identity header in place, deferring authentication to a subsequent server. It uses the P-Preferred-Identity header if present, or absent that of the From header, to select an I-CSCF for subsequent processing, and forwards the request there.

In the absence of a P-Asserted-Identity header, the I-CSCF uses the P-Preferred-Identity if present, or the From header if the P-Preferred-Identity header is also absent, to determine the target for routing the request for origination processing.

If the device URI is known, there will be an explicit entry for it in the HSS, as a public user identity. The I-CSCF then routes the request to the S-CSCF serving this public user identity.

The device URI for an unknown device is by definition unknown to the HSS, so no exact matching entry is present in the HSS. However, when support for unknown devices is desired, a wildcard PSI entry shall be present in the HSS that matches all desired unknown device URIs. For example, the following two values may be sufficient:

sip:MAC%3a!.*!@provider.net

sip:urn%3auuid%3a!.*!@provider.net

The HSS entry should identify a PAC element that handles unknown subscriptions from unknown devices. Subscriptions by unknown devices are thus routed by the I-CSCF to this server for "orig" processing.

The PAC element is responsible for any authentication or authorization it chooses to make for unknown devices. The server then chooses to honour the request or to refuse it. It was invoked to perform origination processing, so the request might need to be routed elsewhere for termination processing. However, for IPCablecom2, the only applicable case is where the origination and termination addresses are the same. So the server may simply honour the request without further routing. It utilizes information in the subscription request (e.g., device type information) to select a suitable default configuration for the device – one that will allow the device to utilize whatever restricted capabilities the provider may choose to permit. Typically, this is only for the purpose of initial communication sufficient to establish a business relationship between the provider and the user of the device, after which the device will change status, becoming *known* to the system. For further information, see [ITU-T J.364].

I.6.13.2 Impacted components

This clause describes the component impacts to support subscription to the UA profile event package before registration.

I.6.13.2.1 UE

A UE should subscribe for the device profile, using the device-specific URI, without first registering using that URI. It shall do so following the procedures of clause I.6.1.2.1 on Signalling Security and the UE.

I.6.13.2.2 P-CSCF

See clause I.6.1.2.2 on Signalling Security and the P-CSCF.

I.6.13.2.3 I-CSCF

See clause I.6.1.2.3 on Signalling Security and the I-CSCF.

I.6.13.2.4 S-CSCF

See clause I.6.1.2.4 on Signalling Security and the S-CSCF.

I.6.13.2.5 HSS

The HSS must handle the case where a Request-URI matches two entries in the HSS – one for a wildcarded PSI and one for a public user identity. In this case, the entry for the public user identity shall take precedence over that for the wildcarded PSI.

I.6.13.2.6 PAC element

The PAC element for a known device URI shall operate as a terminating application server on behalf of the corresponding user. It may detect that the device is known by the presence of a P-Asserted-Identity header naming containing the device URI.

The PAC element for an unknown device URI shall function as an originating PSI server. It may detect that the device is unknown by the absence of a P-Asserted-Identity header.

I.6.13.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for Routing SUBSCRIBEs for configuration information: [ITU-T J.366.4].

I.6.14 SIP timers

I.6.14.1 Description

To accommodate 3GPP air interface processing and transmission delays, 3GPP IMS Release 6 [ITU-T J.366.4] specifies a modified set of SIP timer values (compared with those defined in [IETF RFC 3261]) to be applied by the P-CSCF towards the UE and the UE towards the P-CSCF. For broadband access, this consideration does not apply and standard [IETF RFC 3261] SIP timer values would apply. As part of the 3GPP IMS Release 7 support for "Fixed Broadband", UEs using broadband access technology, and a P-CSCF that interacts with such a UE, use the standard [IETF RFC 3261] SIP timer values.

IPCablecom2 incorporates these 3GPP IMS Release 7 changes for SIP timers.

This solution is dependent on specification of a new access type for the P-Access-Network-Info header, representing IPCablecom2 broadband access network technology. Refer to clause I.6.12.1.2 for further details.

Since the UE and P-CSCF need to use a consistent set of SIP timer values, if the UE does not provide a P-Access-Network-Info header, both the UE and P-CSCF use the standard [IETF RFC 3261] SIP timer values. Note that this is an incremental requirement over the existing 3GPP Release 7 changes.

Note that the 3GPP IMS Release 7 solution may be subject to further study within 3GPP to determine if there are better ways to determine access delays and whether SIP timer values should be modified. As such, IPCablecom2 may realign with any future changes made in this area.

I.6.14.2 Impacted components

The required changes are identified and incorporated into Release 7.

An incremental requirement is that since the UE and P-CSCF need to use a consistent set of SIP timer values, if the UE does not provide a P-Access-Network-Info header, both the UE and P-CSCF use the standard [IETF RFC 3261] SIP timer values.

I.6.14.2.1 UE

Only UEs using 3GPP wireless access technology uses the 3GPP-modified SIP timer values. Other UEs use standard [IETF RFC 3261] SIP timer values.

I.6.14.2.2 P-CSCF

The P-CSCF applies 3GPP-modified SIP timer values towards UEs on 3GPP wireless access technologies. For UEs on other access technologies, the P-CSCF applies standard [IETF RFC 3261] SIP timer values. The P-CSCF makes the determination based on the access type in P-Access-Network-Info. When no P-Access-Network-Info is provided by the UE, standard [IETF RFC 3261] timer values apply.

I.6.14.3 IPCablecom2 IMS Delta specification

The following IPCablecom2 IMS Delta specification contains the necessary requirements for SIP timers: See clause 7.7 of [ITU-T J.366.4].

I.6.15 General changes

I.6.15.1 Description

This clause describes a number of miscellaneous changes to IMS relevant to meet the IPCablecom2 requirements, including terminology clarifications, and the support of both IPv4 and IPv6 addressing.

- [ITU-T J.366.4] uses terminology that implies access specific technology in some cases. The terms "mobile-originating", "mobile-originated", "mobile-terminating", "mobile-terminated" and "mobile-initiated" are used throughout TS 24.229. As part of the 3GPP IMS Release 7 support for "Fixed Broadband", the 3GPP specification, [ITU-T J.366.4] has been modified to correct the terminology, using the terms "UE-originating", "UE-originated", "UE-terminating", UE-terminated" and "UE-initiated". IPCablecom2 implicitly assumes this change in terminology.
- [ITU-T J.366.4] specifies procedures for derivation of public identity, private identity, and home network domain name when the UE contains a UICC but no ISIM. (Refer to clauses 4.2, 5.1.1.1A and Annex C of [ITU-T J.366.4]). Some UEs utilized in IPCablecom2 may have neither an UICC nor an ISIM. In such cases, the UE will be configured or provisioned with the required information. For more information regarding this case, please refer to Appendix III.

The following should be recognized:

- Some procedures in [ITU-T J.366.4] are explicitly described as pertaining to 3GPP Access. Such procedures are not applicable to broadband clients (Example: Clause 5.2.8.1 of [ITU-T J.366.4] "P-CSCF-Initiated call release" contains scenarios related to "radio coverage" and "radio interface resources").
- [ITU-T J.366.4] also contains annexes that are explicitly targeted at GPRS access. Such annexes are self-evidently not applicable to IPCablecom2 broadband access, and corresponding material for IPCablecom2 may be contained in other IPCablecom2 specifications.

I.6.15.2 Impacted components

Changes required for generalization of access terminology (from "mobile-" to "UE") have been identified. These changes generalize [ITU-T J.366.4] but do not impact procedures. As such, no detailed breakdown of component impact is provided in this clause.

I.6.15.3 IPCablecom2 IMS Delta specification

The changes required for generalization of access terminology (from "mobile-" to "UE") are implicitly assumed and [ITU-T J.366.4] is not updated with these changes for simplicity.

I.6.16 Interworking with previous IPCablecom releases

A UE must be able to establish voice sessions with endpoints supported in previous IPCablecom releases. For example, UEs and E-MTAs in the same operator's network must be able to call each other without having the calls routed through another IP carrier, or through the PSTN. Also, UEs must be able to establish calls to TGCP-based MG endpoints in order to interwork with the PSTN.

Service control for UEs is not integrated in any way with service control for E-MTAs. UE service control is shared between the UE and its serving S-CSCF and associated application servers. E-MTA services are provided and controlled via NCS by the CMS. UEs and E-MTAs simply view each other as separate callable entities in the network.

The ability to establish calls between UEs and other endpoints supported in previous IPCablecom releases is enabled by the SIP-based pkt-sig-2 interface that connects the S-CSCF, I-CSCF, and BGCF to the CMS and MGC (see Figure I.3). The requirements to support this interface on the CMS and MGC are defined in [ITU-T J.178].

Appendix II

Quality of service architecture technical overview

(This appendix does not form an integral part of this Recommendation)

II.1 Introduction

This appendix provides an overview of the IPCablecom2 quality of service (QoS) architecture. Specifically, it describes the way in which IPCablecom multimedia is used to provide QoS applications built on top of IPCablecom. To aid the reader in understanding the IPCablecom2 QoS architecture, the high level goals and specific logical components and interfaces defined are discussed in this appendix.

II.1.1 IPCablecom multimedia overview

IPCablecom multimedia defines an IP-based platform for delivering QoS-enhanced multimedia services over DOCSIS 1.1 (ITU-T Rec. J.112) or greater (for the remainder of this appendix, references to DOCSIS assume DOCSIS 1.1 or greater) access networks. This platform expands on the core capabilities of IPCablecom (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 IPCablecom architecture is customized for the delivery of residential telephony services, the IPCablecom multimedia architecture offers a general-purpose platform for cable operators to deliver a variety of IP-based multimedia services that require QoS treatment. For this reason, specific services are not defined or addressed.

Although the IPCablecom multimedia platform is based upon IPCablecom work, the full voice infrastructure defined in IPCablecom is not a prerequisite to the deployment of multimedia services. Rather, it is intended that a particular cable operator may choose to initially deploy either voice or multimedia services, with the assurance that these platforms will seamlessly integrate and interoperate if and when they are deployed in parallel.

II.2 References

This appendix uses the following additional informative references:

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

[ITU-T J.179 App.I] ITU-T Recommendation J.179 (2005), *IPCablecom support for multimedia*. Appendix I: *Background information*.

[ITU-T J.179] ITU-T Recommendation J.179 (2005), *IPCablecom support for multimedia*.

[ITU-T J.362] ITU-T Recommendation J.362 (2006), *IPCablecom2 control point discovery*.

[ITU-T J.365] ITU-T Recommendation J.365 (2006), *IPCablecom2 application manager interface*.

[ITU-T J.366.4] ITU-T Recommendation J.366.4 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 Specification.* (3GPP TS 24.229)

[IETF RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.

[IETF RFC 3890] IETF RFC 3890 (2004), *A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP).*

II.3 Terms and definitions

This appendix uses the following additional term:

II.3.1 IMS Release 6: 3GPP IP multimedia subsystem suite of specifications – Approved version Release 6.

II.4 Abbreviations and acronyms

This appendix uses the following additional abbreviations:

DQoS Dynamic Quality of Service

DSCP Differentiated Services Code Point

P-CSCF Proxy CSCF

WS Web Services

II.5 QoS requirements and scope

The objective of this appendix is to provide an architecture definition for a UE device to obtain access to IPCablecom network resources. In particular, it describes a comprehensive mechanism for an IPCablecom network to request specific QoS resources required to support the media associated with SIP sessions over a DOCSIS network.

This architecture also recognizes that IPCablecom will provide QoS for a wide variety of applications and services (voice, video, etc.); as such, it provides a generic mechanism to request access network resources and does not require applications to be aware of access network topology.

II.5.1 Requirements

The following is a list of requirements that are considered essential for developing a general-purpose QoS architecture to satisfy the services envisioned for IPCablecom2:

- The QoS architecture must service flow creation for UEs that are not QoS aware through a network-initiated policy push.
- Define an IPCablecom2 application manager (IPAM), which will mediate QoS interaction between the P-CSCF and the Multimedia infrastructure.
- Support packet marking and classification from the access network such that a QoS mechanism (e.g., Differentiated Services) can be used in the backbone network.
- The IPAM must receive sufficient information from the P-CSCF regarding each flow which makes up a session such that it can:
  - Construct an appropriate classifier while accommodating NAT traversal mechanisms.
  - Construct a flow spec or alternative traffic profile which reflects the Least Upper Bound of the resource requirements of any alternative codec which may be permitted for the flow including bandwidth, packetization rate, and scheduling type.
  - Determine the type of media so that it can select an appropriate differentiated services code point (DSCP).
- The IPAM must receive sufficient information from the P-CSCF for each session such that it can:
  - Construct a suitable correlation identifier for accounting records.
  - Identify the subscriber for the purposes of accessing subscriber profile data.
  - Recognize if the session must be given higher priority (e.g., an emergency call).
- The interface must allow reservation and commitment of resources to occur in separate steps.

II.5.2 Scope

The current scope of the IPCablecom QoS architecture is limited to the DOCSIS-based access portion of a cable operator's network and on how the IPCablecom network can request QoS resources from the IPCablecom Multimedia framework. Therefore, the architecture described in this appendix does not address the case of a roaming UE that may attach to the IPCablecom network from non DOCSIS-based access networks.

Further, this architecture does not prohibit the use of the QoS capabilities in IPCable2Home enabled networks. However, providing QoS in IPCable2Home network is not within the scope of this appendix.

II.6 QoS architecture framework

Within the overall goal to leverage existing industry standards whenever possible, a specific objective is to align with the IMS architecture and specifications being developed by 3GPP. Specifically, IPCablecom2 will align with IMS Release 6 and reuse many of the basic IMS components and reference points. Another equally important objective is to make use of the rich set of QoS capabilities provided by IPCablecom multimedia.

IPCablecom2 must support a policy push model in order to interface with IPCablecom multimedia. Release 6 of the IMS provides two related mechanisms for providing the Quality of Service and charging for the IP service flows that make up multimedia sessions. Service-based local policy (SBLP) provides a mechanism for the authorization, establishment and modification of IP bearers using an authorization token similar to the IPCablecom Dynamic Quality of Service Architecture [ITU-T J.163]. As in DQoS, the establishment of PDP contexts using SBLP requires active involvement of a QoS aware user equipment.

The second mechanism is flow-based charging (FBC). FBC provides a means to identify, police and charge for the IP flows that make up a session using a network-initiated push mechanism similar to IPCablecom multimedia. However, FBC does not provide a mechanism for the establishment of new bearers (or service flows). Neither SBLP nor FBC as defined in IMS Release 6 provides the complete information necessary to support the establishment of service flows using IPCablecom multimedia. Future alignment with the policy and charging control work being undertaken in IMS Release 7 is possible.

II.6.1 QoS architecture reference model

The IPCablecom2 QoS architecture is illustrated in Figure II.1. The QoS infrastructure defined in IMS Release 6 is not sufficiently access agnostic to satisfy the requirements of IPCablecom2. Therefore, IPCablecom2 uses the IPCablecom multimedia components including the policy server, CMTS, and cable modem. The IPCablecom2 application manager is a specialized application manager which receives session level QoS requests via SOAP from the P-CSCF and creates and manages the IPCablecom multimedia gates for each flow in the session using the IPCablecom multimedia pkt-mm-3 interface.

The QoS architecture does not prohibit the use of the IMS defined Gq reference point for those UEs that may access services over a GPRS network. Figure II.1 illustrates the coexistence of the IMS defined QoS architecture for GPRS based devices with the IPCablecom2 multimedia QoS architecture used for UEs accessing services via a DOCSIS network.

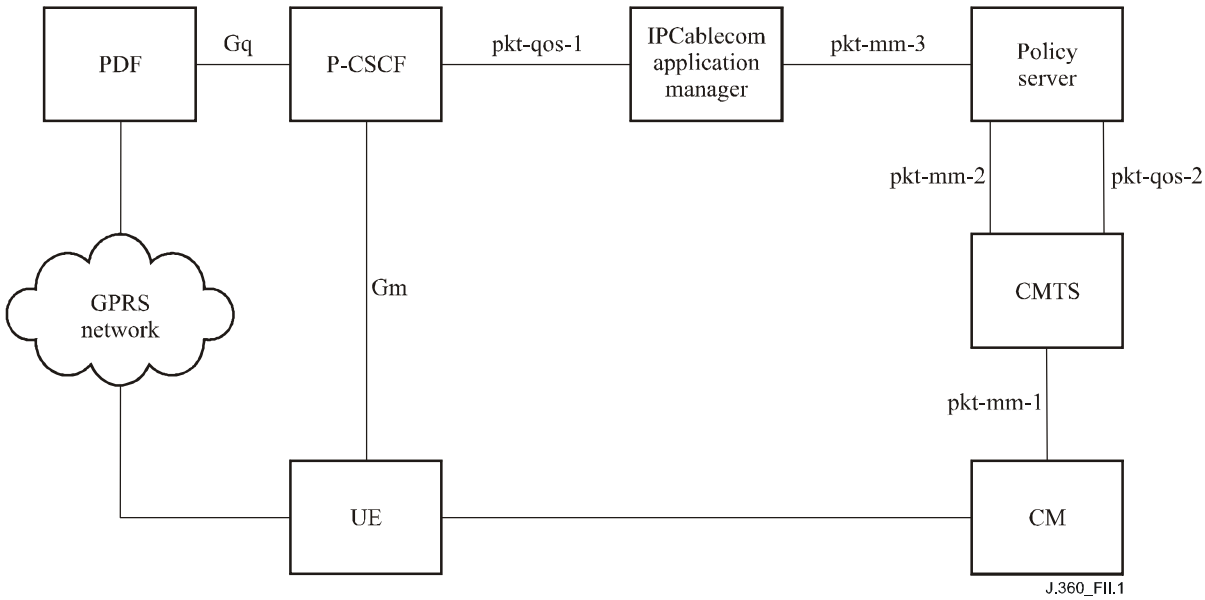


Figure II.1 – QoS signalling reference points

Reference points pkt-mm-1 through pkt-mm-3 are defined by IPCablecom multimedia. IPCablecom2 introduces new QoS reference points pkt-qos-1 and pkt-qos-2. Table II.1 describes these interfaces briefly while Table II.2 provides a brief description of each network element.

