

Superseded

by a later version of this document

PacketCable™ 2.0

Architecture Framework Technical Report

PKT-TR-ARCH-FRM-V05-080425

RELEASED

Notice

This PacketCable technical report is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

© Copyright 2006-2008 Cable Television Laboratories, Inc.
All rights reserved.

Document Status Sheet

Document Control Number: PKT-TR-ARCH-FRM-V05-080425

Document Title: Architecture Framework Technical Report

Revision History: V01 – Released 04/06/06

V02 – Released 10/13/06

V03 – Released 09/25/07

V04 – Released 11/06/07

V05 – Released 04/25/08

Date: April 25, 2008

Trademarks:

CableLabs®, DOCSIS®, EuroDOCSIS™, eDOCSIS™, M-CMTS™, PacketCable™, EuroPacketCable™, PCMM™, CableHome®, CableOffice™, OpenCable™, OCAP™, CableCARD™, M-Card™, DCAS™, and tru2way™ are trademarks of Cable Television Laboratories, Inc.

Abstract

This technical report describes the architecture framework for PacketCable™ networks, including all major system components, the various functional groupings and the network interfaces necessary for delivery of services via a PacketCable network. The intended audience for this document includes developers of equipment intended to be conformant to PacketCable specifications, and network architects who need to understand the overall PacketCable architecture framework.

This technical report describes the PacketCable release. It contains the following information:

- A reference architecture;
- Description of the various functional groupings within the architecture;
- High level goals of the architecture;
- Detailed description specific architectural components;
- Reference Points defined in PacketCable.

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

Table of Contents

1	INTRODUCTION	1
1.1	PACKETCABLE OVERVIEW	1
2	REFERENCES	2
2.1	NORMATIVE REFERENCES	2
2.2	INFORMATIVE REFERENCES	2
2.3	REFERENCE ACQUISITION	3
3	TERMS AND DEFINITIONS	4
4	ABBREVIATIONS AND ACRONYMS	5
5	PACKETCABLE	7
5.1	RELATIONSHIP WITH THE 3GPP IMS	7
5.2	OVERVIEW	8
5.3	PACKETCABLE RELEASES AND ORGANIZATION	12
5.3.1	<i>PacketCable Releases</i>	12
5.3.2	<i>PacketCable Organization</i>	13
5.4	PACKETCABLE DESIGN CONSIDERATIONS	15
5.4.1	<i>Generic Architecture Goals</i>	15
5.4.2	<i>IP Version Support and Interworking</i>	15
5.4.3	<i>Signaling and Service Control</i>	16
5.4.4	<i>Subscriber Data</i>	16
5.4.5	<i>Network Address and Port Translation (NA(P)T) and Firewall Traversal</i>	16
5.4.6	<i>Quality of Service</i>	16
5.4.7	<i>Media Stream Transport and Encoding</i>	17
5.4.8	<i>Provisioning</i>	17
5.4.9	<i>Network Accounting and Usage</i>	17
5.4.10	<i>Security</i>	17
5.4.11	<i>Lawful Intercept</i>	18
6	PACKETCABLE FUNCTIONAL COMPONENTS	19
6.1	LOCAL NETWORK	19
6.1.1	<i>User Equipment (UE)</i>	19
6.1.2	<i>NAT and Firewall</i>	19
6.2	ACCESS NETWORK	19
6.2.1	<i>Cable Modem (CM)</i>	19
6.2.2	<i>Cable Modem Termination System (CMTS)</i>	19
6.2.3	<i>Access Point</i>	20
6.3	EDGE	20
6.3.1	<i>Proxy Call Session Control Function (P-CSCF)</i>	20
6.3.2	<i>STUN and TURN Servers</i>	20
6.3.3	<i>PacketCable Application Manager</i>	21
6.4	CORE	21
6.4.1	<i>Serving CSCF (S-CSCF)</i>	21
6.4.2	<i>Interrogating CSCF (I-CSCF)</i>	22
6.4.3	<i>Home Subscriber Server (HSS)</i>	22
6.4.4	<i>Subscription Locator Function (SLF)</i>	22
6.5	PACKETCABLE MULTIMEDIA	22
6.5.1	<i>Policy Server</i>	23
6.6	APPLICATION	23

6.6.1	<i>Application Server (AS)</i>	23
6.6.2	<i>Multimedia Resource Function (MRF)</i>	23
6.6.3	<i>Presence Server Functions</i>	23
6.7	INTERCONNECT	23
6.7.1	<i>Border Control Functions</i>	23
6.7.2	<i>Breakout Gateway Control Function (BGCF)</i>	24
6.7.3	<i>Public Switched Telephone Network Gateway (PSTN GW)</i>	24
6.7.4	<i>Call Management Server (CMS)</i>	24
6.8	OPERATIONAL SUPPORT SYSTEMS.....	24
6.8.1	<i>Dynamic Host Configuration Protocol (DHCP) Server</i>	24
6.8.2	<i>Domain Name System (DNS) Server</i>	24
6.8.3	<i>ENUM Server</i>	25
6.8.4	<i>Provisioning Server</i>	25
6.8.5	<i>KDC</i>	25
6.8.6	<i>Configuration Server</i>	25
6.8.7	<i>Syslog Server</i>	25
6.8.8	<i>Charging Data Function (CDF)/Charging Gateway Function (CGF)</i>	25
7	PROTOCOL INTERFACES AND REFERENCE POINTS	26
7.1	SIGNALING AND SERVICE CONTROL	26
7.2	SUBSCRIBER DATA	28
7.3	QUALITY OF SERVICE	29
7.4	NETWORK ADDRESS TRANSLATION (NAT) AND FIREWALL TRAVERSAL	30
7.5	MEDIA CODING AND TRANSPORT	32
7.6	PROVISIONING	33
7.7	NETWORK ACCOUNTING AND USAGE.....	35
7.8	SECURITY	36
7.8.1	<i>Access Domain Security</i>	37
7.8.2	<i>Intra-Network Domain Security</i>	38
7.8.3	<i>Inter-Network Domain Security</i>	38
7.9	LAWFUL INTERCEPT	39
7.10	CONTROL POINT DISCOVERY	40
APPENDIX I	ACKNOWLEDGEMENTS	42

Figures

FIGURE 1 - PACKETCABLE REFERENCE ARCHITECTURE	9
FIGURE 2 - PACKETCABLE RELEASES.....	12
FIGURE 3 - PACKETCABLE ORGANIZATION	13
FIGURE 4 - SIGNALING REFERENCE POINTS.....	26
FIGURE 5 - SUBSCRIBER DATA REFERENCE POINTS	28
FIGURE 6 - QOS REFERENCE POINTS	29
FIGURE 7 - NAT AND FW TRAVERSAL REFERENCE POINTS.....	31
FIGURE 8 - MEDIA STREAM REFERENCE POINTS	32
FIGURE 9 - PROVISIONING REFERENCE POINTS	34
FIGURE 10 - ACCOUNTING REFERENCE POINTS.....	35
FIGURE 11 - ACCESS DOMAIN REFERENCE POINTS	37
FIGURE 12 - LAWFUL INTERCEPT REFERENCE POINTS	39
FIGURE 13 - CONTROL POINT DISCOVERY REFERENCE POINT	41

Tables

TABLE 1 - PACKETCABLE SPECIFICATIONS AND REPORTS	14
TABLE 2 - SIGNALING REFERENCE POINT DESCRIPTIONS.....	27
TABLE 3 - SUBSCRIBER DATA REFERENCE POINT DESCRIPTIONS	28
TABLE 4 - QOS REFERENCE POINT DESCRIPTIONS	30
TABLE 5 - NAT AND FW TRAVERSAL REFERENCE POINT DESCRIPTIONS.....	32
TABLE 6 - MEDIA STREAM REFERENCE POINT DESCRIPTIONS	33
TABLE 7 – PROVISIONING REFERENCE POINT DESCRIPTIONS.....	34
TABLE 8 - ACCOUNTING REFERENCE POINT DESCRIPTIONS.....	35
TABLE 9 - ACCESS DOMAIN REFERENCE POINT DESCRIPTIONS.....	37
TABLE 10 - LAWFUL INTERCEPT REFERENCE POINT DESCRIPTIONS.....	40
TABLE 11 - CONTROL POINT DISCOVERY REFERENCE POINT DESCRIPTION.....	41

1 INTRODUCTION

1.1 PacketCable Overview

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

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

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

As noted above, the architecture is designed to support a broad range of services. The PacketCable set of specifications and technical reports define a base architecture, and the components and generic requirements necessary to meet a large number of applications and services. Specific applications and services rely on this base architecture, but are specified in separate releases. The base specifications should be able to accommodate different applications and services with very few, if any, changes.

This release of PacketCable is based on Release 7 of the IP Multimedia Subsystem (IMS) as developed by the 3rd Generation Partnership Project (3GPP). The IMS is a SIP-based architecture for providing multimedia services. PacketCable defines enhancements to the IMS in order to ensure PacketCable addresses requirements that are not already addressed by the IMS.

PacketCable leverages other open standards and specifications wherever possible.

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.

- [ACCT] PacketCable Accounting Specification, PKT-SP-ACCT-I03-070925, September 25, 2007, Cable Television Laboratories, Inc.
- [ARCH] PacketCable 1.5 Architecture Framework, PKT-TR-ARCH1.5-V02-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [CMSS] PacketCable 1.5 CMS to CMS Signaling Specification, PKT-SP-CMSS1.5-I04-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [CODEC] PacketCable Codec and Media Specification, PKT-SP-CODEC-MEDIA-I04-080425, April 25, 2008, Cable Television Laboratories, Inc.
- [CPD] PacketCable Control Point Discovery Specification, PKT-SP-CPD-I03-070925, September 25, 2007, Cable Television Laboratories, Inc.
- [ES-DCI] PacketCable Electronic Surveillance - Delivery Function to Collection Function Interface Specification, PKT-SP-ES-DCI-I02-070925, September 25, 2007, Cable Television Laboratories, Inc.
- [ES-INF] PacketCable Electronic Surveillance - Intra-Network Functions Specification, PKT-SP-ES-INF-I04-080425, April 25, 2008, Cable Television Laboratories, Inc.
- [HSS TR] PacketCable Home Subscriber Server Technical Report, PKT-TR-HSS-V03-071106, November 6, 2007, Cable Television Laboratories, Inc.
- [MM TR] PacketCable Multimedia Architecture Framework Technical Report, PKT-TR-MM-ARCH-V02-051221, December 21, 2005, Cable Television Laboratories, Inc.
- [NFT TR] PacketCable NAT and Firewall Traversal Technical Report, PKT-TR-NFT-V05-080425, April 25, 2008, Cable Television Laboratories, Inc.
- [E-UE Prov] E-UE Provisioning Framework Specification, PKT-SP-EUE-PROV-I01-071106, November 6, 2007, Cable Television Laboratories, Inc.
- [QOS] PacketCable Quality of Service Specification, PKT-SP-QOS-I02-080425, April 25, 2008, 2007, Cable Television Laboratories, Inc.
- [RFC 3261] IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.
- [SEC TR] PacketCable Security Technical Report, PKT-TR-SEC-V05-080425, April 25, 2008, Cable Television Laboratories, Inc.
- [SEC] PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-I02-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [SIP TR] PacketCable SIP Signaling Technical Report, PKT-TR-SIP-V04-071106, November 6, 2007, Cable Television Laboratories, Inc.
- [TGCP] PacketCable 1.5 PSTN Gateway Call Signaling Protocol Specification, PKT-SP-TGCP1.5-I03-070412, April 12, 2007, Cable Television Laboratories, Inc.
- [TS 23.002] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture (Release 7); December 2007.

