PacketCable™ 1.5 Specifications

Electronic Surveillance

PKT-SP-ESP1.5-C01-191120

CLOSED

Notice

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 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-ESP1.5-C01-191120			
Document Title:	Electronic Surveillance			
Revision History:	I01 — Issued January 28, 2005 I02 — Issued April 12, 2007 C01 — Released November 20, 2019			
Date:	November 20, 2019			
Status:	~~Work in Progress~~	~~Draft~~	~~Issued~~	**Closed**
Distribution Restrictions:	~~Focus Team Only~~	~~CL/ Member~~	~~CL/ PacketCable/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 generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Table of Contents

List of Figures

List of Tables

.

1 INTRODUCTION AND BACKGROUND

1.1 Scope

This specification defines the interface between a telecommunications carrier that provides telecommunications services to the public for hire using PacketCable™ capabilities (a "PC/TSP") and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. Companies using PacketCable capabilities will not in the normal case be "telecommunications carriers." Instead they will be providers of information services. However, some companies using PacketCable capabilities may, by virtue of other actions, be "telecommunications carriers" for purposes of the Communications Assistance for Law Enforcement Act (CALEA) with respect to their use of PacketCable capabilities. The purpose of this specification is to assist those companies in meeting their obligations under CALEA. In this regard, a telecommunications carrier 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.

As noted, cable operators are not ordinarily telecommunications carriers, but if a cable operator has taken the steps to become a carrier, and uses PacketCable to provide carrier services, then CALEA might apply to the equipment used to implement PacketCable. For this reason, we are providing consideration of CALEA concerns as part of the PacketCable specification, for the benefit of anyone who might use this architecture/technology as part of their carrier activities.

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 to a LEA when authorized.

1.2 Requirement Language

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

"MUST"	This word or the adjective "REQUIRED" 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 or the adjective "RECOMMENDED" 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 weighted before implementing any behavior described with this label.
"MAY"	This word or the adjective "OPTIONAL" 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 October 1994. It requires telecommunications carriers and manufacturers to provide certain capabilities to LEAs with the proper court authorization. Although a cable operator may not have any obligations under CALEA, a cable operator that has taken steps to become a telecommunications carrier, and uses PacketCable capabilities to provide telecommunications services (as used here, a PC/TSP) that is found in compliance 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, when designing a surveillance protocol, it is prudent to consider and incorporate CALEA requirements.

Although CALEA may not apply to any particular cable operator, in general, it requires certain telecommunications carriers 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.
5. 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 [19] for lawfully authorized electronic surveillance for traditional voice telephony. However, the electronic surveillance features and capabilities for traditional voice telephony provided for in [19] are not readily applicable to telephony provided by means of a cable system, including telephony provided using PacketCable capabilities.[1] Accordingly, CableLabs has produced this specification for electronic surveillance specific to telephony services provided by cable operators which are acting as telecommunications carriers and performing their carrier functions using PacketCable capabilities.

1.4 Electronic Surveillance Assumptions

CALEA 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. Approximately 90% of all surveillance orders are of the first two types; Federal law and laws of 42 states only allow the use of the third technique in the investigation of serious criminal offenses, and when other techniques have not worked, will not work, or are too dangerous.

[1] Although the specifications and requirements of [19] are not applicable to PacketCable-based telephony, the focus group preparing this specification sought to employ similar messaging, where possible, so as 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 [19], employing different parameters and being triggered by different events.

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.[2] 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 would prohibit 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 Call Management System to establish the communication, and utilize enhanced Quality of Service as authorized by the Call Management System, 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. Other than the packets identified in the first sentence of this paragraph, packets sent or received by the intercept subject are considered Information Services.

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 touching 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 not required to deliver call content for the associate to the LEA while the associate is on hold. However, depending on implementation, the PC/TSP might deliver this call content to the LEA.

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

[2] To obtain a court order authorizing the interception of a wire or electronic communication, a law enforcement officer must submit a written application to a court of competent jurisdiction. The application must include information such as the identity of the officer making the application, a complete statement of facts supporting the application, a statement of whether other investigative procedures have been tried and failed or of why they appear reasonably unlikely to succeed or are too dangerous to attempt, and a statement of the period of time for which the interception is required (18 U.S.C. 2518(1)).

