# PacketCable™ 2.0

# PacketCable Electronic Surveillance Delivery Function to Collection Function Interface Specification

# PKT-SP-ES-DCI-C01-140314

**CLOSED**

**Notice**

This PacketCable specification 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. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by CableLabs® in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

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. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third party documents, including open source licenses, if any.

## DISCLAIMER

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. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

# Document Status Sheet

| | |
|---|---|
| **Document Control Number:** | PKT-SP-ES-DCI-C01-140314 |
| **Document Title:** | PacketCable Electronic Surveillance Delivery Function to Collection Function Interface Specification |
| **Revision History:** | I01 - Released 9/14/06 |
| | I02 - Released 9/25/07 |
| | I03 - Released 2/19/13 |
| | C01 - Released 3/14/14 |
| **Date:** | March 14, 2014 |
| **Status:** | ~~Work in Progress~~   ~~Draft~~   ~~Issued~~   **Closed** |
| **Distribution Restrictions:** | ~~Author Only~~   ~~CL/Member~~   ~~CL/ Member/ Vendor~~   **Public** |

## Key to Document Status Codes:

| | |
|---|---|
| **Work in Progress** | An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration. |
| **Draft** | A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process. |
| **Issued** | A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing. |
| **Closed** | A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs. |

## Trademarks:

CableLabs® is a registered trademark of Cable Television Laboratories, Inc. Other CableLabs marks are listed at http://www.cablelabs.com/certqual/trademarks. All other marks are the property of their respective owners.

# Contents

# Figures

# Tables

# 1  SCOPE

## 1.1  Introduction and Purpose

This specification defines the interface between an entity subject to the Communications Assistance for Law Enforcement Act (CALEA) that provides voice-grade telephone services using PacketCable™ capabilities (a "PC/TSP") and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. Under rulings of the Federal Communications Commission (FCC) that are in effect as of the release date of this specification, companies using PacketCable capabilities to provide voice-grade telephone services that are interconnected with the public switched telephone network (PSTN) are treated as "telecommunications carriers" for purposes of CALEA (although not necessarily for other purposes). See American Council on Education v. FCC, 451 F.3d 226 (D.C. Cir. 2006). The purpose of this specification is to assist those companies in meeting their obligations under CALEA. In this regard, an entity subject to CALEA that complies with a publicly available technical requirement or standard adopted by an industry association or standards-setting organization shall be found to be in compliance with the assistance capability requirements of CALEA. Accordingly, a PC/TSP, manufacturer, or support provider that is in compliance with this document will have "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. 1001 et seq.

This specification defines services and features to support Lawfully Authorized Electronic Surveillance, and the interfaces to deliver intercepted communications and reasonably available Call-Identifying Information (CII) to a LEA when authorized.

## 1.2  Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"            This word means that the item is an absolute requirement of this specification.

"MUST NOT"        This phrase means that the item is an absolute prohibition of this specification.

"SHOULD"          This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT"      This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

"MAY"             This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

## 1.3  Electronic Surveillance Requirements

Congress passed CALEA in October 1994. It requires telecommunications carriers and manufacturers to provide certain capabilities to LEAs with the proper legal authorization. The FCC has ruled that providers of "interconnected Voice-over-Internet Protocol" services (that is, voice services that are interconnected with the PSTN) are "telecommunications carriers" within the meaning of CALEA (although not necessarily within the meaning of the Communications Act of 1934, as amended). This conclusion has been upheld by the courts (although, as of the date of this specification, court challenges to this conclusion remain pending). See American Council on Education v. FCC, 451 F.3d 226 (D.C. Cir. 2006). Cable operators (or their affiliates) providing voice telephone service over their cable systems typically meet this criterion and are, therefore, subject to CALEA under current law. An entity subject to CALEA that is in compliance with a publicly available technical requirement or standard adopted by an industry

association or standards-setting organization is deemed to be in compliance with the assistance capability requirements of CALEA. Accordingly, when designing a surveillance protocol, it is prudent to consider and incorporate CALEA requirements.

CALEA requires entities that are "telecommunications carriers" within the meaning of that law to ensure that their equipment, facilities, or services have the capability to:

1.  Expeditiously isolate and enable the LEA to access reasonably available call identifying information.

2.  Expeditiously isolate and enable the LEA to intercept all communications carried by a carrier within a service area to or from the equipment, facilities or services of a subscriber, concurrently with the communications transmission.

3.  Make intercepted communications and call identifying information available to the LEA in a format available to the carrier so they may be transmitted over lines or facilities leased or procured by the LEA to a location away from the carrier's premises.

4.  Meet these requirements with a minimum of interference with the subscriber's services and in such a way that protects the privacy of communications and call identifying information that are not authorized to be intercepted, and that maintains the confidentiality of the LEA's wiretaps.

CableLabs® is an industry association that, in addition to research and development related to cable technologies, may sponsor technical requirements and standards. The Telecommunications Industry Association has promulgated a standard [J-STD-25b] for lawfully authorized electronic surveillance for traditional voice telephony. However, the electronic surveillance features and capabilities for traditional voice telephony provided for in [J-STD-25b] are not readily applicable to telephony provided by means of a cable system, including telephony provided using PacketCable capabilities. Accordingly, CableLabs has produced this specification for electronic surveillance specific to telephone services using PacketCable capabilities provided by cable operators subject to CALEA.

Although the specifications and requirements of [J-STD-25b] are not applicable to PacketCable-based telephony, the focus group preparing this specification sought to employ similar messaging, where possible, to minimize the development efforts for manufacturers of Delivery Function devices and law enforcement Collection Function devices. However, it is important to note that the PacketCable messages defined in this specification are very different from those defined in [J-STD-25b], employing different parameters and being triggered by different events.

## 1.4    Electronic Surveillance Assumptions

CALEA itself does not authorize any law enforcement agency or officer to require any specific design of equipment, facilities, services, features, or system configurations, nor does it prohibit the adoption of any equipment, facility, service, or feature by any provider of communication service.

LEAs may be authorized to conduct any of three specific types of surveillance: (1) "pen register," which records call-identifying information for all calls originated by a subject, (2) "trap and trace," which records call-identifying information for all calls received by a subject, and (3) "interception," which allows LEAs to listen to the conversations of the subject, as well as access to call-identifying information. In recent years approximately 90% of all surveillance orders are of the first two types; Federal law and laws of 42 states generally impose significant restrictions on the use of the third technique.

As a precondition for a PC/TSP's assistance with Lawfully Authorized Electronic Surveillance, a LEA must serve a PC/TSP with the necessary legal authorization identifying the intercept subject, the communications and information to be accessed, and service areas where the communications and information can be accessed. Once this authorization is obtained, the PC/TSP shall perform the access and delivery for transmission to the LEA's procured equipment, facilities, or services.

Communications in progress at the time a PC/TSP receives a legally authorized request will not be subject to surveillance. Only communications initiated after the legally authorized request will be subject to surveillance.

A PC/TSP shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subject or associate, unless the encryption was provided by the PC/TSP and the PC/TSP possesses the information necessary to decrypt the communication (18 U.S.C. 2602(b)(3)). Nothing in

CALEA prohibits a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access.

Only packets sent or received by the intercept subject that utilize the capabilities of the PacketCable Service Execution platform to establish the communication, and utilize enhanced Quality of Service as authorized by the PacketCable Service Execution platform, are considered "calls" as defined by CALEA. Cable operators that have deployed PacketCable capabilities will offer a range of other services to their customers that make use of packet-switched communications, such as email and Internet access. This specification does not address surveillance capabilities relating to these other packets and does not address whether or to what extent CALEA might apply to such other packets under current law.

One or more Delivery Functions may be utilized to deliver the Call Content and call-identifying information associated with a particular surveillance order. For example, Call Content and call-identifying information of a redirected call may not be present at the facilities normally used for surveillance of a subject. It is the responsibility of the PC/TSP to designate a Delivery Function that will deliver Call Content and call identifying information to a CF for a particular surveillance order. Procurement of the physical facilities connecting this Delivery Function to its Collection Function is the responsibility of the LEA.

In most cases, a PC/TSP should be able to intercept calls redirected by a surveillance subject to other locations either in its own network or in the networks of other telecommunications carriers. However, where a subject has redirected incoming calls to a location served by another PC/TSP, the resulting connection may be established without any involvement of the equipment or facilities of the subject's PC/TSP. Instead, the connections will be made directly from the PC/TSP originating the incoming call to the PC/TSP serving the location to which the subject redirected incoming calls. Because the subject's original PC/TSP will not be aware of these resulting connections, access to these connections will have to be obtained from the PC/TSP serving the location to which calls have been redirected.

When a surveillance subject initiates the placement of an associate on hold for a two-way call, the PC/TSP is required to deliver any Call Content directed to or from the subject or associate to the LEA while the associate is on hold as required by law.

A subject's Call Content and call data is transmitted to the LEA over one or more logical channels known as Call Content Connection (CCC) and Call Data Connection (CDC). The actual number of logical channels supported will vary. Factors influencing connection capacity include (1) the number of CCCs and CDCs ordered by the LEA for subjects associated with a given Delivery Function (DF), (2) the number of surveillance orders required to be supported for any single subject, (3) the availability of resources to transport Call Content and call data information from the DF to the CF, (4) the availability of resources to transport Call Content and call data information from the IAP to the DF, and (5) the availability of resources to transport redirected Call Content and call data information between DF's within the PC/TSP network.

Capacity requirements are fundamental to the design and development of any technical standard or specification (as well as for the equipment developed in compliance with such standards). Several technical considerations, pivotal to the design process, are affected by capacity requirements. However, so far, the Attorney General has not identified capacity requirements for entities subject to CALEA that use PacketCable capabilities to provide their affected services. In the absence of these formal capacity requirements, CableLabs must make certain reasonable assumptions about capacity to proceed with developing this standard. CableLabs believes that these assumptions reflect reasonable estimates based on industry's technical expertise as well as law enforcement's historical requirements in the context of other technologies. However, to the extent that these reasonable assumptions differ from whatever formal capacity requirements the Attorney General eventually identifies, substantial modifications to this standard may be required.

As such, the following assumptions are made: (1) the IAP supports a maximum number of intercepts of 5% of its active calls, (2) the DF supports delivery of an intercept to a maximum of five LEA collection destinations for any single subject, (3) the DF to CF interface must be capable of supporting the maximum number of intercepts times the maximum number of intercepts per subject, (4) it is the responsibility of the PC/TSP to provide adequate resources to transport Call Content and call data information from the IAP to the DF based on statistical call models, (5) it is the responsibility of the PC/TSP to provide adequate resources to transport redirected Call Content and call data information between DFs within the PC/TSP network based on statistical call redirection models, and (6) when adequate resources are not available, situations may arise where Call Content and call identifying information are not delivered to the LEA.

## 1.5     Interception with SIP Enabled Systems

SIP based architectures such as PacketCable 2.0 include clients that can play a role in feature execution. Interception at the client is considered detectable and is not required for PacketCable 2.0 Electronic Surveillance. For example, on-hook and off-hook states handled by the client and are not known by the network. SIP clients may also perform client based 3-way calling where the conference is formed and managed transparently from the network. The PacketCable intercept facility will not be able to report these kinds of client based features since the information about the client executed features is not present within the PacketCable network.

SIP based architectures such as PacketCable 2.0 separate feature applications from the network control plane layer. PacketCable 2.0 specifies the SIP based control plane, but not the applications except for PacketCable Business SIP Services (BSS), Residential SIP Telephony (RST), and cellular integration features. Therefore, PacketCable 2.0 does not require nor specify the interception of features or applications, except for the specific cases of RST and cellular integration. Requirements for the interception of BSS features are for future study.

# 2 REFERENCES

## 2.1 Normative References

In order to comply with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Users of this specification should be aware that it may be necessary for them to acquire intellectual property rights (e.g., licenses) from one or more third parties responsible for or involved in the normative references noted below in order to use or implement them.

| | |
|---|---|
| [CODEC-MEDIA] | PacketCable CODEC-MEDIA specification, PKT-SP-CODEC-MEDIA-C01-140314, March 14, 2014, Cable Television Laboratories, Inc. |
| [ISO 8802-3] | ISO/IEC 8802-3:2000, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. |
| [ITU X.690] | ITU-T Recommendation X.690: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), July 2002. |
| [RFC 768] | IETF RFC 768/ST0006, User Datagram Protocol, August 1980. |
| [RFC 791] | IETF RFC 791/STD0005, Internet Protocol, September 1981. |
| [RFC 793] | IETF RFC 793/STD0007, Transmission Control Protocol, September 1981. |
| [RFC 826] | IETF RFC 826/STD00037, Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, November 1982. |
| [RFC 894] | IETF RFC 894/STD0041, Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984. |
| [RFC 2460] | IETF RFC 2460, Internet Protocol Specification, Version 6 (IPv6), December 1998. |
| [RFC 3550] | IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications, July, 2003. |
| [RFC 3551] | IETF RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control, July, 2003. |
| [RFC 4733] | IETF RFC 4733, RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals, December 2006. |
| [RFC 5905] | IETF RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010. |
| [RFC 6442] | IETF RFC 6442 Location Conveyance for the Session Initiation Protocol, December 2011. |

## 2.2 Informative References

| | |
|---|---|
| [DOCSIS RFIv1.1] | Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-C01-050907, September 7, 2005, Cable Television Laboratories, Inc. |
| [FCC 02-108] | FCC 02-108, CC Docket No. 97-213, Order on Remand, April 11, 2002, http://www.askcalea.net/docs/fcc02108.pdf. |
| [FCC 99-230] | FCC 99-230, CC Docket No. 97-213, Third Report and Order, August 31, 1999, http://www.askcalea.net/docs/fcc99230.pdf. |

[GR 506]        Telcordia GR-506, LSSGR: Signaling for Analog Interfaces, December 2006, FR-64.

[J-STD-25b]      ANSI/J-STD-025-B-2003, Lawfully Authorized Electronic Surveillance, December, 2003.

[RFC 4566]      IETF RFC 4566, SDP: Session Description Protocol, July 2006.

[SEC1.5]         PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-I03-090624, June 24, 2009, Cable Television Laboratories, Inc.

[T1.678]         ATIS-1000678.2006, Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2, May 2006 as modified by ATIS-1000678.a.2007, Supplement A to Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, May 2007 and ATIS-1000678.b.2010, Supplement B to Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, August 2010.

