PacketCable™ 2.0

SIP Signaling Technical Report

PKT-TR-SIP-C01-140314

CLOSED

DISCLAIMER

Document Status Sheet

Document Control Number:	PKT-TR-SIP-C01-140314
Document Title:	SIP Signaling Technical Report
Revision History:	V01 – released 04/06/06
	V02 – released 10/13/06
	V03 – released 09/25/07
	V04 – released 11/06/07
	C01 – closed 03/14/14
Date:	March 14, 2014

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

Tables

.

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. PacketCable SIP signaling is closely aligned with IMS. Therefore, the PacketCable SIP signaling normative requirements are defined in 3GPP IMS specifications, and in IMS Delta specifications, which are base 3GPP specifications enhanced to accommodate cable-specific requirements. Specifically, the PacketCable SIP signaling requirements are documented in 3GPP IMS specifications [TS 23.218] and [TS 23.228], and IMS Delta specification [PKT 24.229].

1.2.1 Relationship to PacketCable Features and Services

This Technical Report and its associated 3GPP IMS specifications and IMS Delta specifications serve as a SIP signaling foundation in 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. Therefore, requirements specific to each PacketCable service and feature are out-of-scope for this document, and are defined separately. Figure 1 shows the Technical Report and specifications that define the base PacketCable SIP signaling architecture, and how this service-independent base supports a variety of PacketCable services.

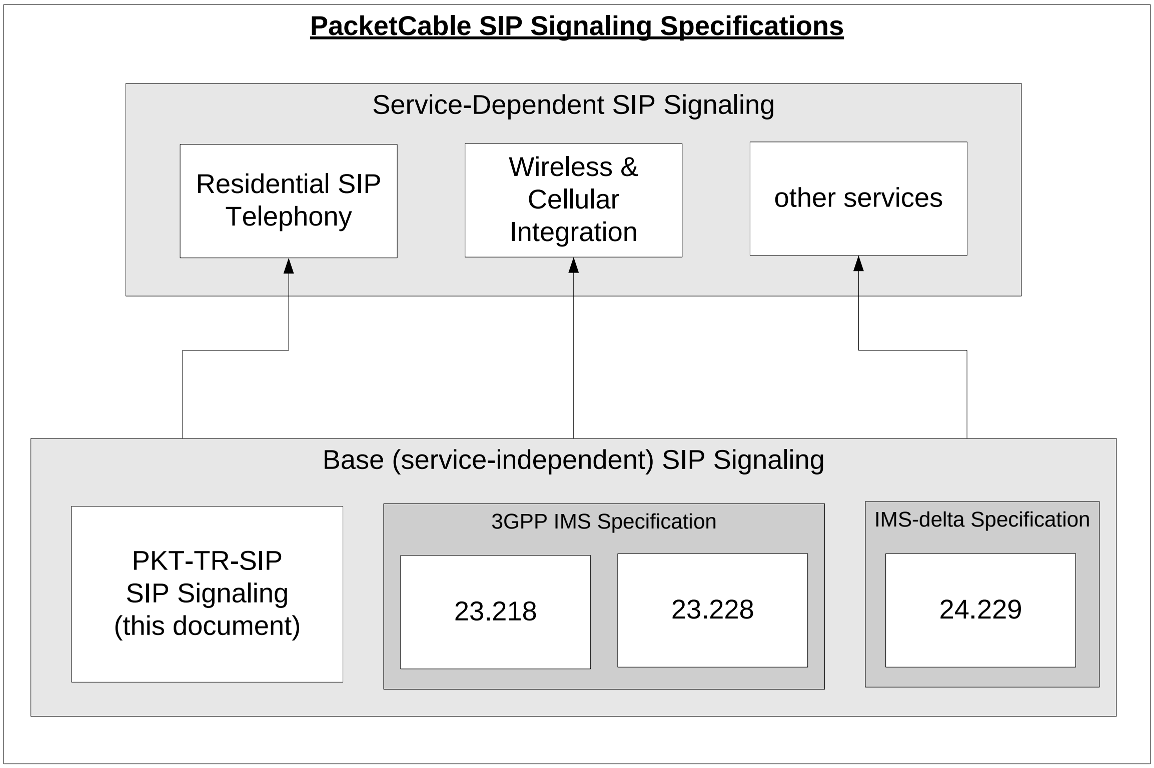

Figure 1 – Relationship between Base SIP Signaling and Services

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 NAT Traversal, and Security, place additional requirements on SIP signaling, and therefore impact the PacketCable base SIP signaling 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 relationships among these various specifications are shown in Figure 2.