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 telecommunications carriers that use PacketCable capabilities to provide telecommunications services. In the absence of these formal capacity requirements, CableLabs has had to make certain reasonable assumptions about capacity in order 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 on 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 (with resulting delays and lost effort in the design and development of equipment consistent with this standard).

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 a maximum of five surveillance orders 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, (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 Definitions and Acronyms

AF: Access Function

ANSI: American National Standards Institute.

Associate: a telecommunication user whose equipment, facilities, or services are communicating with a subject.

CALEA: Communications Assistance for Law Enforcement Act.

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 MTA that 1) makes a request to the proper Call Management System 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 Call Management System 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-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.

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.

CCC: Call Content Connection

CDC: Call Data Connection

CF: Collection Function

CMS: 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.

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."

Controlling Party: the party invoking a feature.

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 [13] to be "a party or place to which a call is being made (*e.g.*, the called party)."

DF: Delivery Function.

***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 [13] 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)."

DOCSIS®: Data Over Cable Service Interface Specification. A set of standards produced by CableLabs that define methods and procedures for use of cable networks to provide information services.

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 herein, also includes the acquisition of call-identifying information. As used in this specification, surveillance 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."

IAP: Intercept Access Point.

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 CMS designated by the PC/TSP which processes calls for the subject.

Intercept Subject: see Subject.

IP: Internet Protocol.

Law Enforcement Agency: a government entity with the legal authority to conduct electronic surveillance.

LEA: Law Enforcement Agency.

LEAF: Law Enforcement Administration Function.

MTA: Multi-media terminal adapter.

Origin: defined in [13] to be "a party initiating a call (*e.g.*, a calling party), or a place from which a call is initiated."

Party hold, join, drop on conference calls: The capability that permits a LEA to identify the parties to a subject-initiated conference call conversation at all times.

PC/TSP: 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.

PCESP: PacketCable Electronic Surveillance Protocol.

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."

POTS: Plain Old Telephone Service. This usually refers to loop start lines with DTMF (tone) dialing or decadic (rotary) dialing.

PSTN: Public Switched Telephone Network.

QoS: Quality of Service.

Reasonably Available: is defined in the Commission's Third Report and Order [14]. 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, or when the terminating subscriber's line is busy, or when the terminating subscriber doesn't answer.

SPAF: Service Provider Administration Function.

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: within this specification surveillance refers to electronic surveillance; see Electronic Surveillance.

Surveillance Subject: See Subject.

TCP: Transmission Control Protocol.

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." Some entities that use PacketCable to provide telecommunications to customers may be "telecommunications carriers" for purposes of CALEA. 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 [13] 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 Device: 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."

TSP: Telecommunication Service Provider. Some TSPs may also be "telecommunications carriers" for purposes of CALEA. See Telecommunications Carrier and PC/TSP.

Unobtrusive: not undesirably noticeable or blatant; inconspicuous; within normal call variances.

U.S.C.: United States Code.

Wire Communications: 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."

2 REFERENCES

2.1 Normative

In order to claim compliance 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. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

[1] IETF RFC 768/ST0006, User Datagram Protocol, August 1980.

[2] IETF RFC 791/STD0005, Internet Protocol, September 1981.

[3] IETF RFC 793/STD0007, Transmission Control Protocol, September 1981.

[4] IETF RFC 826/STD0037, November 1982.

[5] IETF RFC 894/STD0041, Standard for the Transmission of IP Datagrams over Ethernet Networks, 1984.

[6] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996.

[7] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January 1996.

[8] IETF RFC 2327, SDP: Session Description Protocol, April 1998.

[9] 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.

[10] ITU-T Recommendation X.690 (07/02): Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

[11] IETF RFC 1305, Network Time Protocol (Version 3), Specification, Implementation and Analysis, March 1992.

2.2 Informative Reference

[12] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-C01-050907, September 7, 2005, Cable Television Laboratories, Inc.

[13] FCC 02-108, CC Docket No. 97-213, *Order on Remand,* April 11, 2002.

[14] FCC 99-230, CC Docket No. 97-213, *Third Report and Order,* August 31, 1999.

[15] PacketCable 1.5 Audio/Video Codecs Specification, PKT-SP-CODEC1.5-C01-191120, November 20, 2019, Cable Television Laboratories, Inc.

[16] PacketCable 1.5 Event Message Specification, PKT-SP-EM1.5-C01-191120, November 20, 2019, Cable Television Laboratories, Inc.