2.3 Reference Acquisition

- 3rd Generation Partnership Project: <http://www.3gpp.org>
- 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>

3 TERMS AND DEFINITIONS

This PacketCable Technical Report uses the following terms and definitions:

Contact Address	The URI of a User Agent on the network. Contact addresses, in the context of PacketCable are often, but not always, addresses used to deliver requests to a specific User Agent.
DHCPv6	IPv6 version of the Dynamic Host Configuration Protocol.
Dual-stack node	An IPv6/IPv4 host or router that operates with both the IPv6 and IPv4 stacks enabled.
E.164	E.164 is an ITU-T Recommendation that defines the international public telecommunication numbering plan used in the PSTN and other data networks.
Headend	The central location on the cable network that is responsible for injecting broadcast video and other signals in the downstream direction.
IMS Delta specifications	Suite of 3GPP IMS specifications modified to reflect cable-specific deltas necessary to comply with PacketCable.
IPv4-only node	A host or router that implements only IPv4 and does not implement IPv6.
IPv6/IPv4 node	A host or router that implements both IPv4 and IPv6.
IPv6-only node	A host or router that implements only IPv6 and does not implement IPv4.
Multi-System Operator (MSO)	A company that owns and operates more than one cable system.
PacketCable Multimedia	An application agnostic QoS architecture for services delivered over DOCSIS networks.
Presence data	A view of the willingness and availability of a user for communications.
Presence Server Functions	A functional group consisting of specialized Application Servers that support exchange of presence data.
Public User Identity	Used by any user for requesting communications to other users or applications.
SIP User Agent	As defined by [RFC 3261], a logical entity that can act as both a user agent client and user agent server, meaning that it can generate requests and manage the resulting transaction, and it can generate responses to incoming requests and manage the resulting transaction.
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.
Subscriber	An entity (composed of one or more users) that is engaged in a Subscription with a service provider.
Subscription	A contract for service(s) between a user and a service provider.
User	A person who, in the context of this document, uses a defined service or invokes a feature on a UE.
User Agent (UA)	A SIP User Agent.

4 ABBREVIATIONS AND ACRONYMS

This PacketCable Technical Report uses following abbreviations and acronyms:

3GPP	3 rd Generation Partnership Project
ALG	Application Layer Gateway
AM	Application Manager
AF	Application Function
AS	Application Server
BGCF	Breakout Gateway Control Function
CDF	Charging Data Function
CDR	Call Detail Record
CF	Collection Function
CGF	Charging Gateway Function
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
DF	Delivery Function
DNS	Domain Name System
DOCSIS®	Data-Over-Cable Service Interface Specifications
E-CSCF	Emergency Call Session Control Function
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
IBCF	Interconnection Border Control Function
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

KDC	Key Distribution Center
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
NMS	Network Management System
PAM	PacketCable Application Manager
P-CSCF	Proxy Call Session Control Function
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
SLF	Subscription Location Function
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SS7	Signaling System 7
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TGCP	Trunking Gateway Control Protocol
TLS	Transport Layer Security
TR	Technical Report
TrGW	Transition Gateway
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier

5 PACKETCABLE

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

This section provides:

- An overview of the architecture, including a description of the main functional groupings (e.g., Local Network, Access Network, Edge, Core) and logical entities (e.g., UE, P-CSCF, S-CSCF, HSS) within those groupings;
- A set of design goals for the PacketCable architecture and specifications;
- A list of PacketCable specifications and technical reports.

5.1 Relationship with the 3GPP IMS

PacketCable is based on Release 7 of the IP Multimedia Subsystem (IMS) as defined by the 3rd Generation partnership Project (3GPP). 3GPP is a collaboration agreement between various standards bodies. The scope of 3GPP is to produce Technical Specifications and Technical Reports for GSM and 3rd Generation (3G) Mobile System networks. More recently, however, 3GPP has begun to accept and address requirements from other industries (e.g., cable).

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

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

While many of the functional entities and reference points defined in the IMS have broad applicability in other industries, it does not meet all of the cable industry needs. PacketCable enhances the IMS to support the unique technology requirements of the cable industry, and also addresses cable operator business and operating requirements.

3GPP is developing newer releases of the IMS specifications. The initial release of PacketCable 2.0 was based on release 6. The current release of PacketCable 2.0 is based on release 7. Future updates to PacketCable will align with newer releases as necessary.

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

IPv6 support is mandatory in IMS as defined in 3GPP Architectural Requirements. IMS Release 5 specified IPv6 as the only IP version supported. In IMS Release 7, support for IPV4 was added to the specifications for systems providing access to IMS using a fixed broadband interconnection. IMS Release 7 specifications define a few architecture scenarios for interworking between networks supporting different IP versions.

5.2 Overview

The PacketCable architecture is based on the IMS architecture, with some incremental extensions. Extensions include use of additional or alternate functional components compared with the IMS architecture, as well as enhancements to capabilities provided by the IMS functional components.

Some of the PacketCable enhancements to the IMS include:

- Support for Quality of Service (QoS) for IMS-based applications on DOCSIS access networks, leveraging the PacketCable Multimedia architecture [MM TR];
- Support for additional access signaling security and UE authentication mechanisms;
- Support for provisioning, activation, configuration, and management of UEs;
- Support for regulatory requirements such as number portability, preferred carrier, and PacketCable lawful interception.

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

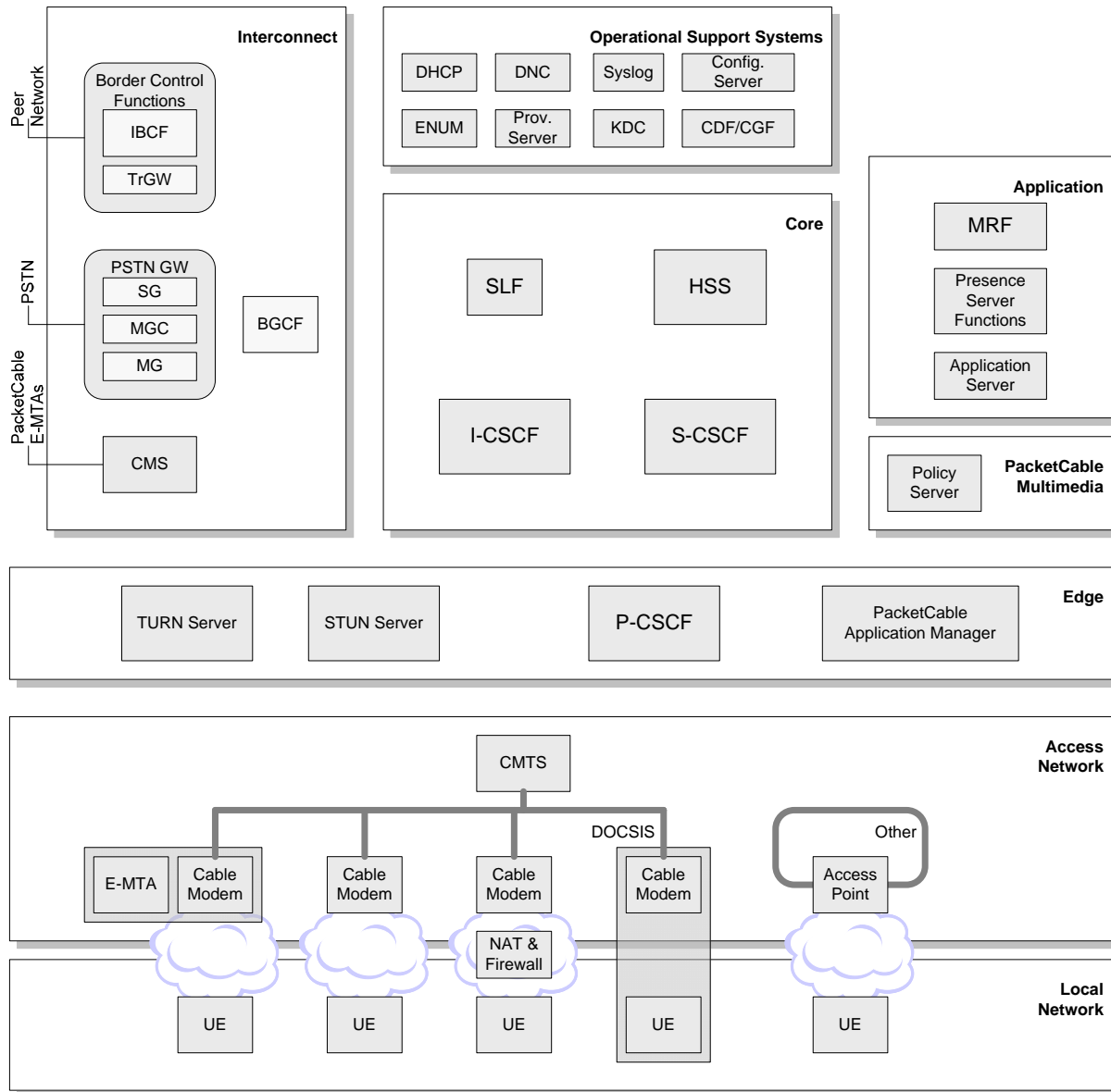


Figure 1 - PacketCable Reference Architecture

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

PacketCable assumes a model composed of users, Public User Identities, UEs, and devices. For example, a user may have multiple User Equipment (UE) devices, each of which may be registered to one or more Public User Identities. A Public User Identity can be an E.164 number or it can be an alphanumeric identifier that makes sense in the context of a SIP Telephony service. Each Public User Identity is generally associated with a user.

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

- **Local Network:** The local network is the network that the User Equipment (UE) uses to connect to the access network. It may be Ethernet, WiFi, Bluetooth, or any other technology used to network or connect UEs. There may be a NAT and Firewall gateway between the local network and the access network. In some instances, the UE may include an access network component. In such instances, the local network is an internal interface within the UE. This is the case with a UE that has an embedded DOCSIS cable modem.

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

- **Access Network:** A UE may reside on or be connected to the DOCSIS access network, or it may obtain services from other access networks (including other cable access networks not under the control of the cable operator that owns the PacketCable Subscription); this is especially important for a mobile UE such as a laptop, WiFi-enabled phone, etc. When a UE is in the cable access network, it can obtain access network QoS by interacting with the cable networks SIP signaling infrastructure, which in turn interacts with the PacketCable Multimedia infrastructure via the PacketCable Application Manager and Policy Server to reserve resources in the cable access network.

PacketCable NCS-based E-MTAs are included in the reference diagram for completeness.