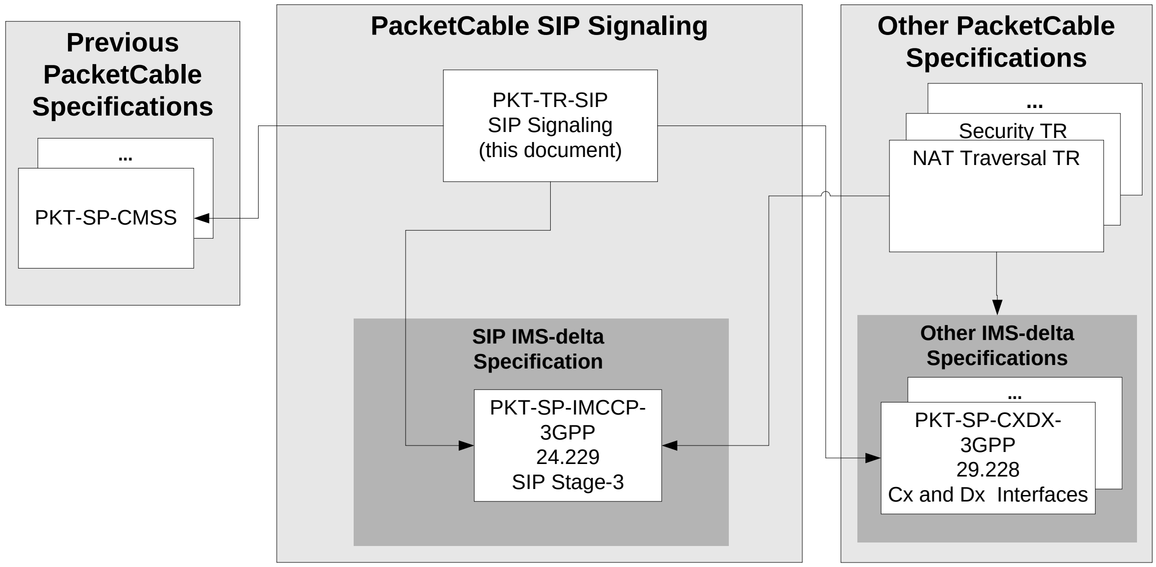

Figure 2 – SIP Signaling Specification Relationships

2 REFERENCES

2.1 Normative References

There are no normative references in this document.

2.2 Informative References

This technical report uses the following informative references.

[ARCH]	PacketCable 1.5 Architecture Framework, PKT-TR-ARCH1.5-V02-070412, April 12, 2007, Cable Television Laboratories, Inc.
[ARCH-FRM TR]	PacketCable Architecture Framework Technical Report PKT-TR-ARCH-FRM-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[ID DAI]	IETF Internet-Draft, DAI Parameter for the "tel" URI, draft-yu-tel-dai-03, August 2007, work in progress.
[ID GRUU REG EVT]	IETF Internet-Draft, Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUU), draft-ietf-sipping-gruu-reg-event-09, July 2007, work in progress.
[ID GRUU]	IETF Internet-Draft, Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP), draft-ietf-sip-gruu-14, June 2007, work in progress.
[PKT 24.229]	PacketCable SIP and SDP Stage 3 Specification 3GPP PKT 24.229, PKT-SP-24.229-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[PKT 29.228]	PacketCable Cx and Dx Interfaces Specification 3GPP TS 29.228, PKT-SP-29.228-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[PKT 33.203]	PacketCable Access Security for IP-Based Services Specification 3GPP TS 33.203, PKT-SP-33.203-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.
[PKT CMSS]	PacketCable 1.5 CMS to CMS signaling specification, PKT-SP-CMSS1.5-I07-120412, April 12, 2012, Cable Television Laboratories, Inc.
[RFC 4566]	IETF RFC 4566, SDP: Session Description Protocol, July 2006.
[RFC 4694]	IETF RFC 4694, Number Portability Parameters for the "tel" URI, October 2006.
[RFC 4769]	IETF RFC 4769, IANA Registration for an Enumservice Containing PSTN Signaling Information, November 2006.
[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-C01-140314, March 14, 2014, Cable Television Laboratories, Inc.