Table II.1 – QoS reference points

Reference point	IPCablecom network elements	Reference point description
pkt-mm-1	CMTS – CM	The CMTS uses DOCSIS defined DSX signalling to instruct the CM to set up, tear down, or change a DOCSIS service flow in order to satisfy a QoS request.
pkt-mm-2	Policy server – CMTS	The interface supports proxy QoS requests on behalf of a UE. This interface is fundamental to the policy-management framework. It controls policy decisions, which are pushed by the policy server (PS) onto the CMTS and is defined by [ITU-T J.179]. In some scenarios, this interface is also used to inform the PS when QoS resources have become inactive.
pkt-mm-3	IPAM-PS	This interface allows the IPCablecom application manager (IPAM), a specialized application manager defined in IPCablecom, to request that the PS install a policy decision on the CMTS on behalf of the UE and is defined by [ITU-T J.179]. This interface may also be used to inform the IPAM of changes in the status of QoS resources.
Gm	UE – P-CSCF	Allows the UE to communicate with the P-CSCF for registration and session control. This reference point is SIP-based and is described in [ITU-T J.366.4].
Mw	CSCF – CSCF	Allows the communication and forwarding of signalling messaging among CSCFs in support of registration and session control. This reference point is SIP-based.

Table II.1 – QoS reference points

Reference point	IPCablecom network elements	Reference point description
Gq	P-CSCF – PDF	The Gq interface is used for session based policy set-up information exchange between the policy decision function (PDF) and the P-CSCF.
pkt-qos-1	P-CSCF – IPAM	This SOAP/XML based interface between the P-CSCF and IPCablecom application manager conveys session level QoS information. The IPAM uses this information to form suitable messages for pkt-mm-3 interface and is defined by [ITU-T J.365].
pkt-qos-2	Policy server – CMTS	The policy server uses the control point discovery protocol to determine the serving CMTS in the network for a given UE. This reference point is based on IPCablecom specification [ITU-T J.362].

Table II.2 – QoS network elements

IPCablecom network element	Brief description
UE	A UE is a client and interacts with the network to access services and provides interfaces to users or entities.
P-CSCF	The P-CSCF parses the SDP in SIP messages and implements the web service client interface to provide QoS by interacting with the application manager. It reserves, commits, and removes QoS on access network.
IPCablecom application manager (IPAM)	The IPCablecom application manager is responsible for managing QoS resources in the access network as requested by the P-CSCF. The IPCablecom application manager receives session level QoS messages from the P-CSCF, and formulates and sends IPCablecom multimedia QoS messages to the policy server.
Policy server (PS)	The policy server acts as an intermediary between application manager(s) and CMTS(s). It applies network policies to application manager messages and proxies then to the CMTS.
Cable modem termination system (CMTS)	The CMTS is a device at a cable headend which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
Cable modem (CM)	DOCSIS compliant cable modem.

II.6.2 Relationship with 3GPP IMS Release 6

The IPCablecom2 Recommendations include an enhanced version of 3GPP IMS Release 6 TS 24.229 to document the QoS requirements for the call control protocol using SIP and SDP. A summary of the modifications to TS 24.229 follows:

- Added requirement to include the "b=" media descriptor and the "TIAS" bandwidth modifier defined in [IETF RFC 3890] to describe the bandwidth required for the session.
- Additional SDP types are added to the SDP profile definition for user agents. The SDP types include:
  - Packet time (a=ptime) – The type must be included by UEs to indicate the packetization time which the UE expects to receive traffic.

– Maximum packet rate (a=maxprate) – This type must be included when the UE is using a non-well known IPCablecom codec.
– NAT (a=Local-Turn) – This type must be included by the UE when it is using a TURN server to transverse a local NAT device.

II.6.3 Relationship with multimedia pkt-mm-11

The IPCablecom multimedia architecture also defines a web services based interface to the application manager from an upstream application server. This interface is labeled pkt-mm-11 in the multimedia technical report [ITU-T J.179 App.I]. While this interface could be used by the P-CSCF to interface with the IPCablecom2 application manager, a new interface was developed to allow for more efficient P-CSCF operation. The multimedia defined interface would require a double translation of the session parameters resulting in extra overhead on the P-CSCF to translate the session parameters into a generic QoS request. The IPCablecom-defined interface allows the P-CSCF to simply pass the session parameters in whole to the IPCablecom AM, which is then responsible for the translation to a valid IPCablecom multimedia QoS message. This approach reduces the amount of translations required and allows the P-CSCF to maintain a more access network agnostic implementation.

II.7 Architecture description

Clause II.6 described a set of logical network entities grouped by specific service functions (QoS), as well as a set of reference points that support the information flows exchanged between the functional groups and network entities. This clause provides a more detailed discussion of those logical elements and the associated reference points which are new to the IPCablecom architecture. It also provides an overview of other topics related to the QoS architecture that are not documented elsewhere.

II.7.1 Functional components

In this clause, additional detail is provided on the IPCablecom2 application manager and P-CSCF and their role as related to the QoS architecture.

II.7.1.1 P-CSCF

In addition to its role in providing the UE connectivity to the IPCablecom network, the P-CSCF is also responsible for reserving, committing and releasing QoS resources for a given session. It is important to note that the P-CSCF does not actually determine the QoS resources necessary for the session, rather it simply proxies the session description information to the IPCablecom2 application manager and indicates whether to reserve or commit the resources for the session. While the architecture supports a two-phase commit operation (reserve followed by a commit), there are no requirements on the P-CSCF to follow this approach. A single-phase commit (reserve and commit resources in a single request) may be used.

Once the session has ended, the P-CSCF releases the resources allocated to the session.

II.7.1.2 IPCablecom2 application manager (IPAM)

The IPCablecom2 application manager is primarily responsible for determining the QoS resources needed for the 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 how much bandwidth is required, 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 session) and managing the association of the flows to the session.

II.7.1.3 Relationship between P-CSCF and IPAM

The IPCablecom multimedia architecture provides a well understood relationship between the IPAM and PS. The relationship between the P-CSCF and IPAM is described here. The QoS architecture was not developed with any pre-conceived relationship between the two network elements. While the choice of how to deploy P-CSCFs and IPAMs and their associated cardinality is mainly a deployment decision, Figures II.2 and II.3 represent what are believed to be the most popular deployment scenarios.

Figure II.2 – One to one

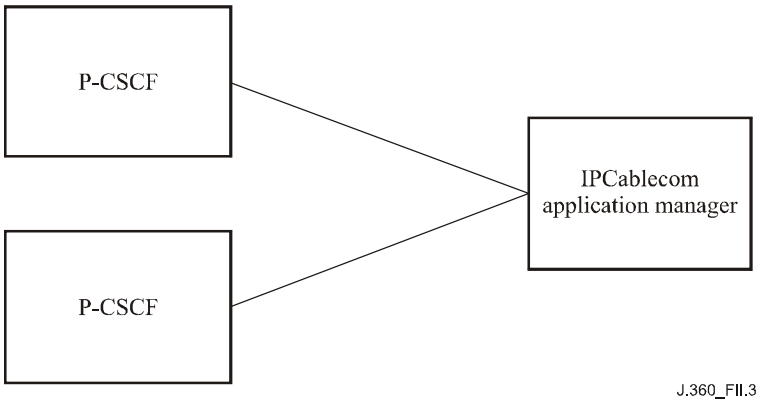


Figure II.3 – Many to one

Figure II.2 illustrates a one-to-one relationship between the P-CSCF and the IPAM. Such a deployment scenario, while extremely simple to manage, may not be the most efficient use of resources. Figure II.3 illustrates a many-to-one relationship between the P-CSCF and the IPAM. This scenario maintains the simplicity of a one-to-one relationship (since the P-CSCF does not have to determine which IPAM to send its request to), but may more efficiently utilize IPAM resources.

Another possible scenario not shown is a one-to-many relationship (or many to many). In this case the P-CSCF may communicate with multiple IPAMs. While such a scenario is supported, no guidance is provided on how the P-CSCF determines which IPAM to send its requests to. Such a scenario may become necessary as the network evolves and different application managers are invoked for different access networks or in certain roaming cases.

II.7.2 Protocol interfaces and reference points

This appendix has identified several interfaces, or reference points, in the IPCablecom2 QoS architecture. The majority of these reference points are existing interfaces defined by IPCablecom multimedia. An overview of the P-CSCF to IPAM protocol interface is provided within this clause as it is the only interface defined by IPCablecom.

It is possible that this interface may not exist in a given vendor's product implementation. For example, if a P-CSCF vendor chooses to integrate the IPAM within the P-CSCF, the P-CSCF to IPAM interface would be internal to that product.

II.7.2.1 P-CSCF – IPAM interface description

The P-CSCF to IPAM interface is based on web services. It allows the P-CSCF to request and delete Quality of Service resources within an IPCablecom multimedia enabled DOCSIS network.

The IPCablecom2 application manager web services interface enables a P-CSCF to request QoS handling in the access network based on the session description protocol (SDP) parameters contained in the offer and answer as defined in [IETF RFC 3264]. The IPAM uses the IPCablecom multimedia pkt-mm-3 interface to communicate these requirements to an IPCablecom multimedia policy server.

II.7.3 Application of QoS policy within IPCablecom

The term policy control has often been used to describe the process by which a new dynamic service flow or bearer is created in the access network at the request of an application. This makes sense since establishing a new service flow in the access network involves the installation of a new dynamic policy in the policy enforcement point. This dynamic policy determines the treatment of the packets which make up the new service flow within the access network throughout the duration of the session.

The focus of this clause is higher levels of policy which may affect the disposition of a user request as it is processed within the network. Such policies could be implemented at several levels in the network in order to further the business needs of the network operators. Levels where policy can be applied include:

- Application level: Applications may employ policy to constrain use of an application based on subscription or other information.
- Signalling network level: For example, network or subscription based restrictions on the use of certain media parameters in an SDP offer may be enforced in an IPCablecom network by the P-CSCF or S-CSCF respectively by sending a negative response to the SIP message as described in clauses 6.2 and 6.3 of [ITU-T J.366.4].
- Bearer network level: Each of the network elements in the bearer network (IPCablecom application manager, policy server and CMTS) serve unique roles as they relate to policy control. A more detailed discussion of the roles for each network element follows:
  - The IPCablecom2 application manager is the entry point from the SIP network into the access network QoS system. The IPAM is in a position to apply policy which takes into consideration the limited service provided by the P-CSCF and potentially subscription based information.
  - The Policy Server may receive messages from multiple application managers including but not limited to IPCablecom application managers. Policies applied at the PS can optimize the use of access network resources between multiple applications and traffic types.
  - The CMTS is responsible for admission control and may have policies which control the allocation of resources between various types of traffic based on session class and possibly on the authorization model used such as IPCablecom and IPCablecom multimedia.

In some cases, similar policy decisions could be made at more than one level in the network. The choice of at what level to implement a given policy will be based on such criteria as:

- Access to required information.
- Performance impacts of implementing policy at that level.
- The ease of implementing policy at a given level.

Ultimately, policy will be implemented at the level in the network which best furthers the business needs of the cable operator.

II.7.4 Routing of QoS request

Assuming a P-CSCF to IPAM relationship as described in clause II.7.1.3, the routing of QoS requests is static, meaning that each P-CSCF is provisioned with a single AM (with the possibility of a secondary AM in the event of a failure) to which all its QoS requests are sent. If a multiple P-CSCF to multiple AM relationship is used, the routing of requests is outside the scope of this effort.

The multimedia architecture is currently silent on how QoS requests are routed between the IPAM and PS and between the PS and CMTS. Given this gap, IPCablecom has defined a dynamic mechanism for PS to CMTS QoS message routing. This procedure is described in [ITU-T J.362] and is based on a path coupled query approach. Where a path coupled query approach is one where the query follows the same path through the network as any other packet destined for a given UE. This mechanism allows the PS to leverage the underlying routing protocols to ensure the proper CMTS is identified based on the IP address of the UE in question.

The IPAM to PS routing of QoS requests is not defined in IPCablecom.

II.8 Example procedures

This clause describes example operational behaviour based on the interfaces and requirements defined in IPCablecom. The Call flows provided in this clause are for reference only to facilitate understanding of the IPCablecom2 QoS architecture.

II.8.1 UE originated successful call

Figure II.4 illustrates a successful UE originated call flow. In the example below, the P-CSCF initiates the QoS process when it receives a SIP message with an SDP offer (usually an INVITE). The P-CSCF passes the SDP offer to the IPAM via the defined QoS interface. The IPAM is then able to translate the preliminary session needs into IPCablecom multimedia requests. This usually results in multiple IPCablecom multimedia gates being created (e.g., a standard audio call would have one upstream gate and one downstream gate).

The IPAM generated IPCablecom multimedia request is then passed to the policy server for policy checks. These policy checks are usually done at the network level, meaning that the policy server ensures the request satisfies network based policies (the amount of resources being requested is within limits, the scheduling type is appropriate for the service, etc.). Once these requests pass the policy server checks, they are passed on to the CMTS for action.

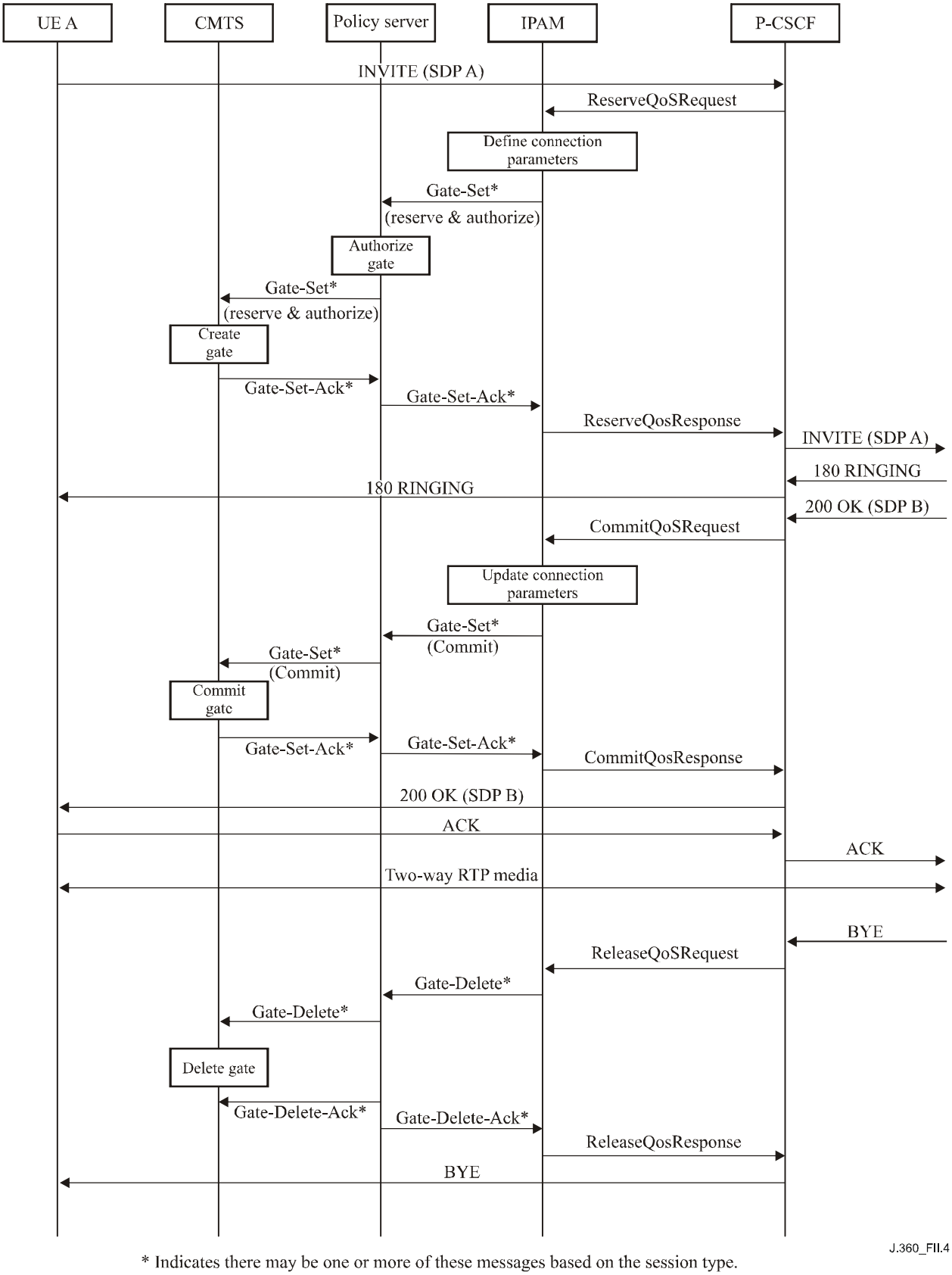
Upon receipt of the resource request, the CMTS is responsible for admission control and resource allocation. This process ensures that the CMTS has adequate resources to honour the request. Once the request has passed admission control and resource allocation, the CMTS installs the necessary flows and notifies the cable modem serving the UE via the DOCSIS defined dynamic service exchange (DSX) messaging interface. At this stage the resources are only reserved; they are not actually available for use. Rather, they have been allocated by the CMTS and can no longer be allocated to other services. Once the CM has been successfully notified of the resource allocation, the CMTS returns a flow identifier to the policy server, which then passes it back to the requesting IPAM.

Once the P-CSCF receives the SDP answer, it has enough information about the remote party to commit the resources for the session. It does this by passing the SDP answer to the IPAM. The IPAM then (in conjunction with the SDP offer) translates this into a new IPCablecom multimedia request which updates the previously reserved resources. As long as the updated request is equal to or less than the reserved resources, it is essentially guaranteed to be granted.

Once the resources are committed, the session can begin using the established flows and receive the desired QoS.

Upon receipt of a BYE, the P-CSCF releases the resources associated with the session through a ReleaseQoSResources request.

Figure II.4 illustrates an example of a UE originated successful call.



* Indicates there may be one or more of these messages based on the session type.

Figure II.4 – Example UE originated successful call

Appendix III

IPCablecom2 security overview

(This appendix does not form an integral part of this Recommendation)

III.1 Introduction

The IPCablecom2 security architecture protects the data, interfaces and components that make up the IPCablecom2 architecture. This appendix describes the security relationships between the elements in the IPCablecom2 architecture.

