PacketCable™

SIP Signaling Technical Report

PKT-TR-SIP-V01-060406

RELEASED

Document Status Sheet

Document Control Number:	PKT-TR-SIP-V01-060406
Document Title:	SIP Signaling Technical Report
PacketCable Release	2
Revision History:	V01 – Released 04/06/06
Date:	April 6, 4004

Trademarks:

Abstract

PacketCable is a CableLabs specification effort designed to extend cable's real-time IP communication service architecture and to accelerate the convergence of voice, video, data, and mobility technologies.

This technical report describes the base SIP signaling requirements to support the PacketCable architecture, applications and services. It contains the following information:

- The reference model for SIP communications;
- For each of the supported SIP extensions, the technical requirements for PacketCable along with the list of impacted components and IMS Delta Specifications;

The PacketCable specifications take precedence over this technical report if the technical report contradicts any specification requirements.

Contents

Figures

1 SCOPE

1.1 Introduction and Purpose

The purpose of this technical report is to provide an overview of the SIP Signaling architecture and describe the high-level requirements to support SIP communications within the PacketCable Architecture. PacketCable is a CableLabs specification effort designed to extend cable's real-time IP communication service architecture; and to accelerate the convergence of voice, video, data, and mobility technologies.

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

1.2 Document Scope and Organization

The PacketCable Architecture Framework Technical Report [ARCH-FRM TR] describes the overall document organization plan for PacketCable. Since PacketCable SIP signaling is closely aligned with IMS, the PacketCable SIP signaling normative requirements are defined in IMS Delta specifications, which are base 3GPP specifications enhanced to accommodate cable-specific requirements. The PacketCable SIP signaling requirements are documented in three IMS Delta specifications, [PKT 23.218], [PKT 23.228], and [PKT 24.229].

1.2.1 Relationship to PacketCable Features and Services

This Technical Report and its associated IMS Delta specifications serve as a SIP signaling 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 signaling base is service independent; and, therefore, requirements specific to each PacketCable service and feature are out-of-scope for this document, and are defined separately. The relationship between this Technical Report, the base SIP signaling IMS Delta specifications, and the PacketCable features and services is shown in Figure 1.

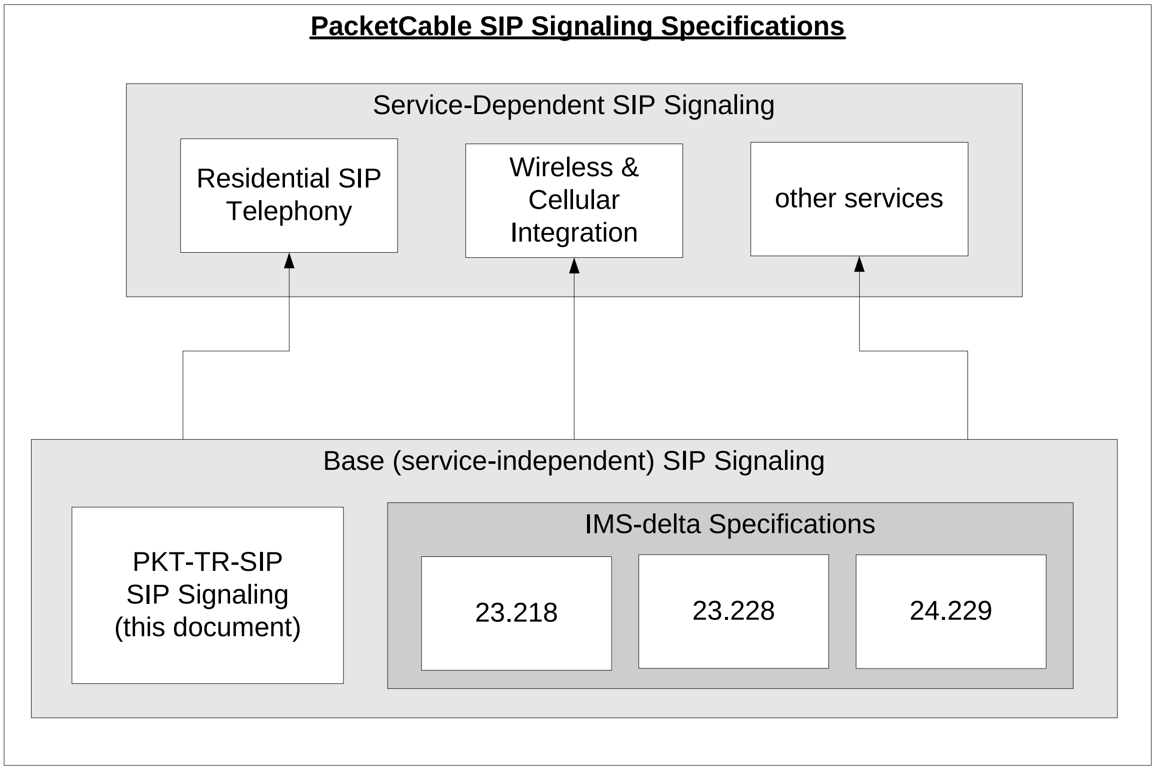

Figure 1 – Relationship between Base SIP Signaling and Services

1.2.2 Relationship to Other PacketCable Specifications

The PacketCable base SIP signaling specifications together define the signaling requirements for the following general capabilities:

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

Other PacketCable specifications such as Accounting, NAT Traversal, and Security, place additional requirements on SIP signaling; and therefore, impact the same IMS Delta specifications, specifically [PKT 24.229]. Also, certain SIP signaling mechanisms impact non-SIP IMS Delta specifications such as [PKT 29.228]. Finally, PacketCable SIP signaling places requirements on [PKT CMSS] to support PacketCable UE to PacketCable E-MTA interworking. The relationship among these various specifications is shown in Figure 2.