[TGCP] PSTN Gateway Call Signaling Protocol Specification, PKT-SP-TGCP1.5-I04-120412, April 12, 2012, 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 7); June 2007.

[TS 23.218] 3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia (IM) session handling; IM call model; Stage 2 (Release 7); June 2007.

[TS 23.228] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 7); June 2007.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: http://www.cablelabs.com
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org
  Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.
  The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt
- Third Generation Partnership Project (3GPP), Internet: http://www.3gpp.org
- Internet Assigned Number Authority (IANA), http://www.iana.org

3 TERMS AND DEFINITIONS

The terms and definitions defined in 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:

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.
Private Identity	A logical identity for purposes of authentication and authorization of a User.
Public User Identity	A logical identity for purposes of communication with a User.
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].

4 ABBREVIATIONS AND ACRONYMS

PacketCable Specifications and Technical Reports use the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
ALG	Application Layer Gateway
AS	Application Server
BGCF	Breakout Gateway Control Function
CMS	Call Management Server
CMTS	Cable Modem Termination System
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS®	Data-Over-Cable Service Interface Specification
E-MTA	Embedded Multimedia Terminal Adapter
ENUM	E.164 Number Mapping
GRUU	Globally Routable User Agent URI
HSS	Home Subscriber Server
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MRF	Multimedia Resource Function
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
P-CSCF	Proxy Call Session Control Function
PSTN	Public Switched Telephone Network
PSI	Public Service Identity
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

SS7	Signaling System 7
TGCP	Trunking Gateway Control Protocol
TR	Technical Report
TrGW	Transition Gateway
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier

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 7 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.