## 2.3     Reference Acquisition

- ANSI available at http://webstore.ansi.org

- ATIS available at www.atis.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

- ISO available at http://www.iso.ch/iso/en/CatalogueListPage.CatalogueList

- ITU available at http://www.itu.int/ITU-T/publications/index.html

- Telcordia Technologies, http://www.telcordia.com/

# 3  TERMS AND DEFINITIONS

This specification uses the following terms:

| | |
|---|---|
| **Associate** | A telecommunication user whose equipment, facilities, or services are communicating with those of a subject. |
| **Call** | A telecommunication originated by or terminated to a customer that enters or leaves the PacketCable network at a PC/TSP-operated PSTN gateway, or a telecommunication that originates or terminates at a PC/TSP customer's E-DVA that 1) makes a request to the proper network proxy for that endpoint, which then authorizes enhanced QoS facilities, 2) is granted the request for enhanced QoS facilities, and 3) uses those enhanced QoS facilities for transfer of packetized information. For purposes of pen register and trap and trace intercepts, a call is a communication that makes a request to the proper network proxy for that endpoint. |
| **Call Content** | See Content. |
| **Call Content Connection** | The logical link between the device performing an electronic surveillance delivery function and the LEA, that primarily carries the Call Content passed between an intercept subject and one or more associates. At the Demarcation Point, Call Content Connections are identified by the combination of Protocol type of UDP (in the IP header), CF address (in the IP header), CF port number (in the IP header), and the CCC-Identifier (in the CCC payload). |
| **Call Data Connection** | The logical link between the device performing an electronic surveillance delivery function and the LEA that primarily carries call-identifying information. At the Demarcation Point, Call Data Connections are identified by the combination of Protocol type of TCP (in the IP header), CF address (in the IP header), CF port number (in the TCP header), and the Call-ID (in the PCESP message). |
| **Call Management System** | A PacketCable element that performs telecommunications-specific functions in the establishment of a call, such as address translation, call routing, directory services, usage recording, and authorization of QoS. |
| **Call under Interception** | A call that is 1) originated by a PC/TSP subscriber that is under an interception order, 2) terminated to a PC/TSP subscriber that is under an interception order, or 3) redirected by the service of a PC/TSP subscriber that is under an interception order to another service provided by the same PC/TSP. Once a call is identified by the PC/TSP as a call under interception, it maintains that status through all redirections utilizing that PC/TSP's network even if the resulting communicating parties are not themselves surveillance subjects. |
| **Call under Surveillance** | A call that is 1) originated by a PC/TSP subscriber that is under a surveillance order, 2) terminated to a PC/TSP subscriber that is under a surveillance order, or 3) redirected by the service of a PC/TSP subscriber that is under a surveillance order to another service provided by the same PC/TSP. Once a call is identified by the PC/TSP as a call under surveillance, it maintains that status through all redirections utilizing that PC/TSP's network even if the resulting communicating parties are not themselves surveillance subjects. |

| | |
|---|---|
| **Call-identifying Information** | Defined in CALEA Section 102(2), 103(a)(2), and 18 U.S.C. § 2601(a) to be "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier" but "does not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." See destination, direction, origin and termination. |
| **Commission** | Defined in CALEA Section 102(3) to be "the Federal Communication Commission." |
| **Communication** | Any wire or electronic communication, as defined in 18 U.S.C. § 2510. |
| **Communication Intercept** | See intercept. |
| **Content** | Defined in 18 U.S.C. § 2510(8) to include "when used with respect to any wire or electronic communications, … any information concerning the substance, purport, or meaning of that communication." |
| **Data Over Cable Service Interface Specification** | A set of standards produced by CableLabs that defines methods and procedures for use of cable networks to provide information services. |
| **Demarcation Point** | A physical point between the PC/TSP's Delivery Function and the LEA's Collection Function where responsibility of the PC/TSP ends and the LEA assumes responsibility. |
| **Destination** | Defined in [FCC 02-108] to be "a party or place to which a call is being made (e.g., the called party)." |
| **Dialed Digit Extraction** | The capability that permits a LEA to receive digits dialed by a surveillance subject after a call is connected. |
| **Direction** | Defined in [FCC 02-108] to be "a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., a redirected-to party or redirected-from party)." |
| **Electronic Communication** | Defined in 18 U.S.C. § 2510(12) to be "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system." |
| **Electronic Storage** | Defined in 18 U.S.C. § 2510(17) to be "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." |
| **Electronic Surveillance** | The statutorily-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission. As used here, the term also includes the acquisition of call-identifying information. The term refers to a single communication intercept, pen register, or trap and trace. Its usage in this specification does not include administrative subpoenas for obtaining a subscriber's toll records and information about a subscriber's service that a LEA may employ before the start of a communication intercept, pen register, or trap and trace. |

| | |
|---|---|
| **Government** | Defined in CALEA Section 102(5) to be "the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance." |
| **Information Service** | Defined in CALEA Section 102(6) to be "(A) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunication; and (B) includes – (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network." See also Telecommunication Carrier and TSP. |
| **Intercept** | Defined in 18 U.S.C. § 2510 (4) to be "the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." |
| **Intercept Access Point** | A point within a communication system where some of the communications or call-identifying information of an intercept subject's equipment, facilities and services are accessed. In the PacketCable network, the Intercept Access Point of a surveillance subject is the CMTS serving the subject, and the proxies designated by the PC/TSP which processes calls for the subject. |
| **Intercept Subject** | See Subject. |
| **Interconnected VoIP Service** | As defined by the FCC, "interconnected VoIP services include those VoIP services that: (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require IP-compatible customer premises equipment; and (4) permit users to receive calls from and terminate calls to the PSTN." Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd 14989 (2005) at ¶ 39. |
| **Law Enforcement Agency** | A government entity with the legal authority to conduct electronic surveillance. |
| **Origin** | Defined in [FCC 02-108] to be "a party initiating a call (e.g., a calling party), or a place from which a call is initiated." |
| **PacketCable Telecommunications Service Provider** | As used in this specification, a PC/TSP is an entity, typically a cable operator, that has (a) taken the steps necessary to be a "telecommunications carrier" for purposes of CALEA, and (b) provides its telecommunications services using PacketCable capabilities. The fact that an entity may use PacketCable, including the use of PacketCable for voice telephony applications, does not mean that the entity is a "telecommunications carrier" for purposes of CALEA or any other regulatory purpose |
| **Party Hold, Join, Drop, On Conferences Calls** | The capability that permits a LEA to identify at all times during a call the parties to a subject-initiated conference call conversation. |

| | |
|---|---|
| **Pen Register** | Defined in 18 U.S.C. § 3127(3) to be "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business." |
| **Reasonably Available** | Defined in the Commission's Third Report and Order [FCC 99-230]. Call identifying information is reasonably available if the information "is present at an Intercept Access Point (IAP) and can be made available without the carrier being unduly burdened with network modifications." Network protocols do not need to be modified solely for the purpose of passing call-identifying information. The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves. |
| **Redirected Call** | A call that is transferred (see Transferred call), or redirected as a service provided to a terminating subscriber, such as unconditionally, when the terminating subscriber's line is busy, or when the terminating subscriber doesn't answer. |
| **Subject** | A telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to a LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity). The "equipment and facilities of the subscriber" in the PacketCable network consist of the CMTS serving the subscriber and the CMS designated by the PC/TSP which processes calls for the subscriber. |
| **Surveillance Subject** | See Subject. |
| **Telecommunication Service Provider** | Some TSPs may also be "telecommunications carriers" for purposes of CALEA. See Telecommunications Carrier and PC/TSP. |
| **Telecommunications Carrier** | Defined by CALEA Section 102(8) as "a person or entity engaged in the transmission or switching of wire or electronic communication as a common carrier for hire, and includes 1) a person or entity engaged in providing commercial mobile service, or 2) a person or entity engaged in providing wire or electronic communications switching or transmission service to the extent that the Commission finds such service is a replacement for a substantial portion of local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title. This does not include 1) persons or entities insofar as they are engaged in providing information services, and 2) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the U.S. Attorney General." Under FCC rulings in effect as of the date of this specification, cable operators that provide interconnected VoIP service over their cable systems are "telecommunications carriers" for purposes of CALEA. See Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd 14989 (2005), aff'd, American Council on Education v. FCC, 451 F.3d 226 (D.C. Cir. 2006). See PC/TSP. |

| | |
|---|---|
| **Telecommunications Support Services** | Defined in CALEA Section 102(7) to be "a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunication network." |
| **Termination** | Defined in [FCC 02-108] to be "a party or place at the end of a communication path (e.g., the called or call-receiving party, or the switch of a party that has placed another party on hold)." |
| **Transferred call** | A call that changes either the originating party or terminating party, based on action taken by one of the parties in the call. |
| **Transmission** | The act of transferring communications from one location or another by a wire, radio, electromagnetic, photoelectronic, or photo-optical system. |
| **Trap and Trace** | Defined in 18 U.S.C. § 3127(4) to be "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." |
| **Unobtrusive** | Not undesirably noticeable or blatant; inconspicuous; within normal call variances. |
| **Wire Communication** | Defined in 18 U.S.C. § 2510 (1) to be "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point or reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication." |

# 4   ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

| | |
|---|---|
| **AF** | Access Function |
| **ANSI** | American National Standards Institute |
| **CALEA** | Communications Assistance for Law Enforcement Act |
| **CC** | Call Content |
| **CCC** | Call Content Connection |
| **CDC** | Call Data Connection |
| **CF** | Collection Function |
| **CII** | Call-Identifying Information |
| **CM** | Cable Modem |
| **CMS** | Call Management System. |
| **DF** | Delivery Function |
| **DOCSIS®** | Data Over Cable Service Interface Specification |
| **E-DVA** | Embedded Digital Voice Adaptor |
| **IAP** | Intercept Access Point |
| **I-CSCF** | Interrogating Call Session Control Function |
| **IP** | Internet Protocol |
| **LEA** | Law Enforcement Agency |
| **LEAF** | Law Enforcement Administration Function |
| **OCB** | Outbound Call Blocking |
| **PC/TSP** | PacketCable Telecommunications Service Provider. |
| **PCESP** | PacketCable Electronic Surveillance Protocol |
| **P-CSCF** | Proxy Call Session Control Function |
| **PSTN** | Public Switched Telephone Network |
| **QoS** | Quality of Service |
| **S-CSCF** | Serving Call Session Control Function |
| **SPAF** | Service Provider Administration Function |
| **TCP** | Transmission Control Protocol |
| **TSP** | Telecommunication Service Provider. |
| **U.S.C.** | United States Code |
| **UDP** | Unit Data Protocol |
| **URI** | Uniform Resource Identifier |
| **VCC** | Voice Call Continuity |
| **VDI** | VCC Domain Transfer URI |

# 5   OVERVIEW

The intercept function is viewed as five broad categories: access, delivery, collection, service provider administration, and law enforcement administration. These functions are discussed in this section without regard to their implementation. The relationships between these functional categories are shown in Figure 1.
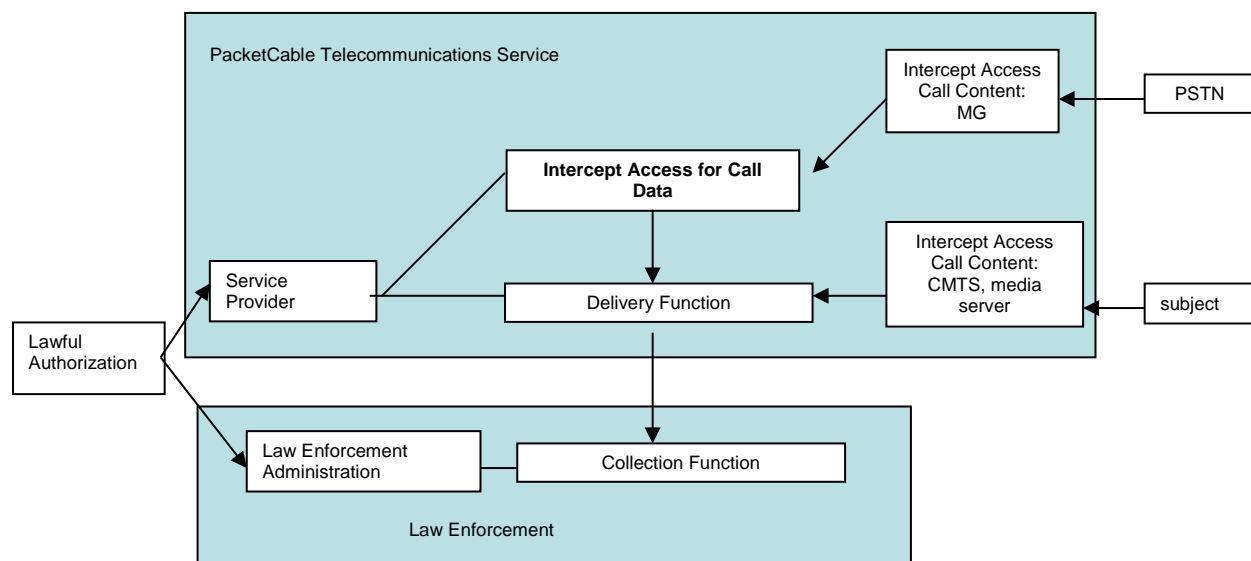


*Figure 1 – Electronic Surveillance Model*

The lawful authorization, while neither a network entity nor an interface reference point, is an important part of electronic surveillance. Surveillance MUST NOT take place without specific lawful authorization.

## 5.1   Subscriber Equipment

PacketCable services, are provided via the broadband access network. This network is characterized as a DOCSIS 1.1 [DOCSIS RFIv1.1] or higher access network, but may be provided over access networks supporting other standards. The access network consists of the Cable Modem (CM), the Cable Modem Termination System (CMTS), and the Media Access Control and Physical access layers.

The subscriber equipment includes those elements of the access network that are located in the customer's home. This includes the CM and the Embedded Digital Voice Adaptor (E-DVA). The cable subscriber may also have wireless mobile devices enabled with PacketCable clients.

The CM is a DOCSIS network element as defined by the DOCSIS specification. The CM plays a key role in handling the media stream. Services which may be provided by the CM include classification of traffic into service flows according to classification filters, rate shaping, and prioritized queuing.

An E-DVA is a single hardware device that incorporates audio and optionally video IP telephony. An E-DVA is incorporated in a DOCSIS cable modem.

An E-DVA supports the following functionality:

- Provides one or more RJ11 interfaces to 2500-series phones.

- Performs call signaling with the P-CSCF to originate and terminate calls.

- Supports QoS signaling with the P-CSCF and the CMTS.

- Supports security signaling with the P-CSCF and other E-DVA devices.

- Supports provisioning signaling with the provisioning server(s).

- Performs encoding/decoding of audio streams.

- Provides multiple audio indicators to phones, such as ringing tones, call waiting tones, stutter dial tone, dial tone, etc.

- Provides standard PSTN analog line signaling for audio tones, voice transport, caller-id signaling, and message waiting indicators.

The PacketCable wireless devices may include a WiFi radio interface for use with a home network connected to the CM. A PacketCable wireless device may also include cellular radio interfaces for cellular network roaming.

The PacketCable system design places much of the session control intelligence at the endpoints, where it can easily scale with technology and provide new and innovative services. This "future-proofing" is an important goal of the design. Unfortunately, it inherently also creates potential opportunities for fraud. For purposes of this specification we assume that the E-DVA and wireless device are not immune to customer tampering, and that the incentive for consumers to attempt to obtain free service will lead to some sophisticated attempts to thwart any network controls placed on the E-DVA and wireless device.

Under these circumstances, it is important to understand that an E-DVA and wireless device under customer control will likely not cooperate with electronic surveillance, and methods are therefore described here that do not depend in any way on cooperation with the E-DVA or wireless device.

## 5.2    Access Function (AF) and Intercept Access Points (IAPs)

The Intercept Access Function, performed by the Intercept Access Points (IAPs), isolates an intercept subject's communication or reasonably available call-identifying information unobtrusively. The Access Function is responsible for the collection of Call Content and reasonably available call-identifying information and making such information available to the Delivery Function.

In a PacketCable network, seven elements are designated as Intercept Access Points:

- The Cable Modem Termination System (CMTS) which controls the set of cable modems attached to the shared medium of the DOCSIS network. The CMTS is responsible for intercepting the Call Content, and certain call-identifying information.

- The Serving Call Session Control Function (S-CSCF), which authenticates the subscriber and links the subscriber to the 2.0 feature set. The S-CSCF is responsible for intercepting the Call-Identifying information.

- The Proxy Call Session Control Function (P-CSCF), which is the PacketCable 2.0 service platform entry point for the subscriber. A security association between the user and P-CSCF may be established. The P-CSCF is responsible for intercepting the Call-Identifying information.

- The Interrogating Call Session Control Function (I-CSCF), which routes off network session signaling towards the subscriber. The I-CSCF may also be the interface to off-network MGCs. The I-CSCF is responsible for intercepting the Call-Identifying information.

- The Media Gateway (MG) is designated as an Intercept Access Point for purposes of intercepting Call Content for redirected calls to the PSTN.

- The Media Gateway Controller (MGC) is designated as an Intercept Access Point for purposes of intercepting the Call-Identifying Information for redirected calls to the PSTN.

The equipment and facilities of each subscriber include two Intercept Access Points (CMTS and S-CSCF), and Call-Identifying Information reasonably available at these IAPs is provided to LEA. Redirected calls in the PacketCable network might not utilize the equipment or facilities of the subscriber who initiated the redirection. Accordingly, the Intercept Access point for a call that has been redirected will be either the S-CSCF/CMTS of the new destination (if redirected to another PacketCable endpoint within the same provider's network) or the MGC/Media Gateway of the PSTN interconnection (if redirected to a PSTN endpoint).

## 5.3    Delivery Function (DF)

The Delivery Function includes the interface responsible for delivering intercepted communication expeditiously from the Intercept Access Functions to the Demarcation Point. The Delivery Function delivers reasonably available CII and CC based on the requirements of the lawful authorization. The Delivery Function includes the ability to:

- Collect and deliver CC and CII for each intercept subject over facilities procured by the LEA.

- Ensure that the CC and CII delivered from the Delivery Function is authorized for a particular LEA.

- To ensure privacy through the protection (i.e., prevent unauthorized access to, or manipulation and disclosure of) intercept controls, intercepted Call Content, and call-identifying information, through methods that are consistent with the normal security policies of the affected PC/TSP.

- Ensure that delivery of surveillance information is only available for the time stated in the lawful authorization.

- Deliver CC and CII using the PCESP protocol.

- Support environments with multiple CSCFs, MGCs, MGs, and CMTSs by accepting Call Content and call data related to a single intercept from multiple IAPs.

- Support multiple DF environments by forwarding Call Content and call data, in the form of Event Messages (EMs), to other DFs.