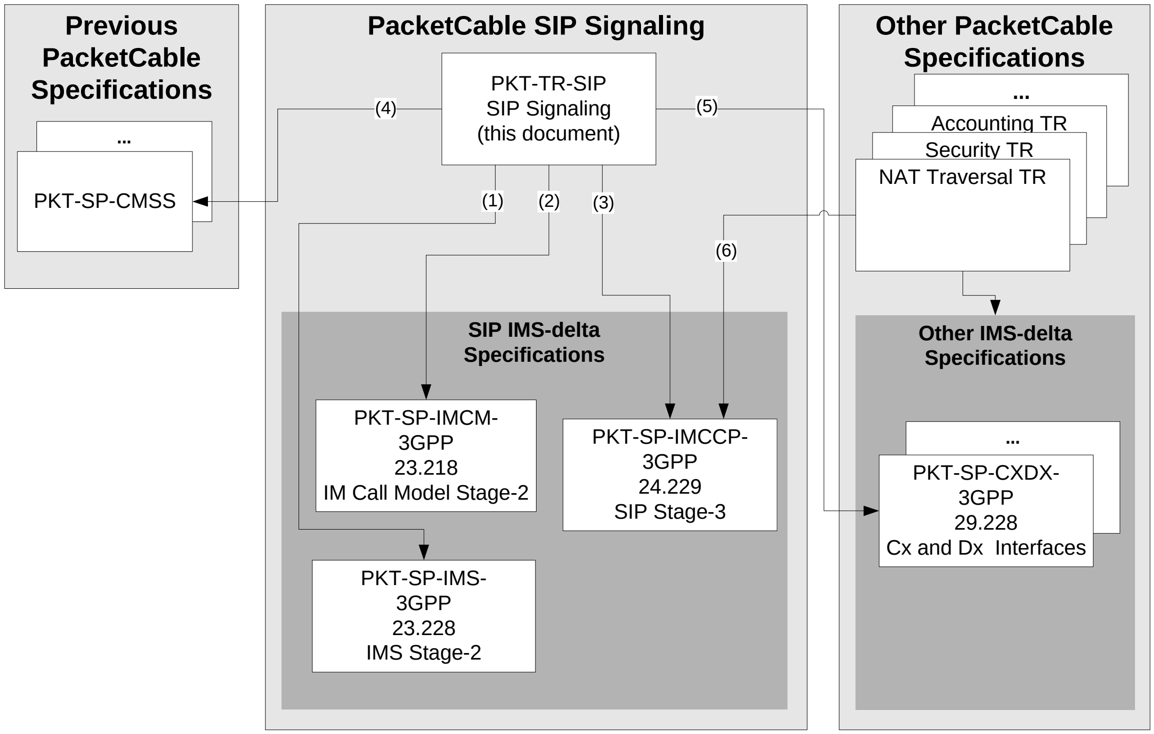

Figure 2 – SIP Signaling Specification Relationships

2 REFERENCES

2.1 Informative References

This technical report uses the following informative references.

[ARCH]	PacketCable 1.5 Architecture Framework, PKT-TR-ARCH1.5-V01-050128, January 28, 2005, Cable Television Laboratories, Inc.
[ARCH-FRM TR]	PacketCable Architecture Framework Technical Report PKT-TR-ARCH-FRM-V01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[CR C1-051535]	Change of originating and terminating terminal terminology, October 2005.
[CR C1-051606]	Incorporating of fixed broadband access impacts into TS 24.229, October 2005.
[CR C1-051655]	Short Session Setup in IMS, October 2005.
[ID ENUM-PSTN]	IETF Draft, IANA Registration for an Enumservice, Containing PSTN Signaling Information, draft-ietf-enum-pstn-03, January 2006.
[ID SIPPING CONFIG]	IETF Draft, A Framework for Session Initiation Protocol User Agent Profile Delivery, March 2006.
[ID GRUU REG EVT]	IETF Draft, Reg Event Package Extension for GRUUs, November 2005.
[ID GRUU]	IETF Draft, Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP), October 2005.
[ID SDP NEW]	IETF Draft, SDP: Session Description Protocol, January 2006.
[ID TEL NP]	IETF Draft, Number Portability Parameters for the "tel" URI, July 2005.
[PACM]	PacketCable Provisioning, Activation, Configuration, and Management Specification, PKT-SP-PACM-I01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[PKT 23.218]	PacketCable IP Multimedia Call Model Stage 2 Specification 3GGP TS 23.218, PKT-SP-23.218-I01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[PKT 23.228]	PacketCable IP Multimedia Subsystem Stage 2 Specification 3GGP TS 23.228, PKT-SP-23.228-I01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[PKT 24.229]	PacketCable SIP and SDP Stage 3 Specification 3GPP PKT 24.229, PKT-SP-24.229-I01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[PKT 29.228]	PacketCable Cx and Dx Interfaces Specification 3GPP TS 29.288, PKT-SP-29.228-D01-xxx, future publication, Cable Television Laboratories, Inc.
[PKT 33.203]	PacketCable Access Security for IP-Based Services Specification 3GPP TS 33.203, PKT-SP-33.203-I01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[PKT CMSS]	PacketCable 1.5 CMS to CMS signaling specification, PKT-SP-CMSS1.5-I02-050812, August 12, 2005, Cable Television Laboratories, Inc.
[RFC 3261]	IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.
[RFC 3262]	IETF RFC 3262, Reliability of Provisional Responses in Session Initiation Protocol (SIP), June 2002.