Design goals for the IPCablecom2 security architecture include:

- Support for confidentiality, authentication, integrity, and access control mechanisms.
- Protection of the network from denial of service, network disruption, theft-of-service attacks.
- Protection of the UEs (i.e., clients) 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 device, UE, and user authentication, secure provisioning, secure signalling, and secure software download.
- Leverage and extend the IMS security architecture in furtherance of the previously stated goals.

III.2 References

This appendix uses the following additional informative references:

[ITU-T J.366.4] ITU-T Recommendation J.366.4 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification*. (3GPP TS 24.229)

[ITU-T J.366.7] ITU-T Recommendation J.366.7 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services*. (3GPP TS 33.203)

[ITU-T J.366.8] ITU-T Recommendation J.366.8 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Network domain security specification.* (3GPP TS 33.210)

[ITU-T J.366.9] ITU-T Recommendation J.366.9 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Generic authentication architecture specification.* (3GPP TS 33.220)

[IETF RFC 1750] IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.

[IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS).*

[IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA).*

[IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).*

[IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).*

[ID SIP-OUTBOUND] *Managing Client Initiated Connections in the Session Initiation Protocol (SIP)*, http://www.ietf.org/internet-drafts/draft-ietf-sip-outbound 02.txt.

[ID TURN] *Obtaining Relay addresses from Simple Traversal of UDP Trough NAT (STUN)*, draft-ietf-behave-turn-00, March 2006.

[TS 23.002] 3GPP TS 23.002 v6.10.0 (2005), *Network architecture*.

[TS 33.222] 3GPP TS 33.222 v6.5.0 (2005), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS).*

III.3 Terms and definitions

This appendix uses the following additional terms and definitions:

III.3.1 IM services identity module (ISIM): The collection of IMS security data and functions on a UICC, may be a distinct application.

III.3.2 IPCablecom multimedia: An application agnostic QoS architecture for services delivered over DOCSIS networks.

III.4 Abbreviations and acronyms

This appendix uses the following additional abbreviations and acronyms:

AKA Authentication and Key Agreement

BSF Bootstrapping Server Function

DDoS Distributed Denial of Service Attack

DNSSEC DNS Security

DoS Denial of Service

GBA Generic Bootstrapping Architecture

IDS Intrusion Detection System

MiM Man in the Middle

PKI Public Key Infrastructure

SA Security Association

UICC UMTS Integrated Circuit Card

USIM Universal Subscriber Identity Module

III.5 IPCablecom2 security

The IPCablecom2 security architecture describes the reference points and logical components and the data flows between these components.

This clause provides:

- A description of the relationship between IPCablecom2 and 3GPP IMS releases.

- An overview of the IPCablecom2 architecture.
- A description of the threats to the IPCablecom2 architecture.
- A description of the IPCablecom2 security mechanisms.

III.5.1 Relationship with 3GPP IMS

IPCablecom2 is based on the 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.

Within the overall IPCablecom goal to leverage existing industry standards whenever possible, there is a specific objective to align with the IMS architecture and specifications being developed by 3GPP. Specifically, IPCablecom2 will reuse many of the basic IMS functional entities and interfaces. Although this appendix discusses IMS, the main goal is to describe the enhancements and modifications to 3GPP specifications. Refer to [TS 23.002] for additional information on the 3GPP IMS architecture.

III.5.2 IPCablecom2 reference architecture

An overview of the IPCablecom2 architecture elements and functional groupings is illustrated in Figure III.1.

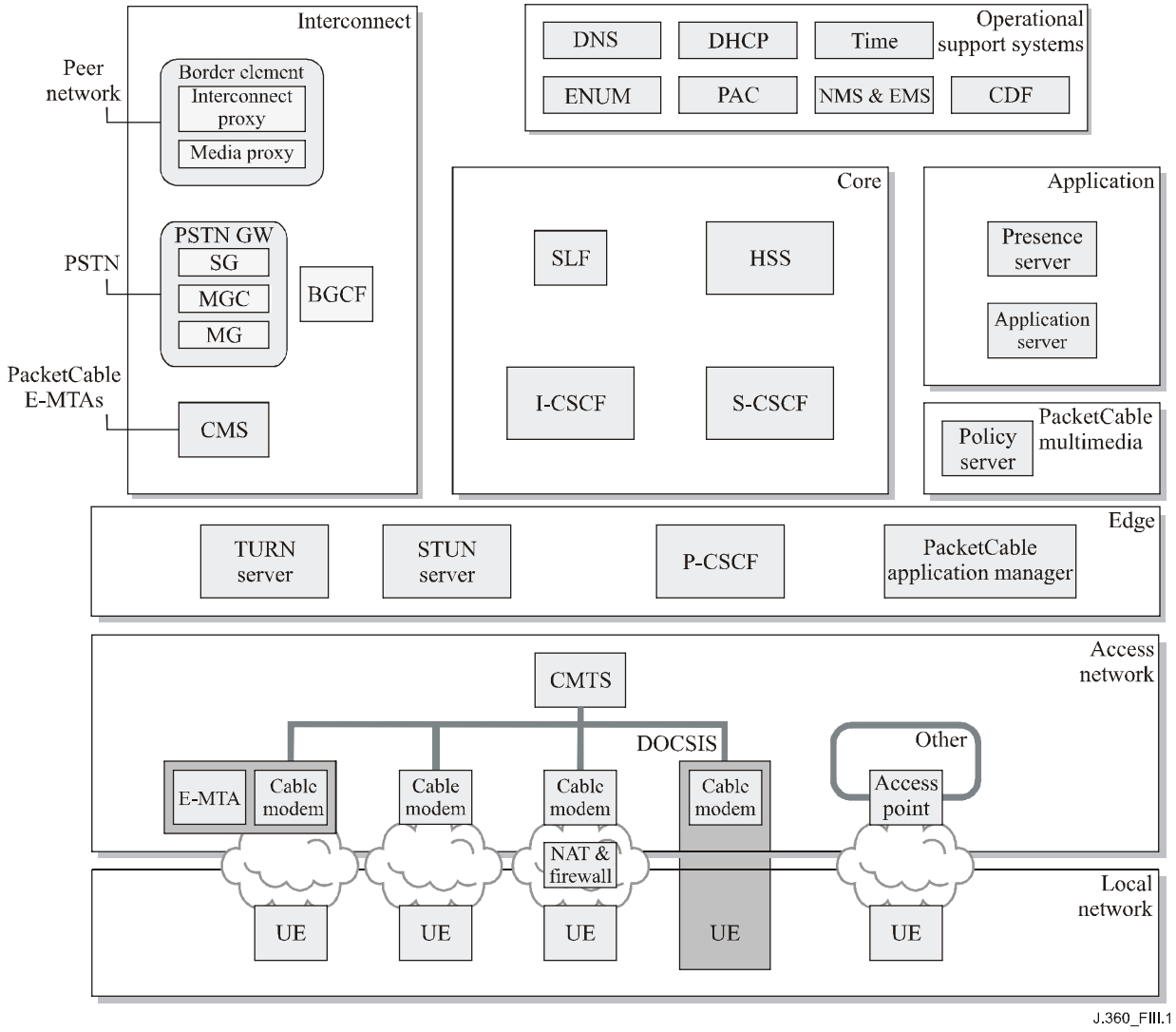


Figure III.1 – IPCablecom reference architecture

The IPCablecom2 architecture is based on the IMS architecture, with the addition of some incremental extensions to support cable networks. These extensions include the use of additional or alternate components, as well as enhancements to capabilities provided by IMS functional components.

Some of the major IPCablecom2 enhancements to the IMS include:

- Support for quality of service for IMS-based applications on cable access networks, leveraging the IPCablecom multimedia architecture.
- 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 for IPCablecom UEs.
- Support for provisioning, activation, configuration and management of IPCablecom UEs.

IPCablecom2 includes both the existing IMS logical components and reference points, and logical elements and reference points added to support IPCablecom2 requirements.

III.5.3 IPCablecom2 security threats

III.5.3.1 General threats: Classification and analysis

Following is an overview of the general threats in the context of a generic IP multimedia communications architecture.

III.5.3.1.1 Trust domain threats

A trust domain is a logical grouping of network elements that are trusted to communicate in a manner consistent with a set of relevant security policies. Trust domains can be demarcated by physical or logical boundaries. Communication across trust domains must always be reviewed for authentication and authorization. Interfaces of interest for an IP multimedia infrastructure are:

- Intra-network domain interfaces, which connect network elements within a service provider's domain. A compromise to any network element can be detrimental to the proper functioning of the network itself. Threats involve almost all the ones mentioned in this clause.
- Inter-network domain interfaces, which connect two domains. The domains can be different service providers, or the same provider. Inter-domain trust levels can dictate the level of trust one can have within a domain (intra-domain), and hence, it is imperative that such interfaces be secured. Further, the security of two domains connected in such a manner relies on all the other connections established by each individual domain.
- Access domain interfaces, which allow UEs to connect to a service provider. This set of interfaces is highly vulnerable to a multitude of security threats, largely due to the fact that access domains typically contain trusted as well as untrusted UEs and network elements. Strong authentication for any kind of network access would be vital for a service provider. If authentication is to be foregone, the services offered and the network elements to which such an unauthenticated access is provided should be minimized.

III.5.3.1.2 Theft of service

"Theft of Service" refers to a multitude of threats, including but not limited to:

- Manipulation of the UE – UEs, especially software UEs, are vulnerable to Trojan attacks and manipulation of behaviour. Mitigation techniques include signed code and embedded UEs.

- Protocol weakness exploitation – Exploitation of weak cryptographic measures can have a large impact, as it typically involves major redeployment. Mitigation techniques include defense in depth architecture.
- Identity spoofing – The act of impersonating another user in order to gain access to services. This can lead to loss of credibility and revenue. Mitigation includes the use of strong authentication and user education.
- UE cloning – The act of imitating a legitimate UE. This is typically an issue when UE identities are deemed sufficient to offer services, such as in architectures without the distinction of a 'user' and a 'client'. The recommendation would be to require UE credentials, to authenticate users before offering services, and to build infrastructures that can identify cloning and mitigate threats.
- Subscription fraud and non-payment of services – Subscriptions established with falsified information and detection of non-payment are beyond the scope of this specification.

III.5.3.1.3 Disruption and denial of service

General DoS attacks aim to cause service interruption by crippling some or all service providing entities in the network. These attacks occur at layer 2 through layer 4 of the OSI reference model. Denial of service attacks focus on rendering a particular network element unavailable, using one of several different mechanisms. DoS attacks include:

- Malformed message attacks – An attacker issues malformed messages that attempt to exploit a weakness in the robustness of a stack. Weaknesses include buffer overflows, or insufficient corner case and error handling. Mitigating this attack requires well-designed software protocol stacks and robustness testing.
- Layer four depletion attacks – An attacker causes excessive state information to be consumed on a victim device, often in the context of state-aware protocol stacks. An example is a TCP-level attack such as a SYN flood, used to exhaust stack resources that keep track of session state. These attacks can be mitigated by intrusion detection systems (IDS) and firewalls, and by well-designed software protocol stacks and robustness testing.
- Bearer-level flooding attacks – Denial of service attacks that focus on rendering a particular network element unavailable, usually by directing an excessive amount of media network traffic at its interfaces. Preventing this attack requires state-aware firewalls that open pinholes for media only if the trusted side of the firewall initiates the connection first. Flooding attacks often make use of spoofed source addresses to open firewall pinholes. Source address verification through 3-way handshakes can mitigate this threat. Quality of service (QoS) can also prevent excessive flows through a router.

Flooding attacks generally make use of IP packets with spoofed source addresses. By preventing packets with spoofed addresses, some flooding attacks can be mitigated. There are several mechanisms to prevent address spoofing:

- Use a challenge/response mechanism such as STUN or TURN.
- Use of TCP makes source address verification easier (3-way handshake).
- Unicast reverse path forwarding (uRPF) – Uses routing tables to determine whether the route to the source of the packet (the reverse path) is pointing to the interface the packet came in on.

Zombie attacks consist of any type of denial of service attack that is launched from an authenticated endpoint. In addition, most zombie attacks make use of many zombies, resulting in a distributed denial of service attack (DDoS). Typically, a Trojan compromises an endpoint in order to leverage the endpoint's authentication. It is very difficult to defend against a zombie attack because the endpoint is authenticated and authorized. Zombie attacks can be thwarted by detecting anomalous traffic behaviour and filtering malicious traffic.

III.5.3.1.4 Signalling channel threats

In a multimedia environment such as a SIP architecture, signalling messages include data pertaining to identity, services, routing and other sensitive and critical data. Multimedia components such as proxies exist in the access domain, exposing them to a greater number of threats.

Attacks on signalling security include:

- Compromise of confidentiality – Signalling information, such as the caller identity and the services to which a customer subscribes may be vulnerable to discovery. The caller's identification information may also be used to locate the caller even if the caller wished to keep their location private.
- Man in the middle (MiM) attacks – Attacks resulting from the interception and possible modification of traffic passing between two communication parties. These attacks are successful if the communicating parties cannot distinguish communications with the intended recipient from those of the attacker. Attacks, some of which are described in other clauses, include impersonating a proxy, undesired redirection, and loss of privacy due to MiM intervention.
- Denial of service attacks – DoS attacks in the signalling channel range from the creation of bogus requests resulting in amplification attacks to falsifying routing headers. The use of multicast to transmit SIP requests greatly increases the potential for DoS attacks.

Many of these threats can be mitigated by requiring mutual authentication, identity assertion, confidentiality, and integrity on the signalling plane.

III.5.3.1.5 Bearer channel threats

Threats to the bearer channel relate to the media traffic transferred between communicating parties.

Attacks on bearer security include:

- Compromise of confidentiality – Confidentiality in this sense is protection of the media messages themselves, which could be an audio session, instant messaging, or other multimedia message transfer. Depending on the security mechanism negotiated, end-to-end confidentiality may not be under the control of the sender.
- Compromise of integrity – Modification, deletion, and replay are all possible attacks to the bearer channel.
- Disruption attacks – As with any media technology, the ability of parties to communicate introduces unwanted communications. This category includes all the "normal" public switched telephone network (PSTN) attacks such as harassment, as well as some new threats relating to degradation and disruption of service in the IP model.

Bearer channel attacks are mitigated by requiring mutual authentication, confidentiality and integrity on the bearer plane to prevent manipulation of data on the bearer plane, and ensuring privacy of sensitive information.

III.5.3.1.6 Reconnaissance

Well-planned attacks on service providers normally start with gaining reconnaissance on a network. Reconnaissance threats can be mitigated by using topology hiding mechanisms, including the introduction of border elements. Enforcing filtering techniques in the access domain allows for traffic policy enforcement at the edge of the network.

III.5.3.1.7 Roaming model considerations

Roaming models can minimize or add to security threats. UEs accessing services through alien environments can expose both the UE and the home network to greater risks. The trust relationship between the home and visited networks is enforced at the inter-domain security boundary.

III.5.3.2 Protocol specific security threats

The following clauses highlight threats to multimedia protocols. While this list does not include every multimedia protocol, it includes the major protocols discussed in the architecture and in later clauses.

III.5.3.2.1 SIP

Examples of attacks that can be performed from information gained by capturing SIP messages on the network include:

- Tampering with message bodies (e.g., sending malformed SIP messages to disrupt a SIP network element; sending fake REGISTER messages to cause signalling messages to be redirected, rendering the hijacked UE unable to initiate or accept sessions).
- Tearing down sessions (e.g., sending BYE or CANCEL messages to end a session prematurely).
- Impersonating a server (e.g., sending false INVITEs).
- Masquerading and faking server responses leading to service unavailability or denial of service (e.g., flooding the network with 302 Redirect or 401 Unauthorized messages).

Some of the important vulnerabilities are explained in the following subclauses.

III.5.3.2.1.1 Registration hijacking

Registration hijacking involves a malicious endpoint that changes the registration of a different, existing endpoint, to point either back to the attacker, or to a different location. Registration hijacking can take several forms:

- SIP endpoint cloning – An attacker user agent (UA) may attempt to register as an existing victim UE. The attacker UE becomes a "clone" of the victim UA, stealing the victim's identity.
- Exploitation of weak identity – If a registrar assesses the identity of a UA, the 'From:' header of a SIP request can be arbitrarily modified and hence open to malicious registration.
- Attackers could de-register some or all users in an administrative domain, thereby preventing these users from being invited to new sessions, resulting in a type of DoS attack.

Refer to section 26.1.1 in [IETF RFC 3261] for more information about registration hijacking. The general method to prevent registration hijacking is to use secure identity assertion.

III.5.3.2.1.2 Faking user identity

Unless authenticated, SIP messages are vulnerable to identity spoofing. Fields such as 'From:' are not required to be filled and 'P-Asserted-Identity', unless populated by a trusted element securely, can be manipulated.

Possible solutions to mitigate such a threat include:

- Use strong credentials, and establish secure tunnels for message flows.
- Use appropriate SIP Identity mechanism like "SIP identity" that supports cryptographically verifiable assertions.

III.5.3.2.1.3 Malformed SIP messages

An attacker can issue malformed SIP messages that attempt to exploit a weakness in the robustness of a SIP stack or the protocol itself. Weaknesses include unwarranted DoS initiation, buffer overflows, or insufficient corner case handling. Mitigating this attack requires stack robustness testing. Specific scenarios that lead to DoS attacks include:

- Using falsified Via header fields identifying a targeted host as the originator of the request and then sending these requests to a large number of SIP network elements.
- Using falsified Route headers in a request that identify the target host and then sending such messages to forking proxies that will amplify messaging sent to the target.

SIP proxy servers by nature accept requests from varied IP endpoints, and are consequently exposed to an increased number of threats.

III.5.3.2.1.4 SIP message storms

SIP message storms can consist of sending random SIP messages so that memory or processing power is exhausted by exhausting state storage or requiring encryption steps, respectively. SIP message storms can happen either from within a network, or from the outside. Mitigation techniques to thwart such attacks include:

- Debugging stacks for resource depletion.
- Use of anti-replay countermeasures.
- Avoiding multiple responses to a single event (e.g., multiple 401 messages for authentication challenge).
- Detecting storms and using appropriate filters to shutdown misbehaving UEs.