- **Edge:** This functional grouping encompasses reference points that are provided to a UE and the access network. A UE obtains access to the SIP Infrastructure through the Proxy-Call Session Control Function (P-CSCF). The P-CSCF proxies SIP messages between the UE and the rest of the architecture and maintains security associations with the UE. The P-CSCF may request access network QoS resources upon session initiation or mid-session changes on behalf of the UE via the PacketCable Application Manager. The PacketCable Application Manager interfaces with the PacketCable Multimedia Policy Server, which pushes QoS policy to the cable access network components. IETF STUN and TURN servers are used to enable media access through NAT & FW devices (the P-CSCF uses a separate STUN server for signaling access through NAT & FW devices). PacketCable E-MTAs are served by their CMS as described in PacketCable 1.5 Architecture Framework Technical Report [ARCH].
- **Core:** The Core contains the basic components required to provide SIP services and subscriber data. The Core functional grouping consists of the following functional components: Interrogating-CSCF (I-CSCF), Serving-CSCF (S-CSCF), Subscription Location Function (SLF), and Home Subscriber Server (HSS).
 - The I-CSCF is the initial entry point into the Core for SIP. The I-CSCF cooperates with the HSS to determine the S-CSCF to be assigned to a Public User Identity, and routes requests originated by a UE to the S-CSCF assigned to the originating UE's Public User Identity. The I-CSCF also routes terminating SIP requests received from within the network or from outside networks. In this case, the I-CSCF consults the HSS to determine the S-CSCF that is assigned to a terminating Public User Identity, and routes the SIP request to that S-CSCF for processing.

- The S-CSCF is responsible for SIP session processing. Calls or multimedia communication sessions initiated to and from Public User Identities are sent to the assigned S-CSCF for authorization and processing. The S-CSCF has a service control framework that evaluates SIP requests against pre-defined filter criteria for a subscriber and determines if the SIP request should be routed to an Application Server for processing. This enables an extensible architecture for rapid introduction of value-added features and services. The S-CSCF may route SIP messages to Application Servers, Presence Servers, MRFs, other CSCFs, or Breakout Gateway Control Functions (BGCFs) as appropriate. The S-CSCF also includes the SIP registrar function, which maps Public User Identities to their registered SIP contact addresses, assigns Globally Routable User Agent URIs (GRUUs), and stores any other parameters associated with the registration, e.g., SIP User Agent capabilities. The S-CSCF obtains subscription data from the HSS.
- The HSS provides access to user profiles and other provisioned subscriber data to the S-CSCF and Application Servers. The HSS also maintains the assignment of a Public User Identities to an S-CSCF. A Subscription may be associated with multiple Public User Identities. An HSS maps a subscription to a S-CSCF; meaning that all the Public User Identities for that subscription will be assigned to the same HSS.
- S-CSCFs and Application Servers may store certain classes of data associated with subscriptions in the HSS.
- The SLF is used to locate an HSS instance for a given Identity when multiple HSSs are present.
- The E-CSCF (not shown in the Figure 1) handles the routing of emergency sessions.
- Applications: The Application Server functional grouping defines Application Servers that may be invoked as part of originating or terminating request treatment on a S-CSCF for a given user, or they may be stand-alone application servers that can be invoked and operate independently. This functional grouping also contains two other components that are utilized by Application Servers:
 - The MRF provides a variety of multimedia functions, including media stream sourcing for network provided tones and announcements, media stream mixing and floor control for audio/video conferencing, and media stream processing such as audio transcoding.
 - The Presence Server Functions group consists of specialized Application Servers that support the exchange of presence data for Public User Identities. The presence data is obtained from a variety of sources in the network and provides a view of the willingness and availability of the user for communications. Privacy handling and subscription authorization of presence data is also handled by this functional group.
- Interconnect: The Interconnect functional grouping enables connections with other networks. Interconnect with the PSTN is handled via the Breakout Gateway Control Function (BGCF), which determines the Media Gateway Controller (MGC) to utilize for PSTN interconnect. The MGC controls Media Gateways (MG) which provides transport layer and bearer interconnect to the PSTN. Signaling Gateways (SG) provide SS7 connectivity. The PacketCable MGC, SG, and MG are used to interconnect to the PSTN. Interconnect with peer Voice over IP (VoIP) networks may be achieved through a group of functions called the Border Control Functions. The Border Control Functions include the Interconnection Border Control Function (IBCF) and optionally the Transition Gateway (TrGW) that may be on a separate platform. The IBCF may perform a variety of tasks, including protocol profile enforcement, IP version interworking, and topology hiding, as needed to inter-work with other networks. The TrGW may relay media for the purposes of IP version interworking and topology hiding. The PacketCable CMS is located in the Interconnect functional grouping to indicate that E-MTAs that it serves can communicate with UEs.
- PacketCable Multimedia: PacketCable Multimedia defines an IP-based platform for delivering QoS-enhanced multimedia services over DOCSIS access networks. The PacketCable Multimedia architecture defines an Application Manager and Policy Server. The Application Manager translates application specific resource requests to PacketCable Multimedia requests and forwards these requests to the Policy Server. The Policy Server enforces network policy and installs the resulting QoS policy on the CMTS for enforcement.

- Operational Support Systems: Operational Support Systems provide various functions like accounting and UE provisioning. The CDF/CGF collects accounting messages from various elements, DHCP helps with the distribution of IP addresses to UEs, ENUM and DNS aid in the resolution of URIs and FQDNs, The Provisioning Server, Configuration Server, and KDC components support provisioning and configuration of UEs,

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

5.3 PacketCable Releases and Organization

5.3.1 PacketCable Releases

The PacketCable architecture continues to evolve as new capabilities are added, and as such is composed of several releases.

- PacketCable 1.0 - This release provides support for a telephony application using E-MTAs;
- PacketCable 1.5 - This release is a superset of PacketCable 1.0 that provides incremental new capabilities and adds SIP for session management within and among PacketCable networks;
- PacketCable Multimedia - This release is separate from the 1.0, 1.5, and 2.0. It provides a service agnostic QoS and accounting framework;
- PacketCable 2.0 - This release is separate from 1.0, 1.5, and Multimedia. It adds support for SIP-based endpoints, and a SIP-based service platform that may be used to support a variety of services.

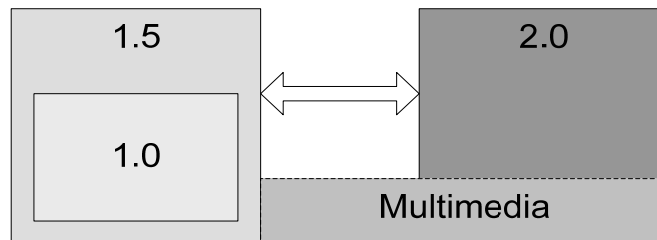


Figure 2 - PacketCable Releases

Figure 2 illustrates the PacketCable releases. PacketCable 2.0 uses PacketCable Multimedia for QoS. PacketCable Multimedia is separate, however, and may be used by other applications as well. Applications that make use of the SIP service platform will be defined in separate standalone releases and are not depicted in Figure 2.

5.3.2 PacketCable Organization

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

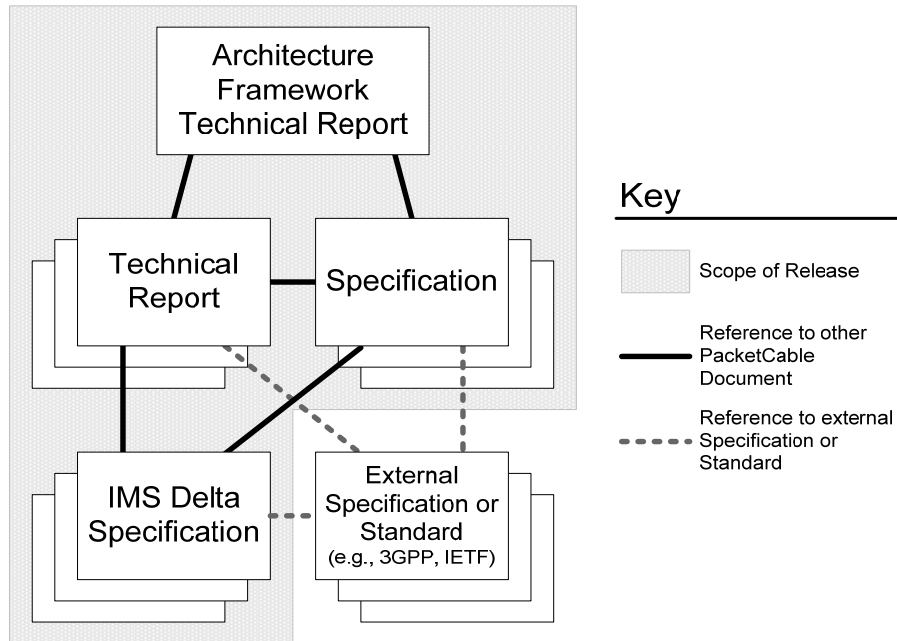


Figure 3 - PacketCable Organization

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

In some cases, these documents do not draw on any IMS architectural components or reference points. However, in general these documents are based upon the IMS, and in some cases enhance the IMS. Documents that are based upon the IMS simply refer to IMS documents in the same way any other document is normatively referenced. Enhancements to the IMS are contained in IMS Delta specifications. IMS Delta specifications are republished IMS specifications that contain changes based upon cable-specific requirements. Depending on the way the IMS documents are organized, an IMS Delta specification may contain changes to accommodate a number of different PacketCable specifications or TRs. For example, the IMS Delta Specification for 3GPP TS24.229 contains changes for the functional areas of SIP, security, and QoS.

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

Table 1 contains a list of Specifications and Technical Reports. Refer to <http://www.packetcable.com> for a complete list of documents.

Table 1 - PacketCable Specifications and Reports

PacketCable Technical Report Reference Number	Technical Report Name
PKT-TR-ARCH-FRM	Architecture Framework (this document)
PKT-TR-SIP	SIP Signaling
PKT-TR-SEC	Security
PKT-TR-HSS	Home Subscriber Server
PKT-TR-NFT	NAT and Firewall Traversal
PacketCable Specification Reference Number	Specification Name
PKT-SP-CPD	Control Point Discovery
PKT-SP-CODEC-MEDIA	Codec and Media
PKT-SP-ACCT	Accounting
PKT-SP-ES-INF	Electronic Surveillance – Intra-Network Functions
PKT-SP-ES-DCI	Electronic Surveillance Protocol – Delivery Function to Collection Function Interface
PKT-SP-QOS	Quality of Service
PKT-SP-PRS	Presence
PKT-SP-EUE-PROV	E-UE Provisioning Framework Specification
PKT-SP-EUE-DATA	E-UE Provisioning Data Model Specification
IMS Delta Specification Reference Number	Specification Name
PKT-SP-23.008	Organization of Subscriber Data Specification 3GPP TS 23.008
PKT-SP-24.229	SIP and SDP Stage 3 Specification 3GPP TS 24.229
PKT-SP-29.228	Cx and Dx Interfaces Specification 3GPP TS 29.228
PKT-SP-29.229	Cx and Dx Interfaces, Diameter Protocol Specification 3GPP TS 29.229
PKT-SP-33.203	Access Security for IP-Based Services Specification 3GPP TS 33.203

As described in Section 1.1, this PacketCable release defines a base architecture upon which applications can be built. While these applications rely on the base architecture, they are independent of the base architecture and are specified in separate releases.