[RFC 3311]	IETF RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method, IETF, September 2002.
[RFC 3312]	IETF RFC 3312, Integration of Resource Management and Session Initiation Protocol (SIP), October 2002.
[RFC 3320]	IETF RFC 3320, Signaling Compression (SigComp), January 2003.
[RFC 3329]	IETF RFC 3329, Security Mechanism Agreement for the Session Initiation Protocol (SIP), January 2003.
[RFC 3455]	IETF RFC 3455, Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP), January 2003.
[RFC 3486]	IETF RFC 3486, Compressing the Session Initiation Protocol (SIP), February 2003.
[RFC 3556]	IETF RFC 3556, Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth, July 2003.
[RFC 3680]	IETF RFC 3680, A Session Initiation Protocol (SIP) Event Package for Registrations, March 2004.
[RFC 4032]	IETF RFC 4032, Update to the Session Initiation Protocol (SIP) Preconditions Framework, March 2005.
[SEC TR]	PacketCable Security Technical Report, PKT-TR-SEC-V01-060406, April 6, 2006, Cable Television Laboratories, Inc.
[TGCP]	PSTN Gateway Call Signaling Protocol Specification, PKT-SP-TGCP1.5-I02-050812, August 12, 2005, Cable Television Laboratories, Inc.
[TS 23.003]	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification TS 23.003 (Release 6); September 2005.
[TS 24.229 v7]	3rd Generation Partnership Project; Technical Specification SIP and SDP Stage 3 Specification TS 24.229 V7.20, September 2005.
[TS 24.229 v6]	3rd Generation Partnership Project; Technical Specification SIP and SDP Stage 3 Specification V6.90, December 2005.

2.2 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone 303-661-9100; Fax 303-661-9199; Internet: http://www.cablelabs.com /
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org
- Third Generation Partnership Project (3GPP), Internet: http://www.3gpp.org
- Internet Assigned Number Authority (IANA), http://www.iana.org
- 3GPP, ETSI, Mobile Competence Centre, 650, route des Lucioles, 06921 Sophia-Antipolis Cedex, http://www.3gpp.org/specs/specs.htm/

3 TERMS AND DEFINITIONS

The terms and definitions defined Section 3 of the 3GPP Technical Specification [PKT 24.229] are generally applicable unless they are redefined below.

PacketCable Specifications and Technical Reports use the following terms and definitions:

Authorized Identity	An instance of an 'Authorized Identity' in a PacketCable network is a representation of an allowed pairing between a Private Identity and a Public Identity.
Contact Address	The URI of a User Agent on the network. Contact addresses, in the context of PacketCable, are addresses used to deliver requests to a specific User Agent.
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).
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.
Identity Credentials	A collection of the information needed to perform authentication of a private identity. The actual information depends on the authentication mechanism.
PacketCable Service Provider	An MSO, operating one or more independent PacketCable Administrative Domains.
PacketCable Service Provider DNS Domain	A DNS Domain Name that is owned and managed by a PacketCable Administrative Domain. It is used to form SIP URIs that convey Public Identifiers.
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.
Private Identity	A logical identity for purposes of authentication and authorization of a User.
Public Identifier	An identifier used to reference a Public Identity.
Public Identity	A logical identity for purposes of communication with a User. A Public Identity cannot be directly referenced - it must be referenced by using one of its Public Identifiers.
SIP User Agent	Same as 'User Agent'.
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 as defined by [RFC 3261].
Subscriber	The primary billed entity for a Subscription.

Subscription	A contract for service(s) between a 'Subscriber' and a 'PacketCable Administrative Domain'.
User	A person who, in the context of this document, uses a defined service or invokes a feature on a Device.
User Agent (UA)	A software entity contained in a device that acts on behalf of the user to send requests to and receive responses from the network for a particular application. In the context of this document, a UA refers to a SIP User Agent as defined by [RFC 3261].
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

PacketCable Specifications and Technical Reports use 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
MSO	Multi-System Operator
NAT	Network Address Translation
NA(P)T	Network Address and Port Translation; used interchangeably with NAT
NCS	Network-Based Call Signaling
NMS	Network Management System

PAC (PAC Element)	Provisioning, Activation and Configuration Element
PACM	Provisioning, Activation, Configuration, and Management
PAM	PacketCable Application Manager
P-CSCF	Proxy Call Session Control Function
PDS	Profile Delivery Server
PSTN	Public Switched Telephone Network
PSI	Public Service Identity
QoS	Quality of Service
RKS	Record Keeping Server
RTP	Real-time Transport Protocol
RTCP	RTP Control Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SG	Signaling Gateway
SIP	Session Initiation Protocol
SIP UE	User Equipment that contains a SIP User Agent.
SLF	Subscription Location Function
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SS7	Signaling System 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 PACKETCABLE SIP SIGNALING

PacketCable applications and services are controlled using Session Initiation Protocol (SIP). PacketCable 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). PacketCable is based on Release 6 of IMS, and enhances IMS where necessary to support PacketCable requirements.