Message storms may arise from registration floods, where a large number of endpoints attempt to register, but fail authentication at the edge of the network and bog down the edge proxies. In addition, edge proxies may allow endpoints to register without authentication, and then defer the UE challenge to servers internal to the network, in which case the internal servers are susceptible to DoS floods. There are several ways to mitigate these types of attacks:

- Require authentication at the edge proxies, to spread the load of authentication and better defend against registration DoS floods.
- Impose flood-control measures – provide a nonce to UEs that authenticate for the first time, which can be used later, under less strict rate limiting.
- Allow the P-CSCF to prioritize signalling, based on previously successful challenges from the same UE.

III.5.3.2.1.5 Session hijacking

Methods of launching a session hijacking attack include the following:

- Modification of SDP information.
- Using messages like "301 moved permanently" to redirect INVITEs to another location (assuming the attacker knows Call-ID, To, From, Cseq fields).

The general method to prevent session hijacking is to require authentication of all SIP messages.

III.5.3.2.1.6 Impersonating a server

SIP servers may be impersonated in the network by an attacker. SIP server impersonation can result in a DoS or privacy breach. It presents a possibly greater problem when SIP mobility is considered. The general method to prevent impersonation is server authentication by UAs.

Refer to section 26.1.2 in [IETF RFC 3261] for more information.

III.5.3.2.1.7 Tampering with message bodies

Refer to section 26.1.3 in [IETF RFC 3261] for more information.

III.5.3.2.1.8 Tearing down sessions

Refer to section 26.1.4 in [IETF RFC 3261] for more information.

III.5.3.2.1.9 Reconnaissance threats

Certain SIP messages and fields facilitate reconnaissance threats. Mitigation of such threats can be facilitated by preventing the usage of certain fields (e.g., OPTIONS) in messages.

III.5.3.2.2 STUN

In general, attacks on STUN can be classified into denial of service attacks and eavesdropping attacks. Denial of service attacks can be launched against a STUN server itself, or against other elements using the STUN protocol.

Many of the attacks require the attacker to generate a response to a legitimate STUN request, in order to provide the UE with a faked MAPPED-ADDRESS. The attacks that can be launched using such a technique include:

- DDoS against a target.
- Silencing a UE.
- Assuming the identity of a UE.
- Eavesdropping.

More detailed information on these attacks and how the threats are addressed by the STUN protocol itself can be found in [IETF RFC 3489].

III.5.3.2.3 TURN

A TURN server acts as a redirector, to funnel media streams through a NAT to a destination. A TURN server therefore has the potential to become a source for a DoS attack that utilizes high-bandwidth media streams. Critical to preventing misuse of a TURN server is a cryptographically verifiable way of establishing an authentication and authorization mechanism to allow recipients of media streams to authorize the TURN server to forward media.

III.5.3.2.4 TLS

Because transport layer security (TLS) is hop-by-hop, it may be compromised within a server that terminates and re-originates signalling.

TLS also relies on a mechanism to establish trust between two communicating entities, such as a public key infrastructure (PKI) within an administrative domain. TLS establishment between servers should involve mutual authentication.

TLS generally relies on transitive trust for hop-by-hop security. If each endpoint has its own local server, and the servers trust each other, then the endpoints can assume through transitive trust that the end-to-end communication is secure.

III.5.3.2.5 HTTP Digest

The primary threat posed to HTTP-Digest authentication involves a MiM (man in the middle) attack. HTTP Digest operates by verifying that a user has a pre-shared password. After the UE requests access to a resource, the server challenges the UE for a password. In the challenge, the server sends down a nonce in the clear that should be used by the UE to generate a securely formed hash of the password. The hashed password is sent to the server in the clear. This method of authentication is susceptible to a MiM using a dictionary attack, in an attempt to find a password

that results in the same secure hash as the value sent back to the server. Consequently, HTTP Digest should be used over secure data paths.

III.5.3.2.6 DNS

The domain name system in general is insecure without the use of DNSSEC. Possible security threats include manipulation of request or response queries leading to redirection or denial of service, and usage of dynamic DNS functionality, if enabled, to manipulate DNS servers and reflect incorrect topologies.

To mitigate some of these threats, DNS should only be used for general information and other configuration mechanisms, such as authentication, used to validate network elements.

III.5.3.2.7 Software-based UEs

IPCablecom support software-based UEs to authenticate and use network services. Software-based UEs present challenges that lead to vulnerabilities:

- Even though software-based UEs may have a provision to connect to a secure hardware keystore, such as a smart card, they generally store credentials in unprotected storage.
- The software image on a soft UE is not tamper-proof.
- Applications on software-based UEs may store a user's password for later automated entry.

III.5.4 IPCablecom2 security architecture overview

This clause describes the IPCablecom2 security architecture, including enhancements to the IMS. The trust domains described in clause III.5.3 are used to decompose the IPCablecom2 architecture. Each trust domain is discussed in further detail in the following clauses.

III.5.4.1 Access domain

UEs connect to the network through the access domain. Interfaces and components present in the access domain are shown in Figure III.2.

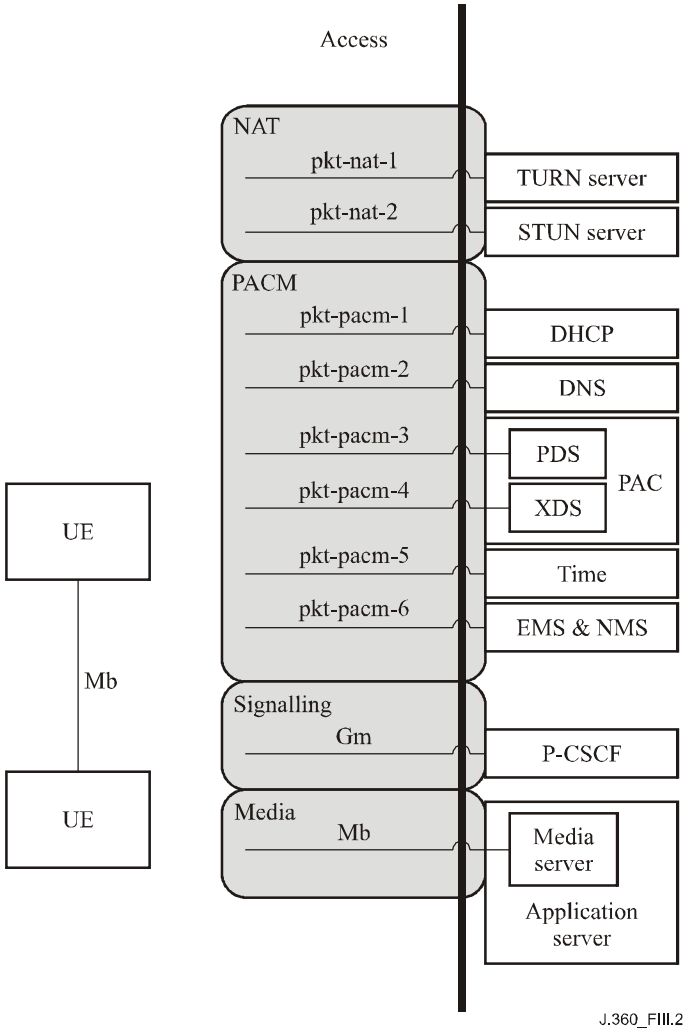


Figure III.2 – Access domain reference points

UE interactions with the network occur in the access domain. Access methods are varied, and include DOCSIS and wireless. Due to these characteristics, the access domain is home to a multitude of threats, as described in clause III.5.3.

Table III.1 provides a high-level overview of the security architecture that results from the IPCablecom2 enhancements to IMS. Each access domain reference point, along with the security mechanism employed for that interface, are included.

Table III.1 – Access domain reference points description

Reference point	IPCablecom2 network elements	Reference point security description
pkt-nat-1	UE – TURN server	TURN: TURN requests are authenticated and authorized within the TURN protocol itself.
pkt-nat-2	UE – External STUN server	STUN: Message integrity is provided by STUN mechanisms.
pkt-pacm-1	UE – DHCP server	DHCP: IPCablecom2 does not define security for the DHCP protocol.
pkt-pacm-2	UE – DNS server	DNS: IPCablecom2 does not define security for the DNS protocol.

Table III.1 – Access domain reference points description

Reference point	IPCablecom2 network elements	Reference point security description
pkt-pacm-3	UE – PDS server	SIP: Message integrity and privacy via IPSec or TLS.
pkt-pacm-4	UE – XDS server	XCAP: Message integrity and privacy via HTTP over TLS.
pkt-pacm-5	UE – Time server	SNTP: IPCablecom2 does not define security for the SNTP protocol.
pkt-pacm-6	UE – EMS & NMS server	Management interface security is out of scope for this specification.
Gm	UE – P-CSCF	SIP: Message integrity and privacy via IPSec or TLS. STUN: Message integrity is provided by STUN mechanisms (as STUN requests are sent to the standard SIP port, P-CSCF must logically contain STUN functionality).
Mb	UE – UE UE – Media server UE – MG UE – E-MTA	RTP: Media security is out of scope for this specification.

III.5.4.2 Intra-network domain

Intra-domain reference points and components are contained within a service provider's network, and consequently, a holistic security policy.

IMS defines the security of intra-domain connections with the Zb interface, as described in [ITU-T J.366.8]. Within IMS, integrity is required and confidentiality is optional when the Zb interface is implemented. IPSec ESP is used to provide security services for the Zb interface between intra-domain components.

IPCablecom enhances the Zb interface by adding TLS to provide security services for intra-domain TCP data flows. Clause III.6.6 describes the Zb reference point TLS requirements.

III.5.4.3 Inter-network domain

Inter-domain reference points connect the operator security domain with external partners and networks. These connections provide interworking between the operator's network and other service providers and networks, including the PSTN. Figure III.3 shows the inter-domain trust boundary.

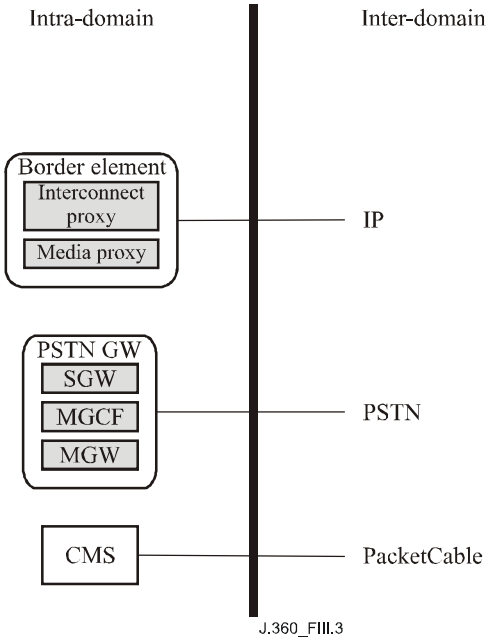


Figure III.3 – Inter-network domain reference points

IMS defines the security of inter-domain connectivity with the Za interface, as described in [ITU-T J.366.8]. Both integrity and confidentiality are required for the Za interface, based on IPSec ESP. Inter-domain traffic in IMS is required to pass through a security gateway (SEG). The SEG terminates reference point Za IPSec tunnels and enforces security policy on inter-domain traffic flows. Figure III.3 shows an architecture including the SEG functionality in the border element, but the SEG may be a separate element.

The PSTN gateway to PSTN reference point is secured using PSTN security mechanisms.

IPCablecom2 adds support for inter-networking to IPCablecom networks. The call management server (CMS) provides translation for IPCablecom messaging. Security for the CMS reference point is detailed in [ITU-T J.170].

III.6 IPCablecom security requirements

The following clauses describe the IPCablecom2 enhancements to the IMS security architecture.

III.6.1 User and UE authentication

3GPP IMS relies completely on credentials stored in a UMTS integrated circuit card (UICC) for access security. The UICC is a platform for security applications used for authentication and key agreement. IPCablecom has a requirement to support multiple types of UEs, such as software UEs, which will not contain or have access to UICCs.

[ITU-T J.366.7] describes the IMS approach to authentication and establishing transport security between the UE and the P-CSCF. The IMS uses a combination of IPSec for integrity and optional confidentiality, and IMS-AKA for authentication. To meet the IMS requirements of minimal round trips, the security elements of the negotiation "piggy-back" on the SIP register messaging flow. [IETF RFC 3329] is used to negotiate security between the UE and the P-CSCF, and IMS-AKA [IETF RFC 3310] is used between the UE and the S-CSCF to perform mutual authentication. [IETF RFC 2617] is extended to pass authentication data from the UE to the S-CSCF. The communications between the UE and the P-CSCF and the communications between the UE and the S-CSCF are related in that the keying material for the security associations between the UE and the P-CSCF are computed from the long-term shared secret stored in the home subscriber server (HSS)

and the UICC in the UE. Figure III.4 shows the high-level message flows for authentication during registration. Some elements and messages are not displayed in order to simplify discussion.

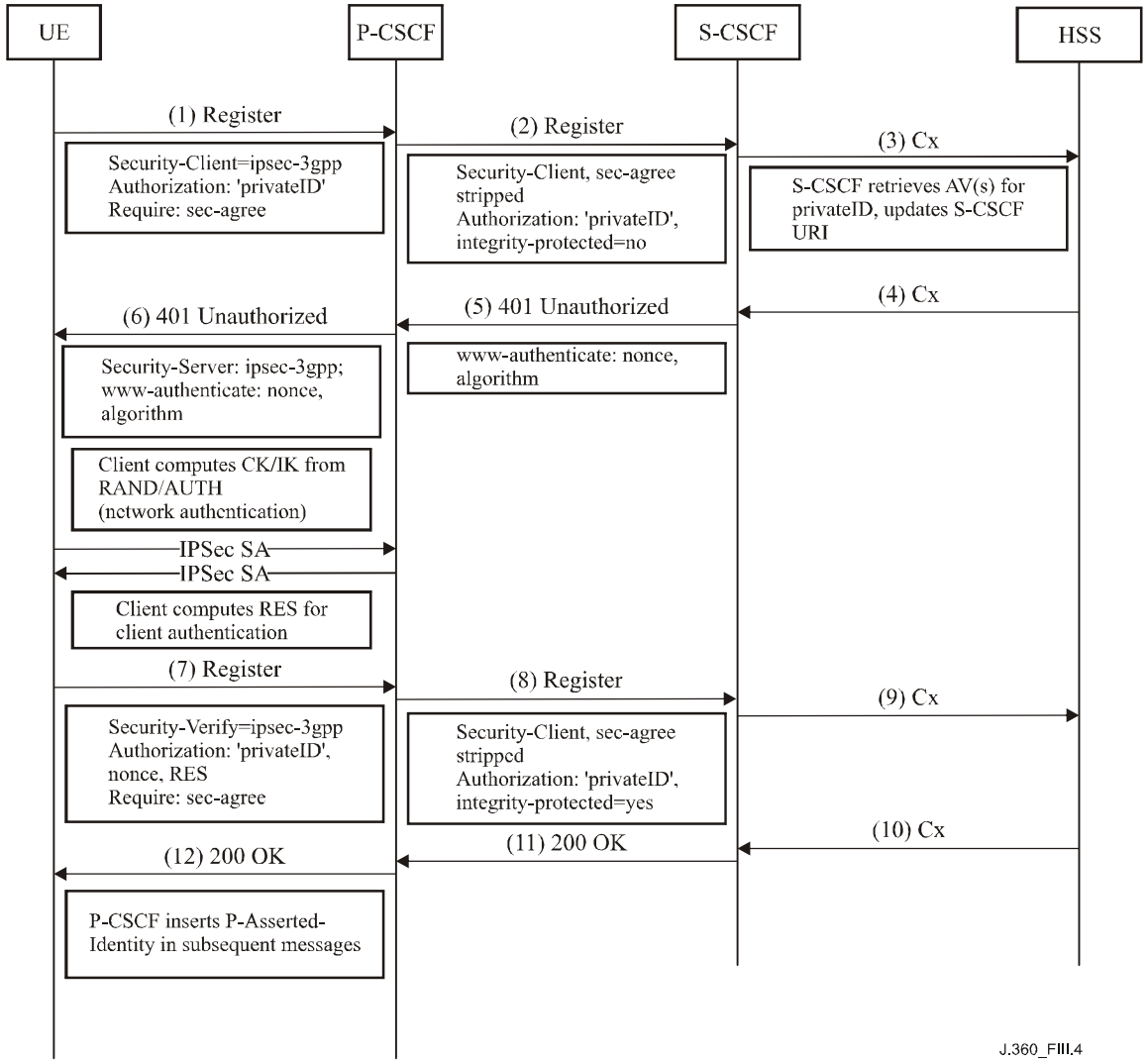


Figure III.4 – IMS registration message flow

For authentication during registration, the following basic steps occur:

1) The UE sends a register request to the P-CSCF. The message includes an [IETF RFC 3329] security-client header which includes the security mechanisms the UE supports. IMS mandates 'ipsec-3gpp'. The message also includes an authorize header which includes the private identity of the subscriber.

2) The P-CSCF strips the security agreement headers, inserts 'integrity-protected=no' in the authorized header, and forwards the register request to the appropriate I-CSCF, which forwards the request to the appropriate S-CSCF of the subscriber's home network.

3) The S-CSCF contacts the HSS to update the S-CSCF URI for that user, and if necessary, requests one or more authentication vectors.

4) The HSS returns one or more authentication vectors if requested. The authentication vectors provide the necessary data for the S-CSCF to create a www-authenticate header and challenge the user.

5) The S-CSCF creates and sends a SIP 401 (Unauthorized) response, containing a www-authenticate header that includes a challenge. This response is routed back to the P-CSCF.

6) The P-CSCF strips the integrity key (IK) and the confidentiality key (CK) from the 401 response to use for IPSec SAs between the P-CSCF and the UE, and sends the rest of the response to the UE.

7) Upon receiving the challenge message, the UE determines the validity of the received authentication challenge. The UE sets up security associations with the P-CSCF using the IK and CK that was derived from the data sent by the HSS, utilizing the long-term shared key in its UICC. The UE then calculates a response (RES) and sends a second register request with an authorization header including the challenge response. This message includes Security-Verify headers as per [IETF RFC 3329].