[17] PacketCable 1.5 Network-Based Call Signaling Protocol Specification, PKT-SP-NCS1.5-C01-191120, November 20, 2019, Cable Television Laboratories, Inc.

[18] PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-C01-191120, November 20, 2019, Cable Television Laboratories, Inc.

[19] ANSI/J-STD-025-A-2003, Lawfully Authorized Electronic Surveillance, April 17, 2003.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone 303-661-9100; Fax 303-661-9199; Internet: http://www.cablelabs.com
- IETF RFCs available at http://www.ietf.org/rfc.html
- FCC available at http://www.fcc.gov
- ISO available at http://www.iso.ch/iso/en/CatalogueListPage.CatalogueList
- ANSI available at http://webstore.ansi.org
- ITU available at http://www.itu.int/ITU-T/publications/index.html

3 ELECTRONIC SURVEILLANCE IN THE PACKETCABLE NETWORK

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

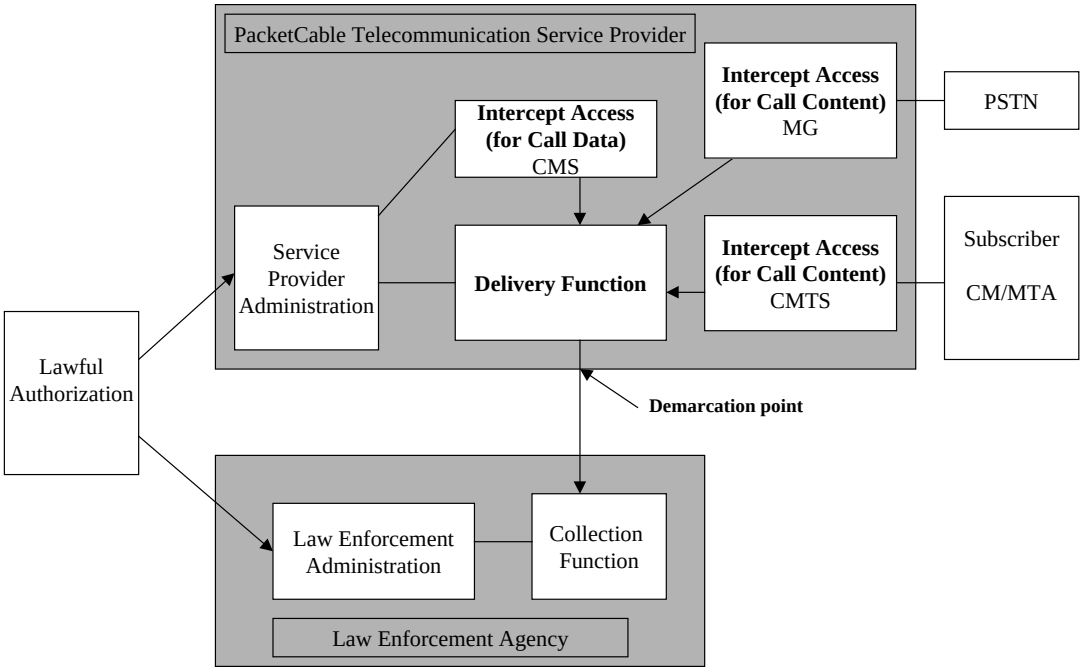

Figure 1 - Electronic Surveillance Model

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.

3.1 Subscriber equipment

The core of providing all PacketCable services, including any telecommunications services that a provider might offer, is the broadband access network. This network is characterized as a DOCSIS® [12] access network, but may be provided over access networks supporting other standards. The access network consists of the cable modem, the cable modem termination system, 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 Cable Modem (CM) and the Multi-media Terminal Adapter (MTA).

The CM is a PacketCable 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 MTA is a single hardware device that incorporates audio and optionally video IP telephony. An MTA may optionally incorporate a DOCSIS cable modem (an Embedded MTA) or may connect through external means to a DOCSIS cable modem (a Standalone MTA).

An MTA supports the following functionality:

- provides one or more RJ11 interfaces to 2500-series phones
- performs call signaling with the CMS to originate and terminate calls
- supports QoS signaling with the CMS and the CMTS
- supports security signaling with the CMS and other MTA 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 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. While this "future-proofing" is a goal of the design, we recognize that it leaves open a wide range of fraud possibilities. The basic assumption is that the MTA is not immune to customer tampering, and that the significant incentive for free service will lead to some very sophisticated attempts to thwart any network controls placed on the MTA.