- Trans-code compressed voice from the target IAP as needed for delivery to the CF in G.711 µ-law format.

Enabling and disabling the Delivery Function is the responsibility of the PC/TSP.

The Delivery Function delivers information over two distinct types of connections: Call Content Connections (CCCs), and Call Data Connections (CDCs). The CCCs are generally used to transport Call Content, such as voice communications. The CDCs are generally used to transport messages which report CII, such as the calling party identities and called party identities.

CII, CC, or both, associated with a particular subject, may need to be delivered to more than one LEA Collection Function simultaneously. This will occur when different LEAs are conducting independent investigations on the same subject. In these circumstances, the Delivery Function duplicates the CC, CII, or both, and delivers authorized information to each LEA. Intercept for one LEA needs to be transparent to any other LEA.

CII, CC, or both, from multiple surveillances, may need to be delivered simultaneously to a single LEA's CF.

## 5.4    Service Provider Administration Function (SPAF)

The Service Provider Administration Function is responsible for controlling PC/TSP Access and Delivery Functions. The PC/TSP administrative functions are outside the scope of this specification.

## 5.5    Collection Function (CF)

The Collection Function is responsible for collecting intercepted CC and CII from the Demarcation Point. The Collection Function is the responsibility of the LEA. Enabling and disabling the activation of the LEA-provided interface is the responsibility of the LEA Administrative Function and is beyond the scope of this specification.

## 5.6    Law Enforcement Administrative Function (LEAF)

The Law Enforcement Administration Function is responsible for controlling the LEA Collection Function. The Law Enforcement Administration Function is the responsibility of the LEA and is beyond the scope of this specification.

# 6   INTERFACE BETWEEN THE DELIVERY FUNCTION (PC/TSP) AND THE COLLECTION FUNCTION (LEA)

The interface between the Delivery Function and the Collection Function is defined as the Demarcation Point.

CCC and CDC information is formatted into discrete messages using a specialized protocol called the PacketCable Electronic Surveillance Protocol (PCESP). The PCESP messages are delivered to a LEA at the Demarcation Point. Multiple electronic surveillances may be delivered at the same Demarcation Point.

The CDC and CCC information will not necessarily be synchronized when received by a LEA. The CC and CII are delivered to a LEA using the independent services of the CCCs and CDCs respectively, and these services can be provided on independent networks or independent facilities.

Procurement, engineering, and sizing of the physical facilities connecting the Delivery Function to the Collection Function are the responsibility of the LEA. Engineering and sizing of the Collection Function is also the responsibility of the LEA.

When the resources necessary for transmission of CC or CII, as provided by a LEA, are insufficient, the information is not required to be queued by the Delivery Function. In other words, intercepted information may be delayed or discarded by the Delivery Function if insufficient transmission capacity is provided by the LEA to the LEA's Collection Function.

## 6.1     General Interface Requirements

It is the responsibility of the PC/TSP to deliver CCC and CDC information to a Demarcation Point. The Demarcation Point shall consist of a physical interconnect adjacent to the DF. The LEA is responsible for providing the equipment, facilities, and maintenance needed to deliver this information from the Demarcation Point to the CF.

This specification defines a default physical and link level interface at the Demarcation Point. It is left to the discretion of any affected PC/TSP whether to provide alternative interconnect choices.

The PC/TSP MUST ensure that only those packets that have been authorized to be examined by the LEA are delivered to the LEA at the Demarcation Point. If, for example there is more than one LEA doing surveillance on the PC/TSP's network at a given point in time, each LEA must only see the data that it is authorized to receive.

Within the bandwidth limits of the facilities linking the DF and CF procured by the LEA, the PC/TSP ensures that delivery of CCC and CDC information to the Demarcation Point is provided a level of service quality that is equal to, or better than, the level of service quality provided to the communication that is being intercepted.  The PC/TSP also ensures that delivery of CCC and CDC information between IAPs and the DF or between DFs in the PC/TSP network is provided a level of service quality that is equal to, or better than, the level of service quality provided to the communication that is being intercepted.

## 6.2     Network Layer Interface

The network layer protocol for delivery of both CDC and CCC information MUST be as defined by both the Internet Protocol (IP) [RFC 791] and the Internet Protocol Version 6 (IPv6) [RFC 2460]. The network layer protocol interface MUST be able to support both IPv4 and IPv6, but is required to use only one IP configuration at any given time as configured by the network operator. The transport protocol for CDC information is as specified in Section 8 of this specification, while transport of CCC information is as specified in Section 7. Both CCC and CDC information MAY be provided over the same physical interface. Information is available in the CCC and CDC information packets to identify the type of packet (either CDC or CCC) and the particular case. The identification is provided either directly by the packet containing the surveillance case identifier, or indirectly by the packet containing an identifier that can be correlated with the case identifier.

The source IP address is contained in the IP header. The source IP address is the address of the DF. The IP header also contains the destination IP address, which is the address of the CF provided during interception provisioning.

All transfer of packets other than those operationally required to maintain the link MUST be from the DF to the CF only. At no time may the LEA send unsolicited packets from the CF to the DF.

## 6.3    Link-layer Interface

The default link-layer protocol between the DF and CF MUST be as defined by the Ethernet protocol [RFC 894] and [RFC 826]. However, alternate link-layer protocols MAY be used at the discretion of the PC/TSP based on negotiated agreements with the LEA.

## 6.4    Physical Interface

The default type of physical interconnect provided by the PC/TSP at the Demarcation Point MUST be an RJ45 10/100BaseT [ISO 8802-3] connection. However, alternate physical interconnects MAY be provided at the discretion of the PC/TSP based on negotiated agreements with the LEA.

## 6.5    Security

Encryption need not be supplied by the PC/TSP on the connections between the DF and the Demarcation Point. However, the LEA MAY choose to provide encryption from the Demarcation Point to the CF by supplying the necessary equipment and facilities.

# 7   CALL CONTENT CONNECTION (CCC) INTERFACE

This section describes the mechanism for delivery of Call Content, via Call Content Connections (CCC) from the PC/TSP's Delivery Function (DF) to the LEA's Collection Function (CF).

The CCC datagrams MUST contain a timestamp that allows the LEA to identify the time at which the corresponding information was detected by the DF. This timestamp MUST have an accuracy of at least 200 milliseconds. The CCC datagram MUST be queued at the DF for transmission to the Collection Function within eight seconds of detection of the corresponding packet by the Intercept Access Point 95% of the time. The delivery of particular CCC datagrams to the CF depends on many factors not under the control of the PC/TSP, such as the bandwidth between the DF and CF. These factors may affect the ability of the PC/TSP to meet the transmission criterion just stated, and this specification does not require the PC/TSP to take steps to counteract delays caused by such factors.

The CCC datagrams MUST contain the CaseID for the intercept. The CaseID appears in Call Data Connection (CDC) records associated with the CCC datagrams. The CaseID length is a maximum of 8 bytes and is formatted as in the CDC records described in Section 8.

The PC/TSP MUST be able to deliver Call Content as either a stream of UDP/IP or, if TCP/IP is available, TCP/IP datagrams, as defined in [RFC 768] for UDP/IP, [RFC 793] for TCP/IP [RFC 791] for IPv4, and [RFC 2460] for IPv6, sent to the port number at the CF as provided during provisioning of the interception. Whether TCP/IP or UDP/IP is to be used will be defined through direction from the LEA.  When no direction is received, TCP/IP MUST be used if available. The TCP/IP or UDP/IP payload MUST adhere to the following format:

*Table 1 – Payload of Call Content Connection Datagrams*

| CCC Identifier (4 bytes) |
| --- |
| Timestamp (8 bytes) |
| |
| CaseID (8 bytes) |
| |
| Intercepted Information (arbitrary length) |
| |
| |
| |
| |

The Timestamp MUST adhere to the NTP time format as defined in[RFC 5905]: a 64-bit unsigned fixed-point number, in seconds relative to 0000 on 1 January 1900. The integer (whole seconds) part is in the first 32 bits and the fractional part (fractional seconds) is in the last 32 bits. The timestamp MUST be accurate to within 200 milliseconds of the time the DF received the datagram.

Intercepted RTP information MUST be of the following format:

*Table 2 – Intercepted Information*

| Original IP Header (20 bytes for IPv4, 40 bytes typically for IPv6) |
| --- |
| |
| |
| |
| |
| Original UDP Header (8 bytes) |
| |
| Original RTP Header (variable length, 12-72 bytes) |
| |
| |
| Original Payload (arbitrary length) |
| |
| |

Note that protocols other than RTP MAY be intercepted, such as for T.38 fax relay.

## 7.1   Call Content Connection Identifier

The CCC-Identifier is provided by the Delivery Function in the CCOpen message. It is a 32-bit quantity, and is used to identify the intercept order to the LEA.

A conversation in the PacketCable network typically consists of two separate packet streams, each corresponding to a direction of the communication. Both are delivered to the Demarcation Point with the same CCC-Identifier. The party listening to the communication is identified by the combination of Destination Address (from Original IP Header) and Destination Port (from Original UDP Header). The Destination Address and Destination Port for both parties involved in the communication are provided in the Session Description (SDP) [RFC 4566] information provided to the LEA as part of the CCOpen message.

The DF MUST generate a CCC-Identifier that is different from all other CCC-Identifiers in use between that DF and a particular LEA. That is, two streams of content delivered to a single LEA must have different CCC-Identifiers, but a single stream of content delivered to multiple LEAs may use a single CCC-Identifier, so long as no other stream being delivered to one of the LEAs is using the same CCC-Identifier.

## 7.2   Original IP Header

This is the IP header [RFC 791] or [RFC 2460], as sent by the endpoint. Contained in this IP header is the IP Source Address (SA) and IP Destination Address (DA), that identify the internet addresses of the source and destination of the packet.

## 7.3   Original UDP Header

This is the User Datagram Protocol (UDP) header [RFC 768], as sent by the endpoint. Contained in this UDP header is the Source Port and Destination Port, both of which are 16-bit quantities that identify the connection to the two endpoints.

## 7.4   Original RTP Header

This is the Real-Time Transport Protocol (RTP) header [RFC 3550], as sent by the endpoint identified in the Source Address and Source Port. This header contains the packet formation timestamp, packet sequence number, and payload type value, as generated by the source endpoint.

The payload type value is defined by [RFC 3551] and is referenced in the Session Description (SDP) [RFC 4566].

## 7.5     Original Payload

The payload field is the bit-sequence as sent by the endpoint identified in the Source Address and Source Port. The payload typically contains the voice samples, as encoded and encrypted by the sending endpoint.

Encryption of the payload is by use of a stream cipher, or other method as described in [SEC1.5]. Keying material is contained in the Session Description (SDP) [RFC 4566], and the algorithm to generate the actual key is described in [SEC1.5].

Encoding of the voice may be done through use of one of the IETF's defined CODEC algorithms (as defined in [CODEC-MEDIA] or through a dynamic payload type defined in the Session Description (SDP) [RFC 4566]. Definition of CODEC algorithms is contained in [CODEC-MEDIA].

## 7.6     Transcoding

[FCC 99-230] defines "transcoding" as the activity that "... occurs whenever a packetized voice signal encounters an edge device without compatible codec support." The transcoding of communications content between encoding algorithms does not effectively alter the original content if the new encoding algorithm supports at least the same capabilities (i.e., encoded frequency range) as the original encoding algorithm. Intercepted content MAY be transcoded from the encoding format used in the PacketCable architecture into a different encoding format if the new encoding format provides at least the same level of information as the original encoding format. This can be accomplished by ensuring that the data is sampled at least the level of the network codec and the encoded bit rate of the delivery codec must be at least as great as the network codec. If transcoding is performed, G.711μ-law MUST be used to transcode AMR, SMV, EVRC, G.728, G.729E, iLBC(15.2), iLBC(13.3), and BV16 as defined n [CODEC-MEDIA]. [RFC 4733] MAY be used to pass DTMF tones. The SDP passed in MediaReport CDCs MUST be updated to properly reflect the transcoded packets. T.38 UDP packets MUST be passed unaltered. If G.711 is used for the intercepted call, the DF MAY pass the original RTP packets, unaltered and unencrypted. Otherwise, the DF MUST transcode compressed voice into G.711 μ-law for delivery to the CF. The DF MUST support the ability to disable transcoding on a per-intercept basis.

# 8    CALL DATA CONNECTION (CDC) INTERFACE

This section describes the mechanism for delivery of call identifying information, via Call Data Connections (CDC) from the PC/TSP's Delivery Function (DF) to the Law Enforcement's Collection Function (CF).

Call-identifying information is formatted into discrete messages using a specialized protocol called the Packet Cable Electronic Surveillance Protocol (PCESP). The PCESP messages are transported to LEA over a CDC interface.

The Call Data Connections in the PacketCable Electronic Surveillance Protocol are implemented as TCP/IP [RFC 793] connections, established by the Delivery Function, to the Collection Function designated by LEA in the surveillance provisioning.

A TCP/IP connection shall be capable of transporting the call identifying information for multiple surveillance cases to a single LEA.

The PCESP messages MUST contain a timestamp that identifies the time the corresponding event was detected by the IAP. This timestamp MUST have an accuracy of at least 200 milliseconds. The PCESP message MUST be queued at the DF for transmission to the Collection Function within eight seconds of detection of the corresponding event by the Intercept Access Point 95% of the time. Refer to Annex A for PacketCable-specific requirements. The delivery of particular PCESP messages to the CF depends on many factors not under the control of the PC/TSP, such as sufficient bandwidth supplied between the DF and CF, and the timely transmission of TCP ACKs by the CF. These factors may affect the ability of the PC/TSP to meet the transmission criterion just stated, and this specification does not require the PC/TSP to take steps to counteract delays caused by such factors.

PCESP messages contain an Accessing Element ID to identify the IAP. The Accessing Element ID is a statically configured element number uniquely assigned within a PacketCable domain.

## 8.1    CDC Messages

The CDC messages report Call-Identifying Information accessed by a PacketCable IAP. These IAPs provide expeditious access to the reasonably available call-identifying information for calls made by a surveillance subject or for calls made to a surveillance subject. This includes abandoned and incomplete call attempts, if known to a PacketCable IAP.

The following CDC messages have been defined to convey information to a LEA for call-identifying events on a call that result from a user action or a signal. Only events that are available to PacketCable elements providing intercept access functionality will be reported using the messages below. Access to call-identifying information MUST NOT deny the availability of any service to either the subject or associates.

The following call-events are defined:

| | |
|---|---|
| **Answer** | A two-way connection has been established for a call under surveillance. |
| **CCChange** | A change in the description of Call Content delivery for a call under interception. |
| **CCClose** | End of Call Content delivery for a call under interception. |
| **CCOpen** | Beginning of Call Content delivery for a call under interception. |
| **CCUnavailable** | The Call Content of the intercepted call is not available to the Delivery Function. |
| **DialedDigitExtraction** | The surveillance subject dialed or signaled digits after a call is connected. |
| **MediaReport** | Exchange of SDP information for new or existing calls for which only call-identifying information is being reported. |
| **NetworkSignal** | The PC/TSP network requested the application of a signal toward the surveillance subject. |

| | |
|---|---|
| **Origination** | The IAP detects that the surveillance subject is attempting to originate a call. |
| **Redirection** | A call under surveillance is redirected (e.g., via termination special service processing). |
| **Release** | The resources for a call under surveillance have been released. |
| **Serving System** | The IAP detects that a PacketCable subscriber has roamed into a cooperative visited cellular network. |
| **SubjectSignal** | The surveillance subject sends dialing or signaling information to the PC/TSP network to control a feature or service. |
| **TerminationAttempt** | The IAP detects a call attempt to a surveillance subject. |

## 8.2    Basic Call Services

This section describes the events that trigger the generation of CDC messages to be delivered to LEA for a basic call. More specifically, it identifies when CDC messages are generated for a basic call and identifies the information each CDC message contains. For purposes of clarity, this section is broken down into two sub-sections, namely:

- Call originated by a surveillance subject
- Call terminating to a surveillance subject

In addition to the CDC messages described in this section, other CDC messages might be generated depending on the events that occur during a basic call. As examples, the NetworkSignal message might be generated for events such as the application of distinctive ringing (terminating call) towards the surveillance subject, and the SubjectSignal message might be generated for an event such as fax tone detection.

### 8.2.1    Originating call from a Surveillance Subject

This section applies to calls originated by a subscriber who is subject to authorized surveillance. The originating subscriber is the "subject". The procedures specified in this subsection take place when the subject's call origination signaling is detected by a PacketCable element providing IAP functionality, regardless of any subsequent event that may result in clearing of the call. This includes abnormal clearing of a call due to HFC network failure.