5.1 PacketCable SIP Signaling Architecture and Reference Points

PacketCable Signaling and Service Control Reference Points are illustrated in Figure 3. Most reference points are IMS-standard, with appropriate deviations for PacketCable as identified in various PacketCable specifications. PacketCable-specific reference points are also included.

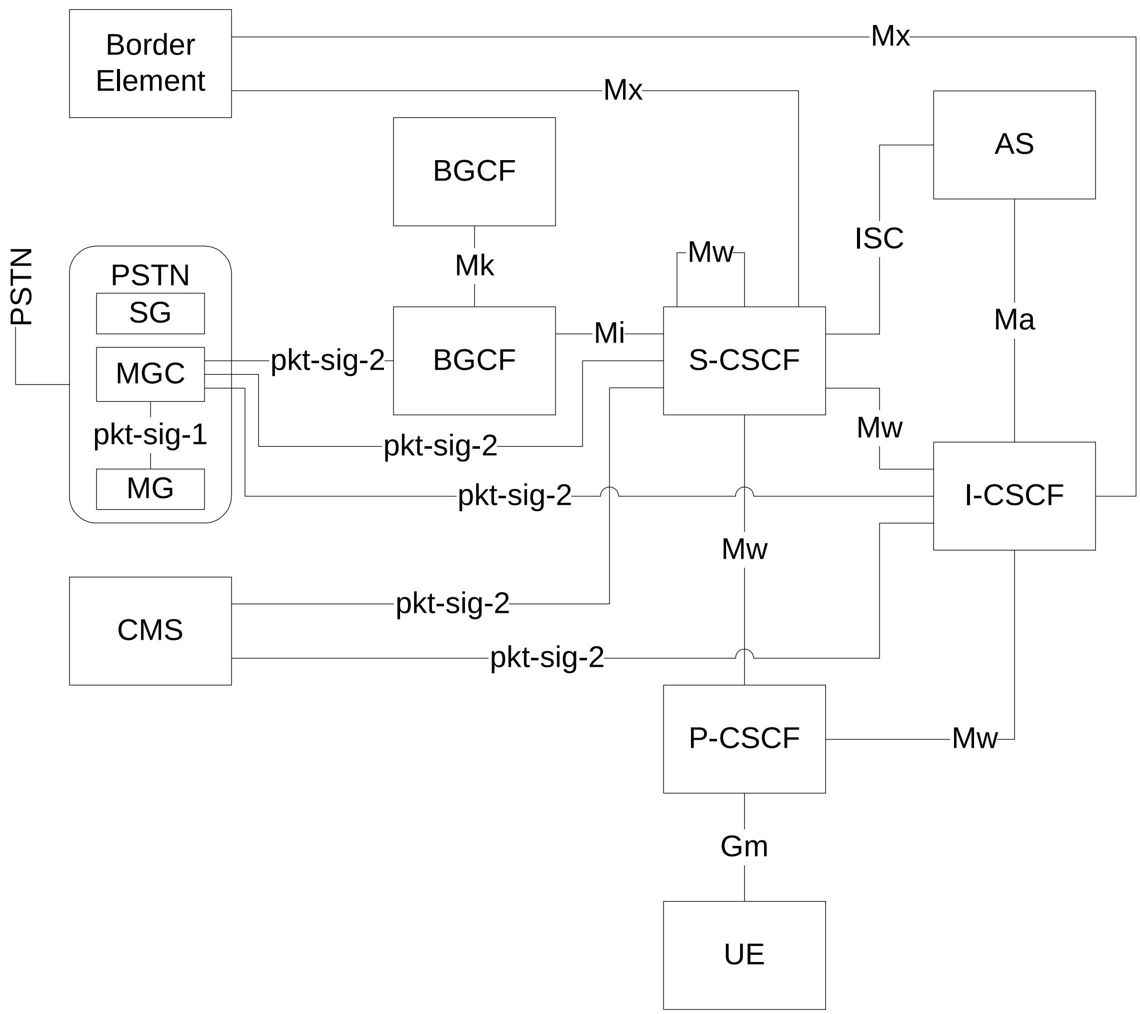

Figure 3 – Call Signaling Reference Points

5.1.1 SIP Signaling Functional Components

5.1.1.1 User Equipment (UE)

PacketCable 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, PacketCable 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.

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 signaling security or compression is enabled or disabled).
- Generates Accounting Events.

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 PacketCable E-MTAs. Rather, E-MTAs are served by their CMS as described in PacketCable 1.5 Architecture Framework Technical Report [ARCH].

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 signaling 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 PacketCable 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.

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.

5.1.1.5 Application Server (AS)

An AS provides value-added PacketCable services and resides in either the user's home network or in a third party location, which could be another network or a standalone 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.

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 signaling level (e.g., acts as a signaling relay and provides obfuscation of address information in headers).