5.4 PacketCable Design Considerations

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

- Signaling and Service Control;
- Subscriber Data;
- Network Address Translation (NAT) and Firewall Traversal;
- Quality of Service;
- Media Stream Transport and Encoding;
- Provisioning, Activation, Configuration, and Management;
- Network Accounting and Usage;
- Security;
- Lawful Intercept.

5.4.1 Generic Architecture Goals

The design goals of the PacketCable architecture include:

- Provide a service-independent architecture that allows new services to be added without impacting the underlying service control platform;
- Provide a modular architecture, where architectural components can be combined in a variety of ways to support a wide range of features. For example, a UE could be built from a mix of basic building blocks such as SIP User Agents, media endpoints, presence watchers, and event subscribers;
- Support many-to-many relationships between users, endpoint devices, and sessions;
- Support a wide variety of UE devices, including soft or hard UEs, smart UEs, wired or wireless UEs;
- Support IPv4 and IPv6 operation;
- Support interworking with previous releases of PacketCable;
- Leverage existing standards and open protocols whenever possible. Most importantly, adopt the IMS architecture and define incremental extensions as necessary.

5.4.2 IP Version Support and Interworking

The design goals for PacketCable IP Version support and interworking include:

- Identify a minimum level of support for IPv4 and IPv6. A compliant UE is an IPv6/IPv4 node, but only one IP version is enabled for both UE operation and management. The dual-stack mode (concurrent IPv4 and IPv6 operation or management modes) is out-of-scope;
- Support IPv6-only access networks (with support for Stateless Address Auto-Configuration in uncontrolled network environments, and support for DHCPv6 in controlled environments), IPv4-only access networks, and both IPv4 and IPv6 access networks (with support for a selection algorithm to choose the IP version prior to contacting the P-CSCF);

- Support network components in the Edge, Core, PacketCable Multimedia, and Interconnect functional groupings that operate in the following modes: IPv6-only, or IPv4-only or IPv6/IPv4;
- Support interconnection with peer networks using different IP version.

5.4.3 Signaling and Service Control

PacketCable Signaling and Service Control design goals include:

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

5.4.4 Subscriber Data

PacketCable Subscriber Data design goals include:

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

5.4.5 Network Address and Port Translation (NA(P)T) and Firewall Traversal

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

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

5.4.6 Quality of Service

PacketCable QoS design goals include:

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

5.4.7 Media Stream Transport and Encoding

PacketCable media stream transport and encoding design goals include:

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

5.4.8 Provisioning

PacketCable Provisioning design goals include:

- Specific provisioning flows for UEs to initialize in IP networks, and obtain PacketCable configuration;
- Specify configuration and management protocols, and data models, for embedded and standalone UEs;
- Support a multi-layered data model for UEs, applications and users; allowing for separate definitions for each layer;
- Support secure software download for embedded and standalone UEs.

5.4.9 Network Accounting and Usage

PacketCable network accounting and usage design goals include:

- Enable the ability to account for network usage and service activities in Real-Time;

In this case, Real-Time is relative to when the events are sent to the central repository and does not imply when the final bill may be available to the customer nor that events are sent to indicate incremental usage of network resources (i.e., on-line charging);

- Allow for multiple network elements to generate events that can be correlated to a given session or subscriber;
- Support the correlation of accounting events across the signaling and bearer planes;
- Facilitate the rapid introduction of features and services by minimizing the impact to other network elements and their need to signal feature and service related information.

5.4.10 Security

PacketCable security design goals include:

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

- Mechanisms for UE authentication, secure provisioning, secure signaling, secure media, and secure software download.

5.4.11 Lawful Intercept

PacketCable lawful intercept design goals include:

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

6 PACKETCABLE FUNCTIONAL COMPONENTS

This section provides additional detail on each of the functions in the PacketCable architecture.

6.1 Local Network

6.1.1 User Equipment (UE)

PacketCable 1.0 and 1.5 supports NCS-based clients for telephony services. PacketCable 2.0 adds support for SIP-based clients with a variety of capabilities, e.g., soft and hard phones, smart phones, wireless and wired phones, Instant Messaging UEs, video communications terminals, etc. Consistent with IMS, PacketCable clients are called User Equipment (UE). All of the various UEs described previously use the same basic infrastructure to obtain multimedia services. UEs may be fixed or mobile devices such as laptops or WiFi-enabled phones. They may reside on the cable access network, or they may obtain services from other access networks. When UEs are in the cable access network, they can obtain access network QoS by interacting with the signaling infrastructure, which in turn interacts with the PacketCable Multimedia Policy Server. The UE is an IPv6/IPv4 node and it may connect to a local network that operates in IPv4, IPv6, or both IPv4 and IPv6. If the local network provides both IPv6 and IPv4 connectivity, the UE may obtain two pools of IP addresses and perform an IP address selection.

6.1.2 NAT and Firewall

An NA(P)T (Network Address and Port Translator) and a Firewall may be present between the local network and the access network. Since NAT may modify IP addresses and ports, and a firewall restricts access, the signaling and bearer planes need to behave differently when these elements are inserted between the UE and the P-CSCF.

6.2 Access Network

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

6.2.1 Cable Modem (CM)

The CM is the Customer Premise Equipment (CPE) used in conjunction with the CMTS to provide broadband data transport service over the Cable HFC Access Network. An E-MTA is a PacketCable NCS-based client with an embedded cable modem. While the E-MTA does not communicate directly with the network, it is important to note that a NCS-based telephony service and SIP-based service may be provided through the same CM. PacketCable 2.0 UEs may also be embedded with a CM.

The DOCSIS access network should be DOCSIS 3.0-compliant in order to support full IPv6 operations with network access QoS using PacketCable Multimedia. DOCSIS 2.0 and prior versions of DOCSIS specifications have limitations that may not allow native IPv6 transport for PacketCable applications.

6.2.2 Cable Modem Termination System (CMTS)

The CMTS resides in the cable operator's headend, and, in conjunction with the CM, it is used to provide broadband data transport service over the Cable HFC Access Network. Beginning with version 1.1, DOCSIS defines a means to provide QoS on the access network. PacketCable Multimedia defines a means for IP-enabled services to request QoS from the DOCSIS network. PacketCable defines how QoS can be provided for SIP-based services via PacketCable Multimedia and DOCSIS.

6.2.3 Access Point

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

6.3 Edge

6.3.1 Proxy Call Session Control Function (P-CSCF)

A UE accesses the SIP Infrastructure through a P-CSCF. The P-CSCF shields the SIP network from access network specific protocol details (such as QoS) and provides scaling for the infrastructure by handling certain resource intensive tasks when interacting with the UE. It also represents the trust boundary for SIP between untrusted parts of the network (Access Network, Local Network) and trusted parts of the network (Core, Application, Interconnect, Operational Support Systems). The functions performed by the P-CSCF are:

- Routing SIP messages from the UE to the I-CSCF or S-CSCF and vice versa;
- Maintaining security associations between itself and the UE and asserting the identity of authenticated Public User Identities;
- Interacting with the PacketCable Application Manager for QoS management;
- Providing functionality to allow the UE to traverse NATs and maintain NAT bindings for SIP signaling;
- Generation of accounting correlation IDs and Accounting Events.

IPv6 support is, at a minimum, required on the P-CSCF to provide IPv6 access to the core SIP infrastructure. The P-CSCF may also include the SIP/SDP IP version interworking functions.

6.3.2 STUN and TURN Servers

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

Three STUN servers are employed by the PacketCable network, one employed as a functional component of the P-CSCF (not shown in Figure 1) and two as standalone STUN servers:

- The STUN server as a functional component within the P-CSCF is used by SIP UEs in order to maintain the NAT bindings for signaling. These STUN messages also act as keepalives, allowing the UE to determine P-CSCF availability and detect NAT reboots.
- The STUN server shown in Figure 1 is used to determine one of several possible candidate media addresses using the STUN protocol.
- The TURN server is an extended STUN server that receives STUN Allocate requests, and sends STUN responses. The TURN server is capable of acting as a data relay, receiving data on the address it provides to UEs, and forwarding it to the UEs. This data relay functionality allows media to traverse NATs in cases when other NAT traversal techniques are insufficient.

6.3.3 PacketCable Application Manager

The PacketCable Application Manager is responsible for a variety of tasks. Most importantly, it is responsible for determining the QoS resources needed for a session based on the received session descriptors and managing the QoS resources allocated for a session.

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

6.4 Core

6.4.1 Serving CSCF (S-CSCF)

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

- SIP Registrar function, which binds registered Public User Identities (AORs) to a set of Contact addresses, assigns GRUUs, as well as stores any other parameters associated with the registration, e.g., user agent capabilities and the address(es) of the P-CSCF which can be used to reach the Contacts;
- SIP user authentication and authorization;
- Application Server selection and filtering;
- Routing of messages to the P-CSCF of UEs serviced by the S-CSCF;
- Routing of messages to an I-CSCF for Public User Identities not serviced by the S-CSCF;
- Routing of messages to a BGCF for calls to the PSTN;
- Origination Processing: processing of incoming dialog-initiating requests from SIP UAs contained in UEs or Application Servers served by the S-CSCF;
- Terminating Processing: processing of outgoing SIP messages terminating to a Public User Identity served by the S-CSCF. This includes support for forking of SIP messages for the case in which multiple contact addresses are registered for that Public User Identity;
- External routing queries, using applications such as ENUM, in order to determine where the call should be routed;
- Network initiated release of sessions;
- Generation of Accounting Events.

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

Subscriptions are associated with S-CSCFs. Subscription data is stored in one or more Home Subscriber Servers (HSSs). The S-CSCF interacts with the SLF to identify the relevant HSSs to obtain user data for the users it serves.

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

6.4.2 Interrogating CSCF (I-CSCF)

The I-CSCF supports:

- Interacting with the HSS to determine the binding between a Subscription (and associated Public User Identities) and a S-CSCF;
- Querying the HSS to obtain the S-CSCF and then routing SIP requests from another network operator to the correct S-CSCF;
- Routing of messages to ASs using Public Service Identities (PSIs);
- Routing of messages to an IBCF for VoIP peering.

6.4.3 Home Subscriber Server (HSS)

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

- Association between a Subscription and S-CSCF;
- Subscription profile information (filter criteria);
- Subscription security information;
- Transparent data for usage by Application Servers.

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

- Session establishment - The HSS supports the session establishment procedures. For terminating traffic, it provides information on which S-CSCF is assigned to handle a Public User Identity.
- Security - The HSS supports various authentication schemes by storing security-related data and providing this data as required to support UE security procedures.
- Service Provisioning - The HSS provides access to the service profile data for use by the S-CSCF. The HSS may also store application-specific data for Application Server.

6.4.4 Subscription Locator Function (SLF)

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

6.5 PacketCable Multimedia

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

The PacketCable Multimedia architecture defines the interaction between a CMTS, Policy Server, and Application Manager. The CMTS is included as part of the Access Network and is described in Section 6.2.2. The Application Manager is specific to each application. PacketCable defines a PacketCable Application Manager, which is described in Section 6.3.3. The Policy Server, which is a unique PacketCable Multimedia element that may communicate with a variety of Application Managers, is described below.