For completed calls originating from a subject under a Call Content intercept order, ten call-identifying messages are generated for delivery to the LEA - Origination, CCOpen, (downstream), CCOpen (upstream), Answer, CCChange (downstream), CCChange (upstream), CCClose (downstream), CCClose (upstream), CCUnavailable and Release.

For completed calls originating from a surveillance subject under a Pen Register surveillance order, five call-identifying messages are generated for delivery to the LEA - Origination, MediaReport (upstream), MediaReport (downstream), Answer, and Release.

Information about partial dialing is generally not known to the PacketCable IAP. For failed or abandoned call attempts, when dialing information is presented to an IAP, an Origination message is generated for delivery to LEA. General number translations completed by the network are reported in call-identifying messages, such as network provided speed dial or 8YY.

### 8.2.2    Call Termination to a Surveillance Subject

This section applies to calls terminating to a subscriber who is subject to authorized surveillance. The terminating subscriber is the "subject." The procedures specified in this subsection take place when a call termination attempt to a subject is detected by a PacketCable IAP, regardless of a subsequent event that may result in clearing of the call. This includes abnormal clearing of a call due to HFC network failure.

For completed calls terminating to a subject under a Call Content interception order, ten call-identifying messages are generated for delivery to the LEA - TerminationAttempt, CCOpen (downstream), CCOpen (upstream), Answer,

CCChange (downstream), CCChange (upstream), CCClose (downstream), CCClose (upstream), CCUnavailable and Release.

For completed calls terminating to a subject under a Trap and Trace surveillance order, five call-identifying messages are generated for delivery to the LEA - TerminationAttempt, MediaReport (upstream), MediaReport (downstream), Answer, and Release.

For abandoned call attempts to a subject under surveillance, a TerminationAttempt message is generated for delivery to LEA.

## 8.3    Specific Call Services

### 8.3.1    Caller ID

Caller ID sent by the subject or inserted by the network on behalf of the subject is reported within an origination message. Caller ID received by the subject is reported within a termination attempt message.

### 8.3.2    Call Hold

Call Hold is implemented in the client for RST. The feature status of call hold for a two way call is managed by the client and is not available to the network. The network detects the change in SDP for held media as a result of call hold and reports change in SDP in the media report message. If a call is being intercepted under a Call Content interception order, the lack of Call Content during a period of time indicates either silence suppression being performed by the endpoint, or indicates the call has been put on hold.

### 8.3.3    Call Redirection (Call Forwarding)

Call redirection is invoked when a call attempts to terminate to a surveillance subject, the S-CSCF in conjunction with the application server determines that the subject has subscribed to special call handling services, and the conditions for feature invocation are met. Call redirection, or call forwarding, may take on a number of varieties in the PacketCable network, such as call forwarding variable, call forwarding busy, selective call forwarding, and call forwarding to voice mail. Call Redirection within a PacketCable environment may appear to subscribers to be similar or equivalent to traditional "call forwarding" within the PSTN. It is technically quite different, however, in ways that affect a PC/TSP's ability to support surveillance in some contexts. When the call redirection is done immediately upon the termination attempt, the following sequence of messages is an example of what will be sent to the LEA, as determined by events detected at the IAP(s):

- TerminationAttempt (for the original terminating call to the surveillance subject)

- NetworkSignal (for ringsplash)

- Redirection (to identify the redirection event and the redirected-to party)

- CCOpen (downstream, if Call Content interception order)

- CCOpen (upstream, if Call Content interception order)

- Answer (if redirected call is answered by redirected-to party)

- CCChange (downstream, if Call Content interception order)

- CCChange (upstream, if Call Content interception order)

- CCClose (downstream, if Call Content interception order)

- CCClose (upstream, if Call Content interception order)

- Release (when a completed redirected call ends)

If the redirection is done after the termination attempt, but before the call is answered, the following sequence of messages is an example of what will be sent to the LEA, as determined by events detected at the IAP(s):

- TerminationAttempt (for the original terminating call to the surveillance subject)

- CCOpen (downstream, for the original call, if Call Content interception order)

- CCOpen (upstream, for the original call, if Call Content interception order)

- NetworkSignal (for distinctive ringing [if applicable and not busy])

- CCClose (downstream, for the original call, if Call Content interception order)

- CCClose (upstream, for the original call, if Call Content interception order)

- Redirection (to identify the redirection event and the redirected-to party)

- CCOpen (downstream, if Call Content interception order)

- CCOpen (upstream, if Call Content interception order)

- Answer (if redirected call is answered by redirected-to party)

- CCChange (downstream, if Call Content interception order)

- CCChange (upstream, if Call Content interception order)

- CCClose (downstream, if Call Content interception order)

- CCClose (upstream, if Call Content interception order)

- Release (when redirected call ends, if answered by redirected-to party)

If a call redirected by the surveillance subject's service is subsequently redirected again by the redirected-to party's service within the PacketCable, an additional Redirection messages MUST be generated for the second redirection.

If a call originated by a surveillance subject is redirected by the associate's service within the PacketCable network, a Redirection message MAY be generated.

### 8.3.4   Call Waiting

Call Waiting is a client based service for RST. As such, information regarding call waiting is not available in the PacketCable 2.0 network. A call in wait is treated as a separate call termination. While the call is waiting, it is treated the same as a call in the alerting state.

### 8.3.5   Call Transfer

Call Transfers may be blind or consultative. Call Transfer is executed by the SIP client in RST. Consultative Call Transfer begins with the formation of a 3-way call and is reported as described in Section 8.3.6. The subject hangs up and then BYEs are sent to the associates, which are reported as Releases to both calls. The subject then sends a REFER to one of the associates to instruct the associate to call the other associate involved in a 3-way call. The REFER is reported to the LEA as a Subject Signal message. The NOTIFY confirmation of the REFER sent to the subject is reported as a Network Signal message.

Blind transfer is similar to consultative call transfer in PacketCable 2.0, except the subject hangs up prior to the formation of the 3-way call. Blind transfer is reported in an identical fashion as consultative call transfer.

### 8.3.6   Three-Way Calling

Three-way calling is often implemented as a network conference bridge or client based conference capability. Three-way calling, or ad-hoc conferencing, is implemented on the SIP client in RST. Therefore, the scope of this section is limited to client based conferences. This section describes the sequences of call-identifying messages on the CDC that will be generated when a surveillance subject initiates a three-way call. In this case, the typical user interface is as follows. The initiator (party A, a surveillance subject in this example) has one established call (either as originator or as terminating party) with party B, places that call on hold, originates a second call to party C, then does a hookflash to cause a three-way call. A subsequent hookflash drops party C, and a subsequent onhook terminates all the calls.

When the client performs the bridging function, the CDC will indicate two independent basic calls, the first (between A and B) either originated by or terminated at the surveillance subject, and the second (between A and C) originated by the surveillance subject. Nothing further is known by the IAP to be reported on the CDC. Under an interception order, the two separate Call Content connections will contain the mixed conversations, i.e., the

intercepted communication from A to B will contain A+C, and the intercepted communication from A to C will contain A+B. When any one party disconnects, the calls involving that party are terminated.

### 8.3.7    Call Block

A blocked call will follow the same procedures for a basic call up to the point that it is blocked, at which point a Release message will be sent. If the call had been answered prior to the time that the blocking resulted in the call being aborted, then a Release message will be sent to the LEA. If Call Content had been intercepted and delivered to the LEA prior to the time that the blocking resulted in the call being aborted, then CCClose messages will be sent to the LEA. Up to the point of blocking, the relevant CDC messages and Call Content will be delivered to the LEA.

Inbound call blocking, such as solicitor call blocking, may require the caller to record their name or other input. This input is then offered to the subject. who can then accept or reject the call. The recording of the caller is reported to the agency within Call Content. The rejection of the solicitor call by the subject MUST be reported as a release message. If the acceptance or rejection of the call by the subject is communicated to the call blocking application server via DTMF tones from the target UE, then a Dialed Digit Extraction message containing the tones MUST be reported to the LEA.

### 8.3.8    AutoCallback

Automatic Callback (AC) allows a client to automatically call back the last called address (Target-Address is the URI of the last INVITE sent from the client), whether the INVITE was answered by the called party or not.

Auto Callback is executed by the SIP client in RST. The subject's client repeats call attempts to the associate's client. Each call attempt is reported as a new call origination. The subject may also subscribe to the associate's call state to determine when the associate is idle and may be prepared to accept a new call origination. The NOTIFY sent by the associate to indicate call state and received by the subject is reported as a Network Signal.

### 8.3.9    Auto Recall

Automatic Recall (AR) allows a UE to automatically call back the last calling address (Target-Address – the P-Asserted-ID of the caller) that sent an INVITE to this UE, whether the INVITE was answered by this client or not.

Auto Recall is executed by the SIP client in RST. The subject's client repeats call attempts to the associate's client. Each call attempt is reported as a new call origination. The subject may also subscribe the associate's call state to determine when the associate is idle and may be prepared to accept a new call origination. The NOTIFY sent by the associate to indicate call state and received by the subject is reported as a Network Signal.

### 8.3.10   E911 Emergency and N11 Services

911 emergency and N11 service calls are viewed as normal call originations and the description in Section 8.2.1, applies. In this case the dialed digits are "911" or "N11". If the dialed number is translated to another number, and the information is available at the IAP, then both the dialed digits (user input) and translated to number (called party) are presented to the LEA.

### 8.3.11   Mid-Call CODEC Change

During a call established with the PacketCable network, the endpoints may decide (based on recognition of a modem or fax tone, or other conditions such as transcoding) that the previously negotiated coding method is inadequate to meet the customer needs. For a call under interception, CCChange messages are generated for delivery to the LEA. Contained in the CCChange message are updated SDP descriptions [RFC 4566] of the media flows. A Media Report message is reported to indicate the change in codecs or media type.

### 8.3.12   Post-Cut-Through Dialing

When a call is connected to a PC-TSP's service for processing and routing, the surveillance subject could dial digits after the initial call setup is completed and the call path is cut-through within the PC/TSP network. (Cut-through occurs when the upstream resources are committed. Digits dialed prior to upstream committal are not subject to Dialed Digit Extraction.) When this occurs, the "post-cut-through digits" are delivered to the LEA in one or more DialedDigitExtraction message(s). The delivery of these digits may be enabled or disabled (as a toggle) as required by law. Dialed digits from the associate are subject to DDE reporting only if the digits are routed to the surveillance subject's terminal.

### 8.3.13  Network Registrations

A client requesting service from the PacketCable 2.0 network will first need to complete a network registration if a current registration does not already exist. The Serving System message reports network registrations, registration updates and de-registrations. The message reports the identification of the TSP currently providing service to a subscriber, especially a roaming mobile subscriber. Note that where the VCC capability is implemented, a VCC subscriber may be simultaneously registered with both a PacketCable 2.0 network and a circuit cellular network. For these VCC cases, registration in each network is reported independently.

### 8.3.14  Voice Call Continuity and Domain Transfers

When a subject, who is a VCC subscriber, is in the Circuit Cellular domain, the PacketCable MSO MUST report all call associated events as if the subject were in the PacketCable domain with the exception of Domain Transfer events as noted below. For example, when the subject has roamed to the Circuit Cellular domain and originates a call, the PacketCable MSO MUST report an Origination message.

PacketCable mobile devices may be capable of sustaining continuous voice service of a call when moving between PacketCable and circuit cellular networks. This is referred to as a domain transfer of an active voice call. The Redirection Message MUST be reported when a call is transferred between PacketCable and circuit cellular networks. When a domain transfer event is reported using the Redirection event message, other event messages are not reported (e.g., Origination, Answer, Release).   The domain transfer event MUST be reported when the subject is a VCC subscriber.

### 8.3.15  Miscellaneous Features

This section describes the interception of an example set of features that may be present in a PacketCable network with RST services.

Do Not Disturb is another form of inbound call blocking where all calls to the subscriber are blocked, unless the caller is able to bypass the block by entering a PIN or being a member of a subscriber DND caller bypass list. Blocked in bound calls are reported as a Call Termination attempt with a release message.

Subscriber Programmable PIN is an interactive voice service allowing the user to provision feature data. These services are intercepted as a call to the application where tones sent by the subject are reported as Dialed Digit Extraction messages.

Network assisted Distinctive Alerting as described in RST is intercepted and reported as a NetworkSignal message. The NetworkSignal message includes an indication of the pattern selected for the network assisted distinctive ring.

Message Waiting Indicator to the subject is reported as a NetworkSignal message.

Network assisted Speed Dialing as described in RST is intercepted as a SubjectSignal message.

Customer Originated Call Trace requests to the network are reported as a SubjectSignal message.

Screen List Editing is an interactive voice service allowing the user to provision feature data. These services are intercepted as a call to the application where tones sent by the subject are reported as Dialed Digit Extraction messages. Audio prompts from the Screen List Editing application server to the subject are reported as CC under Call Content intercept orders.

### 8.3.16  Call Content Not Available

The CCUnavailable message must be presented to the CF if the VoIP network is aware that the network does not have access to content for a call that is under content interception. The CCUnavailable message is applicable only to Call Content intercepts.

## 8.4    CDC Message Descriptions

The messages that identify the call events, described in Section 8.1, convey the basic information that reports the disposition of a call. This section describes those event messages and the supporting information. Each message is described in detail using a table. Within each table, the available fields are listed as Required or Conditional. Required fields MUST always be included. Conditional fields MUST be included when the condition for reporting is satisfied.

PacketCable 2.0 CDC messages are augmented from prior PacketCable CDC message releases and are therefore backwards compatible with prior PacketCable releases. A PacketCable 2.0 delivery function may filter 2.0 specific messages and parameters when delivering messages to a PacketCable 1.x collection function. This allows cable networks to upgrade their networks with PacketCable 2.0 capabilities and still be able report CDC messages to 1.x collection functions. The collection functions can receive CDC messages from PacketCable 2.0 networks prior to the collection functions being upgraded for full 2.0 capability.

### 8.4.1   Answer

The Answer message reports when a call under surveillance is answered. Transmission is usually cut-through at this time, in both directions, due to the receipt of an off-hook indication from the terminating end-user, or other user-network interaction.

The Answer message MUST be generated for the calls originated by or terminating to a surveillance subject when one of the following events is detected by an IAP:

- An outgoing call from a surveillance subject is answered or cut-through in both directions, including when the call is originated in the circuit cellular domain but routed to the packet cable domain as part of VCC call processing.

- A surveillance subject answers a previously unanswered call originating from an on-net or off-net associate.

- A redirected call identified by the PC/TSP as a call under surveillance is answered or cut-through in both directions.

The Answer message MUST NOT be generated based on 200 OKs (in response to INVITEs) associated with Domain Transfer events (from the circuit cellular domain to the packet cable domain) associated with a subject who is a VCC subscriber.

When reporting party identity information (i.e., Answering Party ID) the PC/TSP MUST report all known identities using the sub-elements of Answering Party ID. The PC/TSP is NOT REQUIRED to populate all sub-elements of Answering Party ID if doing so would be redundant (e.g., if the answering party's uri is provided in the SIP header sub-element, it is not necessary also to report the uri in the uri sub-element).

The Answer message MUST include the following information.

*Table 3 – Answer Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message. |
| Answering Party ID | R | Included to identify the destination of the call which may be different that that previously reported in the Origination/Termination Attempt message called party id parameter called party id. If the call terminated within a particular PC/TSP's PacketCable network, this is the number of the answering party. If the call terminated on a PSTN gateway, this is the identity of the last known destination for this call. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.2 CCChange

The CCChange message MUST be generated for calls under interception when one or more of the following events is detected by an IAP:

- A change in the resource state (reserved to committed or vice versa) for this call on the HFC access network.

- A change in the bandwidth for this call on the HFC access network.

- A change in the Session Description information (such as codec change) for either the originating or terminating endpoint.

A CCChange message MAY be generated individually for each flow direction, downstream and upstream, or as a single message for both directions. Downstream indicates media being sent to the subject and upstream indicates media being sent from the subject. Subject_SDP contains the SDP media description for the downstream direction and Associate_SDP contains the SDP media description for the upstream direction.

The Subject_SDP attribute MUST be included if it changed from the SDP in the previous CCOpen or CCChange message. The Associate_SDP attribute MUST be included if it changed from the SDP in the previous CCOpen or CCChange message.

The Resource_State attribute MUST be included if the state of the underlying resources that carry the media stream changed.

The CCChange message is triggered for surveillances that require the delivery of Call Content, and its main purpose is to provide the LEA with updated information necessary to decode the voice packets for the call. Typically the CCChange message identifies the beginning of the delivery of Call Content information.