8) The P-CSCF strips the security agreement headers, inserts 'integrity-protected=yes' in the authorize header, and forwards to the appropriate I-CSCF which forwards to the appropriate S-CSCF.

9) The S-CSCF compares the authentication challenge response received from the UE with the expected response received from the HSS. If they match, the S-CSCF updates HSS data using the Cx interface.

10) The HSS provides the S-CSCF with subscriber data over the Cx interface, including service profiles, which contain initial filter criteria.

11) The S-CSCF forwards a 200 OK response to the UE. The 200 OK contains a P-Associated-URI header which includes the list of public user identities that are associated to the public user identity under registration.

12) The P-CSCF forwards the 200 OK to the UE. Because the user has now been authenticated and there is an existing security association between the P-CSCF and the UE, the P-CSCF inserts a P-Asserted-Identity header in all subsequent messages from that UE.

IPCablecom has requirements to support UEs and authentication schemes not considered in the IMS architecture, as well as additional transport security mechanisms. IPCablecom2 enhances the IMS specifications in several areas in order to support these requirements.

III.6.1.1 Description

The IPCablecom2 architecture supports the following authentication mechanisms:

- IMS AKA.
- SIP digest authentication.
- Certificate-based authentication.

The architecture must also accommodate UEs with multiple authentication credentials. For example, a UE may have a certificate for accessing services while on a cable network, and a UICC for accessing services while on a cellular network.

A subscriber may have multiple credentials for the same private identity. A subscriber may have multiple UEs, with different capabilities related to those credentials. For example, a subscriber may have an MTA with a certificate for home use, and a UICC-based UE for travelling.

III.6.1.1.1 IMS AKA

IMS AKA authentication with UICC credentials will continue to operate as described in 3GPP specifications.

III.6.1.1.2 SIP digest authentication

IPCablecom2 supports SIP authentication as described in [IETF RFC 3261]. SIP authentication uses a challenge-response framework for authentication of SIP messages and access to services. In this approach, a user is challenged to prove their identity, either during registration or during other SIP dialogues initiations.

SIP authentication in IPCablecom2 is handled in a similar manner to IMS AKA, and follows [IETF RFC 3261] and [IETF RFC 2617]. This approach minimizes impact to the existing IMS authentication flow by maintaining existing headers and round trips. Unlike IMS AKA, however, challenges are not precomputed. In order to maximize the security of SIP digest authentication, cnonces and qop "auth-int" directives are used, which requires challenges to be computed in real-time at the S-CSCF.

Figure III.5 shows the message flow for SIP based authentication during a registration.

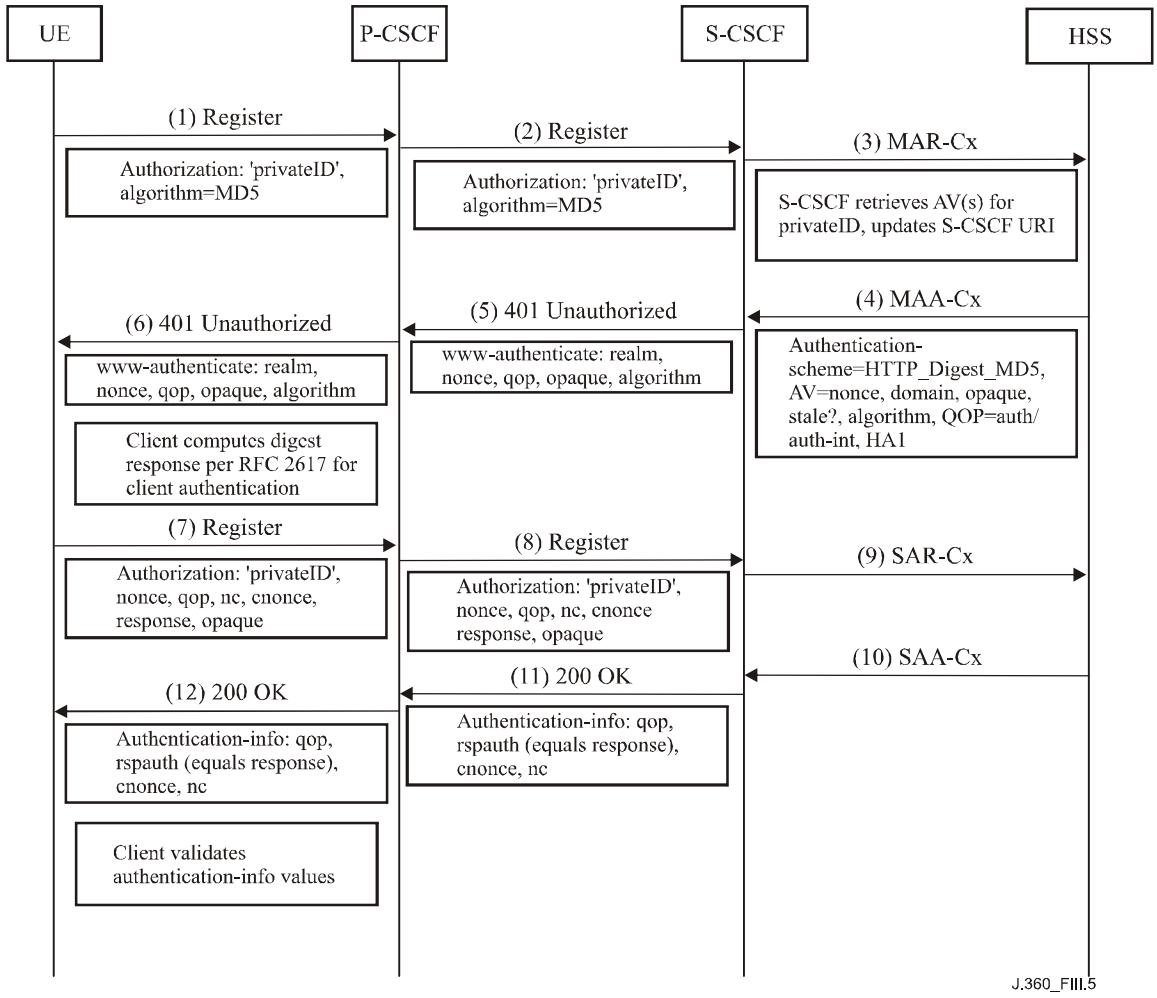


Figure III.5 – SIP digest authentication

For SIP digest authentication during registration, the following basic steps occur. [IETF RFC 3329] headers and other SIP header contents are not shown for simplicity.

1) The UE sends a register request to the P-CSCF. The message includes an authorization header which includes the private identity of the subscriber. An example authorization header is shown below:

```
REGISTER sip:home.atlanta.com SIP/2.0
Authorization: Digest username="alice_private@atlanta.com",
      realm=" atlanta.com", nonce="", uri="sip:home.atlanta.com",
      response="", algorithm="MD5"
```

IPCablecom adds the algorithm parameter to the initial IMS register message in order to inform the network what type of challenge to create. This is to support multiple credential types per user.

2) The P-CSCF forwards the register request to the appropriate I-CSCF, which forwards the request to the appropriate S-CSCF of the subscriber's home network.

3) The S-CSCF contacts the HSS using a MAR command towards the HSS on the Cx interface. The MAR message includes the private identity of the subscriber, the S-CSCF information, and the number of authentication vectors requested. This information is used by the HSS to update the S-CSCF URI for the private identity and to deliver the correct authentication vector information to the S-CSCF.

4) The HSS returns a MAA message on the Cx interface. The MAA message includes the public identities and authentication vectors for that subscriber. The contents of the authentication vector for SIP digest are detailed in a later clause. The main differences are the lack of a CK and IK, and the contents of the SIP-Authenticate data element. Instead of AKA data, the SIP-Authenticate AVP contains data the S-CSCF requires for computing a Digest response, primarily HA1.

5) The S-CSCF creates a SIP 401 (Unauthorized) response, which includes a challenge in the www-authenticate header field, and other [IETF RFC 3261] fields. An example header is shown below:

```
SIP/2.0 401 Unauthorized
      WWW-Authenticate: Digest realm="atlanta.com",
        nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
        qop=auth,auth-int, opaque="5ccc069c403ebaf9f0171e9517f40e41",
              algorithm="MD5"
```

Details on nonce creation are described in a later clause. Based on local policy, the server sends back the qop parameters the client must choose from.

6) This response is routed back to the P-CSCF, and then to the UE.

7) Once the UE receives the challenge, the UE calculates the response based on items in the WWW-Authenticate header and additional items (e.g., cnonce) generated by the UE. The values in the Authorize header are calculated as per [IETF RFC 3261], and thus [IETF RFC 2617]. The qop value is selected from the choices provided by the S-CSCF. cnonce values are computed as described in a later clause. The UE sends a second register request with the Authorization header. An example Authorization header is shown below:

```
REGISTER sip:home.atlanta.com SIP/2.0
      Authorization: Digest
              username="alice_private@atlanta.com", realm="atlanta.com",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              uri="sip:home.atlanta.com", qop=auth-int, nc=00000001,
              cnonce="0a4f113b",
              response="6629fae49393a05397450978507c4ef1",
              opaque="5ccc069c403ebaf9f0171e9517f40e41", algorithm="MD5"
```

8) The P-CSCF forwards the message to the appropriate I-CSCF which forwards to the appropriate S-CSCF.

9) Upon receiving the second register from the UE, the S-CSCF calculates the challenge in the same manner as the UE, in order to compare the two results and thus authenticate the subscriber. Using parameters from the HSS such as HA1, and the parameters from the Authorization header such as cnonce, the S-CSCF computes the challenge response as per [IETF RFC 3261] and thus [IETF RFC 2617]. The computation is performed in a manner consistent with the qop parameter sent by the UE.

   If the two challenge results are identical, the S-CSCF performs a SAR procedure on the Cx interface, informing the HSS the user is registered and requesting the user profile.

10) The HSS returns a SAA message to the S-CSCF containing the user profile, which includes, among other things, the collection of all the public user identities allocated for authentication of the private user identity, as well as the initial filter criteria.

11) The S-CSCF sends a 200 OK response to the register request. The response includes an Authentication-Info header, which allows the UE to authenticate the network, or S-CSCF. The rspauth value is calculated per [IETF RFC 2617]. The header also includes a nextnonce value. The 200 OK message is forwarded to the UE. An example Authentication-Info header is shown below:

```
SIP/2.0 200 OK
        Authentication-Info:
        qop=auth-int, rspauth="7729fae49393a05397450978507c4ef1",
        cnonce="0a4f113b",nc=00000001,
        nextnonce="8829fae49393a05397450978507c4ef1"
```

12) The 200 OK is routed to the appropriate P-CSCF, and then to the UE.

13) The UE validates the rspauth value, to authenticate the network, or S-CSCF.

Because the user has now been authenticated and there is an existing security association between the P-CSCF and the UE, the P-CSCF inserts a P-Asserted-Identity header in all subsequent messages from that UE.

Adding support for SIP digest impacts the IMS specifications in the following ways:

- New digest algorithms are allowed to be present in the www-authenticate and authorization headers.
- The HSS must compute and store new types of digest responses.
- UEs must be able to support and compute new types of digest responses.
- The home network (or S-CSCF) authenticates to the UE by including an Authentication-Info header in the 2xx response following a successful authentication of the UE.

Impacts to specific components are discussed in clause III.6.1.2.

III.6.1.1.3 Certificate-based

Certificate-based authentication is out of scope for this version of this appendix.

III.6.1.2 Impacted components

The following clauses describe the impacts to IMS components in order to accommodate IPCablecom authentication requirements.

III.6.1.2.1 UE

In order to support new forms of authentication, IPCablecom UEs must send the appropriate 'algorithm' parameter in initial register requests.

IPCablecom UEs supporting digest authentication must conform to [IETF RFC 3261], and thus [IETF RFC 2617]. UEs must send the 'algorithm' parameter set to the appropriate digest algorithm in the initial register request. Upon receiving a challenge from the S-CSCF in a 401 Unauthorized message, UEs must create an authorization header including a challenge response as described in [IETF RFC 2617] based on the algorithm parameter in the www-Authenticate header. cnonce and nc parameters must be included in the challenge response. The cnonce should be 32 octets encoded as ASCII hexadecimal as per [IETF RFC 2617], following the guidelines of [IETF RFC 1750]. The qop value used for the response calculations and returned in the authorization header must be one of the values received in the 401 www-Authenticate header from the S-CSCF. UEs must be able to validate Authentication-Info header values returned from the S-CSCF with the 200 OK message.

UEs must be able to securely store usernames and passwords in a manner that minimizes risk. UEs may optionally prompt users for username and password input.

III.6.1.2.2 S-CSCF

In order to support new forms of authentication, the S-CSCF must understand new values for the 'algorithm' parameter in the authorization headers sent by UEs. This value must then be used for the 'Authentication-Scheme' AVP in Cx procedures.

In order to support SIP digest, the S-CSCF must be able to calculate digest responses as described in [IETF RFC 3261] and [IETF RFC 2617]. The S-CSCF will receive HA1 from the HSS over the Cx interface, and the S-CSCF must use this HA1 value to create the digest response for this private identity. This response is compared to the response received by the UE, so it must be calculated in the same manner. The qop value received from the UE must be used for the response calculation. If the S-CSCF calculated response is identical to the response received from the UE, the S-CSCF sends a 200 OK containing an Authentication-Info header per [IETF RFC 2617]. The nextnonce parameter must be used in the Authentication-Info header.

Because the security of digest depends greatly on the calculation of the nonce, the S-CSCF must follow these guidelines when regarding nonce creation and use:

- The nonce must be 32 octets encoded as ASCII hexadecimal as per [IETF RFC 2617].
- The nonce must be generated following pseudo random number generation such as [IETF RFC 1750].
- Nextnonce is always sent in Authentication-Info responses (e.g., 2xx responses) to successful authentication of the UE.

Based on local policy, the S-CSCF should:

- Accept a previously used nonce with a valid nonce-count, for example, to allow for PRACK and other types of requests received before a 2xx response.
- Only accept a previously used nonce for a specific period of time. It is recommended to use a time value of 10 minutes or less.
- Only accept a previously used nonce for a specific number of times. It is recommended to use a value of 5 times or less.
- Accept an old nonce based on the above policy rules even if nextnonce was sent.

The above policy rules are mainly related to the case where signalling security is disabled in the network.

III.6.1.2.3 HSS

In order to support new authentication schemes, the Cx interface and procedures must be extended. Digest authentication adds new parameters to the Cx interface, specifically the SIP-Auth-Data-Item AVP present in both MAR and MAA procedures. The authentication vector provides the S-CSCF

with HA1 and other elements to allow the S-CSCF to compute responses. For further details, see Appendix IV.

III.6.1.3 Signalling security

The IMS defines IPSec for the secure signalling between UEs and edge proxies. The UICC provides credentials for authentication and IPSec. The security mechanism is negotiated using [IETF RFC 3329] SIP security agreement. However, the only mechanism allowed for negotiation in IMS is ipsec-3gpp.

IPCablecom2 adds TLS as an option for signalling security between the UE and the P-CSCF. The use of TLS by the UE is optional, and is based on the following advantages:

- TLS is the recommended security mechanism specified in [IETF RFC 3261].
- There is a general shift towards the use of TCP to better handle longer messages.
- TLS supports NAT traversal at the protocol layer.
- TLS is implemented at the application level instead of the kernel level, which provides some advantages such as easier support in multiple environments.

Adding support for TLS for signalling leads to the consideration of TLS credentials.

- Mutually authenticated TLS – UE and server both provide certificates when establishing signalling security. The server must validate the UE certificate, and the UE must validate the server certificate. Mutual authentication provides a high degree of security.
- Server side authentication – Only the server provides a certificate when establishing signalling security. This approach avoids the extra computational overhead of a PKI operation on the UE. Provides a medium level of security, with lower CPU requirements on the UE. May be used to secure HTTP digest sessions.

Both of these models require the P-CSCF and the UE to support PKI features, such as certificate validation and certificate management.

Adding support for TLS also leads to the consideration of TLS port assignments and TLS connection management. IPCablecom2 will use the standard SIP ports for UDP, TCP and TLS. UEs negotiating optional TLS before SIP messaging connect to the SIPS port of 5061. Otherwise, UEs use the standard SIP UDP/TCP port of 5060. Requests and responses are performed according to procedures in [ID SIP-OUTBOUND].

IPCablecom2 supports an optional TLS session prior to SIP signalling, if the UE and P-CSCF support it. This provides security on the initial register message. [IETF RFC 3329] headers are still used during the registration process, to provide security against bid-down attacks and maintain consistency with the existing IMS registration message flow.

Figure III.6 shows signalling security negotiation during a successful register dialogue. Only signalling security headers are shown for simplicity.