6.5.1 Policy Server

The Policy Server primarily acts as an intermediary between Application Manager(s) and CMTS(s) for QoS session management. It applies network policies to Application Manager requests and proxies messages between the Application Manager and CMTS.

6.6 Application

6.6.1 Application Server (AS)

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

6.6.2 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., media analysis);
- Floor Control (i.e., manage access rights to shared resources in a conferencing environment).

6.6.3 Presence Server Functions

The Presence Server Functions is a group consisting of specialized Application Servers that support exchange of presence data. They act as the focal point for connecting sources of presence information and interested parties.

6.7 Interconnect

6.7.1 Border Control Functions

Interconnect with peer networks may be supported through a group of functions referred to as the Border Control Functions. The Border Control Functions include the IBCF and may include the TrGW. The IBCF and TrGW are logical functions that may reside on separate platforms.

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;
- Network topology hiding.

The TrGW relays media between peer networks to provide functions such as IPv4/6 interworking and network address/port translation.

In general, PacketCable does not define specific functional requirements that the Border Control Functions must support. Instead, it is left to each operator to determine the need for and requirements supported by the Border Control Functions.

6.7.2 Breakout Gateway Control Function (BGCF)

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

6.7.3 Public Switched Telephone Network Gateway (PSTN GW)

The PSTN GW consists of the Signaling Gateway (SG), Media Gateway Controller (MGC), and the Media Gateway (MG). The SG, MGC, and MG 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.

6.7.4 Call Management Server (CMS)

A PacketCable Call Management Server (CMS) provides support for telephony services for NCS clients (i.e., E-MTAs). The CMS provides most of the telephony features while interacting directly with Application Servers (e.g., unified messaging servers and conference servers) to provide additional applications to E-MTAs. It may not allow for features to operate transparently across E-MTAs and UEs owned by the same user. The PacketCable CMS communicates with the CSCFs as a peer.

6.8 Operational Support Systems

The PacketCable network is expected to have the following servers as part of the Operational Support System.

6.8.1 Dynamic Host Configuration Protocol (DHCP) Server

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

6.8.2 Domain Name System (DNS) Server

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

6.8.3 ENUM Server

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

6.8.4 Provisioning Server

The Provisioning Server is a PacketCable-defined component responsible for the provisioning, configuration, and management of an embedded UE. The configuration data contains the information necessary for an eUE to provide services. It is also the element that conveys runtime configuration changes from the network to the eUE.

The Provisioning Server supports three provisioning flows: Secure, Hybrid, and Basic. The Secure Provisioning Flow uses Kerberized SNMPv3 for secure configuration. The Hybrid Provisioning Flow uses SNMP for configuration. The Basic Provisioning Flow uses DHCP for configuration. SNMP is used for management in all three provisioning flows. Secure Management is accomplished via SNMPv3. Additional Management Stations can also be configured for monitoring and management. Monitoring is accomplished via SNMP, Syslog, and local logs on the eUE.

6.8.5 KDC

For PacketCable, the term KDC is utilized for a Kerberos security server. The Kerberos protocol with the PacketCable specified PKINIT extension is used for key management on the interfaces between an embedded UE and the Provisioning Server.

Following eUE authentication using the PKINIT protocol, the KDC grants Kerberos tickets to the eUE. A ticket contains information used to configure security for the provisioning signaling between the eUE and the Provisioning server (if the eUE is to be managed over a secured interface).

6.8.6 Configuration Server

The Configuration server is responsible for providing the configuration to an embedded UE. For embedded UEs this is accomplished using TFTP, and optionally HTTP protocols.

6.8.7 Syslog Server

Embedded UEs can transmit management event notifications using the Syslog protocol. The network entity receiving these notifications is the Syslog server.

6.8.8 Charging Data Function (CDF)/Charging Gateway Function (CGF)

The Charging Data Function (CDF) receives charging events from the various PacketCable network elements via the IMS defined Rf reference point. It can then use the information contained in the charging events to construct Call Detail Records (CDRs). The CDRs produced by the CDF are transferred to the Charging Gateway Function (CGF). The CGF acts as a gateway to the Billing Support Systems. Since each cable operator has CDR requirements unique to their service offerings and billing systems, the interface between the CDF and CGF as well as to the Billing Support System is undefined.

Some PacketCable elements deliver PacketCable-defined Event Messages (EMs) to a Record Keeping Server (RKS). The RKS may be used to support a CMS, CMTS, MGC, and Policy Server. However, the RKS is not included in the reference architecture.

7 PROTOCOL INTERFACES AND REFERENCE POINTS

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

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

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

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

7.1 Signaling and Service Control

PacketCable Signaling and Service Control Reference Points are illustrated in Figure 4. Most reference points are IMS-defined, with appropriate enhancements for PacketCable as identified in various PacketCable specifications. PacketCable-specific reference points are also included.

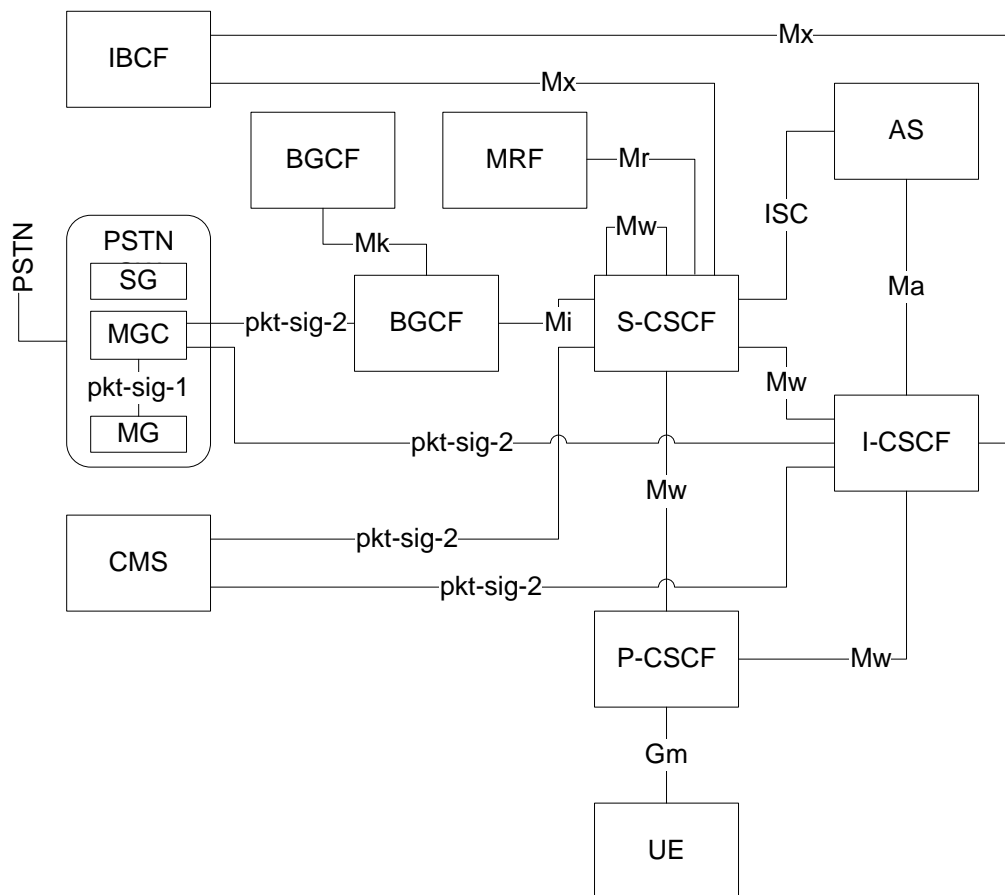


Figure 4 - Signaling Reference Points

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

Table 2 - Signaling Reference Point Descriptions

Reference Point	PacketCable Network Elements	Reference Point Description
Mx	I-CSCF – IBCF S-CSCF – IBCF	Allows an S-CSCF or I-CSCF to communicate with an IBCF when interworking with another network. For example, a session between the home and peer network could be routed via an IBCF 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. It also allows the CMS to exchange SIP messages with the S-CSCF and I-CSCF for calls between E-MTAs and UEs.
Ma	I-CSCF – AS	Allows the I-CSCF to forward SIP requests destined to a Public Service Identity hosted by an Application Server directly to the Application Server.
Mr	S-CSCF – MRF	Allows an S-CSCF to exchange session signaling with an MRF to provide multimedia functions, such as network-provided tones and announcements, multi-port conferencing, and media stream transcoding.
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 – I-CSCF	CMSS protocol as defined in the PacketCable CMS to CMS Signaling Specification [CMSS]. Allows PacketCable E-MTAs to establish voice sessions with PacketCable elements. Also allows the BGCF and I-CSCF to exchange session signaling with a PacketCable MGC for the purpose of interworking with the PSTN.

Refer to the PacketCable SIP Signaling Technical Report [SIP TR] for more information.

7.2 Subscriber Data

PacketCable subscriber data is stored in the HSS located within the home network. The HSS serves the S-CSCF, I-CSCF, and various Application Servers including the Presence Server. The appropriate HSS for a given subscriber can be located by querying the SLF.

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

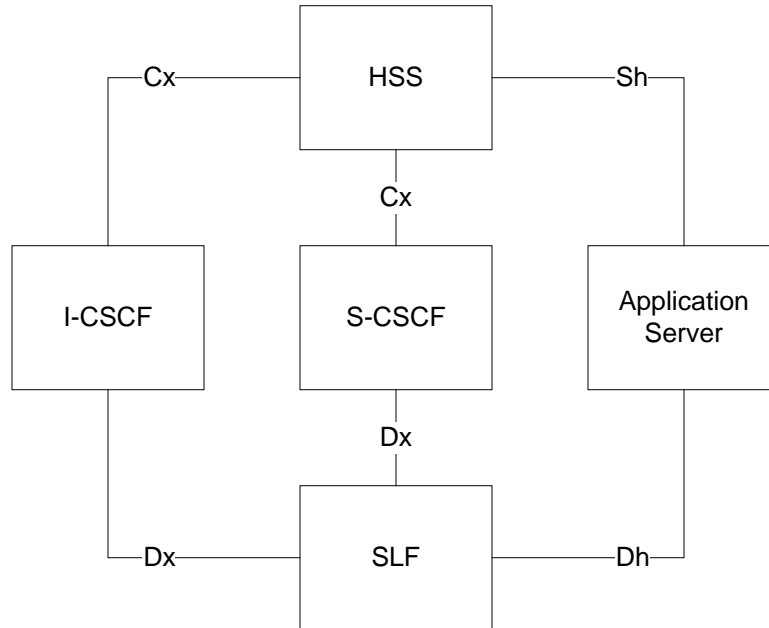


Figure 5 - Subscriber Data Reference Points

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

Table 3 - Subscriber Data Reference Point Descriptions

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

Refer to the PacketCable HSS Technical Report [HSS TR] for more information.