The CCChange message MUST NOT be used to indicate a change in the CCC_ID. If the CCC_ID changes, the CCC will be closed by means of a CCClose, and a new CCC, with a new CCC_ID, will be opened by means of a CCOpen.

The CCChange message MUST include the following information.

*Table 4 – CCChange Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message. |
| Subject SDP | C | The Session Descriptor Protocol (SDP) information for the subject endpoint (downstream direction), if it is changed. |
| Associate SDP | C | The Session Descriptor Protocol (SDP) information for the associate endpoint (upstream direction), if it is changed. |
| CCC ID | R | The CCC_ID value that will appear in all intercepted packets for this call. The latest value of the CCCID MUST be present in this field. |
| Resource State | C | Indicates the state of the underlying resources that carry the media stream (reserved or committed), if changed. |
| Flow Direction | R | Indicates the direction(s) of the media stream(s). |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.3   CCClose

The CCClose message reports the end of delivery of Call Content for a call under interception. The CCClose message MUST be generated for calls under interception when a Call Content Channel has been opened (via a CCOpen message) and that Call Content connection is released. The CCClose may be triggered by a BYE, 4xx or 5xx response (release).

A CCClose message MAY be generated individually for each flow direction, downstream and upstream, or as a single message for both directions.

The CCClose message MUST include the following information.

*Table 5 – CCClose Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| CCC ID | R | The CCC-ID value that appeared in all intercepted packets for this call. |
| Flow Direction | R | Indicates the direction(s) of the media stream(s). |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.4   CCOpen

The CCOpen message MUST be generated for calls under interception when one of the following events is detected by an IAP:

- When an SDP offer, answer transaction is complete and resources are reserved on the HFC access network if media is available in the network.

- In the case of an off-net call, either the one way (send) or two (send/receive) path has been enabled on the Media Gateway.

- When an incoming off-net call is forwarded to an off-net location at the same Media Gateway.

The Subject_SDP attribute MUST be included in CCOpen messages when the Flow_Direction attribute equals "Downstream" or "Downstream and Upstream". The Associate_SDP attribute MUST be included in CCOpen messages when the Flow_Direction attribute equals "Upstream" or "Downstream and Upstream".

A CCOpen message MAY be generated individually for each flow direction, downstream and upstream, or as a single message for both directions. Downstream indicates media being sent to the subject and upstream indicates media being sent from the subject. Subject_SDP contains the SDP media description for the downstream direction and Associate_SDP contains the SDP media description for the upstream direction.

The CCOpen message MUST include the following information.

*Table 6 – CCOpen Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message. |
| Subject SDP | C | The Session Descriptor Protocol (SDP) information for the subject endpoint (downstream direction). |
| Associate SDP | C | The Session Descriptor Protocol (SDP) information for the associate endpoint (upstream direction). |
| CCC ID | R | The CCC_ID value that will appear in all intercepted packets for this call. |
| Flow Direction | R | Indicates the direction(s) of the media stream(s). |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.5   DialedDigitExtraction

The DialedDigitExtraction message reports surveillance subject-dialed digits after a call is connected to a TSP's service for processing and routing. These digits, called "post-cut-through digits," are digits dialed or signaled by the surveillance subject after the initial call setup is completed and the call path is cut-through within the PC/TSP network. (Cut-through occurs when the upstream resources are committed. Digits dialed prior to upstream committal are not subject to Dialed Digit Extraction.) The digits may be reported on a digit-by-digit basis, accumulated until a buffer is full, or accumulated until a timer expires, accumulated until the call is released.

A PC/TSP may report dialed digits other than those that are call completing and has no obligation to determine which dialed digits actually complete a call.

Dialed Digit Extraction of associate asserted digits applies only if the digits are routed to the subject's terminal.

The DialedDigitExtraction message MUST be generated when the surveillance subject dials or signals digits after a call is connected to a PC/TSP's service and the following event is detected by a DF:

- Digit-by-digit reporting is performed and a digit is detected; or

- Digit accumulation reporting is performed and one of the following occurs:

  i. A maximum of 32 digits have been accumulated in the buffer; or

  ii. 20 seconds have elapsed since detection of the first digit in the buffer; or

  iii. The call is released.

The DialedDigitExtraction message MUST include the following information.

*Table 7 – DialedDigitExtraction Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. |
| Digits | R | Identifies the digits dialed or signaled by the surveillance subject after the call is cut-through in both directions. |

The Event Time attribute in the DialedDigitExtraction message MUST be set to the time the first digit in the message is detected.

A digit is defined as a character representing Dual Tone Multi Frequency (DTMF) tones and having values from the following numbers, letters, and symbols, "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "#", "*", "A", "B", "C", and "D".

### 8.4.6   MediaReport

The MediaReport message reports the exchange of SDP information for calls involving the intercept subject's equipment, facilities or service, including for new and open media channels. The MediaReport message applies to calls for which only call-identifying information is being reported to law enforcement.

The MediaReport message MUST be generated for calls for which only call-identifying information is being reported when one of the following events is detected by an IAP:

- SDP is received for a new media flow.
- New SDP is received for an open media flow.

The MediaReport message is not required for calls for which Call Content is being reported since the CCOpen and CCChange messages report SDP information for such calls.

A MediaReport message MAY be generated individually for each flow direction, downstream and upstream, or as a single message for both directions.

The Delivery Function MUST deliver the following SDP attributes (if present) in a MediaReport message:

- v=  protocol version
- o=  This is the owner/creator and session identifier
- s=  session name
- i=  session information
- u=  URI of description
- e=  email address
- p=  phone number
- c=  connection information
- m=  media information
- a=  zero or more session attribute lines (can be used to indicate active or held media)

The Delivery Function MUST NOT deliver any other SDP attributes than listed above in a MediaReport message. The MediaReport message MUST include the following parameters:

*Table 8 – MediaReport Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message. |
| Subject SDP | C | The call identifying information from the SDP for the subject endpoint (downstream direction), if the subject's SDP is being reported in the message. |
| Associate SDP | C | The call identifying information from the SDP for the associate endpoint (upstream direction), if an associate's SDP is being reported in the message. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.7   NetworkSignal

The NetworkSignal message reports requests made by the PC/TSP network to apply signals to the surveillance subject.

The NetworkSignal message MUST be generated when the IAP receives a positive acknowledgment to a request for the immediate generation of a signal toward the intercept subject. Refer to Annex A for PacketCable-specific requirements.

When reporting party identity information (i.e., Signaled To Party ID) the PC/TSP MUST report all known identities using the sub-elements of Signaled To Party ID.  The PC/TSP is NOT REQUIRED to populate all sub-elements of Signaled To Party ID if doing so would be redundant (e.g., if the signaled to party's uri is provided in the SIP header sub-element, it is not necessary also to report the uri in the uri sub-element).

The NetworkSignal message MUST include the following information.

*Table 9 – NetworkSignal Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | C | Uniquely identifies a call within a system. Present if the Network Signal is associated with a call. |
| Signaled To Party ID | R | Identifies the signaled-to party. |
| AlertingSignal | C | May include ringing or distinctive alerts, reported if alert info is present in the 180 ring. |

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Signal | C | Reported if NetworkSignal is other than alerting. Enumerated as: MWI per NOTIFY NOTIFY for feature activation NOTIFY for associate call state REFER 200OK to PRACK for early media |
| Other | C | Used to report undefined network signals |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.8   Origination

The Origination message MUST be generated for the calls originated by a surveillance subject when one of the following events is detected by an IAP:

- Call origination signaling by a surveillance subject is detected, and the call is routed toward an on-net or off-net destination, including when a call is originated in the circuit cellular domain but routed to the packet cable domain as part of VCC call processing. This MAY include translation of digits entered by the subject to another set of digits (e.g., 800-number translation).

- Call origination signaling by a surveillance subject is detected, and the call could not be completed, including, but not limited to, when the signaled dialing information has no digits or partially dialed digits.

- Call origination signaling by a surveillance subject is detected, and the subject signaled the call to be abandoned before the call could be routed to its destination.

The Origination message MUST NOT be generated based on INVITEs associated with domain transfer events (from the circuit cellular domain to the packet cable domain) associated with a subject who is a VCC subscriber.

Multiple INVITES can result from a call origination in certain call scenarios. The Delivery Function MUST buffer INVITEs for a configured time duration or until a resulting positive or negative response is received before reporting an Origination message to the collection function.

When reporting party identity information (i.e., Calling Party ID and Called ID) the PC/TSP MUST report all known identities using the sub-elements of Calling Party ID or Called ID.  The PC/TSP is NOT REQUIRED to populate all sub-elements of Calling Party ID or Called ID if doing so would be redundant (e.g., if the calling party's uri is provided in the SIP header sub-element, it is not necessary also to report the uri in the uri sub-element).

The Origination message MUST include the following information.

*Table 10 – Origination Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. The unique Call_ID included in the Origination message is used to correlate other messages. |
| Calling Party ID | C | Include only when the identity of the called party is known. This is not present for calls that were partially dialed or could not be completed by the accessing system. The Calling Party ID includes the public identity of the calling party and may also include a Display Name if present in the origination signaling. |
| Called ID | C | Included when available. Identifies the intended ID of the recipient of the call origination. |
| User Input | C | The digits input by the user if available from the network. |
| Translations Input | C | Identifies input to a translation process (e.g., 800 number, network-based speed dial input). Either User_Input or Translation_Input MUST be present. |
| Transit Carrier ID | C | Include when a transit carrier is used to transport the call. |
| Subject Location | C | Include the geographic location or street address if available in the network, and authorized by the warrant. |
| SystemID | R | Provided to identify the system serving the intercept subject When the serving system is a cellular system, a cellular network ID may be reported. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.9   Redirection

The Redirection message reports the redirection of a call under surveillance. The Redirection message is generated for calls redirected by the surveillance subject or the surveillance subject's service, such as when call termination special features are encountered, or by his direct actions on a terminating call.

The Redirection message MUST be generated for calls under surveillance when one of the following events is detected by an IAP:

- An incoming call to a surveillance subject is redirected (forwarded) to another number by the subject's service.

- A call originated by a surveillance subject is redirected (forwarded) to another number by the terminating party's service.

- A call is domain transferred from a PacketCable 2.0 network to a partner network circuit cellular domain.

- A call is domain transferred from a partner network circuit cellular domain to a PacketCable 2.0 network.

The Redirection message MUST be generated when a call under surveillance is forwarded or transferred by a party other than a surveillance subject, and the subject's PC/TSP is aware of the operation.

When reporting party identity information (i.e., Redirected from Party ID, Redirected to Party ID) the PC/TSP MUST report all known identities using the sub-elements of Redirected from Party ID or Redirected to Party ID. The PC/TSP is NOT REQUIRED to populate all sub-elements of Redirected from Party ID or Redirected To Party ID if doing so would be redundant (e.g., if the redirected to party's uri is provided in the SIP header sub-element, it is not necessary also to report the uri in the uri sub-element).

The Redirection message MUST include the following information.

*Table 11 – Redirection Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message |
| New Call ID | C | Included when the redirected call will be identified by a different Call-ID in future CDC messages. |
| Redirected from Party ID | C | Identifies the redirected-from party. Reported when available. Identifies the Surveillance Subject when reporting domain transfers. |
| Redirected to Party ID | C | Identifies the redirected-to party (redirected-to or transferred-to party). Identifies the VDI used to execute a domain transfer from a partner network circuit cellular domain to a PacketCable 2.0 network. Identifies the VDN used to execute a domain transfer from a PacketCable 2.0 network to a partner network circuit cellular domain. |
| Transit Carrier ID | C | Include when a transit carrier is used to transport the redirected call. |
| SystemIdentity | R | Provided to identify the serving system when the intercept subject is authorized for service by the TSP. For domain transfers reported with a Redirection Message this indicates the MSO PacketCable network when the domain transfer is from a partner network circuit cellular domain to a PacketCable 2.0 network, or a circuit cellular roaming partner network when the domain transfer is from a PacketCable 2.0 network to a partner network circuit cellular domain |

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Redirection Reason | R | Identifies the network event that triggered reporting of the Redirection message.  Enumerated as:<br>- Domain Transfer to PacketCable network<br>- Domain Transfer from PacketCable network<br>- Call forwarding Variable<br>- Call Forwarding Do Not Answer<br>- Call Forwarding on Busy<br>- Selective Call Forwarding<br>- Other<br>- Unknown |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.10  Release

The Release message reports the release of resources used for a call under surveillance. The Release message MUST be generated for calls under surveillance that had previously reported an Origination or Termination Attempt event, when one of the following events is detected by an IAP:

- A signaled completed call release (subject, network or associate initiated) is detected by an IAP, and resources are released, including cases where the subject, who is a VCC subscriber, is in the circuit cellular domain.

- A call abnormal release is detected by an IAP for an existing call, and the resources are released.

The Release message MUST NOT be reported when the connection between the surveillance subject's MS and the VCC AS is torn down because of the occurrence of a domain transfer event (from the packet cable domain to the circuit cellular domain) associated with a subject who is a VCC subscriber.

The Release message MUST include the following information.

*Table 12 – Release Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message. |
| Release reason | R | Describes reason for call release as indicated in network signaling. |
| Subject Location | C | Include the geographic location or street address if available in the network and lawfully authorized by the warrant. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.11  Subject Signal

The SubjectSignal message reports dialing and signaling initiated by the surveillance subject to control (including invocation and use) a feature or service (e.g., call forwarding).

The signal could be call-associated or non call-associated. Digits dialed post cut-through MUST NOT be provided in a SubjectSignal message.

The SubjectSignal message MUST be generated when the IAP receives information indicating the surveillance subject's initiation of a signal unless the information reported would be redundant with the information reported by other CDC messages (e.g., Origination message). Refer to Annex A for PacketCable-specific requirements.

When reporting party identity information (i.e., Signaled From Party ID, Signaled To Party ID) the PC/TSP MUST report all known identities using the sub-elements of Signaled From Party ID or Signaled To Party ID.  The PC/TSP is NOT REQUIRED to populate all sub-elements of Signaled from Party ID or Signaled to Party ID if doing so would be redundant (e.g., if the signaled to party's uri is provided in the SIP header sub-element, it is not necessary also to report the uri in the uri sub-element).

The SubjectSignal message MUST include the following information.

*Table 13 – SubjectSignal Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | C | Uniquely identifies a call within a system. Present if the Network Signal is associated with a call. |
| Signaled From Party ID | R | Include to identify the signaled-from party. |
| Signaled To Party ID | C | Include to identify the signaled-to party when available. |
| Signal | C | If not reported as DialedDigits or Feature Key then enumerated as: Client call status reported via NOTIFY REFER Other signaling formation (could be used for distinctive ring back or other purposes) |
| DialedDigits | C | Dial string within INVITE. |
| FeatureKey | C | Short code to application server. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.12  Termination Attempt

The TerminationAttempt message MUST be generated for incoming calls to a surveillance subject when the following event is detected by an IAP:

- an incoming off-net or on-net call to a surveillance subject is detected, including when the call is routed to the circuit cellular domain by the VCC AS for completion to a subject who is a VCC subscriber.

When reporting party identity information (i.e., Calling Party ID, Called Party ID, Redirected From Info) the PC/TSP MUST report all known identities using the sub-elements of Calling Party ID, Called Party ID, or Redirected From Party ID.  The PC/TSP is NOT REQUIRED to populate all sub-elements of Calling Party ID,

Called Party ID, or Redirected From Party ID if doing so would be redundant (e.g., if the redirected from party's uri is provided in the SIP header sub-element, it is not necessary also to report the uri in the uri sub-element).

The TerminationAttempt message MUST include the following information.

*Table 14 – TerminationAttempt Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. The unique Call_ID included in the Termination message is used to correlate other messages. |
| Calling Party ID | C | Identifies the originating party, when available. This includes the display name of the calling party if present. |
| Called Party ID | C | Include if more specific than the surveillance subject identity (surveillance subject DN) associated with the Case_ID. |
| Redirected From Info | C | Include if information about previous redirections for the incoming call is available to the IAP. |
| Subject Location | C | Include the geographic location or street address if available in the network and lawfully authorized by the warrant. |
| SystemID | R | Provided to identify the system serving the intercept subject When the serving system is a cellular system, cellular network ID may be reported. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.13  ServingSystem

The ServingSystem Message reports a registration, a change, or an attempted change to the serving TSP, service area, or intercept subject's addressing information, e.g., for personal mobility.

The ServingSystem message MUST be reported when:

- a request to register or deregister an intercept subject's addressing information is directed or forwarded to a registrar (e.g., a SIP Proxy forwards a Register request to a SIP Registrar).