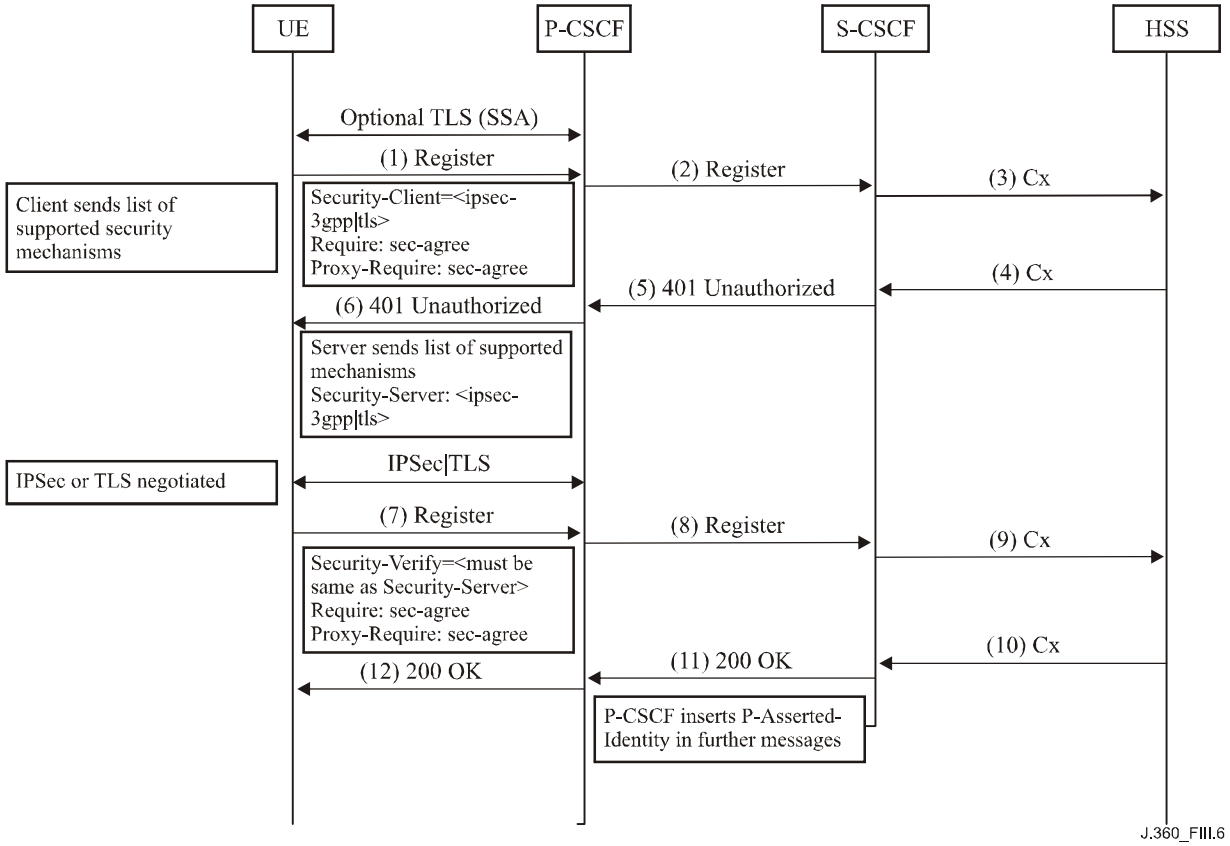


Figure III.6 – Transport security

To support TLS for signalling security between the UE and the P-CSCF, the IMS specifications must be enhanced to allow TLS as an optional SIP security mechanism to be negotiated. [IETF RFC 3329] includes TLS as a security mechanism that can be negotiated, thus the only change is to IMS specifications.

As shown, TLS capable UEs may negotiate server side authenticated TLS before SIP messaging, for instance when a user requires privacy. [IETF RFC 3329] headers are used to negotiate signalling security during the SIP registration, to protect against bid-down attacks, and to maintain consistency with current IMS message flows.

At a high-level, the impacts to IMS components are:

- UE must support the ability to negotiate TLS using [IETF RFC 3329].
- UE may establish TLS before SIP messaging.
- P-CSCF must support the ability to negotiate TLS using [IETF RFC 3329].
- P-CSCF may support TLS before SIP messaging.

III.6.1.3.1 Impacted components

The following clauses describe the impacts to IMS components in order to negotiate signalling security.

III.6.1.3.1.1 UE

In order to support the negotiation of signalling security, IPCablecom UEs must support TLS as defined in [IETF RFC 2246].

UEs must support the construction and interpretation of [IETF RFC 3329] headers containing the mechanism-name of 'tls'.

III.6.1.3.1.2 P-CSCF

The P-CSCF must be able to establish TLS sessions based on a request from a UE. The P-CSCF should always request UE certificates, but if it receives none, should establish server side authenticated TLS. If mutually authenticated TLS is established, the P-CSCF must set integrity-protected=yes in Authorization headers. If mutually authenticated TLS is not established, the P-CSCF sets integrity-protected=no. These rules are in addition to the existing rules for IPSec establishment. While server side authenticated TLS provides integrity, mutually authenticated TLS more closely resembles the 3GPP case of IPSec combined with AKA.

The P-CSCF must support the [IETF RFC 3329] mechanism-name of 'tls'. This may be negotiated as either mutual or server side authenticated TLS, depending on the capabilities of the UE. The same rules for assigning integrity-protected values apply as above.

Certificates should be validated according to [IETF RFC 3280].

III.6.1.3.1.3 S-CSCF

The S-CSCF can challenge any SIP message. Messages containing Authorize headers with integrity-protected set to 'no' should always be challenged, as this flag indicates the lack of signalling security between the UE and the P-CSCF on non-initial register requests. If the S-CSCF successfully challenges a subscriber, the S-CSCF must insert the P-Asserted-Identity header in subsequent messages from that subscriber if the P-Asserted-Identity header does not exist.

III.6.1.3.2 Disabling signalling security

While not recommended, signalling security may be disabled at the P-CSCF. By disabling signalling security, UEs and the network are exposed to many of the threats described in clause III.5.3, especially when combined with a weaker form of authentication such as SIP digest.

The IPCablecom2 SIP signalling (Appendix I) and the IPCablecom2 [ITU-T J.366.4] delta specification contain detailed information on the procedures for disabling signalling security. The major difference in procedures for disabling signalling security is that non-register dialog requests should now be challenged.

III.6.2 Identity assertion

IPCablecom environments require a way for trusted network elements to convey the identity of subscribers to other elements or services, and to remove the identity when communicating with untrusted networks. Identity assertion is the mechanism by which elements and services can trust the identity of a user.

As described in [ITU-T J.366.4], IMS assigns the task of identity assertion to P-CSCFs for all SIP messages, based on the strict flow described in clause III.6.1. Once the IPSec security associations (SA) are established and the subscriber is authenticated, the P-CSCF asserts the identity of the subscriber. By monitoring SIP messaging towards the UE, the P-CSCF observes the 200 OK message from the subscribers S-CSCF. This information, plus the presence of SAs to the UE allow the P-CSCF to substantiate successful authentication of the UE.

IPCablecom2 enhances IMS with the following requirements:

- A P-CSCF with an established TLS session with a UE that observes a 200 OK response from the S-CSCF for that subscriber can assert the identity of the public identity used by that UE.
- A P-CSCF without an established TLS session that observes a 200 OK response from the UEs S-CSCF during SIP authentication cannot assert the identity of that UE. In this case, the S-CSCF asserts the identity after successful authentication of the subscriber.

III.6.3 NAT traversal security

The following clauses describe STUN and TURN security.

III.6.3.1 STUN

The STUN protocol [IETF RFC 3489] defines the countermeasures for the attacks described in clause III.5.3.2.2. These include network architecture recommendations as well as message integrity mechanisms provided by STUN itself. No additional mechanisms are proposed for this version of this appendix.

III.6.3.2 TURN

The TURN server represents a network resource that is utilized for the duration of a connection, therefore security for this resource is an important consideration.

The TURN protocol [ID TURN] defines the countermeasures for the attacks described in clause III.5.3.2.3. These include network architecture recommendations as well as message integrity mechanisms provided by TURN itself. No additional mechanisms are proposed.

NOTE – Security for TURN is being updated. Details will be provided once the TURN draft becomes available.

III.6.4 Configuration security

III.6.4.1 Generic bootstrapping architecture

The 3GPP authentication infrastructure has been recognized for its ability to enable application functions in the network and on the user side to establish shared keys. Therefore, 3GPP designed the "bootstrapping of application security" to authenticate the subscriber by defining a generic bootstrapping architecture (GBA) based on the AKA protocol. GBA reference points and components are shown in Figure III.7.

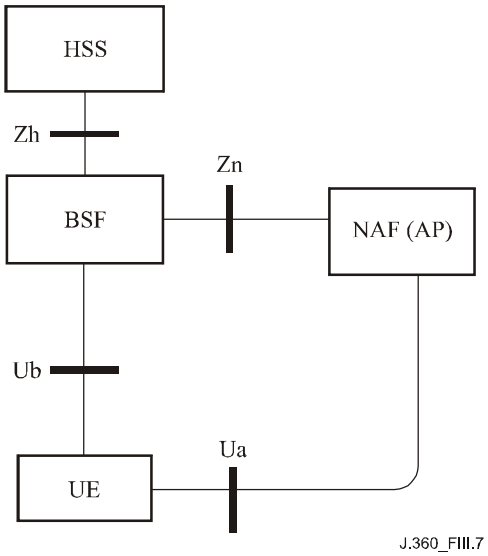


Figure III.7 – GBA reference points and components

IMS currently describes the generic bootstrapping architecture (GBA) based on the AKA protocol. This architecture provides a means for a UE to bootstrap to a server, in order to receive configuration information, and to derive keys that can be used by the UE and application servers to secure communications on the Ua interface.

According to [ITU-T J.366.9], a generic bootstrapping server function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards used between the UA and network application function (NAF). For this purpose, the BSF shall acquire the GBA user security settings (GUSS) from the HSS, and shall restrict the applicability of the key material to a specific NAF by using a key derivation procedure. As described in [ITU-T J.366.9], the IMS uses the GBA to authenticate and receive configuration information over IPSec. The IMS requires a UICC-based ISIM for this process, as it relies on IMS AKA for authentication and IPSec for secure transport.

Because IPCablecom2 is extending IMS to support non-UICC deployment scenarios, the AKA protocol cannot be used by all IPCablecom clients to achieve mutual authentication between the UE and the BSF. Consequently, a new procedure is needed. IPCablecom adds an option for the Ub interface to support HTTP Digest over TLS for GBA authentication and key derivation.

Note that in IPCablecom2, the NAF is an XCAP server, which provides the configuration to the UE.

For UEs that do not support IPSec and AKA, when the UE starts communicating with the NAF, it must establish a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate. The UE must verify that the server certificate corresponds to the FQDN of the NAF it established the tunnel with. No UE authentication is performed as part of TLS (i.e., there is no UE certificate necessary). The Zh, Zn and Ua are standard interfaces defined in [ITU-T J.366.9].

The Ub interface uses the HTTP Digest mechanism to establish the credentials (e.g., session key(s)) between the UE and the BSF.

The new bootstrapping exchange on the Ub interface is illustrated in Figure III.8.

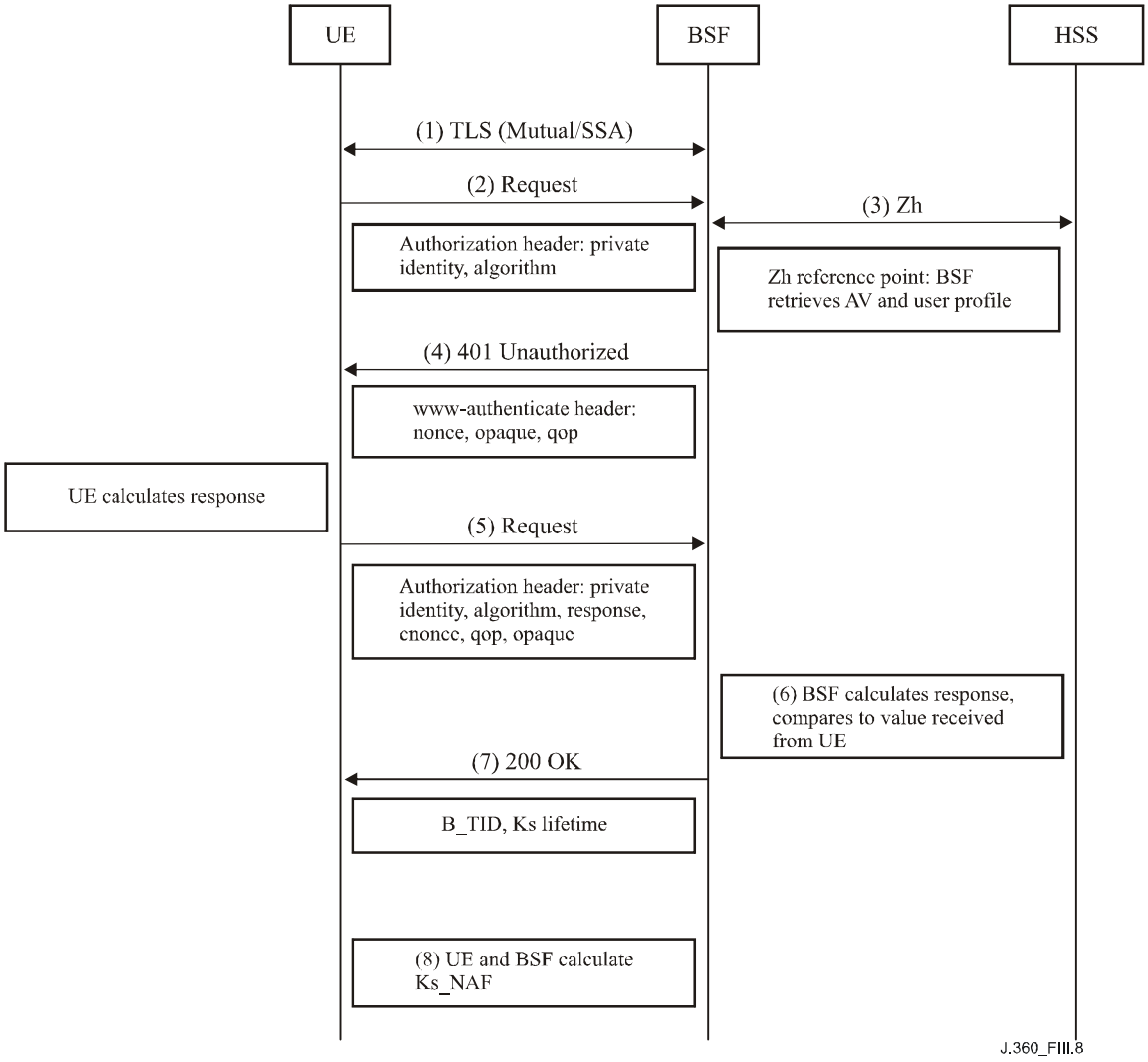


Figure III.8 – GBA message flow

The following steps describe the bootstrapping procedure for HTTP Digest over TLS.

1) The UE starts the bootstrapping procedure by initiating a TLS session with the BSF. The UE and BSF negotiate server side authenticated TLS. The UE authenticates the BSF by the certificate presented by the BSF. The BSF does not require authentication from the UE at this point.

2) The UE starts the bootstrapping procedure by sending an HTTP Request message to the BSF containing the private identity in an Authorization header. The UE indicates the algorithm it supports in the algorithm parameter of the Authorization header.

3) The BSF sends a MAR command to the HSS to retrieve an authentication vector for that user. The HSS responds with the appropriate authentication vector for that user and algorithm in a MAA message. The authentication vector contents are enhanced as in SIP digest to allow the BSF to calculate a challenge to the UE as described in [IETF RFC 2617].

   NOTE 1 – In a multiple HSS environment, the BSF may have to obtain the address of the HSS where the subscription of the user is stored by querying the SLF, prior to step 3.

4) The BSF responds to the UE request with a 401 Unauthorized message containing a www-authenticate header to force the UE to authenticate itself. The www-authenticate header includes a nonce, created following the guidelines described earlier in this appendix

(i.e., 32 octets encoded in ASCII hexadecimal). The algorithm parameter informs the UE of the algorithm it should use to calculate its response.

5) Upon receiving the challenge, the UE uses the data received in the www-authenticate header to create a second HTTP Request with the challenge response in an Authorization header. The challenge response is calculated per [IETF RFC 2617]. A cnonce must be included. The UE must select a qop value from the list of qop values sent by the BSF. The message is sent to the BSF over the TLS session.

6) The BSF checks the validity of the challenge response sent from the UE by calculating the response on its own and comparing the values. The BSF calculates the response per [IETF RFC 2617]. It uses the HA1 value supplied by the HSS over the Zh reference point.

7) If the challenge response sent by the UE is identical to the response calculated by the BSF, the BSF must send a 200 OK message including the B-TID to the UE to indicate successful authentication. In addition, in a 200 OK message, the BSF shall supply the lifetime of the key Ks.

   The B-TID value must be generated in the format of NAI by taking the base64 encoded nonce value from step 4, and the BSF server name, i.e., base64encode(nonce)@BSF_servers_domain_name.

   NOTE 2 – Before base64 encoding the nonce from step 4, the nonce must first be converted from a hexadecimal ASCII-encoded value to a binary-encoded value.

8) Both the UE and the BSF must use the TLS master secret from the existing TLS session for Ks. Both the UE and the BSF must use the Ks to derive the key material Ks_NAF. Ks_NAF must be used for securing the reference point Ua.

   Ks_NAF is computed as Ks_NAF=KDF(Ks, "gba-h", RAND, IMPI, NAF_Id) where KDF is the key derivation function described in Annex B of [ITU-T J.366.9]. The binary-encoded nonce is substituted for the AKA-based RAND variable when calculating Ks_NAF. Ks is the master secret from the existing TLS session.

   The UE and the BSF must store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key is updated.

   The key Ks is used to derive keys for communications with application severs, such as the provisioning, activation and configuration (PAC) element, using the Ua reference point.

III.6.4.2 Secure software download

Secure software download is out-of-scope for this version of this appendix.

III.6.5 Media security

Media security is out-of-scope for this version of this appendix.

III.6.6 Using TLS for intra-domain security

As defined by IMS-delta specification [ITU-T J.366.8], the Zb reference point connects IMS components within the same trust domain in a secure manner. Implementation of the Zb interface is optional. If implemented, the Zb interface must use IPSec ESP for authentication and integrity. Confidentiality (encryption) is optional.

IPCablecom2 adds TLS support for intra-domain security, for the following reasons:

- TLS is the recommended security mechanism specified in [IETF RFC 3261].
- TLS supports NAT traversal at the protocol layer.
- TLS is implemented at the application level instead of the kernel level, which provides some advantages such as easier support in multiple environments.

IPCablecom2 components with SIP interfaces are required to support TLS for intra-domain security, in addition to IMS defined IPSec.

Unless specified within this clause, SIP interfaces requiring TLS MUST be compliant with the TLS specification [IETF RFC 2246] and any requirements specified in [IETF RFC 3261] relating to its usage in SIP.

TLS [IETF RFC 2246] supports the negotiation and use of compression methods. However, since these methods are not specified within TLS [IETF RFC 2246], compression MUST NOT be used.

III.6.6.1 TLS authentication algorithms

The HMAC-SHA-1 (with 160-bit key) algorithm must be supported in order to provide data origin authentication and data integrity services in TLS. AES-XCBC is not required.