7.3 Quality of Service

The Quality of Service approach for PacketCable is based on PacketCable Multimedia. In the original PacketCable Multimedia architecture, all Service Control Domain functions were lumped into a single entity called the Application Manager (AM), of which there can be many. The PacketCable architecture resolves this domain into more discrete elements with defined reference points. For the purposes of providing Quality of Service, an Application Manager (AM) serves as the interface between the PacketCable SIP architecture and the PacketCable Multimedia architecture. Its function is to receive QoS messages from the P-CSCF and to formulate appropriate messages to the PacketCable Multimedia Policy Server. While this AM function could be integrated into a PacketCable Multimedia Policy Server, it should be considered as a separate function since it has unique requirements separate from those of the Policy Server, such as the resolution of a single session-based QoS request into a series of individual QoS requests for each IP flow. The PacketCable version of the AM is the PacketCable Application Manager (PAM).

Figure 6 illustrates the relationship between the PacketCable Application Manager, the P-CSCF, and the PacketCable Multimedia Policy Server. Note also that the PacketCable Application Manager shown here as a distinct function may be packaged along with a PacketCable Multimedia Policy Server or, alternatively, with a P-CSCF.

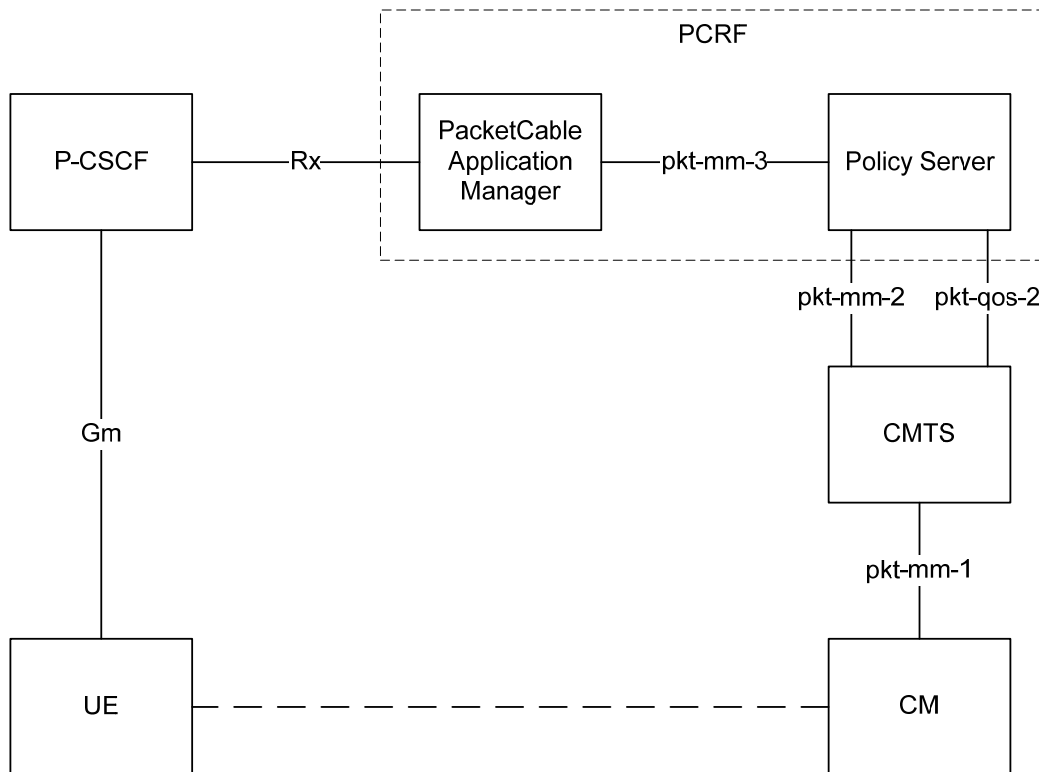


Figure 6 - QoS Reference Points

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

Table 4 - QoS Reference Point Descriptions

Reference Point	PacketCable Network Elements	Reference Point Description
Gm	UE – P-CSCF	Refer to Table 2.
Rx	P-CSCF – PAM	The Rx interface is used for session-based policy set-up information exchange between the P-CSCF and the PacketCable Application Manager. Note that this is the same interface that is used between the P-CSCF and the Policy and Charging Rules Function (PCRF) in the case of GPRS access.
pkt-qos-2	Policy Server – CMTS	The Policy Server uses the Control Point Discovery Protocol [CPD] to determine the serving CMTS in the network for a given UE.
pkt-mm-1	CM – CMTS	The CMTS instructs the CM to setup, teardown or change a DOCSIS service flow via DSx signaling. This reference point is defined in PacketCable Multimedia [MM TR].
pkt-mm-2	Policy Server – CMTS	Policy decisions are pushed by the Policy Server onto the CMTS, and the CMTS provides responses. This reference point is defined in PacketCable Multimedia [MM TR].
pkt-mm-3	Application Manager – Policy Server	Allows the Application Manager to request the Policy Server to install policy decisions on the CMTS. This reference point is defined in PacketCable Multimedia [MM TR].

Refer to the PacketCable QoS specification [QOS] for more information.

7.4 Network Address Translation (NAT) and Firewall Traversal

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

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

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

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

PacketCable uses the ICE methodology to obtain and advertise the "best" reachable address for media. This methodology makes use of STUN and TURN in order to obtain candidate addresses. These candidate addresses are then advertised by the UE using SDP attributes described in the ICE methodology. The UE then uses STUN to

perform reachability tests, allowing it to pick the best address that uses the least network resources and results in the least network delay while maintaining the state in the UE (rather than in the network). It also allows for interworking with E-MTAs, since the address advertised in the media or connection lines of the SDP will always be a reachable address.

The PacketCable NAT and Firewall Traversal Technical Report [NFT TR] provides additional details on the ICE methodology, including a description of how UEs locate STUN and TURN servers. TURN is an extension to STUN to support media relay. It also describes how NAT bindings are opened and maintained for SIP signaling using IETF defined Outbound procedures.

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

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

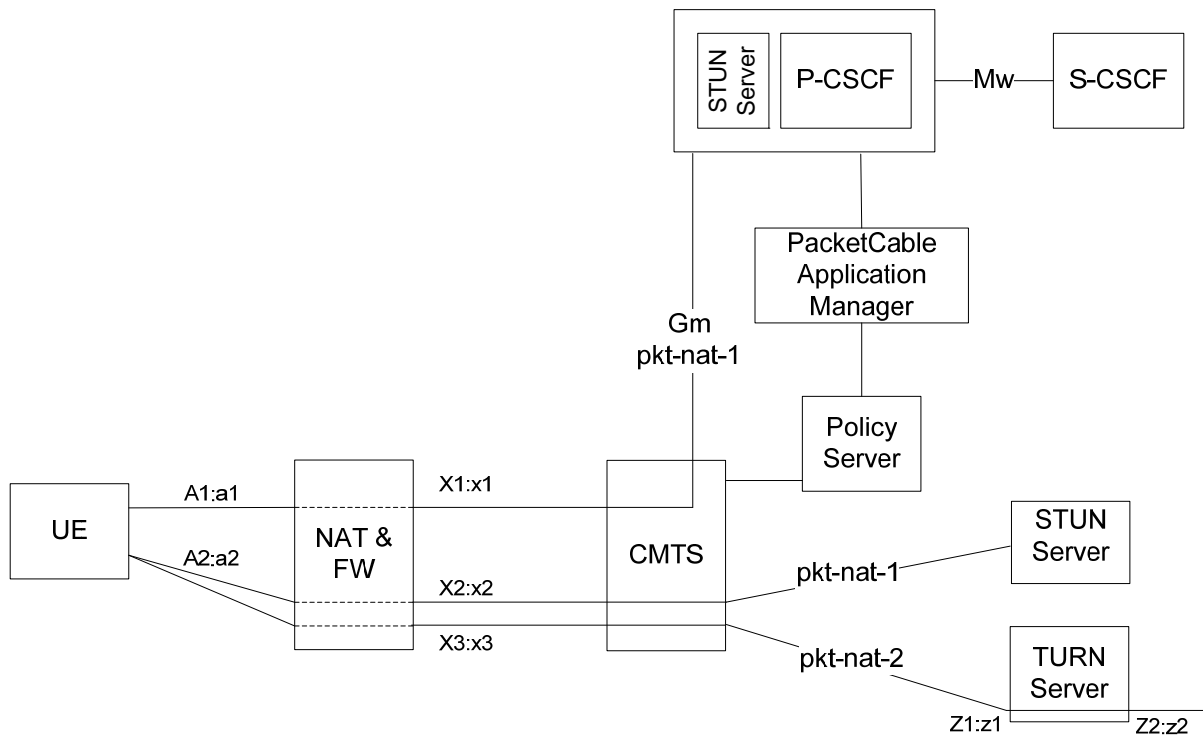


Figure 7 - NAT and FW Traversal Reference Points

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

Table 5 - NAT and FW Traversal Reference Point Descriptions

Reference Point	PacketCable Network Elements	Reference Point Description
Gm	UE – P-CSCF	Refer to Table 2.
Mw	P-CSCF – S-CSCF	Refer to Table 2.
pkt-nat-1	UE – STUN Server UE – P-CSCF	Enables the UE to determine one of several possible candidate media addresses using STUN, in support of the ICE methodology. Also used to keep NAT bindings active to a P-CSCF via a keepalive mechanism. The use of STUN for signaling and media is specified by the IMS, but a reference point was not defined. The reference point designation ‘pkt-nat-1’ is used here to highlight the interface’s applicability to the PacketCable architecture.
pkt-nat-2	UE – TURN Server	Allows the UE to access a TURN server in order to support the traversal of a NAT that does not perform Address Independent Mapping. The use of TURN for media relay is specified by the IMS, but a reference point was not defined. The reference point designation ‘pkt-nat-2’ is used here to highlight the interface’s applicability to the PacketCable architecture.

Refer to the PacketCable NAT and Firewall Traversal Technical Report [NFT TR] for more information.

7.5 Media Coding and Transport

PacketCable uses RTP to transport most communication services (primarily voice and video). The primary media flows in the PacketCable architecture are shown in Figure 8.

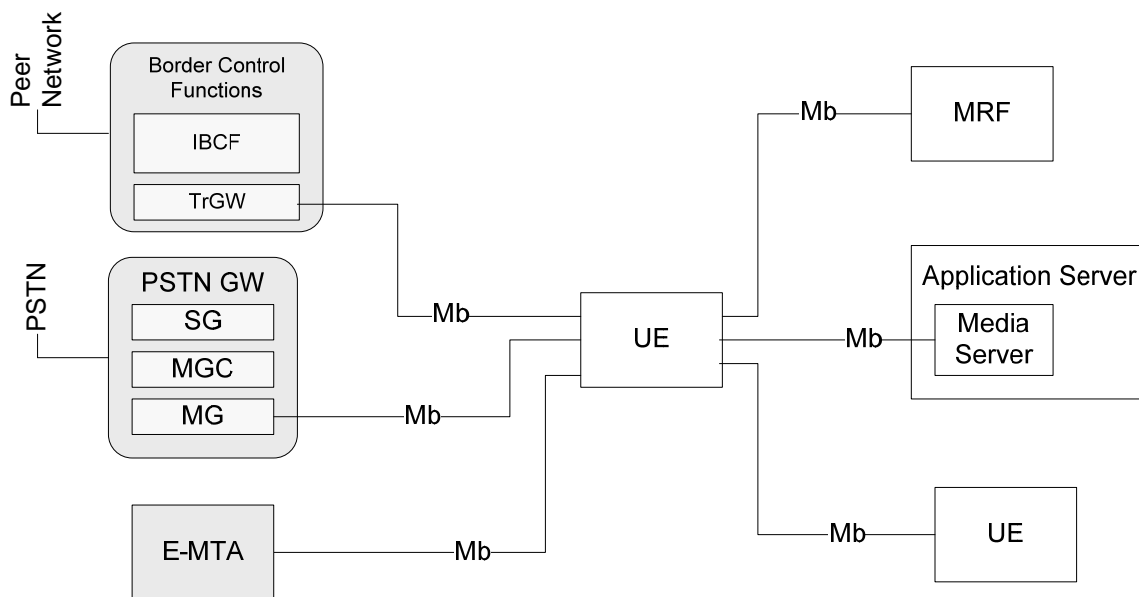


Figure 8 - Media Stream Reference Points

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

Table 6 - Media Stream Reference Point Descriptions

Reference Point	PacketCable Network Elements	Reference Point Description
Mb	UE – UE UE – MG UE – TrGW UE – AS UE – E-MTA UE – MRF	Allows media-capable components to send and receive media data packets. Specifically, a UE can exchange media with another UE, an MG, an Application Server, a TrGW, an E-MTA, and an MRF.