- a request to register or deregister an intercept subject's addressing information is processed, failed, or timed out by a registrar (e.g., a SIP Registrar processes a SIP Register request).

- when the intercept subject is authorized for service by a TSP.

The ServingSystem message reports network registration events for PacketCable SIP clients, as well as PacketCable VCC subscriber UEs supported with a Cable Operators cellular HLR. ServingSystem message parameters reported for PacketCable VCC subscriber UEs provide equivalent information to parameters described in [J-STD-25b].

The ServingSystem message MUST include the  following information.

*Table 15 – ServingSystem Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| SystemIdentity | R | Provided to identify the serving system when the intercept subject is authorized for service by the TSP. When the serving system is a cellular system, a cellular network ID may be reported. |
| NetworkAddress | C | Present if available for circuit cellular and packet cellular clients. Used to identify visited network element information assisting registration, such as a packet cellular address.<br>This parameter is not present for SIP registration events. |
| RequestIdentity | C | Included to identify an address registration or deregistration request within a system, when available. This parameter is not present for cellular registration events. |
| AddressRegistrationType | C | Indicates whether an address registration, address deregistration, or both were detected. Provided when appropriate. This parameter is not present for cellular registration events. |
| ResisteringPartyIdentity | C | Identifies the party for whom address registration, deregistration, or both, are being attempted. Provided when appropriate. |
| RequestingPartyIdentity | C | Included to identify the party requesting the address registration, deregistration, or both, when different from the RegisteringPartyIdentity. This parameter is not present for cellular registration events. |
| RegistrarIdentity | C | Identifies the registrar to which the address registration request, deregistration request, or both, are destined. Provided when appropriate. This parameter is not present for cellular registration events. |
| RequestAddressInformation | C | Address information attempted to be registered, deregistered, or both, when present. This parameter is not present for cellular registration events. |
| ResponseAddressInformation | C | Address information included in the response to the attempt to register, deregister, or both register and deregister address information, when present. This parameter is not present for cellular registration events. |
| FailureReason | C | Included to indicate the reason that an address registration, deregistration, or both, were unsuccessful, when the registration, deregistration, or both are unsuccessful. This parameter is not present for cellular registration events. |
| ExpirationPeriod | C | Included to identify the address-independent registration lifetime applicable to the registered addresses, when known. This parameter is not present for cellular registration events. |

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

### 8.4.14  CCUnavailable

The CCUnavailable message shall be presented to the CF if the VoIP network is aware that the network does not have access to content for a call that is under content interception.

The CCUnavailable message MUST include the following information.

*Table 16 – CCUnavailable Message*

| Attribute Name | Required or Conditional | Comment |
|---|---|---|
| Case_ID | R | Identifies the Surveillance Subject. |
| Accessing Element ID | R | Identifies the accessing element. |
| Event Time | R | Identifies the date and time that the event was detected. |
| Call ID | R | Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message. |
| UnavailabilityReason | C | Include to indicate the reason that content was not available to the VoIP network, when known. |
| EncapsulatedSignalingMsg | R | The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject. |

## 8.5    CDC Messages and Parameter Definitions

This section provides ASN.1 definitions for the CDC Messages and associated parameters. Some of these definitions come from [J-STD-25b]. The Location attribute format is defined in Location Conveyance for the Session Initiation Protocol, [RFC 6442]. These definitions may contain terms, parameters, and values that are not currently used in this PacketCable specification, but are included in their entirety to ensure consistency with Electronic Surveillance solutions defined for other environments.

CDC messages and parameters MUST conform to the Distinguished Encoding Rules [ITU X.690]. This specification uses IMPLICIT tagging for more compact encoding.

```
PCESP  {iso(1) identified-organization(3) dod(6) internet(1) private(4)
        enterprise(1) cable-Television-Laboratories-Inc(4491) clabProject(2)
        clabProjPacketCable(2) pktcLawfulIntercept(5) pcesp(1) version-20(20)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

ProtocolVersion ::= ENUMERATED {
  -- Versions IO1 and IO2 do not support protocol versioning.
  v3(3),  -- Version supporting PacketCable Electronic Surveillance
          -- Specification I03
  v4(4),  -- Version supporting PacketCable Electronic Surveillance
          -- Specification I04 and PacketCable 1.5 Electronic Surveillance
          -- Specification I01
  v20(20), -- Version Supporting PacketCable Electronic Surveillance Specification
          -- IO1
```

```
   ...}

CdcPdu ::= SEQUENCE {
  protocolVersion       [0] ProtocolVersion,
  message               [1] Message,
  ...
}

Message ::= CHOICE {
  answer                [1]  Answer,
  ccclose               [2]  CCClose,
  ccopen                [3]  CCOpen,
  reserved4             [4]  NULL,                -- Reserved
  origination           [5]  Origination,
  reserved6             [6]  NULL,                -- Reserved
  redirection           [7]  Redirection,
  release               [8]  Release,
  servingSystem         [9]  ServingSystem,
  terminationattempt    [10] TerminationAttempt,
  reserved11            [11] NULL,                -- Reserved
  ccchange              [12] CCChange,
  reserved12            [13] NULL,                -- Reserved
  reserved14            [14] NULL,                -- Reserved
  dialeddigitextraction [15] DialedDigitExtraction,
  networksignal         [16] NetworkSignal,
  subjectsignal         [17] SubjectSignal,
  mediareport           [18] MediaReport,
  reserved19            [19] NULL,             -- Reserved
  reserved20            [20] NULL,             -- Reserved
  ccUnavailable         [21] CCUnavailable,
  ...
}

Answer ::= SEQUENCE {
  caseId            [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime         [2] EventTime,
  callId            [3] CallId,
  answering         [4] PartyId               OPTIONAL,
  signalingMsgs     [5] EncapsulatedSignalingMessages,
  ...
}

CCChange ::= SEQUENCE {
  caseId            [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime         [2] EventTime,
  callId            [3] CallId,
  cCCId             [4] EXPLICIT CCCId,
  subject           [5] SDP                    OPTIONAL,
  associate         [6] SDP                    OPTIONAL,
  flowDirection     [7] FlowDirection,
  resourceState     [8] ResourceState          OPTIONAL,
  signalingMsgs     [9] EncapsulatedSignalingMessages,

  ...
}

CCClose ::= SEQUENCE {
  caseId            [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime         [2] EventTime,
  cCCId             [3] EXPLICIT CCCId,
```

```
flowDirection       [4] FlowDirection,
signalingMsgs       [5] EncapsulatedSignalingMessages,
...
}

CCOpen ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  ccOpenOption        CHOICE {
     ccOpenTime       [3] SEQUENCE OF CallId,
     reserved0        [4] NULL,                 -- Reserved
     ...
                      },
  cCCId               [5] EXPLICIT CCCId,
  subject             [6] SDP                   OPTIONAL,
  associate           [7] SDP                   OPTIONAL,
  flowDirection       [8] FlowDirection,
  signalingMsgs       [9] EncapsulatedSignalingMessages,
  ...
}

CCUnavailable ::= SEQUENCE  {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  unavailabilityReason [4] VisibleString        OPTIONAL,
  signalingMsgs       [5] EncapsulatedSignalingMessages,
  ...
}

DialedDigitExtraction ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  digits              [4] VisibleString (SIZE (1..32, ...)),
                          -- string consisting of digits representing
                          -- Dual Tone Multi Frequency (DTMF) tones
                          -- having values from the following numbers,
                          -- letters, and symbols:
                          -- "0", "1", "2", "3", "4", "5", "6", "7",
                          -- "8", "9", "#", "*", "A", "B", "C", "D".
                          -- Example: "123AB" or "*66" or "345#"
  ...
}

MediaReport ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  subject             [4] SDP                   OPTIONAL,
  associate           [5] SDP                   OPTIONAL,
  signalingMsgs       [6] EncapsulatedSignalingMessages,

  ...
}

NetworkSignal ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
```

```
eventTime             [2] EventTime,
callId                [3] CallId,
                          -- Signal
                          -- The following three parameters are used to report
                          -- information regarding network-generated signals.
                          -- Include at least one of the following three
                          -- parameters to identify the network-generated signal
                          -- being reported.
alertingSignal        [4] AlertingSignal                      OPTIONAL,
featureSignal         [5] FeatureSignal                       OPTIONAL,
other                 [6] VisibleString (SIZE (1..128, ...))  OPTIONAL,
-- Can be used to report undefined network signals

signaledToPartyId     [7] PartyId,
signalingMsgs         [8] EncapsulatedSignalingMessages,
...
}

Origination ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  calling             [4] SEQUENCE OF PartyId OPTIONAL,
  called              [5] PartyId          OPTIONAL,
  input               CHOICE {
     userinput        [6] VisibleString  (SIZE (1..32, ...)),
     translationinput [7] VisibleString  (SIZE (1..32, ...)),
     ...
                      },
  location            [8] Location   OPTIONAL,
                          -- Include, when the location information is reasonably
                          -- available to the IAP and delivery is authorized,
                          -- to identify the location of an
                          -- intercept subject's terminal
  transitCarrierId    [9] TransitCarrierId  OPTIONAL,
  systemId            [10] SystemID,
  signalingMsgs       [11] EncapsulatedSignalingMessages,
  ...
}

Redirection ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  old                 [3] CallId,
  redirectedto        [4] PartyId,
  transitCarrierId    [5] TransitCarrierId    OPTIONAL,
  reserved0           [6] NULL,                -- Reserved
  reserved1           [7] NULL,                -- Reserved
  new                 [8] CallId              OPTIONAL,
  redirectedfrom      [9] PartyId             OPTIONAL,
  redirectionreason   [10] RedirectionReason,
  systemIdentity      [11] SystemIdentity,
  signalingMsgs       [12] EncapsulatedSignalingMessages,
  ...
}

Release ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
```

```
  releaseReason        [4] VisibleString,
  location             [5] Location                 OPTIONAL,
                           -- Include, when the location information is reasonably
                           -- available to the IAP and delivery is authorized,
                           -- to identify the location of an
                           -- intercept subject's terminal
  signalingMsgs        [6] EncapsulatedSignalingMessages,
  ...
}

ServingSystem ::= SEQUENCE  {
  caseId               [0] CaseId,
  accessingElementId   [1] AccessingElementId,
  eventTime            [2] EventTime,
  systemIdentity       [4] SystemIdentity,
  networkAddress       [5] VisibleString (SIZE (1..128)) OPTIONAL,
  requestId            [6] CallId                   OPTIONAL,
  registrationType     [7] AddressRegistrationType    OPTIONAL,
  registering          [8] PartyId                    OPTIONAL,
  requesting           [9] PartyId                    OPTIONAL,
  registrar            [10] PartyId                   OPTIONAL,
  requestAddressInfo   [11] CHOICE  {
     generic sequence  [0] SEQUENCE OF SEQUENCE  {
     address           [0] PartyId,
     expirationPeriod  [1] INTEGER -- in seconds
      },
      sip   [1] SET OF UTF8String
  }   OPTIONAL,

  responseAddressInfo  [12] CHOICE  {
     generic sequence  [0] SEQUENCE OF SEQUENCE  {
     address           [0] PartyId,
     expirationPeriod  [1] INTEGER   -- in seconds
     },
     sip               [1] SET OF UTF8String
  }                    OPTIONAL,
  failureReason        [13] UTF8String              OPTIONAL,
  expirationPeriod     [14] CHOICE  {
     generic sequence  [0] INTEGER,   -- for all addresses, in seconds,
     sip               [1] UTF8String
  }                    OPTIONAL,             -- maps SIP Expires header

  signalingMsgs        [15] EncapsulatedSignalingMessages,

  ...
}

SubjectSignal ::= SEQUENCE {
  caseId               [0] CaseId,
  accessingElementId   [1] AccessingElementId,
  eventTime            [2] EventTime,
  callId               [3] CallId                 OPTIONAL,
  signal               [4] SEQUENCE {
                           -- The following four parameters are used to report
                           -- information regarding subject-initiated dialing and
                           -- signaling. Include at least one of the following four
                           -- parameters to identify the subject- initiated dialing
                           -- and signaling information being reported.
  clientRequest            [0] ClientRequest                      OPTIONAL,
  dialedDigits             [1] VisibleString (SIZE (1..128, ...))  OPTIONAL,
  featureKey               [2] VisibleString (SIZE (1..128, ...))  OPTIONAL,
  otherSignalingInformation [3] VisibleString (SIZE (1..128, ...))  OPTIONAL,
                     -- Can be used to report undefined subject signals
```

```
    ...
                        },
  signaledFromPartyId [5] PartyId,
  signaledToPartyId   [6] PartyId                OPTIONAL,
  signalingMsgs       [7] EncapsulatedSignalingMessages,
    ...
}

TerminationAttempt ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  calling             [4] PartyId                OPTIONAL,
  called              [5] PartyId                OPTIONAL,
  reserved0           [6] NULL,                  -- Reserved
  redirectedFromInfo  [7] RedirectedFromInfo  OPTIONAL,
  location            [8] Location     OPTIONAL,
                          -- Include, when the location information is reasonably
                          -- available to the IAP and delivery is authorized,
                          -- to identify the location of an
                          -- intercept subject's terminal
  SystemID            [9] SystemId
  signalingMsgs       [10] EncapsulatedSignalingMessages,
    ...
}



-- Parameter Definitions

AddressRegistrationType ::= ENUMERATED {
      unknown                       (0),
      registration                  (1),
      deregistration                (2),
      registrationAndDeregistration  (3)
}


AccessingElementId ::= VisibleString (SIZE(1..15, ...))
                        --  Statically configured element number

-- This parameter identifies the type of alerting (ringing) signal that is
-- applied toward the surveillance subject. See GR-506-CORE, LSSGR: Signaling
-- for Analog Interfaces (A Module of the LATA Switching Systems Generic
-- Requirements [LSSGR], FR-64) [GR 506].

AlertingSignal ::= ENUMERATED  {
  notUsed             (0),  -- Reserved
  alertingPattern0    (1),  -- normal ringing
  alertingPattern1    (2),  -- distinctive ringing: intergroup
  alertingPattern2    (3),  -- distinctive ringing: special/priority
  alertingPattern3    (4),  -- distinctive ringing: electronic key
                            -- telephone srvc
  alertingPattern4    (5),  -- ringsplash, reminder ring
  reserved6           (6),  -- normal call waiting tone
  reserved7           (7),  -- incoming additional call waiting tone
  reserved8           (8),  -- priority additional call waiting tone
  reserved9           (9),  -- distinctive call waiting tone
  bargeInTone         (10), -- barge-in tone (e.g., for operator barge-in)
  alertingPattern5    (11), -- distinctive ringing: solution specific
  alertingPattern6    (12), -- distinctive ringing: solution specific
  alertingPattern7    (13), -- distinctive ringing: solution specific
```

```
  alertingPattern8       (14),  -- distinctive ringing: solution specific
  alertingPattern9       (15),  -- distinctive ringing: solution specific
  ...
}


CallId ::= SEQUENCE {
  sequencenumber  [0] VisibleString (SIZE(1..25, ...)),
  systemidentity  [1] SystemIdentity,
  ...
}
-- The Delivery Function generates this structure from the
-- Billing-Correlation-ID (contained in the Event Messages).
-- The sequencenumber is generated by converting the
-- Timestamp (32 bits) and Event-Counter (32 bits) into
-- ASCII strings, separating them with a comma.
-- The systemidentity field is copied from the
-- Element-ID field

SytemIdentity ::= CHOICE {
      UnknownLabel [0] VisibleString (SIZE (1..15))
            --Used for backwards compatibility.
      SystemIdentityType  [1] SystemIdentitytype
            --Used for reporting IP address formats and
      --reporting multiple identity types.
}

SystemIdentitytype ::= SEQUENCE {
      UnknownLabel [1] VisibleString (SIZE (1..15)) OPTIONAL,
      ipV4        [2] VisibleString (SIZE (1..15))  OPTIONAL,
      ipV6        [3] VisibleString (SIZE (1..128)) OPTIONAL,
      fqdn        [4] VisibleString    OPTIONAL,
            -- Fully Qualified Domain Name and the trailing ".". may not be included.
}

CaseId ::= VisibleString (SIZE(1..25, ...))

CCCId ::= CHOICE {
  combCCC             [0] VisibleString (SIZE(1..20, ...)),
  sepCCCpair          [1] SEQUENCE{
  sepXmitCCC          [0] VisibleString (SIZE(1..20, ...)),
  sepRecvCCC          [1] VisibleString (SIZE(1..20, ...)),
  ...
                        },
  ...
}
-- The Delivery Function MUST generate this structure
-- from the CCC-Identifier used for the corresponding
-- Call Content packet stream by converting the 32-bit
-- value into an 8-character (hex-encoded) ASCII string
-- consisting of digits 0-9 and letters A-F.

ClientRequest ::= ENUMERATED {
  refer                   (1),
  notifyForClientCallStatus (2),
  ...
}

EncapsulatedSignalingMessage ::= SEQUENCE {
    signalingProt           [0]  UTF8String,
                              -- Contains the MimeType registered for this signaling
                              -- protocol. If none is registered,
                              -- this field contains the value unknown
```

```
      sigMsg                   [1] OCTET STRING
}

EncapsulatedSignalingMessages ::= SET OF EncapsulatedSignalingMessage
-- It is defined as a SET to include all the buffered signaling messages.

EventTime ::= GeneralizedTime

FeatureSignal ::= ENUMERATED {
  mwiPerNotify              (1),
  notifyForFeatureActivation (2),
  notifyForAssociateCallState (3),
  refer                     (4),
  report200OKToPRACK        (5),
  ...
}


FlowDirection ::= ENUMERATED {
  downstream                (1),
  upstream                  (2),
  downstream-and-upstream   (3),
  ...
}

Location ::= SEQUENCE      {
  locationType   [0] UTF8String,
                 -- Examples for locationType: "SIP INVITE PANI-header,"
                   -- "SIP location header per Session Initiation Protocol Location
                   -- Conveyance, IETF RFC 6442 Location Conveyance for the Session
                   -- Initiation Protocol, December 2011.
                 -- "SIP location message body," "GPS Data," "Cellular Network"
  location       [1] UTF8String
                 -- location of the subject's terminal.
}

PartyId ::= SEQUENCE {
  reserved0           [0]  NULL              OPTIONAL, -- Reserved
  reserved1           [1]  NULL              OPTIONAL, -- Reserved
  reserved2           [2]  NULL              OPTIONAL, -- Reserved
  reserved3           [3]  NULL              OPTIONAL, -- Reserved
  reserved4           [4]  NULL              OPTIONAL, -- Reserved
  reserved5           [5]  NULL              OPTIONAL, -- Reserved
  dn                  [6]  VisibleString (SIZE(1..15, ...))  OPTIONAL,
  userProvided        [7]  VisibleString (SIZE(1..15, ...))  OPTIONAL,
  reserved6           [8]  NULL              OPTIONAL, -- Reserved
  reserved7           [9]  NULL              OPTIONAL, -- Reserved
  ipAddress           [10] VisibleString (SIZE(1..128, ...))  OPTIONAL,
  reserved8           [11] NULL              OPTIONAL, -- Reserved
  trunkId             [12] VisibleString (SIZE(1..32, ...))  OPTIONAL,
  reserved9           [13] NULL              OPTIONAL, -- Reserved
  genericAddress      [14] VisibleString (SIZE(1..128, ...))  OPTIONAL,
  genericDigits       [15] VisibleString (SIZE(1..32, ...))  OPTIONAL,
  genericName         [16] VisibleString (SIZE(1..48, ...))  OPTIONAL,
  port                [17] VisibleString (SIZE(1..32, ...))  OPTIONAL,
  context             [18] VisibleString (SIZE(1..32, ...))  OPTIONAL,
  uri                 [19] SET OF UTF8String              OPTIONAL,
  sipHeader           [20] SET OF SipHeader               OPTIONAL,
  nai                 [21] UTF8String                     OPTIONAL,
  mac802              [22] VisibleString                  OPTIONAL,
  fqdn                [23] UTF8String                     OPTIONAL,
}
```

```
RedirectedFromInfo ::= SEQUENCE {
  lastRedirecting        [0] PartyId            OPTIONAL,
  originalCalled         [1] PartyId            OPTIONAL,
  numRedirections        [2] INTEGER (1..100, ...)  OPTIONAL,
  ...
}


RedirectionReason ::= ENUMERATED {
  domain-Transfer-to-PacketCable-network    (0),
  domain-Transfer-from-PacketCable-network  (1),
  call-Forwarding-Variable                  (2),
  call-Forwarding-Do-Not-Answer             (3),
  call-Forwarding-on-Busy                   (4),
  selective-Call-Forwarding                 (5),
  other                                     (6),
  unknown                                   (7),
  ...
}

ResourceState ::= ENUMERATED {reserved(1), committed(2), ...}

SystemId ::= VisibleString (SIZE(1..25, ...))


SDP ::= UTF8String
-- The format and syntax of this field are defined in [8].

TransitCarrierId ::= VisibleString

END -- PCESP
```