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.

5.1.1.8 Public Switched Telephone Network Gateway (PSTN GW)

The PSTN GW consists of the Signaling Gateway (SG), Media Gateway Controller (MGC) and the Media Gateway (MG). The SG, MGC, and MG functional elements are defined in previous releases of PacketCable, and are re-used in this release of PacketCable, with the addition of a PacketCable 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 signaling conversion at a transport layer between SS7 based transport and the IP based transport used in the PacketCable network. The SG does not interpret the application layer, but does interpret the layers needed for routing signaling messages.

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

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

5.1.1.9 Call Management Server (CMS)

A PacketCable Call Management Server (CMS) provides support for telephony services for NCS clients (i.e., E-MTAs). In PacketCable, 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.

5.1.2 SIP Signaling Reference Points

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

Table 1 - Call Signaling Reference Points

Reference Point	PacketCable 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 signaling to the BGCF for the purpose of interworking with the PSTN networks.
Mk	BGCF – BGCF	Allows one BGCF to forward the session signaling 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 signaling 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 PacketCable TGCP Specification [TGCP].
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 signaling with the CMS to enable PacketCable E-MTAs to establish voice sessions with UEs. Also allows the BGCF, I-CSCF, and S-CSCF to exchange session signaling with the MGC for the purpose of interworking with the PSTN.

5.2 PacketCable 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.

PacketCable 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 PacketCable will align with these newer releases as necessary.

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 are made optional for PacketCable.

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

5.2.1.1 Bandwidth Modifiers for RTCP

[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 PacketCable, support of the RTCP bandwidth modifiers is optional at the UE. If the UE supports this extension, then it must honor 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).

5.2.1.2 P-Associated-URI

[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 PacketCable, support of P-Associated-URI header is optional at the UE.

5.2.1.3 SIP Compression

[RFC 3486] provides a SIP message compression capability that reduces signaling bandwidth usage and latency on the radio access network. Support of SIP compression at the UE is optional for PacketCable. 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.

5.2.1.4 SIP Timers

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

5.2.2 Modularity

PacketCable 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 PacketCable.

5.2.2.1 Reliable Provisional Response

[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 PacketCable, support of PRACK is mandatory at the UE, and it's 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.

5.2.2.2 UPDATE

[RFC 3311] defines a SIP request called UPDATE that is used to update media sessions before answer (primarily for preconditions). Support of UPDATE in PacketCable 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 doesn't support it based on what was received in the incoming Allow header.

5.2.2.3 Reg Event Package

[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 PacketCable, support of the Reg event package is optional at the UE. If supported, the UE must provide configuration controls to disable its use.

5.2.2.4 P-Access-Network-Info header

[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 PacketCable, 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.

5.2.2.5 Disabling Signaling Security

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

1. Signaling security off - signaling security is always off across all UEs served by the P-CSCF.
2. Signaling security on - signaling security is enabled for all UEs served by the P-CSCF.
3. Signaling security negotiated: signaling security is on for UEs that support it (note, signaling security support is mandatory for PacketCable UEs), and off for UEs that don't support it.

5.2.3 Services

The base PacketCable 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.

5.2.3.1 Tel URI Number Portability and Carrier Routing

[ID TEL NP] defines Tel URI parameters to support call routing based on the number portability routing number, and equal access carrier ID. Support of these parameters is required for calls destined for the PSTN. For PacketCable, 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, a UE that supports the Tel URI must support these parameters as well.

5.2.3.2 Globally Routable User Agent URI (GRUU)

[ID 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 PacketCable, 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 don't support GRUU.

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 defined in [ID GRUU REG EVT] that enables multiple GRUU URIs to be communicated in a NOTIFY to the Reg event package.

6 PACKETCABLE IMS REQUIREMENTS

This section describes the requirements that are currently not supported in IMS Release 6, but that are needed in the PacketCable SIP Signaling architecture.

6.1 SIP Secure Signaling

PacketCable allows signaling security to be disabled between the UE and the P-CSCF. This section first outlines the signaling security model defined in 3GPP for IMS communications and then describes the impacts to IMS for allowing access to IMS-services without secure SIP signaling between the UE and P-CSCF.

6.1.1 Description

The IMS security architecture [PKT 33.203] 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 signaling (i.e., signaling 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.

Signaling security is a mandatory capability of the UE in the PacketCable SIP architecture. However, PacketCable allows signaling security to be disabled in the following ways:

1. The UE may be configured [PACM] to have signaling security disabled; or
2. The P-CSCF may be configured to have signaling security disabled for all UE that access IMS services through that P-CSCF.

In addition, there are certain requests that may not require signaling security. In PacketCable IMS, the only such request is subscription to the ua-profile event package as defined in [ID SIPPING CONFIG].

6.1.2 Impacted components

This section describes the IMS components impacted by allowing access to IMS-services without secure SIP signaling 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 the [SEC TR].

6.1.2.1 UE

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

In PacketCable, 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 signaling security is disabled.
- The UE is configured to have signaling security disabled as described in [PACM], and the UE has not received an indication from the P-CSCF during initial registration that signaling security is required.

If the UE includes the "sec-agree" option tag in the Require header as defined in [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 [RFC 3329].

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

If the UE successfully registers without having established a security association, then the following applies for any initial request or standalone 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 Section 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.