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

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

Refer to the PacketCable Codec-Media Specification [CODEC] for more information.

7.6 Provisioning

PacketCable plans to support multiple provisioning frameworks to support embedded and standalone UE implementations. The current framework, termed E-UE Provisioning, is aimed at embedded devices and re-uses the currently deployed DHCP- and SNMP-based PacketCable Provisioning model. It relies on the DOCSIS specifications for the eCM provisioning, along with PacketCable extensions. It also specifies the components, interfaces, and requirements for eUE provisioning.

The E-UE Provisioning framework addresses the following areas:

- Provisioning
 - Connectivity to the local IP network
 - P-CSCF discovery
 - Initialization prior to Configuration
- Configuration
 - Configuration Data Model
 - Configuration File Format and Delivery
- Management
 - Management Data model
 - Management and monitoring protocols

Figure 9 illustrates the E-UE provisioning reference points.

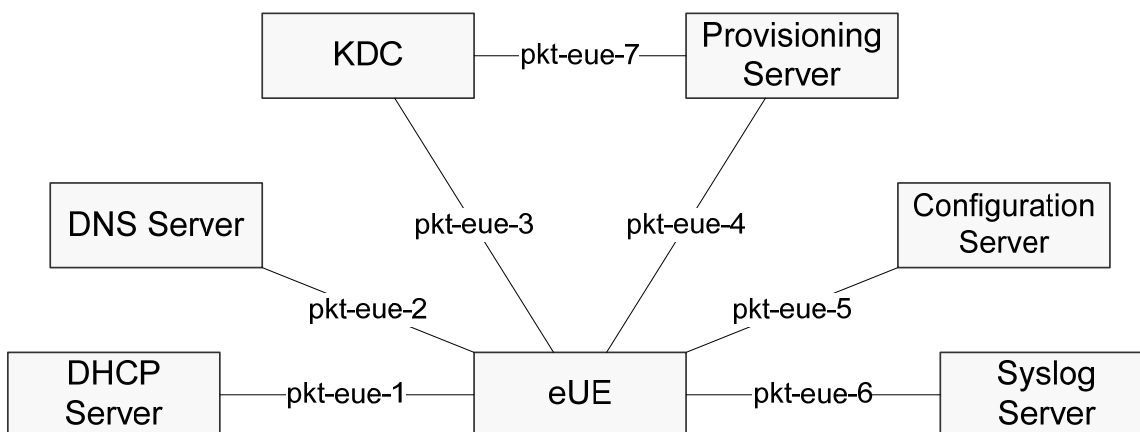


Figure 9 - Provisioning Reference Points

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

Table 7 – Provisioning Reference Point Descriptions

Reference Point	PacketCable Network Components	Reference Point Description
pkt-eue-1	eUE – DHCP	Allows the eUE to obtain IP network participation information (e.g., IP address, DNS server addresses).
pkt-eue-2	eUE – DNS	Allows the eUE to resolve DNS names for location of network elements or routing of messages.
pkt-eue-3	eUE – KDC	Allows the eUE to authenticate itself to the Key Distribution Center (KDC) using the Kerberos protocol.
pkt-eue-4	eUE – Provisioning Server	Allows the eUE to authenticate and exchange device capabilities with the Provisioning Server. The eUE also uses this interface to obtain configuration information and to notify the provisioning server of the configuration retrieval status. The protocol used for authentication is Kerberos. The protocol for notification is SNMP.
pkt-eue-5	eUE – Configuration Server	Allows the eUE to obtain the Configuration File using TFTP or, optionally, HTTP.
pkt-eue-6	eUE – Syslog Server	Allows the eUE to report management events via Syslog.
pkt-eue-7	KDC-Provisioning Server	Allows the KDC to obtain information pertaining to the eUE, such as the provisioned IP address and FQDN (associated with the eUE's Mac Address).

Refer to the E-UE Provisioning Specification [E-UE Prov] for more information.

7.7 Network Accounting and Usage

The IMS defines reference points that allow it to support different types of IMS Connectivity Access Networks (CANs). PacketCable Accounting assumes the Cable HFC Access Network along with the PacketCable Multimedia Architecture define a new type of IP-CAN for incorporation into the overall IMS architecture.

Figure 10 shows the main PacketCable components involved with Offline Charging and the reference points between each of the components.

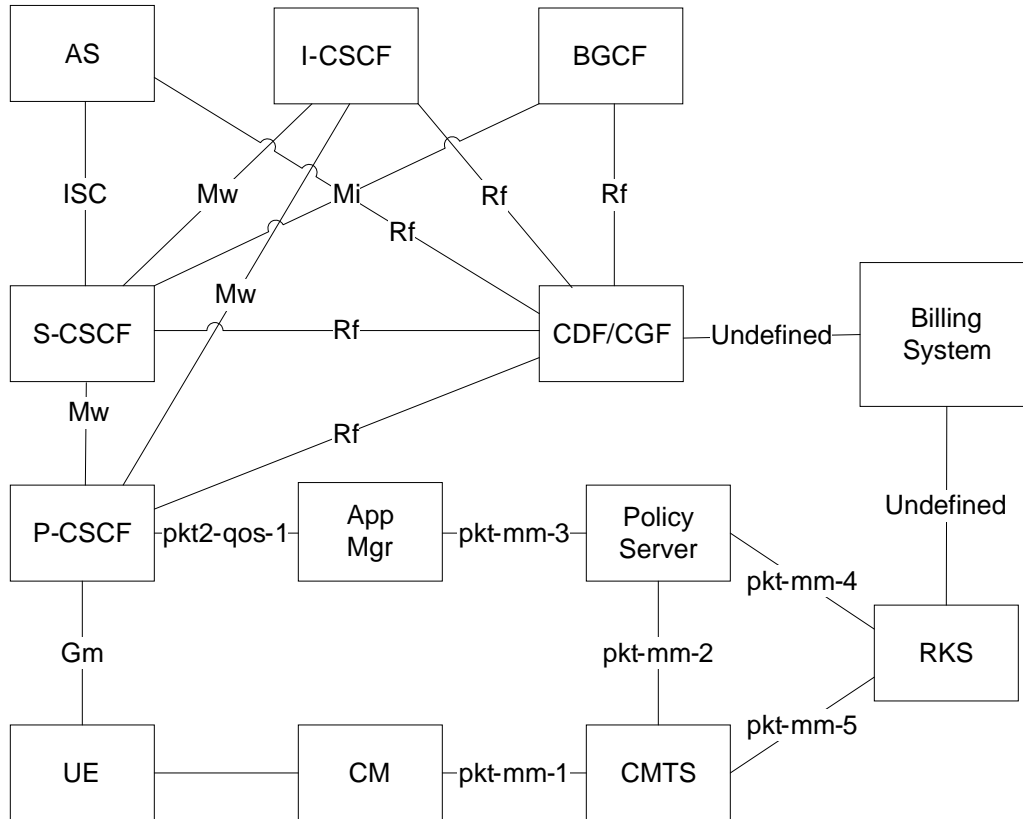


Figure 10 - Accounting Reference Points

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

Table 8 - Accounting Reference Point Descriptions

Reference Point	PacketCable Network Components	Reference Point Description
Gm	UE – P-CSCF	Refer to Table 2.
Mw	P-CSCF – S-CSCF I-CSCF – S-CSCF P-CSCF – I-CSCF	Refer to Table 2.
Mi	BGCF – S-CSCF	Refer to Table 2.
ISC	S-CSCF – AS	Refer to Table 2.

Reference Point	PacketCable Network Components	Reference Point Description
Rf	CSCF – CDF/CGF	DIAMETER-based reference point from between the IMS nodes (P-CSCF, S-CSCF, and AS) to the CDF/CFG.
pkt-qos-1	P-CSCF – Application Manager	Refer to Table 4.
pkt-mm-1	CM – CMTS	Refer to Table 4.
pkt-mm-2	Policy Server – CMTS	Refer to Table 4.
pkt-mm-3	Application Manager – Policy Server	Refer to Table 4.
pkt-mm-4	PS – RKS	RADIUS-based reference point between the PS and the Record Keeping Server (RKS). This reference point is defined in PacketCable Multimedia [MM TR].
pkt-mm-5	CMTS – RKS	RADIUS-based reference point between the CMTS and the RKS. This reference point is defined in PacketCable Multimedia [MM TR].

Refer to the PacketCable Accounting Specification [ACCT] for more information.

7.8 Security

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

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

These trust domains are used to decompose the PacketCable architecture.

Refer to the PacketCable Security Technical Report [SEC TR] for more information.

7.8.1 Access Domain Security

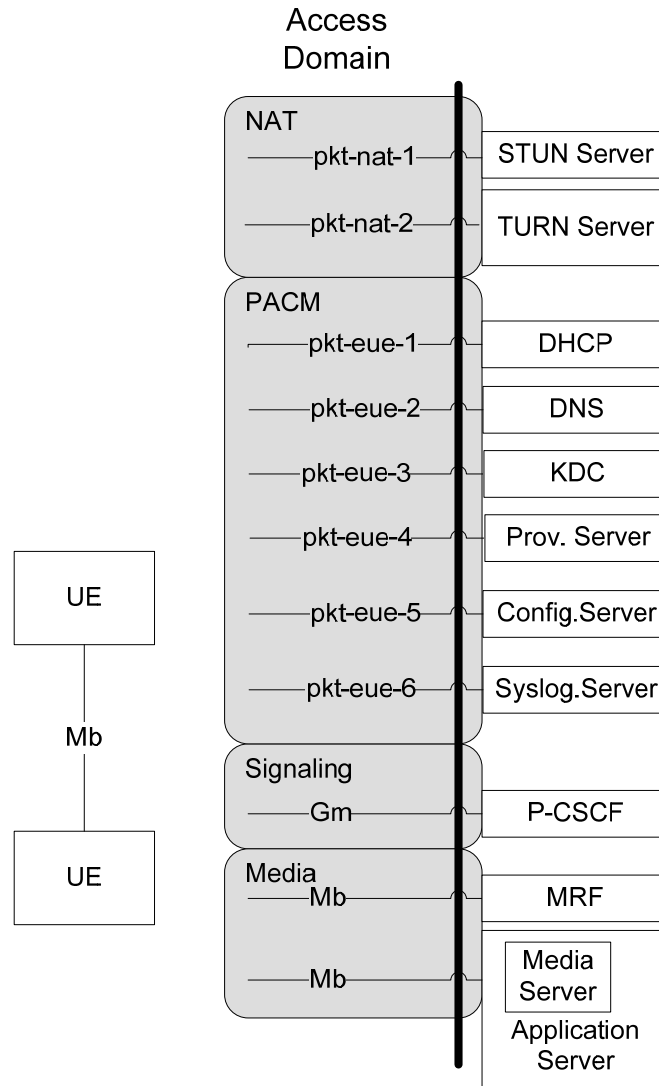


Figure 11 - Access Domain Reference Points

UE interactions with the network occur in the Access domain. Table 9 provides a high-level overview of how the Access Domain reference points are secured.