# Annex A   PacketCable Specific Requirements

## A.1    Timing Requirements

Within a PacketCable environment, the timestamp in PCESP messages MUST have the same value as the timestamp in the correlation ID within the corresponding SIP signaling.

## A.2    DialedDigitExtraction CDC Message

In order to report post-cut-through digits to a LEA, the DF MUST instruct the CMTS, aggregation routers or MGWs (Call Content IAPs) to forward a copy of both the upstream and downstream RTP packets to the DF for pen-register intercepts for which the Dialed Digit Extraction feature is enabled. The CCIAPs MUST then forward the intercepted packets to the DF. However, the DF MUST instruct the CCIAPs to forward both the upstream and downstream packets to the DF for Call Content intercepts regardless of whether Dialed Digit Extraction feature is enabled or not.

If the Dialed Digit Extraction feature is enabled on the DF, the DF MUST decrypt network provided cryptology and decode the received upstream RTP packets, detect and extract any dialed digits that may be reported in the audio stream or as [RFC 4733] encoded packets, generate one or more DialedDigitExtraction CDC messages and send these messages to the Collection Function(s) related to the intercept as described in 6.4.6. If the DF receives DTMF digits in both the audio stream and in [RFC 4733] simultaneously for the same call, then the [RFC 4733] packets take precedence for delivery to the LEA.

The DF MUST forward the received RTP packets using G.711 μ-law coding to the Collection Function(s) related to the intercept if the intercept is of type call-content. For pen-register and trap-and-trace intercepts, the DF MUST NOT forward any received RTP packets to the Collection Function(s) regardless of whether Dialed Digit Extraction feature is enabled or not.

## A.3    Correlating Content Packets with Event Messages

Event messages relating to content channels sent to the DF contain a CCC_ID which is used to correlate with the CCC_ID contained in the content (CCC) streams. A DF MUST provide the CCC_ID to a CMTS and MGW. This CCC_ID will appear in the content streams if content replication has been enabled.

Each DF MUST dedicate a UDP port pair per domain (one port for CDC and one for CCC). If there is a single DF used for multiple domains, then the DF SHOULD uniquely identify and correlate the CCC and CDC messages by a combination of the CCC_ID and the port pair (which is unique per domain).

In the case where there is a different DF in each domain, the uniqueness is accomplished by ensuring that there is a unique UDP port pair used by the DF in receiving message for a given domain (e.g., one port pair for the domain the DF belongs to and one pair for each DF sending it messages from other domains).

## A.4    Timing Information

The PacketCable Electronic Surveillance Specification relies on multiple components (CSCFs, MGC, MG, DF) to gather and deliver call data and Call Content to the LEA. Once the call data and Call Content are delivered to the LEA, the LEA will rely on timestamps in the various messages to correlate the reported events. In order to ensure the LEA has sufficiently accurate timing information, PacketCable network elements that generate Event Messages (CSCFs, CMTS, MGC) or timestamp RTP packets (DF) MUST use Network Time Protocol (NTP) time synchronization as defined in [RFC 5905].

## A.5    Filtering CDC Events in Redirected (Forwarded) Calls

Using call-forward, the subject can forward a call to an associate, thus removing the subject from the call. The forwarded-to associate would then be under surveillance. In this scenario, it is usually not appropriate to deliver the complete set of call data events for the forwarded-to associate. For example, signals sent to the associate or received from the associate are generally not subject to surveillance. In most cases, it will only be appropriate under CALEA

to deliver some subset of call data events to the LEA. Therefore, the DF MUST support the ability to filter which call data events it reports to the LEA based on the following requirements.

The filter MUST be applied on a per-intercept basis. The filter MUST only apply when the DF is sending a message to the LEA. The filter MUST NOT apply when the DF is forwarding an EM to another DF.

When activated, the filter MUST allow only the following events to be reported to the LEA:

- Answer
- CCChange
- CCClose
- CCOpen
- CCUnavailable
- MediaReport
- Release
- TerminationAttempt
- Redirection

The DF MUST activate the filter when any one of the following conditions exist:

- The DF receives a CORRELATE message as well as a NOTIFY from the subject's S-CSCF indicating that the Call Forward feature has been invoked and the subject is listed as the party that is forwarding the call.
- The DF receives a SIP 302 from the subject's S-CSCF generated from the subject's client.

The filter remains active for the duration of the call. Interception of the associate in the forwarded call and the related filter ends when the forwarded call terminates.

Calls forwarded to a subject are not subject to the filter at the DF.

# Annex B  SIP Messages Mapped to PacketCable CDC Reports (informative)

## B.1    Message Mappings

This clause defines the mapping of SIP messages to surveillance messages defined in this specification. Table 17 identifies SIP message mappings when the subject originates a session. Table 18 identifies SIP message mappings when a session is terminated to the subject.

Mappings for the SIP protocol occur when the network's call processing equipment is in the path of the SIP signaling message exchange. These mappings do not apply when the network's call processing equipment is not in the path of the SIP signaling message exchange.

Note:  The SIP response "100 Trying" may be present in SIP call flows, depending upon the implementation in the CSCF, the User Agent, and the placement of the IAP. Reporting of the "100 Trying" to law enforcement is not required.

Portions of the mapping are consistent with SIP mapping found in ATIS-1000678.2006, Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2, [T1.678].

Note that a media report MUST be reported at the completion of an SDP offer/answer transaction. This can occur with a wide variety of SIP messages. Therefore, the media reports included in the tables below illustrate the process, but are not exhaustive.

*Table 17 – SIP Message Mapping - Subject Origination*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| INVITE | | Origination | Indication that a call has been initiated by the Subject. |
| | 180 Ringing | NetworkSignal (alerting) | Indication that an associate's device has been alerted. |
| | 181 Call is Being Forwarded | NetworkSignal (other) | Indication that the call has been forwarded by or on behalf of the associate. |
| | 200OK (to INVITE) | Answer<br>Media Report (if SDP offer/answer is complete) | Indication that the call has been answered. |
| | 3xx, 4xx, 5xx, 6xx | Release (with release reason/code) | Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 3xx, 4xx, 5xx, or 6xx). For 3xx redirection, the redirection information is also provided with the Release message. |
| ACK | | Media Report | When the ACK contains media information, the information is reported via the Media Report message. |
| BYE | | Release | Indication the call has been or is being released. |
| CANCEL (INVITE) | | none | The Subject requests a cancel of an INVITE request. |

*Table 18 – SIP Message Mapping - Subject Termination*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| | INVITE | TerminationAttempt | Indication there has been an attempt to terminate a call to the subject. |
| 180 ringing

181 forwarded | | SubjectSignal (otherSignalingInformation)
Redirection (forwarding) | Indication that the subject's device has been alerted.
Indication that the call attempt has been forwarded by or on behalf of the subject. |
| 200 OK (to INVITE) | | Answer
Media Report (if SDP offer/answer is complete) | Call is answered (by subject or agent). |
| 4xx, 5xx, 6xx | | Release | Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 4xx, 5xx, or 6xx). |
| 3xx | | Release | The original session is released.
The redirection information is provided in the Contact field of the Release message. |
| | ACK | Media Report | When the ACK contains media information, the information is reported via the media report. |
| | BYE | Release | Indication the call has been or is being released. |
| | CANCEL | none | An associate client has requested an INVITE request be cancelled. |

*Table 19 – SIP Message Mapping - Subject Registration*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| REGISTER | | ServingSystem | The subject requests registration of contact information. |
| | 200OK | ServingSystem | Include registration information. |
| | 4xx, 5xx | ServingSystem | Include failure reason. |

*Table 20 – SIP Message Mapping - REFER*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| REFER | | Subject Signal | The subject requests referral. |
| | REFER | Network Signal | The associate requests referral. |

*Table 21 – SIP Message Mapping - NOTIFY*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| NOTIFY | | Subject Signal | The subject reports notification. |
| | NOTIFY | Network Signal | The subject receives notification. |

*Table 22 – SIP Message Mapping - DirectSignalReporting Message*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| INVITE ACK BYE CANCEL REGISTER REFER NOTIFY MESSAGE | 1xx, 2xx, 3xx, 4xx, 5xx, 6xx | DirectSignalReporting | This optional CDC message is used to report signals not addressed elsewhere in this specification. |
| 1xx, 2xx, 3xx, 4xx, 5xx, 6xx | INVITE ACK BYE CANCEL REGISTER REFER NOTIFY MESSAGE | DirectSignalReporting | This optional CDC message is used to report signals not addressed elsewhere in this specification. |

*Table 23 – SIP Message Mapping - Client Executed Hold and Retrieve*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| Re-INVITE (hold) | | Media Report | Indicates that subject has requested inactive media to associate. |
| | 200 OK (to re-INVITE (hold)) | Media Report | Indicates the associate response to an inactive media request. |
| Re-INVITE (retrieve) | | Media Report | Indicates that the subject has requested active media to be resumed |
| | 200 OK (to re-INVITE (retrieve)) | Media Report | Indicates the associate response to a resume active media request. |
| | Re-INVITE (hold) | Media Report | Indicates that subject has received a request for inactive media from the associate. |
| 200 OK (to re-invite (hold)) | | Media Report | Indicates the subject response to an inactive media request. |

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| | Re-INVITE (retrieve) | Media Report | Indicates that the subject has received a request for active media to be resumed from the associate |
| 200OK (to re-INVITE (retrieve)) | | Media Report | Indicates that subject response to an active media resume request. |

Table 24 illustrates message mapping for subject client based conferencing. The initial condition assumed by the table is that the subject client is already active in a two way call. The table commences when the subject places the active call on hold. The subject then dials a third party and joins the two calls by mixing the voice at the client. Note that there is no network detected signal when the client initiates the voice mix.

*Table 24 – SIP Message Mapping - Client Based Conferencing*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| Re-INVITE | | | Indicates that subject has requested inactive media to associate. (The initial call is placed on hold). |
| | 200OK (to re-INVITE (hold)) | Media Report | Reports change in media if required. |
| Call Origination Sequence | | See Table 17 | The subject originates a second call, which is reported as a call origination as shown in Table 17. |
| Re-INVITE (retrieve) | | | The subject requests a conference, which is performed at the client. The message indicates that the held call is resumed as active prior to the conference mix at the client. Two active calls are now sent to the subject client. |
| | 200 OK (to re-INVITE (hold)) | Media Report | Reports change in media if required. |
| BYE | | Release | The subject ends the conference. BYEs are sent to end the call legs to associates. |

Table 25 illustrates message mapping for subject client based consultative transfer. The initial condition assumed by the table is that the subject client is already active in a two way call. Consultative transfer first establishes a 3-way call. After the subject hangs up, one associate is referred to the other to complete the transfer. The Table 25 commences when the subject places the active call on hold. The subject then dials a third party and joins the two calls by mixing the voice at the client. At this point a 3-way call is formed. Note that there is not a network detected signal when the client initiates the voice mix. The subject hangs up, which initiates the call transfer between the two associates via REFER. The two associates then proceed to set up a new call leg to complete the transfer.

*Table 25 – SIP Message Mapping - Client Based Consultative Transfer*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| 3-way call sequence | | See Table 24 | The subject UE begins an attendant call transfer by creating a client executed 3-way call. See Table 24 for the messages reported. |
| REFER | | Subject Signal | Subject hangs up and client call transfer is initiated. |
| | 202 Accepted | | |
| | NOTIFY | Network Signal | Subject is notified of completion of REFER. |
| BYE | | Release | Subject UE sends BYE to end dialog. |
| | REFER | Network Signal | Subject is recipient of transfer request. |
| Call Origination sequence | | See Table 17 | Subject places call after receiving REFER. |

Outbound Call Blocking (OCB) is a feature that is of interest to electronic surveillance only when the originator is a subject. This is because if the OCB call is not blocked (either do the dialed digits not being on the call blocked list or by the correct entering of an optional PIN) and the dialed digits route the call to a terminating subscriber that is a subject, this looks like any normal basic call termination to a subject. That mapping is already covered in Table 18.

OCB also makes use of the SIP capability of early media support in order to provide the necessary announcement prompts for the optional PIN as well as to indicate that the call was blocked if the dialed digits of the OCB originating subscriber appear in the blocked list. [T1.678] does not currently address any early media situations (e.g., PRACK, 183 Session Progress) so the mapping of these messages for this capability is proposed here in Table 26.