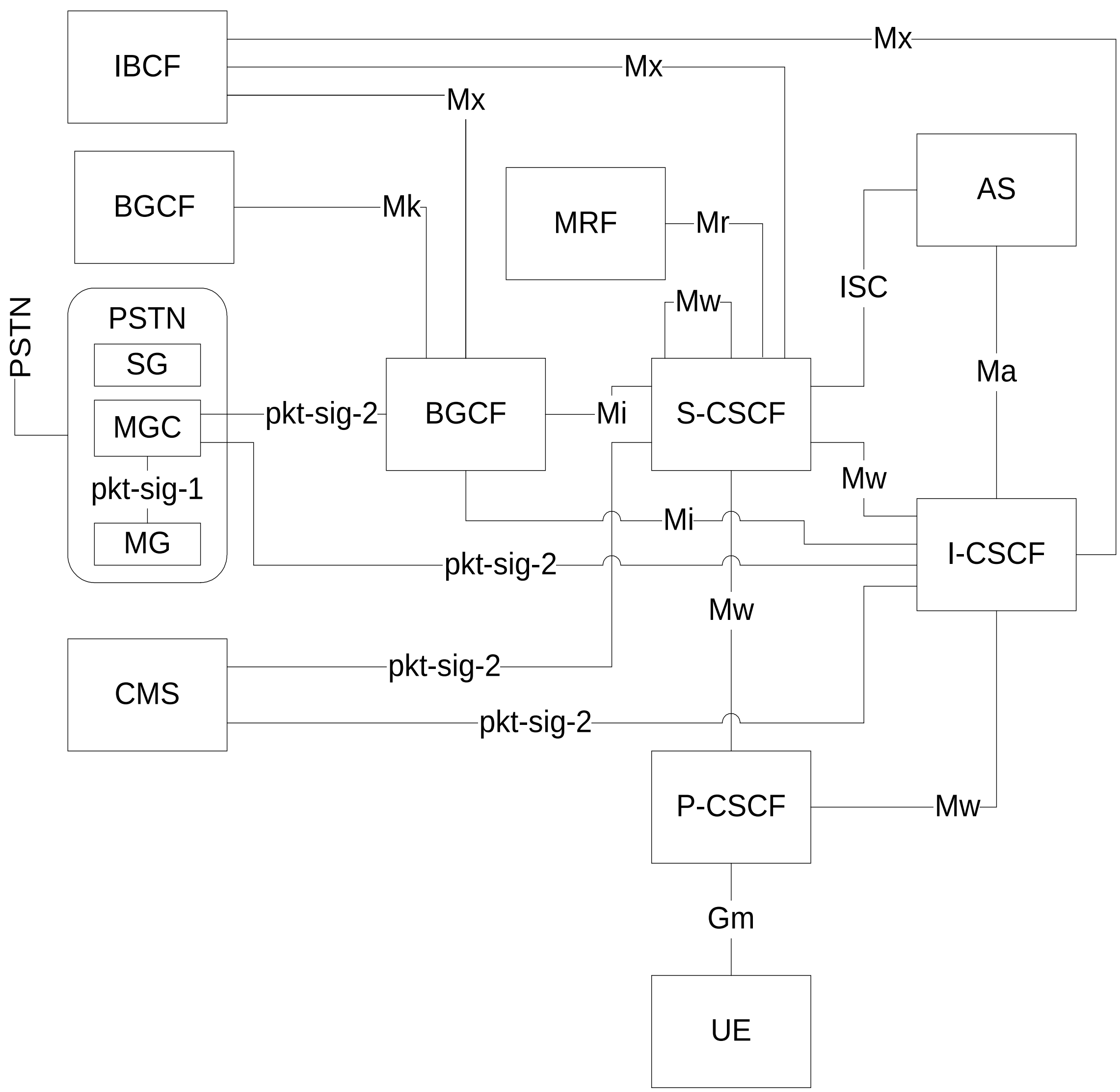

Figure 3 – Call Signaling Reference Points

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 devices (e.g., UE embedded in a Cable Modem), or mobile devices (e.g., WiFi-enabled mobile phone, or softphone application running on a laptop). They may reside on the cable access network, or they may obtain services over 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 User Identities.
- Tracks the registration status of Public User Identities, and removes security association with the UE when a Public User 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 User 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. Note that the S-CSCF does not 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 User Identities (AORs) to a set of contact addresses, assigns Globally Routable User Agent URIs, stores 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 registered contacts), and 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 IBCF for topology hiding and other inter-network interworking functions.
- Origination Processing: processing of incoming dialog-initiating SIP requests originated by Public User Identities served by the S-CSCF, including the invocation of Application Servers required to support the originating services of the user.
- Terminating Processing: processing of outgoing dialog-initiating SIP requests terminating to Public User Identities served by the S-CSCF. This includes invocation of any Application Servers required to support the terminating services of the user, and support for forking of SIP requests when multiple contact addresses are registered for the target Public User Identity.
- 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.

Public User Identities are assigned to an S-CSCF at registration time. Once a Public User Identity is assigned to an S-CSCF, all subsequently registering instances of that Public User Identity must be assigned to the same S-CSCF. Also all Public User Identities that share 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 registrar function of the S-CSCF, and by the SIP User Agents that are implemented in endpoints and other network components such as Application Servers and MGCs. A registering instance of a Public User Identity is assigned a Globally Routable URI during the registration process. Other entities in the network can then use this GRUU to send dialog-initiating requests to that specific registered instance of the Public User Identity when multiple instances are registered. This capability 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 S-CSCF.

- 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 or peer network, or from an MGC for calls originating in the PSTN, to the correct terminating S-CSCF, or to the BGCF.
- Routes incoming dialog-initiating requests received from an Application Server acting on behalf of a user to the correct originating 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 User 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 Multimedia Resource Function (MRF)

The MRF provides a number of common multimedia functions that can be shared by multiple applications. The MRF multimedia functions include:

- Mixing of incoming media streams (e.g., for multi-port conferencing);
- Sourcing of media streams (e.g., for multimedia announcements);
- Processing of media streams (e.g., audio transcoding, media analysis);
- Floor Control (i.e., manage access rights to shared resources in a conferencing environment).