Under these circumstances, it is important to realize that an MTA 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 MTA.

3.2 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, four 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 Call Management System (CMS) which provides service to the subscriber. The CMS 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 CMS), and call-identifying information reasonable 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 CMS/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).

3.3 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 call-identifying information and call content based on the requirements of the lawful authorization. The Delivery Function includes the ability to:

- collect and deliver call content and reasonably available call-identifying information for each intercept subject over the procured law enforcement facilities
- ensure that the call content and call-identifying information delivered from the Delivery Function is authorized for a particular LEA
- protect (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 call content and reasonably available call-identifying information using the PCESP protocol
- support environments with multiple CMSs, 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

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 call-identifying information, such as the calling party identities and called party identities.

Call-identifying information, call content, 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. The Delivery Function duplicates the call content, call-identifying information, or both, and deliver authorized information to each LEA.

Call-identifying information, call content, or both, from multiple surveillances may need to be delivered simultaneously to a single LEA's CF.

3.4 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.

3.5 Collection Function (CF)

The Collection Function is responsible for collecting intercepted communication and call-identifying information 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.

3.6 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.

4 INTERFACE BETWEEN THE DELIVERY FUNCTION (PC/TSP) AND 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 call content and call-identifying information 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 is 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 call content or call-identifying information, 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.

4.1 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.

4.2 Network Layer Interface

The network layer protocol for delivery of both CDC and CCC information MUST be as defined by the Internet Protocol (IP) [2]. The transport protocol for CDC information is as specified in Section 6, while transport of CCC information is as specified in Section 5. 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.

Contained in the IP header is the source IP address, which is the address of the DF, and 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.

4.3 Link-layer Interface

The default link-layer protocol between the DF and CF MUST be as defined by the Ethernet protocol [5] and [4]. However, alternate link-layer protocols MAY be used at the discretion of the PC/TSP based on negotiated agreements with the LEA.

4.4 Physical Interface

The default type of physical interconnect provided by the PC/TSP at the demarcation point MUST be an RJ45 10/100BaseT [9] connection. However, alternate physical interconnects MAY be provided at the discretion of the PC/TSP.

4.5 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.

5 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 Law Enforcement's Collection Function (CF).

The CCC datagrams MUST contain a timestamp that allows Law Enforcement 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.

Call Content MUST be delivered as a stream of UDP/IP datagrams, as defined in [1]and [2], sent to the port number at the CF as provided during provisioning of the interception. The UDP/IP payload MUST adhere to the following format:

Table 1 - Payload of Call Content Connection Datagrams

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

The Timestamp MUST adhere to the NTP time format as defined in [11]: 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 will be of the following format:

Table 2 - Intercepted Information

Original IP Header (20 bytes)
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.

5.1 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 Law Enforcement Agency.

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) [8] 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.

5.2 Original IP Header

This is the IP header [2], 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.

5.3 Original UDP Header

This is the User Datagram Protocol (UDP) header [1], 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.

5.4 Original RTP Header

This is the Real-Time Transport Protocol (RTP) header [6], 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 [7] and is referenced in the Session Description (SDP) [8].

5.5 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 [18] Keying material is contained in the Session Description (SDP) [17], and the algorithm to generate the actual key is described in [18].

Encoding of the voice may be done through use of one of the IETF's defined CODEC algorithms (as defined in [) or through a dynamic payload type defined in the Session Description (SDP) [8]. Definition of CODEC algorithms is contained in [15].

5.6 Transcoding

[14] 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. For example, the G.711 encoding algorithm is acceptable for use in transcoding content originally encoded in the G.728 or G.729E algorithms. If transcoding is performed, G.711(μ-law) MUST be used to transcode G.728, G.729E, iLBC(15.2), iLBC(13.3), and BV16. RFC2833 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. The DF MUST support the ability to disable transcoding on a per-intercept basis.

6 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 [3] 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 Appendix 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.[3] 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.

6.1 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 shall 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.

[3] In addition, when a subject has redirected a call (especially when the call is redirected through several other locations that are the subject of surveillance) there may be delays in delivering both CCC and CDC traffic that will exceed 8 seconds. In these cases, the PC/TSP will deliver the relevant information as soon as reasonably practicable.