Table 9 - Access Domain Reference Point Descriptions

Reference Point	PacketCable Network Elements	Reference Point Security Description
pkt-nat-1	UE – STUN Server	STUN: Message integrity is provided by STUN mechanisms.
pkt-nat-2	UE – TURN Server	TURN: STUN Allocate requests are authenticated and authorized within the STUN protocol itself.
pkt-eue-1	eUE – DHCP	DHCP: Security for this interface is out-of-scope. Security threats are mitigated via follow-on Kerberos procedures in the Secure Provisioning Flow.

Reference Point	PacketCable Network Elements	Reference Point Security Description
pkt-eue-2	eUE – DNS	DNS: Security for this interface is out-of-scope. Security threats are mitigated via follow-on Kerberos procedures in the Secure Provisioning Flow.
pkt-eue-3	eUE – KDC	Kerberos: Authentication, message integrity and privacy are provided within the Kerberos protocol.
pkt-eue-4	eUE – Provisioning Server	Kerberos, SNMP: Authentication, message integrity, and privacy (optional in SNMPv3) are provided within the Kerberos and SNMP protocols in the Secure Provisioning Flow only.
pkt-eue-5	eUE – Configuration Server	TFTP, HTTP (optional): Message integrity of the configuration file contents, and optional privacy, is provided via pkt-eue-4 signaling in the Secure Provisioning Flow only.
pkt-eue-6	eUE – Syslog Server	Syslog: Security for this interface is out-of-scope.
Mb	UE – UE UE – MG UE – TrGW UE – MRF UE – AS UE – E-MTA	RTP: Media security is out of scope for this specification. Note Figure 11 only shows a few representative media flows.

7.8.2 Intra-Network Domain Security

Intra-network domain reference points and components are contained within a service provider's network, and consequently, a holistic security policy. These reference points are generally secured using the Zb reference point, or TLS may be used when TCP is employed for SIP. The Zb reference point uses IPsec Encapsulating Security Payload (ESP).

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

- pkt-qos-2 – Cryptographic challenge mechanism defined by the Control Point Discovery protocol.
- pkt-laes-4 – Cryptographic mechanisms defined by SNMPv3.
- pkt-laes-6 – Cryptographic challenge mechanism defined by the Control Point Discovery protocol.
- pkt-eue-7 – Authentication, message integrity, and privacy are provided within the Kerberos protocol.

7.8.3 Inter-Network Domain Security

The Inter-network domain reference points consist of:

- IBCF – Peer Network – Secured using the Za reference point, which uses IPsec ESP. Inter-domain traffic in the IMS is required to pass through a Security Gateway (SEG). The SEG supports the Za reference point and enforces security policy on inter-domain traffic flows. It is assumed that the IBCF includes the SEG functionality, but the SEG may be a separate element.
- PSTN Gateway – PSTN – PSTN security is not defined.
- CMS – Endpoints - Security for the CMS reference point is defined in the PacketCable Security Specification [SEC].

7.9 Lawful Intercept

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

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

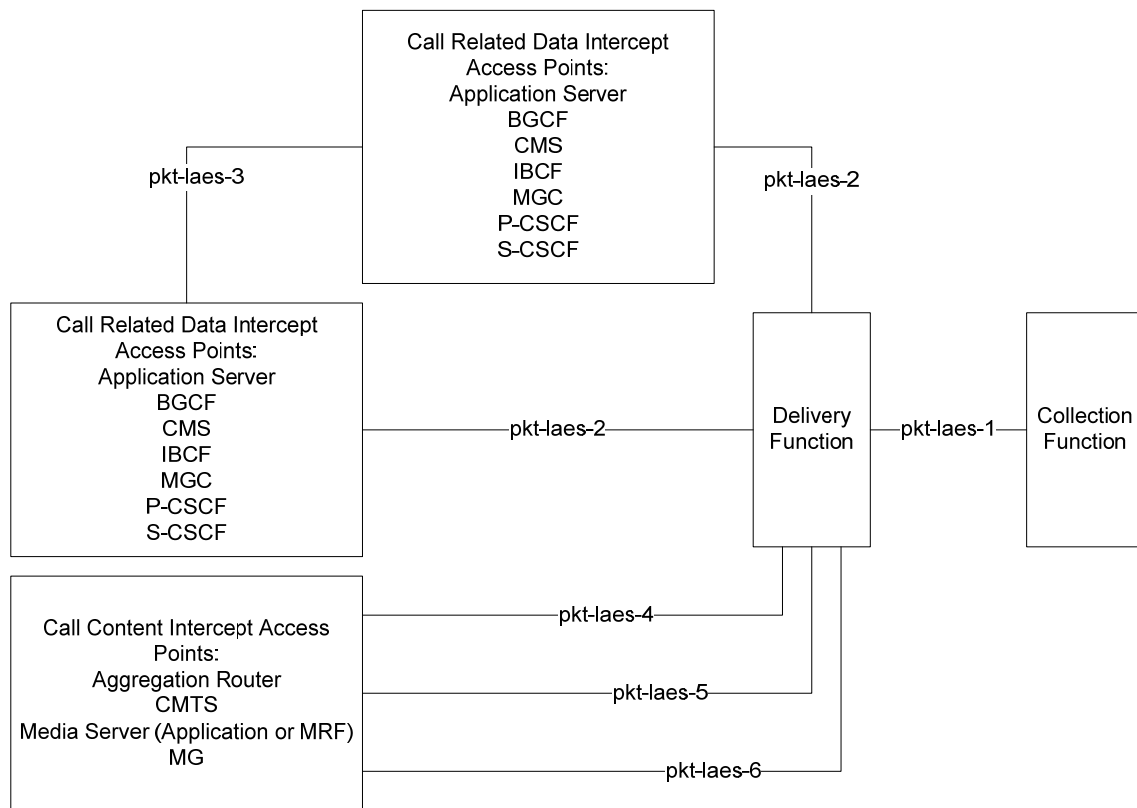


Figure 12 - Lawful Intercept Reference Points

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

Table 10 - Lawful Intercept Reference Point Descriptions

Reference Point	PacketCable Network Elements	Reference Point Description
pkt-laes-1	DF – CF	Correlated call-related data and call content are reported to the law agency collection function. Defined in [ES-DCI].
pkt-laes-2	Session Control Element – DF	Intercepted call-related events are reported to the DF. This reference point is DIAMETER based.
pkt-laes-3	Session Control Element – Session Control Element	Allows session control elements to dynamically provision intercept in peer elements for calls where the targeted subject's assigned control elements are no longer involved in the call. Call redirect is one example. This reference point is SIP based.
pkt-laes-4	DF – Content Access Points	The DF dynamically provisions content intercept points. This reference point is SNMPv3 based.
pkt-laes-5	Content Access Point – DF	Intercepted call content is reported to the DF. This reference point is media over UDP based.
pkt-laes-6	DF – Content Access Points	The DF, as the Requestor, uses the Control Point Discovery Protocol [CPD] to determine the appropriate Call Content IAPs, acting as Control Points, in the network for call content intercept.

Refer to the PacketCable Electronic Surveillance - Intra-Network Functions Specification [ES-INF] and the PacketCable Electronic Surveillance - Delivery Function to Collection Function Interface Specification [ES-DCI] for more information.

7.10 Control Point Discovery

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

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

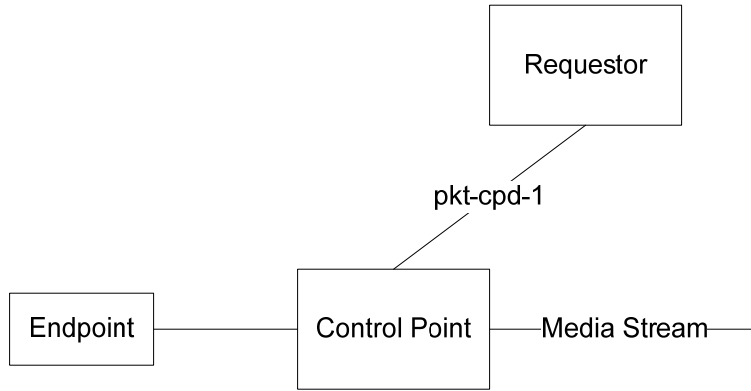


Figure 13 - Control Point Discovery Reference Point

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

Table 11 - Control Point Discovery Reference Point Description

Reference Point	PacketCable Network Elements	Reference Point Description
pkt-cpd-1	Requestor – Control Point	The requestor uses the Control Point Discovery Protocol to determine the appropriate control point in the network for a given UE. Other reference points in the architecture are based on this reference point.

Refer to the PacketCable Control Point Discovery Specification [CPD] for more information.

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 the V01 Technical Report:

Flemming Andreasen – Cisco
Sumanth Channabasappa – CableLabs
Steve Dotson – CableLabs
Tom Hallin – Motorola
David Hancock – CableLabs
Kevin Johns – CableLabs
Paul Kyzivat – Cisco
Gordon Li – Broadcom
Brian Lindsay – Nortel
Bernard McKibben – CableLabs
Jean-François Mulé – CableLabs
Venkatesh Sunkad – CableLabs

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to the V02 Technical Report:

Sumanth Channabasappa – CableLabs
Steve Dotson – CableLabs
David Hancock – CableLabs
Kevin Johns – CableLabs
Brian Lindsay – Nortel Networks
Sean Schneyer – Ericsson

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to the V03 Technical Report:

Sumanth Channabasappa – CableLabs
Steve Dotson – CableLabs
David Hancock – CableLabs
Kevin Johns – CableLabs
Bernard McKibben – CableLabs
Sandeep Sharma – CableLabs

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to the V04 Technical Report:

Sumanth Channabasappa – CableLabs

Steve Dotson – CableLabs

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to the V05 Technical Report:

Sumanth Channabasappa – CableLabs

David Hancock - CableLabs

Stuart Hoggan – CableLabs

Kevin Johns - CableLabs

Sandeep Sharma - CableLabs

Each of the PacketCable Specifications and Technical Reports acknowledge individuals who contributed to the development of that document. Their work has contributed to this Technical Report as well.

Eric Rosenfeld and Kevin Johns – CableLabs