III.6.6.2 Key exchange algorithms for TLS

The following are the requirements relating to methods for key exchange within the TLS protocol:

- Rivest Shamir Adleman (RSA) must be supported.
- Diffie Hellman (DH) must be supported.

III.6.6.3 Use of X.509 certificates in TLS

X.509 certificates are used for authentication in TLS, and all X.509 certificates should be signed by a trusted party. Self-signed certificates may be used.

III.6.6.4 Random number generator for TLS

Random number generation implementations tend to be a weak. Many semiconductor manufacturers are adding secure random number generators to their integrated circuits, which should be used if available. If no hardware is available, strong pseudo-random number generator software may optionally be used in keeping with [IETF RFC 1750].

The following are the requirements relating to random number generation:

- A hardware random number generator may be supported.
- Pseudo random number generator software must be supported if a hardware random number generator is not supported.

III.6.6.5 TLS encryption algorithms

The following are the TLS client and TLS server requirements related to cryptographic algorithms for providing encryption services for TLS-SA:

- 3DES CBC-mode (with 3 independent 56-bit keys) must be supported.
- AES CBC (with 128-bit key) must be supported.
- Null encryption may be supported.

III.6.6.6 Ciphersuites for TLS

TLS specifies various ciphersuites for use within the TLS protocol, as discussed in detail in [IETF RFC 3268]. Ciphersuites represent the recommended combinations of encryption authentication and key exchange algorithms to be used within the TLS.

The following are the requirements related to Ciphersuites.

- "TLS_RSA_WITH_NULL_SHA" may be supported.
- "TLS_RSA_WITH_3DES_EDE_CBC_SHA" should be supported.
- "TLS_RSA_WITH_AES_128_CBC_SHA" must be supported
- "TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA" should be supported.

- "TLS_DH_RSA_WITH_AES_128_CBC_SHA" must be supported.

III.6.6.7 TLS authentication

TLS allows either unidirectional authentication where the server is authenticated to the client only, or bidirectional authentication where both client and server authenticate to each other. Unidirectional authentication is the usual method used in the public Internet; however, for network signalling and control applications, bidirectional authentication is mandatory to allow both parties to know they are communicating with the desired endpoint.

The following are the requirements related to TLS authentication.

- Bidirectional authentication for TLS applications must be supported.

III.6.7 Certificate validation

[IETF RFC 3280] should be used for guidance on validation of certificates.

III.6.8 Certificate revocation

Certificate revocation is out of scope for this version of this appendix.

Appendix IV

IPCablecom2 home subscriber server (HSS) overview

(This appendix does not form an integral part of this Recommendation)

For further study.

Appendix V

IPCablecom2 NAT and firewall traversal overview

(This appendix does not form an integral part of this Recommendation)

V.1 Introduction

This appendix provides an overview of how the IPCablecom2 architecture and associated UEs support the traversal of NA(P)T and firewall devices (commonly referred to as NAT) for media and signalling flows as well as for provisioning and management. To aid the reader in understanding the IPCablecom2 NAT traversal approach and methodologies, the high level goals and specific logical components and interfaces defined are discussed in this appendix.

V.2 References

This appendix uses the following additional informative references.

[ITU-T J.179] ITU-T Recommendation J.179 (2005), *IPCablecom support for multimedia*.

[ITU-T J.364] ITU-T Recommendation J.364 (2006), *IPCablecom2 provisioning, activation, configuration and management*.

[IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) terminology and considerations*.

[ID BEHAVE] IETF draft, draft-ietf-behave-nat-udp-04, *Network Address Translation (NAT) Behavioural Requirements for Unicast UDP*, 6 September 2005.

[ID ICE] IETF draft, draft-ietf-mmusic-ice-07, *Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*, 6 March 2006.

[ID OUTBOUND] IETF draft, draft-ietf-sip-outbound-03, *Managing Client Initiated Connections in the Session Initiation Protocol (SIP)*, 20 March 2006.

[IETF RFC 3489] IETF RFC 3489 (2003), *Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NAT) (STUN).*

[ID TURN] IETF draft, draft-ietf-behave-turn-00, *Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)*, February 2005.

V.3 Terms and definitions

Various terms related to NAT are defined in [IETF RFC 2663]; please refer to it for the general NAT terms and definitions not present below. In addition, this appendix uses the following terms:

V.3.1 ALG: An Application layer gateway within a NAT device which attempts to sniff application signalling and modify application addresses appropriately in order to take care of changes caused by the NAT.

V.3.2 **NAT**; **NAPT**: NATs perform IP address translation, typically interconnecting private and public address domains. NAPT devices also translate ports in order to save IP addresses. In this appendix, the term NAT also refers to NAPT devices.

V.4 Abbreviations and acronyms

This appendix uses the following additional abbreviations:

DQoS Dynamic Quality of Service

UDPTL UDP Transport Layer

VPN Virtual Private Network

V.5 IPCablecom2 NAT requirements and scope

The objective of this appendix is to provide an architecture definition for a UE to obtain access to the IPCablecom2 network in the presence of one or more NAT device(s). In particular, it outlines a comprehensive set of mechanisms for a UE to maintain both signalling and media bindings to ensure both media and signalling traffic destined for the UE is able to traverse the NAT as well as to allow the UE to be provisioned and managed when located behind a NAT.

In addition, this architecture provides support for failover of signalling paths through a backup Proxy-CSCF (P-CSCF).

Finally, this architecture recognizes that UEs will have to interwork with non-IPCablecom2 devices that do not support the required NAT traversal mechanisms and provide for these cases.

The following clause captures the set of architecture requirements necessary to achieve the objective.

V.5.1 Requirements

The following list contains requirements that a general-purpose NAT traversal solution should satisfy to support the services envisioned for IPCablecom2:

- Support multiple UEs (on one or more devices) behind a single NAT.
- No requirements will be imposed on the NAT devices, nor require the network to be aware of the presence of a NAT.
- Support both inbound and outbound requests to and from UEs through one or more NAT device(s).
- 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: the solution should not employ application-specific mechanisms which could not be used by other non-SIP based solutions. The solutions, actually used, may require application support.
- Avoid unnecessarily long media paths due to media pinning.
- Re-establish communications in failure situations (e.g., the NAT device re-boots and NAT bindings are lost).

V.5.2 Scope

The scope of the IPCablecom2 NAT traversal solution is limited to NATs within the access network. In the case of cable access, this implies NATs that are between the UE and CMTS. Note that IPCablecom E-MTAs are out of scope for this appendix However, some additional requirements may be placed on IPCablecom E-MTAs in order to ensure they interoperate with

IPCablecom2 UEs following the traversal procedures described in this appendix and other specifications.

V.5.3 Limitations

This appendix does not address NAT and firewall traversal of ITU-T T.38 fax media streams over user datagram protocol transport layer (UDPTL).

Operator call-back for emergency calls (such as 911) made without first registering is not currently supported.

V.6 NAT background

Network address translators (NATs) translate addresses between one IP address realm and another. This mapping is most commonly done between a private Internet address space using addresses set aside for that purpose and a public Internet address space. This mapping is commonly referred to as a NAT binding as the NAT has bound together the tuple of PrivateIP:PrivatePort to PublicIP:PublicPort to allow the subsequent response packets from the external endpoint to be forwarded to the proper internal host. The term NAT in this appendix also refers to network address port translation (NAPT) devices which also translate port addresses in order to reduce the number of public addresses used on the public address side of the NAT (see [IETF RFC 2663] section 4 for more details).

In addition to address translation, NAT devices also exhibit firewall characteristics. In other words, they block traffic coming across the NAT (from outside to inside the NAT/FW device) based on certain filtering rules.

V.6.1 Types of NA(P)T and firewall devices

The following subclauses use the definitions from the IETF BEHAVE working group as defined in [ID BEHAVE].

V.6.1.1 Types of NATs

The definitions from [ID BEHAVE] are included here for convenience:

Endpoint independent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to any external IP address and port.

Address dependent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external IP address, regardless of the external port. If the packets are sent to a different external IP address, the mapping will be different.

Address and port dependent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external address and port. If packets are sent to a different IP address and/or port, then a different mapping will be used.

This address mapping behaviour is described in Table V.1 by making use of the illustration in Figure V.1.

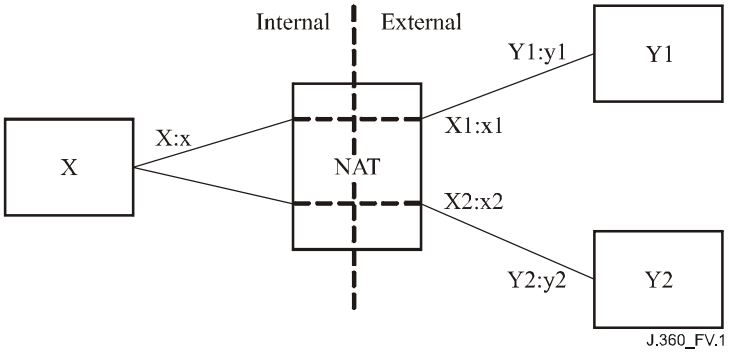


Figure V.1 – Types of NATs (Address mapping)

In Figure V.1, address X:x inside the NAT is translated to address X1:x1 when communicating with Y1:y1 outside the NAT. The same address X:x translates to X2:x2 when communicating with Y2:y2.

Table V.1 – Types of NATs (Address mapping)

Type of NAT	Mapping description
Endpoint independent mapping	X1:x1 always equals X2:x2 for all values of Y2:y2
Address dependent mapping	X1:x1 equals X2:x2 only if Y1 equals Y2
Address and port dependent mapping	X1:x1 equals X2:x2 only if Y1:y1 equals Y2:y2

Note that for small NATs (e.g., residential CPE NATs), a single IP address (usually from the public space) is normally assigned as the external IP address (i.e., X1 = X2). However, larger NATs will assign the external IP address from a pool of available IP addresses.

V.6.1.2 Filtering behaviour

Filtering behaviour in [ID BEHAVE] is described in terms of similar categories:

- Endpoint independent filtering: sending packets from the internal side of the NAT to any external IP address is sufficient to allow any packets back to the internal endpoint.
- Address dependent filtering: in order to receive packets from a specific external endpoint, it is necessary for the internal endpoint to send packets first to that specific external endpoint's IP address.
- Address and port dependent filtering: receiving packets from a specific external endpoint, it is necessary for the internal endpoint to send packets first to that external endpoint's IP address and port.

Table V.2 describes this filtering behaviour which can be described in terms of the examples shown in Figure V.1.

Table V.2 – Types of filtering behaviour

Type of NAT	Filtering example
Endpoint independent filtering	Packets sent from X:x to Y1:y1 will enable packets from Y1:y1 or Y2:y2 to be received.
Address dependent filtering	Packets sent from X:x to Y1:y1 will enable packets to be received from Y1:z for any port z but will not allow packets to be received from any other IP address.
Address and port dependent filtering	Packets sent from X:x to Y1:y1 will only allow packets to be sent from Y1:y1 to X:x.

V.6.2 NA(P)T and firewall traversal considerations

While NAT devices provide a rather simple solution to IP address exhaustion, the consequence is that these devices break many existing applications; in particular, applications and real-time communication protocols such as SIP, which depend on the exchange of addressing information within the protocol itself (sometimes in SIP header lines, or more generally, inside the SDP message body of some SIP messages). If the address within the protocol is unreachable, the recipient of the message will be unable to successfully respond resulting in failed sessions. Given the growing problem NAT devices present to communications protocols, several solutions have been used in the past and proposed for the future. The following list provides a snapshot of some of the more prevalent approaches and their drawbacks:

- Application layer gateway (ALG): One solution is for the NAT device to contain an Application layer gateway which looks inside the protocol messages and modifies them based on the NAT bindings it has created. However, this requires constant update of the ALG as protocols evolve so that the expected operation is preserved. In addition, this approach fails when the protocol includes an integrity check or is encrypted.
- Another approach is that proposed by the IETF MIDCOM group. In this approach, a signalling element directly controls the NAT device to open firewall pinholes for the media and to obtain the NAT binding information needed to update any IP addressing information (e.g., SDP) within the protocol. However, this requires NAT device support and requires that the signalling device is somehow able to determine which NAT device to control.
- Other proposed solutions include directly inserting a media relay (an additional address translator) in the path or tunneling through the NAT device using VPN technology. Each of these methods has its pros and cons but the major disadvantage is that it forces the media along the same path as the signalling. This may not result in the most optimum media routing in certain circumstances.
- The present short-term solution defined within the IETF is to make use of the ICE methodology [ID ICE], with STUN [IETF RFC 3489] and TURN [ID TURN] for media and outbound [ID OUTBOUND] for signalling. ICE allows an endpoint to discover, advertise and find the best address for communicating using the mechanisms described [ID ICE] while outbound allows the endpoint to actively manage its connectivity to the SIP network by creating and maintaining flows to its provisioned proxy(s) as described in the outbound [ID OUTBOUND].
- Other solutions are being examined within the IETF BEHAVE working group. However, this involves longer-term modification of NAT behaviour in order to solve these problems.

In addition to the problem of protocols which embed IP address information within their payload, NAT devices cause other problems such as:

- NAT devices have timeouts associated with NAT bindings and firewall pinholes. For UDP based transports, these bindings tend to have rather short lifetimes; and if traffic is absent for a period of time, the bindings become invalid and pinholes close. To avoid this situation, mechanisms must be in place to maintain the bindings/pinholes for both media and signalling.
- The IETF RTP protocol specifies that, for UDP and similar protocols, RTP should use an even destination port number and the corresponding RTCP stream should use the next higher (odd) destination port number. However, NAT translations will make this practice invalid since they typically do not maintain these port relationships across the NAT.
- Another issue of concern is the routing of inbound signalling to UE devices. This signalling must be routed through the NAT over a connection for which there is an existing NAT binding.

Given the requirements provided in clause V.5.1, the current IETF solution using ICE (for media) and OUTBOUND (for signalling) was chosen for IPCablecom2. Not only do these solutions satisfy the stated requirements, but they have the benefit of growing industry support.

V.7 IPCablecom2 NAT architecture

Figure V.2 is a reference diagram showing key components and interfaces related to NAT/FW traversal in the IPCablecom2 architecture. The cable modem is not shown since it does not contain any functions specifically related to or impacted by NAT traversal.

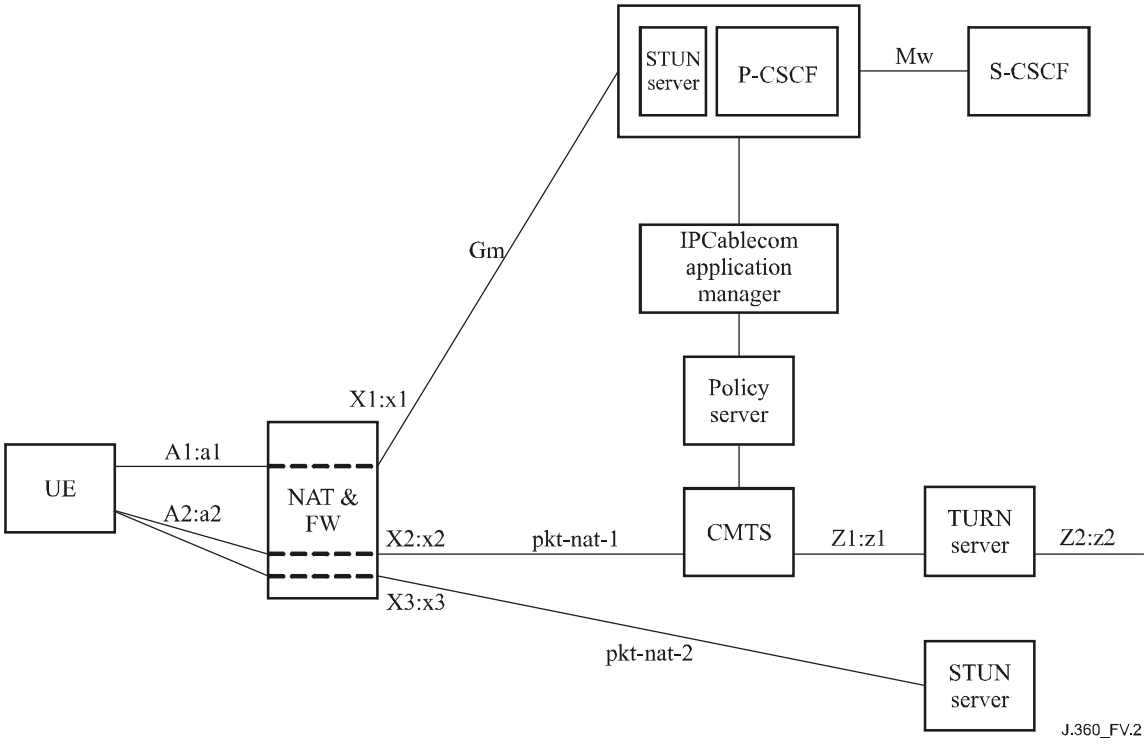


Figure V.2 – NAT and FW traversal reference points

The network addresses shown in the Figure V.2 are of the form "IP_address:port". Note that:

- For UE devices, the same IP address is normally used for media and signalling: A1 = A2.
- For residential CPE NAT/FW devices (e.g., deployed in residential environment), normally X1=X2=X3. For larger NATs, with large numbers of client devices, the external IP address may be selected from a pool of IP addresses.

It is understood that there are other network topologies with NAT devices that may be encountered, such as a network NAT. These other networks are currently outside the scope of IPCablecom2 and thus are not addressed within this appendix. Some network topologies (such as points of interconnection) may be deemed in scope and covered in other documents.

Table V.3 – IPCablecom2 NAT reference points

Reference points	IPCablecom2 network elements	Reference point description
Gm	UE – P-CSCF	Allows the UE to communicate with the P-CSCF for registration and session control. This reference point is SIP-based and is defined in [ITU-T J.366.4]
Mw	CSCF – CSCF	Allows the communication and forwarding of signalling messaging among CSCFs in support of registration and session control. This reference point is SIP-based and is defined in [ITU-T J.366.4]
pkt-nat-1	UE – STUN server/P-CSCF	A STUN-based interface defined by [IETF RFC 3489] and used by the UE to determine the IP address assigned to its serving NAT or to keep NAT bindings active to a P-CSCF via a keep-alive mechanism.
pkt-nat-2	UE – TURN server	A TURN-based interface defined by [ID TURN] and used by the UE to request TURN server resources for relaying media packets to/from the requesting UE.