6.1.2.2 P-CSCF

In PacketCable, the P-CSCF must support signaling security requirements as defined in the [SEC TR].

The P-CSCF may be configured to have signaling security "disabled" or "required" for all UE that access IMS-services through that P-CSCF. The P-CSCF may also be configured to have signaling security "optional"; in this case, the P-CSCF determines whether signaling 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 signaling 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 [RFC 3329]. In this case, the P-CSCF must ignore the security mechanism agreement related procedures specified in [PKT 24.229].
- The P-CSCF should allow unprotected non-REGISTER requests.

If the P-CSCF is configured to have signaling 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 [RFC 3329]. In this case, the P-CSCF must ignore the security mechanism agreement related procedures specified in [PKT 24.229].
- 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 [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 signaling 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 [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.

6.1.2.3 I-CSCF

In PacketCable, the I-CSCF must support signaling security requirements as defined in the [SEC TR].

6.1.2.4 S-CSCF

In PacketCable, the S-CSCF must support signaling security requirements as defined in the [SEC TR].

The S-CSCF may be configured to have signaling security "required" for all UE that access IMS-services through that S-CSCF. The S-CSCF may also be configured to have signaling 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 signaling 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 [PKT 24.229] 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 [PKT 24.229], 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.

6.1.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements for SIP Secure Signalling:

[PKT 24.229]

6.2 Support of IPv4 and IPv6

6.2.1 Description

3GPP Release 6 [TS 24.229 v6] specifies that UEs and IMS subsystem entities are assigned IPv6 addresses. As part of the 3GPP IMS Release 7 support for "Fixed Broadband", 3GPP has been extended to allow UEs and IMS subsystems to be assigned IPv4 addresses, IPv6 addresses, or both. PacketCable requires IPv4 support and both types of addresses must be supported by PacketCable UEs and IMS components.

Some procedures in [PKT 24.229] are explicitly described as specific to IPv6. Such procedures are not applicable to IPv4 clients. (i.e., "Change of IPv6 address due to privacy").

6.2.2 Impacted components

Changes required for support of IPv4 are identified as part of [CR C1-051606] and incorporated into [PKT 24.229]. 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 (Section 4.2).
    - Use of IPv6 in PacketCable 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 (Section 5.4.3.2).
    - Interworking between an IPv4-based PacketCable 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 IPv4 DHCP procedures (Section 9.2.1).

- This particular change is not relevant to PacketCable since alternate procedures are used for P-CSCF discovery, but it is included to incorporate all related changes from the 3GPP R7 CR.

6.2.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements for Support of IPv4 and IPv6:

[PKT 24.229], Sections 4.2, 5.4.3.2, and 9.2.1.

6.3 SIP Compression

6.3.1 Description

3GPP IMS Release 6 [PKT 24.229] mandates the UE and P-CSCF to support Signaling Compression (SigComp) as defined in [RFC 3320] and SIP Compression as defined in [RFC 3486]. SIP Compression is mandated to minimize delays over low bandwidth 3GPP access. For the cable broadband access part of PacketCable, 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.

PacketCable incorporates these 3GPP IMS Release 7 changes for SIP Compression: Support for Signaling Compression (SigComp) as defined in [RFC 3320] and SIP Compression as defined in [RFC 3486] is optional for PacketCable 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 Section 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, PacketCable may re-align with any future changes made in this area.

6.3.2 Impacted components

The required changes are identified as part of [CR C1-051606] and incorporated into [TS 24.229 v7].

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.

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.

6.3.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements for SIP Compression:

[PKT 24.229], Section 8

6.4 Reliability of SIP Provisional Responses

6.4.1 Description

The reliability of provisional response in the SIP protocol is an extension defined in [RFC 3262] in support of multiple applications. First, it is necessary when establishing sessions using the SIP preconditions extension. Second, 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. PacketCable will update these requirements to enable the UE, based on configuration data, to interwork with non-3GPP UEs that don't support this SIP extension.

6.4.2 Impacted components

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

6.4.2.1 UE

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

6.4.3 Impacted IMS Delta Specifications

The following PacketCable IMS Delta specification contains the necessary requirements for Reliability of SIP Provisional Responses:

[PKT 24.229] Section 5.1 and Annex A - Table A.4

6.5 SIP UPDATE

6.5.1 Description

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

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

6.5.2 Impacted components

The impacts to enable a UE to interwork with endpoints that don't support the SIP UPDATE extension are localized to the UE itself.

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.

6.5.3 PacketCable Impacted IMS Delta Specifications

The following PacketCable IMS Delta specification contains the necessary requirements for SIP UPDATE:

[PKT 24.229] Section 5.1 and Annex A - Table A.4

6.6 SIP Preconditions

6.6.1 Description

The support for preconditions in SIP, as defined in [RFC 3312] and updated by [RFC 4032], is an optional feature of the PacketCable Signaling architecture. Originally mandated by IMS, the requirements for SIP preconditions have been relaxed based on the agreed [CR C1-051655]: 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.

6.6.2 Impacted components

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

6.6.2.1 UE

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

The PacketCable UE should negotiate the use of SIP pre-conditions. The UE should indicate its support for SIP pre-conditions 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 pre-conditions. 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.