5.1.1.7 Interconnection Border Control Function (IBCF)

The IBCF provides inter-network interworking functions at the SIP/SDP layer, including::

- 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.
- Address and topology hiding at the signaling level (e.g., acts as a signaling relay and provides obfuscation of address information in headers).

The IBCF may also control a Transition Gateway (TrGW). The TrGW in turn relays media between peer networks to provide inter-network interworking functions at the RTP/RTCP layer such as IPv4/6 interworking, media security interworking, and network address/port translation.

5.1.1.8 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.

5.1.1.9 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.

5.1.1.10 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 – IBCF S-CSCF – IBCF BGCF – IBCF	Allows an S-CSCF, I-CSCF, or BGCF to communicate with an IBCF when interworking with another network. For example, a session between the home and peer network could be routed via the IBCF in order to provide interworking between IPv6 and IPv4 SIP networks.
Mi	S-CSCF – BGCF I-CSCF – BGCF	Allows the S-CSCF or I-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.
Mr	S-CSCF – MRF	Allows an S-CSCF to exchange session signaling with an MRF in order to access multimedia resources such as network-provided tones and announcements, audio mixing for multi-way conferences, and audio transcoding.
Gm	UE – P-CSCF	Allows the UE to communicate with the P-CSCF for registration and session control.

Reference Point	PacketCable Network Elements	Reference Point Description
pkt-sig-1	MGC – MG	Allows the MGC to control the MG in support of calls between the PacketCable network and PSTN. This reference point supports the 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

PacketCable is based on Release 7 of the IP Multimedia Subsystem (IMS) as defined by the 3rd Generation partnership Project (3GPP). The IMS was initially developed as a wireless-centric architecture, designed to meet the business and operational needs of the wireless industry. More recently, however, 3GPP has begun to accept and address requirements from other industries, including cable. As a result, the IMS Release 7 supports most, but not all of the cable industry requirements. This section describes the PacketCable SIP signaling enhancements to the IMS to support the unique technology, business, and operational requirements of the cable industry.

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

5.2.1 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 two modes of operation:

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.

5.2.2 Number Portability and Carrier Routing

[RFC 4694] 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 network core components and mandatory for the MGC. The BGCF may support the 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.

6 PACKETCABLE IMS REQUIREMENTS

This section describes the requirements and procedures that are currently not supported in IMS Release 7, 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.

IMS generally requires all SIP messages to and from the UE to be sent protected over the security association (there are certain exceptions, such as the initial REGISTER request described above, responses toward the UE, and emergency services). The security association provides data origin authentication, which enables the P-CSCF to assert the identity of the user. Like IMS, PacketCable requires signaling security to be a mandatory capability of the UE. However, PacketCable allows signaling security to be disabled in the following ways:

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

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 signaling 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, 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 must 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.

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 UEs that access IMS-services through that P-CSCF.

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 must reject the request with a 494 (Security Agreement Required) response.

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

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 UEs 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 UEs, 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 must 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 must 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 must 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.

6.2 Number portability and Equal-Access Carrier Routing

6.2.1 Description

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

6.2.2 Local Number Portability

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, based on local policy, route the call based on the LNP routing number, and 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).

As deployment options, the LNP database query can also be performed by a network entity earlier in the signaling chain, specifically by the BGCF, I-CSCF, or originating S-CSCF. For example, it would make sense to have the BGCF do the LNP query (instead of the MGC) for deployments where calls are routed to the PSTN via a 3rd-party IP carrier. Or, an operator could choose to have the query done by the I-CSCF or S-CSCF to take advantage of the fact that LNP data is being returned by an existing ENUM query (see [RFC 4769]). Routing policies to handle the case where the S-CSCF or I-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.

6.2.3 Equal-Access Carrier Routing

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 per-subscriber basis. Rather, a carrier may be presubscribed for all subscribers on a network-wide 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.

6.2.4 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 [RFC 4694], and the "dai" parameter defined in [ID DAI]. 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.

6.2.4.1 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.

6.2.4.2 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. 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 I-CSCF, BGCF, 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.

6.2.4.3 I-CSCF

An I-CSCF can receive a SIP INVITE request from an originating S-CSCF. There are certain scenarios where the I-CSCF is required to convert a Tel URI in the Request URI of the INVITE to a globally routable SIP URI for subsequent routing. If the conversion fails, then the I-CSCF may, based on local policy, route the INVITE to the BGCF.