Table 26 shows all the possible outcomes of a call originated by a subject who also has the OCB feature. These are the digits dialed are on the blocked list and the outgoing call is then blocked, the digits dialed are on the blocked list and the subject does not correctly enter the optional override PIN (after an optional and administrable number of retries), and the digits dialed are on the blocked list and the subject correctly enters the optional override PIN so the call then completes like any other basic call that does not have any OCB interaction.

*Table 26 – SIP Message Mapping - Outbound Call Blocking*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| INVITE | | Origination | Indication that a call has been initiated by the Subject. |
| | 183 session progress | Media Report | When the 183 Session Progress contains media information, the information is reported via the Media Report message. |
| PRACK | | Media | When the PRACK contains media information, the information is reported via the Media Report message, i.e., the media information is different from the initial INVITE. |

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| | 200 OK (to PRACK) | Network Signal (other) | The 200 OK (to PRACK) indicates that the OCB announcement is being played and possibly requesting a PIN to be entered. The PIN is inband so no Surveillance message can collect this. The DF will have to detect the inband PIN that the subject dials so that a DialedDigitExtraction message can be generated, if DDE is active on that surveillance. |
| | | Media Report | When the 200 OK (to PRACK) contains media information, which it could if the PRACK contained media information, the information is reported via the Media Report message, i.e., the media information is different from the 183 Session Progress. |
| | 403 Forbidden | Release | This will be sent by the OCB AS when the digits dialed by the subject are on the call block list or if a PIN was requested and the PIN entered by the subject was invalid (this is only done after an optional number of administrable retries). |
| | 180 Ringing | NetworkSignal (alerting) | Indication that an associate's device has been alerted. Only occurs if the digits dialed were not on the call block list or if they were on the call block list the optional PIN was correctly entered. |
| | 181 Call Is Being Forwarded | NetworkSignal (other) | Indication that the call has been forwarded by or on behalf of the associate. Only occurs if the digits dialed were not on the call block list or if they were on the call block list the optional PIN was correctly entered. |
| | 200 OK (to INVITE) | Answer | Indication that the call has been answered. Only occurs if the digits dialed were not on the call block list or if they were on the call block list the optional PIN was correctly entered. |
| | 3xx, 4xx, 5xx, 6xx | Release (with release reason/code) | Indication that the call has been or is being released. Only occurs if the digits dialed were not on the call block list or if they were on the call block list the optional PIN was correctly entered. This is an alternative response from the associate instead of the 200 OK (to INVITE). The Release message indicates the reason for release (i.e., the SIP response code of 3xx, 4xx, 5xx, or 6xx). For 3xx redirection, the redirection information is also provided with the Release message. |

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| ACK | | None | For the OCB service the ACK from the subject only occurs upon the reception of a 403 Forbidden which can be the result of either the digits dialed by the subject being on the call block list or the optional PIN that was requested was incorrectly entered by the subject (this is only done after an optional number of administrable retries). The Release Surveillance message was already sent for this call upon the reception of the 403 Forbidden by the subject. |
| BYE | | Release | Indication the call has been or is being released, in this case by the subject. Only occurs if the digits dialed were not on the call block list or if they were on the call block list the optional PIN was correctly entered. |
| | BYE | None | Indication the call has been or is being released, in this case by the associate. Only occurs if the digits dialed were not on the call block list or if they were on the call block list the optional PIN was correctly entered. This will cause the subject to also send a BYE and thus the Release message as described above. |
| CANCEL (INVITE) | | None | The Subject requests a cancel of an INVITE request. |

Solicitor Call Block can have interactions with electronic surveillance either when the subject is the originator that dials a subscriber that has the solicitor block service or the subject is the terminating party of the call that has the also has the solicitor block service active. Thus two tables are shown for the mapping of the SIP messages to Surveillance Messages, one for when there is a subject origination and one for when there is a subject termination (similar to the two tables shown for a basic call mapping scenario earlier in this section).

As with the OCB feature, the Solicitor Block feature again makes use of SIP's early media capability. This is to provide announcements to prompt the caller to leave a greeting, then play back to the called party the recorded greeting of the caller and offer them the options of how to dispose of the call, and then the possible rejection of the call is also provided back to the caller. As with OCB because [T1.678] provides no guidance on the usage of early media the mapping of these messages for this capability is proposed here in the following two tables.

Table 27 shows all the possible outcomes of a call originated by a subject to a subscriber that has the solicitor block service active. This includes being prompted to leave a greeting, the called party accepting the call after listening to the recorded greeting, as well as the cases where either the called party rejects the call after hearing the greeting or the subject does not provide a greeting when prompted. Table 27 shows all the possible outcomes of a call termination to a subject that has the solicitor block service active. This includes listening to the recorded greeting and being given the options of how to proceed with the offered call, the case where the call is accepted by the subject after listening to the greeting, and the case where the call is rejected by the subject after listening to the greeting.

*Table 27 – SIP Message Mapping - Solicitor Call Blocking (Subject Origination)*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| INVITE | | Origination | Indication that a call has been initiated by the Subject. |
| | 183 Session Progress | Media Report | When the 183 Session Progress contains media information, the information is reported via the Media Report message. Can occur upon the initial Solicitor Block invocation and when the called party decides to reject the call after listening to the greeting recorded by the subject or the called party did not respond to the disposition request at all. |
| PRACK | | Media Report | When the 183 Session Progress contains media information, the information is reported via the Media Report message. Can occur upon the initial Solicitor Block invocation and when the called party decides to reject the call after listening to the greeting recorded by the subject or the called party did not respond to the disposition request at all. |
| | 200 OK (to PRACK) | Network Signal (other) | The 200 OK (to PRACK) indicates that the Solicitor Block announcement is being played. The first time it is received the announcement is requesting the subject to record a greeting. If it is received a second time, the subject will be getting an announcement that the called party has rejected their call either because the associate explicitly rejected the call or that no call disposition response had been received from the associate for the call. |
| | | Media Report | When the 200 OK (to the PRACK) contains media information, which it could if the PRACK contained media information, the information is reported via the Media Report message, i.e., the media information is different from the 183 Session Progress. |
| | 480 Unavailable | Release | This will be sent by the Solicitor Block AS when either the subject did not enter a greeting for delivery to the associate who has the Solicitor Call Block feature or if the called party has rejected their call either because the associate explicitly rejected the call or that no call disposition response had been received from the associate for the call. Indication that the call has been or is being released. The Release message indicates the reason for release. |
| | 200OK (to INVITE) | Answer | Indication that the call has been answered. Only occurs if the called party (the associate) accepts the call after listening to the subject's recorded greeting. NOTE: That the flow for this feature never has the subject getting an indication that the called party is alerting so no NetworkSignal is generated as there is for the normal basic call. |

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| | 3xx, 4xx, 5xx, 6xx | Release | Indication that the call has been or is being released. Only occurs if the called party (the associate) accepts the call after listening to the subject's recorded greeting. This is an alternative response from the associate instead of the 200 OK (to INVITE). The Release message indicates the reason for release (i.e., the SIP response code of 3xx, 4xx, 5xx, or 6xx). For 3xx redirection, the redirection information is also provided with the Release message. |
| ACK | | Media Report | When the ACK contains media information, the information is reported via the Media Report message. Only occurs if the called party (the associate) accepts the call after listening to the subject's recorded greeting |

*Table 28 – SIP Message Mapping - Solicitor Call Blocking (Subject Termination)*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| | INVITE | TerminationAttempt | Indication there has been an attempt to terminate a call to the subject. This INVITE is sent by the Solicitor Block AS to the subject and will have early media being set up. |
| 180 ringing | | SubjectSignal (otherSignalingInformation) | Indication that the subject's device has been alerted. |
| 181 forwarded | | Redirection (forwarding) | Indication that the call attempt has been forwarded by or on behalf of the subject. |
| 200 OK (to INVITE) | | Answer | Call is answered (by subject or agent). This is the early media but it is still the official answer of this call termination. |
| 4xx, 5xx, 6xx | | Release | Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 4xx, 5xx, or 6xx). Possible subject response instead of the 200 OK (to INVITE) and the 200 OK (to INVITE (2)) below. |
| 3xx | | Release | The original session is released. The redirection information is provided in the Contact field of the Release message. Possible subject response instead of the 200 OK (to INVITE) and the 200 OK (to INVITE (2)) below. |

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| | ACK (to 200 OK (to INVITE)) | Network Signal (other) | The ACK indicates that a Solicitor Call Blocking announcement is being played, i.e., the recorded greeting of the caller and a request as to how to dispose of the call. The call disposition is signaled inband by the subject so there is no SIP message that captures this for changing into a Surveillance message. The DF will have to detect the inband digit dialed indicating the subject's selection so that a DialedDigitExtraction message can be generated, if DDE is active on that surveillance. |
| | | Media Report | When the ACK contains media information, which it could if the 200 OK (to INVITE) contained media information, the information is reported via the Media Report message, i.e., the media information is different from the initial INVITE. |
| | INVITE(2) | Media Report | This INVITE contains the media information for the real calling party. This only occurs if the subject accepts the call after hearing the greeting recorded by the caller. |
| 200 OK (to INVITE (2) | | Media Report | When the 200 OK (to INVITE (2)) contains media information, the information is reported via the Media Report message. This only occurs if the subject accepts the call after hearing the greeting recorded by the caller, i.e., the media information is different from the 200 OK (to INVITE). |
| | ACK (to 200 OK (to INVITE (2))) | Media Report | When the ACK (to 200 OK (to INVITE (2))) contains media information, the information is reported via the Media Report message, i.e., the media information is different from INVITE (2). This only occurs if the subject accepts the call after hearing the greeting recorded by the caller. |
| BYE | | Release | This can occur if the subject rejects the call after hearing the caller's recorded greeting. It can also occur at the end of the call after the subject accepts the call upon hearing the caller's recorded greeting and the subject is initiating the call clearing. |
| | BYE | None | Indication the call has been or is being released., initiated by the associate in this instance and only occurs if the subject accepts the call after hearing the greeting recorded by the caller. This will cause the subject to send a BYE and thus the Release message as described above. |
| | Cancel (INVITE) | None | An associate has requested an INVITE request be cancelled. |

Automatic Recall (AR) allows a UE to automatically call back the last calling address that sent an INVITE to this UE, whether the INVITE was answered by this client or not. The AR feature should work even when the last call received at the client did not supply a caller ID. The feature is activated by the subject after the original call attempt

and is executed by the UE. The following table illustrates the electronic surveillance reports when a subject has activated Auto Recall to an associate who is currently busy. An initial call is attempted to the associate, who is busy. The subject then subscribes to the dialog event package of the associate to be notified when the associate becomes idle. The subject is notified of the associate's call state. The subject's UE then automatically places a call to the associate when the associate becomes idle. Table 29 illustrates the surveillance message mapping for the auto recall feature. The initial conditions for the table are subject has received a call attempt to an associate and the subsequently activated the feature with a star code that is consumed by the client.

*Table 29 – SIP Message Mapping - Auto Recall*

| SIP Message Sent by Subject | SIP Message Received by Subject | Surveillance Message | Description |
|---|---|---|---|
| INVITE | | Origination | Indication that a call has been initiated by the subject |
| | 486 Busy | Release | Indicates associate is busy |
| | NOTIFY | NetworkSignal | Indicates subject has received event package requested in prior subscribe. Call status of associate is included in this case. (This assumes NOTIFY is associated with a telephony service, although the network may not be able to tell if the NOTIFY is related to a telephony service.) |
| | 180 Ringing | NetworkSignal (alerting) | Indication that an associate's device has been alerted. |
| | 200OK (to INVITE) | Answer | Indication that the call has been answered. |
| | 3xx, 4xx, 5xx, 6xx | Release | Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 3xx, 4xx, 5xx, or 6xx). For 3xx redirection, the redirection information is also provided with the Release message. |
| ACK | | Media Report | When the ACK contains media information, the information is reported via the Media Report message. |
| BYE | | Release | Indication the call has been or is being released. |
| CANCEL (INVITE) | | None | The Subject requests a cancel of an INVITE request. |

Automatic Callback (AC) allows a UE to automatically call back the last called address whether the INVITE was answered by the called party or not. The feature is activated after an initial call origination and is executed by the UE. The execution of the feature is similar to that of Auto Recall. The UE places a call to the associate and automatically subscribes to a UA profile event package if the associate is busy. The UE places a second call to the associate once the associate become idle. The message mapping is identical to Auto Recall as shown in Table 29 above. The initial conditions prior to Table 29 in this case are the subject has placed a call attempt to an associate and subsequently has activated the feature with a star code that is consumed by the client.

Table 30 illustrates message mapping for domain transfer events (from the circuit cellular domain to the packet cable domain) associated with a subject who is a VCC subscriber. The initial condition assumed by the table is that the subject is in the circuit cellular domain and is already active in a two way call. It is assumed that the UE was previously registered in both the CS and PacketCable domains (i.e., UE is dual-registered). If the UE is not already registered in the PacketCable domain, PacketCable registration procedures are first invoked and a ServingSystem surveillance message will be sent. The table commences when the subject UE initiates domain transfer from the circuit cellular domain to the packet cable domain by sending an INVITE with VDI.

*Table 30 – SIP Message Mapping - Domain Transfer from Circuit
Cellular Domain to Packet Cable Domain*

| Message received by VCC AS | Message sent by VCC AS | Surveillance Message | Description |
|---|---|---|---|
| INVITE with VDI | re-INVITE sent toward the remote party | none | Indication that domain transfer from the circuit cellular domain to the packet cable domain is required, and to modify the bearer path from the subject UE to the remote party. |
|  | 200OK (response to re-INVITE sent toward the remote party) | Redirection with Redirection Reason parameter coded as "Domain Transfer to PacketCable network" | Indication that domain transfer has successfully occurred. |
|  | BYE toward subject UE | none | To release the original CS bearer channel to the UE. |

Table 31 illustrates message mapping for domain transfer events (from the packet cable domain to the circuit cellular domain) associated with a subject who is a VCC subscriber. The initial condition assumed by the table is that the subject is in the packet cable domain and is already active in a two way call. It is assumed that the UE was previously registered in both the CS and PacketCable domains (i.e., UE is dual-registered). If the UE is not already registered in the CS domain, CS registration procedures are first invoked and a ServingSystem surveillance message will be sent. The table commences when the subject UE initiates domain transfer from the packet cable domain to the circuit cellular domain by sending a CS domain SETUP message with VDN.

*Table 31 – Message Mapping - Domain Transfer from Packet Cable Domain to Circuit Cellular Domain*

| Message received by VCC AS | Message sent by VCC AS | Surveillance Message | Description |
|---|---|---|---|
| CAMEL/WIN Query with VDN |  | none | Indication that domain transfer from the packet cable domain to the circuit cellular domain is required. |
| SIP INVITE on behalf of subject UE | SIP re-INVITE sent toward the remote party | none | To modify the bearer path from the subject UE to the remote party for domain transfer. |
| SIP 200OK (response to re-INVITE sent toward the remote party) |  | Redirection with Redirection Reason parameter coded as "Domain Transfer from PacketCable network" | Indication that domain transfer has successfully occurred. |
|  | SIP BYE to subject UE | none | To release the original PC bearer channel to the UE. |

# Appendix I    Acknowledgements

We wish to thank the participants contributing directly to this document:

# Appendix II    Revision History

The following Engineering Change Notice was incorporated in PKT-SP-ES-DCI-I02-070924.

| ECN | ECN Date | Summary |
| --- | --- | --- |
| ES-DCI-N-07.0414-1 | 5/21/07 | Updates to add IPv6 |

The following Engineering Change Notices were incorporated in PKT-SP-ES-DCI-I03-130219

| ECN | ECN Date | Summary |
| --- | --- | --- |
| ES-DCI-N-11.0658-4 | 8/22/2011 | Domain transfer and additional updates |
| ES-DCI-N-12.0693-2 | 1/21/2013 | PartyId Reporting |
| ES-DCI-N-12.0694-1 | 1/21/2013 | TCP Option for CC Delivery to CF |

The following Engineering Change Notices were incorporated in PKT-SP-ES-DCI-C01-140314

| ECN | ECN Date | Summary | Author |
| --- | --- | --- | --- |
| ES-DCI-N-13.0698-1 | 1/27/2014 | Delivery of associate CC during subject-initiated call hold | Robert Forsythe |
| ES-DCI-N-14.0701-1 | 3/10/2014 | CaseID added to intercepted traffic | Bernie McKibben |