V.7.1 Relationship to IPCablecom multimedia

Functional elements from the IPCablecom multimedia architecture [ITU-T J.179] are also shown in Figure V.2. This includes the application manager (AM) as well as the policy server (PS). Although this appendix does not impact IPCablecom multimedia operation, there is a requirement for the AM to supply appropriate packet classifier definitions for media flows to the CMTS.

The AM builds packet classifiers for media flows using the default IP address and port as advertised in the "m=" and "c=" lines of the SDP. When a UE invokes the ICE procedure and gathers candidate addresses, it is required to use the TURN server assigned address and port as the default address in the SDP.

When a TURN server is used, the default address advertised in the SDP as illustrated in Figure V.2 is "Z2:z2". However, this is of no value in defining a packet classifier, so some unique filter must be available in the SDP for describing the flows from addresses "X2:x2" and "Z1:z1". Since the client knows where to send the packets, it knows the value of "Z1:z1" and will need to supply this via SDP (a new SDP attribute defined in [ITU-T J.366.4]).

V.7.2 Relationship to 3GPP IMS Release 6

IPCablecom2 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 current IMS Release 6 architecture does not provide support for NAT and firewall traversal. Given this limitation and the requirement for IPCablecom2 to support the traversal of NAT and firewall devices, IPCablecom2 has added the necessary requirements to the existing IMS Release 6 documents. The changes to IMS are confined to two Technical Specifications, ITU-T Rec. J.366.3 and [ITU-T J.366.4].

The changes to ITU-T Rec. J.366.3 add requirements for supporting NAT and firewall traversal from the architecture perspective.

The changes to [ITU-T J.366.4] document procedures related to both signalling and media traversal of NAT and firewall devices. These changes involve adding support for the IETF [ID OUTBOUND] for signalling and the IETF Interactive Connectivity Establishment [ID ICE] for media. Clause V.8 provides a high-level overview of the associated interfaces and network element roles as they relate to NAT traversal.

V.7.3 Relationship to IPCablecom E-MTAs

This appendix does not apply to IPCablecom E-MTAs. However, the proposed solution does imply a requirement on IPCablecom E-MTAs to be able to accept an empty (no payload) RTP packet with a payload type of 20 as a keep-alive for maintaining NAT bindings for media.

V.7.4 Provisioning and management

In addition to supporting the traversal of NAT devices for signalling and media, it is also imperative that the UE be able to be provisioned and managed when behind a NAT. Provisioning refers to the processes involved in the initialization of user attributes and resources on user equipment and network components to provide services to a user. Management refers to the protocols, methodologies, and interfaces that enable monitoring, regulating, and ensuring availability of offered services in a service provider network.

V.7.4.1 Provisioning

The IPCablecom2 provisioning process relies on standard SIP signalling, in particular the SUBSCRIBE/NOTIFY methods. The unique aspect of the provisioning process is that it happens prior to UE registration, which is when NAT bindings are typically created. Given this pre-registration procedure, the P-CSCF needs to leverage IETF Outbound concepts to ensure it can deliver the response to the Subscribe request and the subsequent Notification. This is most easily accomplished by requiring the P-CSCF to add a record route header and insert a flow token in the user portion of the URI used in the record route header field value. The flow token acts as an identifier for the flow over which the SUBSCRIBE was received. The flow allows the P-CSCF to identify the source IP address and port contained in the IP header of the SUBSCRIBE request.

In addition, the UE needs to ensure that the NAT bindings remain active on the life of the subscription so that the associated NOTIFY can be delivered.

V.7.4.2 Management

UE management is currently out of scope and thus no procedures on how to manage a UE behind a NAT have been developed.

V.8 Architecture description

Clause V.7 described a set of logical network entities grouped by specific service functions (NAT), as well as a set of interfaces that support the information flows exchanged between the functional groups and network entities. This clause provides a more detailed discussion of those logical elements and the associated interfaces to the IPCablecom2 architecture. It also provides an overview of other topics related to the NAT architecture that are not documented elsewhere.

V.8.1 Functional components

In this clause, additional detail is provided on each of the functional elements in the IPCablecom2 architecture and their role in NAT and firewall traversal.

V.8.1.1 P-CSCF

The P-CSCF's primary role in NAT traversal is to ensure that requests and responses occur across a flow for which there is an existing NAT binding. When a registration occurs, the P-CSCF stores a flow identifier token in the SIP path header, so that for incoming requests that contain a URI with that flow identifier token, it can identify which flow to use.

The P-CSCF also supports the rport extension to ensure that all responses to the UE including those from mid-dialog requests are sent to the same source IP address and port over which the request was received to ensure their ability to traverse the NAT.

The P-CSCF also acts as a STUN server to allow the UE to use STUN for keep-alives and to check for changes in NAT bindings (e.g., to check for NAT re-boots that would result in removal of the flow).

V.8.1.2 S-CSCF/Registrar

The S-CSCF/Registrar is responsible for generating and assigning the globally routable user agent uniform resource identifier (GRUU) for the UE as well as the associated P-CSCF. The S-CSCF/Registrar stores the instance-id associated with the GRUU as well as the reg-id and path header and includes these as part of the contact information.

V.8.1.3 UE

The UE is responsible for managing the overall NAT discovery process and for invoking the various protocol mechanisms to implement the NAT traversal approach. Depending on the UE type (stand-alone, embedded, etc.), the following protocols or mechanisms are necessary:

- Outbound for signalling.
- STUN client and server for maintaining NAT bindings (signalling and media), connectivity checks (ICE) and candidate address gathering (ICE).
- TURN client for media relay.
- ICE methodology for media.

Before the UE can receive inbound session requests (or responses to outbound session requests), it will need to invoke the procedures defined in [ID OUTBOUND] during the registration process to create a flow to its assigned P-CSCF. Once flows have been created, the UE can then initiate sessions and receive session requests through the NAT.

During the session establishment process, the UE initiates the ICE methodology to gather, advertise and test candidate addresses.

The UE also makes use of the rport extension parameter of the Via header as defined in IETF RFC 3581 for symmetric response routing of SIP messages.

V.8.1.4 STUN servers

STUN servers receive STUN binding requests and provide a response containing the source IP address and port contained in the IP header of the STUN binding request. Two STUN servers are shown in Figure V.2:

- The STUN server shown as a functional component within the P-CSCF is used by the UE in order to maintain the NAT bindings for signalling. These STUN messages may also act as a keep-alive, allowing the UE to determine P-CSCF availability.

- The external STUN server in the lower right hand corner of Figure V.2 is used as part of the ICE methodology [ID ICE] to determine one of several possible candidate media addresses using STUN [IETF RFC 3489]. For the example media stream shown with source IP address "A2:a2", the UE obtains translated address "X3:x3" via the STUN server.

V.8.1.5 TURN server

In addition to the STUN servers, the architecture also contains a TURN server. This may be required if the NAT device does not use endpoint independent mapping (see clause V.6.1.1). When used to transfer media, the TURN server acts as a media relay. The UE sends packets from address "A2:a2" to the TURN server address "Z1:z1". The source address of these packets is first translated by the NAT to "X2:x2" and then relayed by the TURN server so that the source address becomes "Z2:z2". The TURN server also relays media packets in the opposite direction, i.e., packets sent to "Z2:z2" will be sent to "X2:x2" and then via the NAT to "A1:a2". Note that the TURN server provides address independent filtering (see clause V.6.1.2), this retaining some of the filtering characteristics of a NAT, but does not maintain port restrictions, i.e., if traffic is sent to an IP address, it is allowed from that address regardless of what port from which it comes.

Note that only a single example media stream is illustrated in Figure V.2. In fact there may be multiple media streams and each media stream may have an RTP stream as well as an RTCP control channel using RTCP. NAT translations and the corresponding mechanisms for communicating are relevant to both.

V.8.2 Protocol interfaces and reference points

This appendix has identified several interfaces, or reference points, in the IPCablecom2 NAT traversal architecture. An overview of the various protocol interfaces is provided within this clause.

V.8.2.1 NAT traversal for media

UEs communicate via a network that provides signalling components as well as STUN and TURN servers to enable NAT traversal. UE support includes the STUN and TURN protocols as well as the ICE methodology. The associated requirements are provided in the following subclauses. The diagram in Figure V.3 illustrates an abstract view of the architecture.

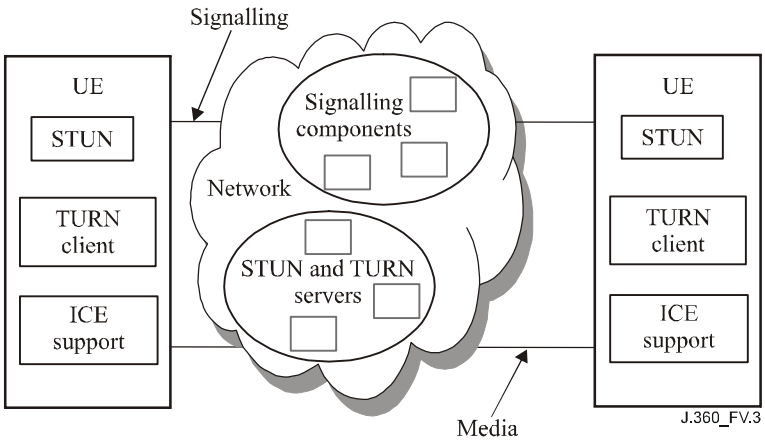


Figure V.3 – Abstract reference diagram

V.8.2.1.1 ICE

The ICE methodology [ID ICE] consists of the following steps:

- Gathering candidate addresses for media communications.
- Advertising the candidate addresses along with the active transport address in the m/c lines of the SDP.

- Doing connectivity checks on the candidate addresses in order to select a suitable address for communications.
- Depending on the results of the connectivity checks, one of the candidate addresses may be promoted to become the active transport address.
- Maintaining the bindings for media.

If one of the endpoints does not support ICE, that endpoint will ignore any of the "a=candidate" attributes and will not provide any of these attributes. In that case, the default value in the m/c lines will be used and connectivity checks will not be done.

V.8.2.1.2 PKT-NAT-1

Simple traversal of UDP through NAT (STUN) provides a toolkit of functions. These functions allow entities behind a NAT to learn the address bindings allocated by the NAT, to keep those bindings open, and communicate with other STUN-aware devices to validate connectivity. STUN requires no changes to NATs, and works with an arbitrary number of NATs in tandem between the application entity and the public Internet.

STUN is a simple client-server protocol. A client sends a request to a server, and the server returns a response. There are two types of requests – Binding Requests, sent over UDP, and Shared Secret Requests, sent over TLS over TCP. Shared Secret Requests ask the server to return a temporary username and password. This username and password are used in a subsequent Binding Request and Binding Response, for the purposes of authentication and message integrity.

Binding requests are used to determine the bindings allocated by NATs. The client 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 client.

Once the client learns the WAN address of its local NAT, it will advertise this learned address as a candidate address in the SDP for remote endpoints to try and reach through the ICE process.

V.8.2.1.3 PKT-NAT-2

TURN is useful for applications that require a client to place a transport address into a protocol message, with the expectation that the client will be able to receive packets from a single host that will send to this address. Examples of such protocols include SIP, which makes use of the session description protocol (SDP). SDP carries an IP address on which the client will receive media packets from its peer. TURN is a simple client-server protocol. It is identical in syntax and general operation to STUN, in order to facilitate a joint implementation of both. TURN defines a request message, called Allocate, which asks the TURN server to allocate a public IP address and port. TURN can run over UDP and TCP, as it allows for a client to request address/port pairs for receiving both UDP and TCP.

A TURN client first discovers the address of a TURN server based on configuration (see [ITU-T J.364]). This can be preconfigured as an IP address, domain name, or FQDN. This will allow for different TURN servers for UDP and TCP. Once a TURN server is discovered, the client sends a TURN Allocate request to the TURN server. TURN provides a mechanism for mutual authentication and integrity checks for both requests and responses, based on a shared secret. Assuming the request is authenticated and has not been tampered with, the TURN server allocates a transport address to the TURN client, called the allocated transport address, and returns it in the response to the Allocate Request. Normally, the allocated transport address will be on one of the interfaces on the TURN server itself. However, it is also allowed for the TURN server to be behind a NAT, in which case the allocated transport address may correspond to the NAT, which is then mapped to the private address of the TURN server. Proper operation of the TURN server will require it to have many bindings established in the NAT ahead of time; the means for doing so are outside the scope of this appendix.

Once the client is assigned a TURN address, it will advertise this address in the "c=" line of the SDP. As a result the TURN server will be the first used address until the other candidate address is found to be a better path through the ICE process.

V.8.2.2 Gm (NAT traversal for signalling)

This clause provides a high-level overview of the procedures defined in [ID OUTBOUND] and roles of the various IPCablecom2 network elements. Note that the term flow is used in [ID OUTBOUND] and in the following clauses to describe a network layer connection that uses the same IP addresses and ports (UDP or TCP) at either end of the connection.

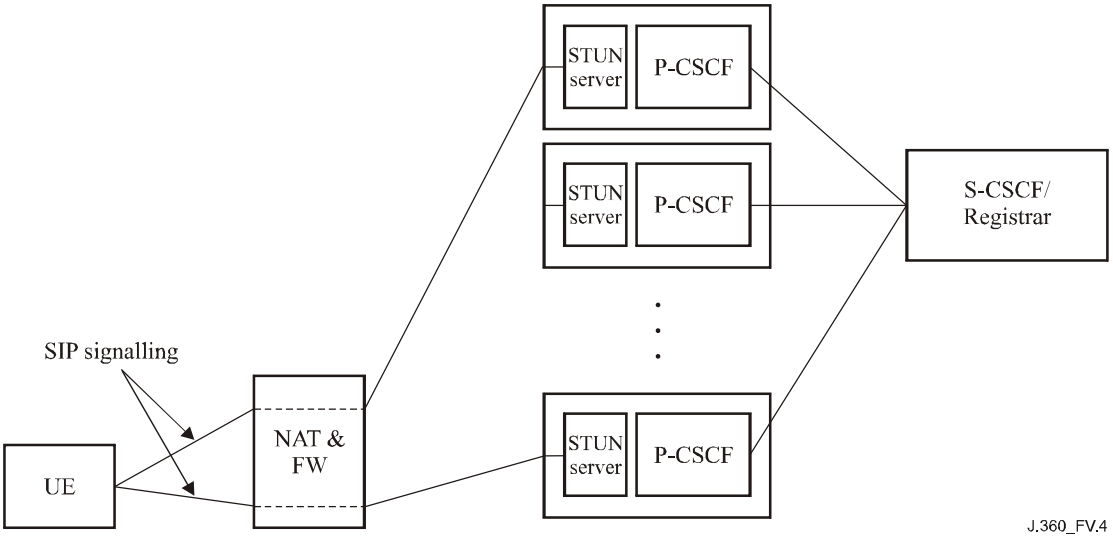


Figure V.4 – NAT traversal for SIP signalling

As illustrated in Figure V.4, a UE may be able to connect to any number of P-CSCFs. However, in order for the UE to receive incoming calls, the signalling must follow a path for which there is an existing NAT binding. Several such bindings may exist over multiple flows to edge proxies (e.g., for redundancy purposes). The problems of NAT traversal for SIP signalling then involve:

- Establishing an outbound connection: Setting up one or more signalling connections or flows to P-CSCF;
- Maintaining the NAT bindings and keeping FW pinholes open for those flows; and
- Inbound signalling: Being able to route the signalling to an appropriate P-CSCF and from there to the UE over a flow for which there is an existing NAT binding.

V.8.2.2.1 Establishing an outbound connection

SIP registration is used to set up an outbound connection and establish NAT bindings for that flow. During registration:

- The UE establishes a unique instance-id that remains constant over re-boots.
- The UE also uses a reg-id as described in [ID OUTBOUND] in order to identify each flow that is established with a P-CSCF. STUN is used to keep the flow (i.e., the NAT bindings and pin-holes) alive.
- The UE includes the instance-id and the reg-id when it registers. If it registers over multiple flows, then it would use the same instance-id, but a different flow-id for that different flow.
- The P-CSCF that forwards the REGISTER and includes a Path header [ID OUTBOUND] in order to establish a signalling path between P-CSCF that is terminating the specific connection/flow and the S-CSCF/Registrar. The P-CSCF includes within the user portion of

a loose route in the path header a unique identifier to identify the flow over which the registration occurs. The P-CSCF then maps any future requests that include that identifier to that flow.

The Registrar stores:

- The instance-id and reg-id as part of the contact information in addition to the time the binding was last updated.
- The Path header.

Note that multiple registrations across alternative flows (different reg-ids) allow the UE to pre-establish redundant signalling channels.

In the case where unregistered UEs are allowed to establish dialogs (e.g., emergency calls, subscribing to configuration profiles, etc.), any signalling during the life-time of that session must be maintained over the flow established for that session. This puts a requirement on the P-CSCF to record route and to ensure that signalling for that session occurs over that flow until the session ends.

V.8.2.2.2 Maintaining NAT bindings

As indicated above, STUN is used by the UE in order to:

- maintain the NAT bindings and keeping FW pinholes open for the signalling;
- determine if there is a failure of the connection; and
- determine if the NAT binding has changed as a result of a NAT re-boot.

The STUN server runs on the P-CSCF on the same port that is used for signalling for that flow. The UE makes STUN requests over the flow as a keep-alive mechanism for the flow as well as to determine if NAT bindings have changed as a result of a NAT re-boot.

V.8.2.2.3 Inbound signalling

Note that signalling in both directions must be established over a flow with existing NAT bindings. In the case of UDP, this implies that SIP messages are sent and received over the same UDP port.

As a result of registrations, the S-CSCF/Registrar is able to maintain contact information (including reg-ids) and path headers in order to be able to access a given UE instance over one or more flows. Therefore, it can route an incoming call to a UE instance over a given flow; and if that fails, do a re-try over an alternative flow.

Appendix VI

IPCablecom2 IPv6 and IPv4 strategy overview

(This appendix does not form an integral part of this Recommendation)

For further study.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2007