The PacketCable enhancements to the I-CSCF to support number portability are similar to the number portability enhancements described above for the S-CSCF. If an I-CSCF that is configured to support number portability determines that a call is destined for the PSTN, then it shall determine whether or not the called number is ported. If the called number is ported, then the I-CSCF shall determine the actual routing number, and add an "rn" parameter identifying the routing number and an "npdi" parameter indicating that an LNP database dip has been performed to the Tel URI in the Request URI of the INVITE.

6.2.4.4 BGCF

The BGCF receives INVITE requests from the S-CSCF or I-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 BGCF procedures to support both number portability and carrier routing. The BGCF must provide configuration controls such that support of these two capabilities can be independently enabled or disabled based on local operator policy.

If the BGCF is configured to support number portability, then it shall determine whether or not the called number is ported. If the called number is ported, then the BGCF shall determine the actual routing number, and add an "rn" parameter identifying the routing number and an "npdi" parameter indicating that an LNP database dip has been performed to the Tel URI in the Request URI of the INVITE.

If the BGCF is configured to support a network-wide pre-subscribed carrier, then it will add a "cic" parameter identifying the locally configured carrier ID, and a "dai" parameter identifying how the carrier was obtained, to the Tel URI in the INVITE Request URI. Addition of these parameters may be based on routing policy, and on the attributes of the request being routed. The BGCF must allow for the case where these parameters were added by another network component earlier in the signaling chain, and hence not overwrite the parameters if already provided.

If the BGCF is configured to support number portability, then it will determine whether or not the called number is ported. If the called number is ported, then the I-CSCF will determine the actual routing number, and add an "rn" parameter identifying the routing number and an "npdi" parameter indicating that an LNP database dip has been performed to the Tel URI in the Request URI of the INVITE.

The BGCF may include the Tel URI "cic" and "rn" parameters in its routing decision. How these parameters affect routing is not specified.

6.2.4.5 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", "dai") 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.

6.3 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].

7 IPV4/6 INTERWORKING

This section provides an overview of the various IPv4/6 interworking mechanisms that are supported in 3GPP IMS Release 7.

IP Version interworking can be supported at the SIP application layer through the IMS-ALG function as defined in [TS 23.228]. The IMS-ALG is a logical function that may be provided by the IBCF (refer to [TS 23.228] Annex I). The P-CSCF may also contain an IMS-ALG function to support IP Version interworking (refer to [TS 23.228], Annex G.2 and G.3).

The IMS-ALG supports IP Version interworking by requesting transport addresses, of the IP version type to be interworked, from a transport layer NAT-PT/NAPT-PT function, and then performing the necessary modifications to SIP and SDP. The IMS-ALG acts as a B2BUA, and modifies the SDP with the IP address obtained from the NAT-PT/NAPT-PT function. The TrGW provides the NAT-PT/NAPT-PT function for an IMS ALG that is a function of an IBCF. The IMS Access Gateway provides the NAT-PT/NAPT-PT function for an IMS ALG that is a function of a P-CSCF. The TrGW and IMS Access Gateway maintain pools of transport layer IP addresses for IPv4 and IPv6. The TrGW / IMS Access Gateway binds IPv6 network addresses with IPv4 network addresses and vice versa, and forwards media packets based on the bindings.

An IBCF containing the IMS-ALG function may be used as an entry and exit point for an IMS network when IP Version interworking capabilities are required. [TS 23.228], Annex I, contains example session flows illustrating use of the IBCF as exit and entry points. For example, an originating IPv6 IMS network may route a request through an IBCF / IMS ALG when it determines interworking to an IPv4 network is required. As another example, an IPv6 IMS network may provide an IBCF / IMS ALG an as entry point for IPv4 networks.

Use of the IBCF for IP Version Interworking addresses cases where an IMS network supports a homogeneous IP version type. For cases where an IMS network has a mix of IPv4 and IPv6 UEs, the P-CSCF IMS ALG capability can be used to facilitate IP Version interworking between such devices.

Appendix I 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