6.6.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements for SIP Preconditions:

[PKT 24.229], Section 5.1.3, 5.1.4, and 6.1

6.7 SDP bandwidth modifiers for RTCP

6.7.1 Description

Standard SDP, as specified in [ID SDP NEW], does not provide a mechanism to explicitly control RTCP bandwidth. Instead, RTCP bandwidth is implicitly fixed at 5% of the session bandwidth. [RFC 3556] introduces two new SDP bandwidth modifiers for RTCP that 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 PacketCable access network. However, there is value in having a PacketCable 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 PacketCable UEs.

6.7.2 Impacted components

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

6.7.2.1 UE

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

6.7.3 PacketCable IMS Delta Specification

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

[PKT 24.229], Section 6

6.8 Registration state event package

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

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.

6.8.2 Impacted components

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

6.8.2.1 UE

Support of "A SIP Event Package for Registrations" [RFC 3680] is optional for the PacketCable UE. If the UE does not support the registration-state event package described in [RFC 3680], it does not perform procedures in [PKT 24.229] related to subscription and notification of registration-state information.

The primary implications of non-support for [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 Section 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 Section 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 [PKT 24.229].

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 Section 6.12.2.1).

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 PacketCable network performs network-initiated deregistration or re-authentication, and there are UEs which do not support the registration-state event package.

6.9 Number portability

6.9.1 Description

PacketCable supports local number portability and equal access carrier routing. This section describes how number portability and carrier routing data is obtained and used in a PacketCable network.

To support local number portability, the PacketCable 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 PacketCable 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 PacketCable 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. PacketCable assumes that the when such a Tel URI resolves to a SIP URI, an LNP Query is not required by the PacketCable 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 document.

When a Tel URI containing an E.164 number cannot be resolved to a SIP URI, the PacketCable 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 PacketCable 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 document (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, see [ID ENUM-PSTN].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 document.

To support equal access carrier routing, the PacketCable network selects the route to the PSTN based on the dialed 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 PacketCable requirements do not call for support of a presubscribed carrier on a subscriber basis. Rather, a carrier may be pre-subscribed 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 pre-subscribed carrier, for the case where a pre-subscribed 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.

PacketCable supports the number portability and carrier routing requirements using the Tel URI LNP and carrier routing parameters defined in [ID TEL NP], and the dial-around-indicator parameter defined in [PKT CMSS].

6.9.2 Impacted components

In order to support number portability and carrier routing, the number portability information must be carried in the SIP signaling. Specifically, the Tel URI needs to support the "rn", "cic", and the "npdi" parameters as defined in [ID TEL NP], and the "dai" parameter defined in [PKT CMSS]. 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.

6.9.2.1 UE

The only responsibility of the UE in support of carrier routing is to identify a user-dialed carrier to the network on an originating call. The UE does this by recognizing user-dialed 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 dialed digits, including the dialed 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 behavior are out of scope of this document.

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

6.9.2.2 S-CSCF

As specified in [PKT 24.229], 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.

PacketCable 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 a E.164 address to a SIP URI, (should this be possible with some mechanisms), are out of scope of this document.

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 [PKT 24.229], the input to the routing decision is the called telephone number identified in the Tel URI of the INVITE request URI. PacketCable 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 pre-subscribed 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.

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 PacketCable 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 document.

6.10 Globally routable user agent URI (GRUU)

6.10.1 Description

The support of SIP Globally Routable User Agent URI (GRUU) as defined in [ID GRUU] is optional for the UE in the PacketCable SIP architecture. GRUU benefits PacketCable 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.

6.10.2 Impacted components

This section describes the component impacts for support of GRUU.

6.10.2.1 UE

A PacketCable UE supporting GRUU must comply with the User Agent requirements and guidelines defined in [ID GRUU].

- 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 Section 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.

6.10.2.2 S-CSCF

The S-CSCF acting as the SIP registrar must comply with all the requirements defined in [ID GRUU]. In particular, the S-CSCF must be capable of responding to registration requests that ask for GRUU URIs to be returned. In this case, it must 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 PacketCable 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.

6.10.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specifications contain the necessary requirements for Globally routable user agent URI (GRUU):

[PKT 23.218]

[PKT 23.228]

[PKT 24.229]

[PKT 29.228]

6.11 Registration state event package extension for GRUU

6.11.1 Description

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

Reg-event package extension for GRUU support per [ID GRUU REG EVT] is optional in the PacketCable SIP Signaling 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 PacketCable 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.

6.11.2 Impacted components

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

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 Section 6.10.

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.

6.11.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements for Registration state event package extension for GRUU:

[PKT 24.229]

6.12 Private 3GPP headers

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

Note: P-headers described in [RFC 3455] which are not identified in this section are supported by PacketCable without change.

6.12.1 Description

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 [PKT 24.229], it contains the registered public user identity and its associated set of implicitly registered public user identities (Note: this differs from the description in [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 PacketCable, support for the P-Associated-URI header is optional for the UE.

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 [PKT 24.229], Section 5.2.10;
- Determination of whether SIP Compression is needed between the UE and P-CSCF, as described in Section 6.3;
- Optimization of the values of SIP timers, as described in Section 6.14; and
- Optimization of services based on access network type.

In PacketCable, 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 PacketCable must be registered with the appropriate standards body.

6.12.2 Impacted components

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

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 Section 6.8).
- If the public user identity used for registration is barred, the UE 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 [PKT 24.229], with the following clarification:

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

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.

6.12.2.3 S-CSCF

If the P-Associated-URI header is not supported by the UE and signaling 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.

6.13 Routing SUBSCRIBEs for configuration information

6.13.1 Description

PacketCable 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 a PacketCable 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 SUBCRIBE requests for configuration information to be properly router 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 Section 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 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. (See [TS 23.003] Section 13.5 and [PKT 23.228] Section 5.4.12.) 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 honor 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 PacketCable, the only applicable case is where the origination and termination address are the same. So the server may simply honor 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 [PACM].

6.13.2 Impacted components

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

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 Section 6.1.2.1 on Signaling Security and the UE.

6.13.2.2 P-CSCF

See Section 6.1.2.2 on Signaling Security and the P-CSCF.

6.13.2.3 I-CSCF

See Section 6.1.2.3 on Signaling Security and the I-CSCF.

6.13.2.4 S-CSCF

See Section 6.1.2.4 on Signaling Security and the S-CSCF.

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.

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 this 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.

6.13.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements Routing SUBSCRIBEs for configuration information:

[PKT 24.229]

6.14 SIP Timers

6.14.1 Description

To accommodate 3GPP air interface processing and transmission delays, 3GPP IMS Release 6 [PKT 24.229] specifies a modified set of SIP timer values (compared with those defined in [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 [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 [RFC 3261] SIP Timer values.

PacketCable 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 PacketCable broadband access network technology. Refer to Section 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 [RFC 3261] SIP Timer Values. Note this 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, PacketCable may re-align with any future changes made in this area.

6.14.2 Impacted components

The required changes are identified as part of [CR C1-051606] and incorporated into [TS 24.229 v7].

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 [RFC 3261] SIP Timer Values.

6.14.2.1 UE

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

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 [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 [RFC 3261] Timer values apply.

6.14.3 PacketCable IMS Delta Specification

The following PacketCable IMS Delta specification contains the necessary requirements for SIP Timers:

[PKT 24.229], Sections 7.7

6.15 General Changes

6.15.1 Description

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

- [PKT 24.229] 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 24.229. As part of the 3GPP IMS Release 7 support for "Fixed Broadband", the 3GPP specification [PKT 24.229] has been modified to correct the terminology, using the terms "UE-originating", "UE-originated", "UE-terminating" UE-terminated" and "UE-initiated". PacketCable implicitly assumes this change in terminology.

- [PKT 24.229] 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 [PKT 24.229] Sections 4.2, 5.1.1.1A, and Annex C). Some UEs utilized in PacketCable 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 [SEC TR].

The following should be recognized:

- Some procedures in [PKT 24.229] are explicitly described as pertaining to 3GPP Access. Such procedures are not applicable to broadband clients (Example: Section 5.2.8.1 "P-CSCF-Initiated call release" contains scenarios related to "radio coverage" and "radio interface resources".
- [PKT 24.229] also contains annexes that are explicitly targeted at GPRS access. Such annexes are self-evidently not applicable to PacketCable broadband access, and corresponding material for PacketCable may be contained in other PacketCable specifications.

6.15.2 Impacted components

Changes required for generalization of access terminology (from "mobile-" to "UE") are identified as part of [CR C1-051535].

> These changes generalize [PKT 24.229] but do not impact procedures. As such, no detailed breakdown of component impact is provided in this section.

6.15.3 PacketCable IMS Delta Specification

The changes required for generalization of access terminology (from "mobile-" to "UE") are implicitly assumed and [PKT 24.229] is not updated with these changes for simplicity.

6.16 Interworking with Previous PacketCable Releases

A UE must be able to establish voice sessions with endpoints supported in previous PacketCable 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 PacketCable 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 2). The requirements to support this interface on the CMS and MGC are defined in [PKT CMSS].

Appendix I Open Issues

- Address the problem of how to find the target user in an environment where multiple forms of a URI point to the same user. For example, the following URI forms can all point to the same user:
  - TEL: <global address digits>
  - TEL: <local address digits>;context=<context>
  - TEL: <global address digits>;<tel URI parms>
  - SIP: <global address digits>@operator.com;user=phone
  - SIP: <local address digits>;context=<context>@operator.com; user=phone
  - SIP: <global address digits>;<tel URI parms>@operator.com; user=phone
- Identify the mechanisms required to support configuration of "unknown" devices. For example, the P-CSCF currently blocks most non-REGISTER requests from unregistered users, but is allowed to route SUBSCRIBE to UA-profile in order to enable configuration of devices that are not known to the system (i.e., devices with a public identity that does not have an entry in the HSS). Mechanisms are needed to ensure that the error case where a "known" device sends a SUBSCRIBE to UA-profile before registration is properly handled.

Appendix II Acknowledgements

This Technical Report was developed and influenced by numerous individuals representing many different vendors and organizations. CableLabs hereby wishes to thank everybody who participated directly or indirectly in this effort.

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to this Technical Report:

Pierre Couillaud (Broadcom)

Paul Kyzivat (Cisco)

Samer Hawwa (Ericsson)

Sean Kelley (Motorola)

Brian Lindsay (Nortel)

David Hancock - CableLabs