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

ConferencePartyChange

A third, or more additional parties are added to an existing call to form a conference call, or any party in a conference call is placed on hold, or retrieved from hold.

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 or via a call transfer

Release

The resources for a call under surveillance have been released.

ServiceInstance

The IAP detects that a defined service event has occurred.

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.

6.2 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 dial tone (originating call) and ringing (terminating call) towards the surveillance subject, and the SubjectSignal message might be generated for an event such as fax tone detection.

6.2.1 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 communication intercept order, nine call-identifying messages are generated for delivery to the LEA - Origination, CCOpen, (downstream), CCOpen (upstream), Answer, CCChange (downstream), CCChange (upstream), CCClose (downstream), CCClose (upstream), 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.

6.2.2 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 communication interception order, nine call-identifying messages are generated for delivery to the LEA - TerminationAttempt, CCOpen (downstream), CCOpen (upstream), Answer, CCChange (downstream), CCChange (upstream), CCClose (downstream), CCClose (upstream), 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.

6.3 Specific Call Services

The following sections address a set of specific services offered by a PC/TSP and identify the information, in the form of CDC messages, that are sent to a LEA when the services are invoked by a subscriber under surveillance.

In addition to the CDC messages described in this section, other CDC messages might be generated as a result of events that occur during the use of specific call services.

6.3.1 Call Hold

Information about held two-way calls is available in the PacketCable environment when the surveillance subject signals requests to the CMS to place a call on hold and to retrieve a call from hold. In these cases, SubjectSignal messages are generated for delivery to LEA. If a call is being intercepted under a communication 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.

6.3.2 Call Redirection

Call redirection is invoked when a call attempts to terminate to a surveillance subject, the CMS determines that the subject has subscribed to special call handling services, and the conditions for feature invocation are met.[4] 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 communication interception order),
- CCOpen (upstream, if communication interception order),
- Answer (if redirected call is answered by redirected-to party),
- CCChange (downstream, if communication interception order),
- CCChange (upstream, if communication interception order),
- CCClose (downstream, if communication interception order),
- CCClose (upstream, if communication interception order), and
- 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 communication interception order),
- CCOpen (upstream, for the original call, if communication interception order),
- NetworkSignal (for ringing [if not busy]),
- CCClose (downstream, for the original call, if communication interception order),

[4] 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.

- CCClose (upstream, for the original call, if communication interception order),
- Redirection (to identify the redirection event and the redirected-to party),
- CCOpen (downstream, if communication interception order),
- CCOpen (upstream, if communication interception order),
- Answer (if redirected call is answered by redirected-to party),
- CCChange (downstream, if communication interception order),
- CCChange (upstream, if communication interception order),
- CCClose (downstream, if communication interception order),
- CCClose (upstream, if communication interception order), and
- 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, an additional Redirection messages MAY be generated for the second redirection.

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

6.3.3 Call Waiting

If a subject subscribes to call-waiting service, he/she may be engaged in a communication and be alerted by another termination attempt. The subject can switch back and forth between the two calls by using the flash hook. For call waiting, the two calls behave as two separate calls and would follow the basic call procedures described in Sections 6.2.1 and 6.2.2, as appropriate. In addition, a ServiceInstance message may be sent indicating that the Call Waiting service has been invoked.

If the subject toggles back and forth between the calls, alternately placing one associate on hold and communicating with the other, the LEA notification is as given for held calls described in Section 6.3.1.

6.3.4 Call Transfer

Two different services may be offered to PacketCable subscribers for call transfer. The first, called *blind transfer*, allows a party of an active call to redirect their end of the call to another party and immediately drop out, whether the redirected call completes or not. This is typically done by switchboard operators, and is also performed internally within a PacketCable network in implementing other services.

The second type of call transfer, called *consultative transfer*, is a variant of three-way-calling, where the three-way call first established, then the initiator drops out and the remaining parties are directly connected.

A blind transfer occurs only on an active call, i.e., one that has already generated a Origination or TerminationAttempt, Answer, and (if a communication interception order) CCOpen (downstream), CCOpen (upstream), CCChange (downstream), and CCChange (upstream) messages to LEA. When performed by a surveillance subject on an active call, the blind transfer may result in the following call-identifying messages:

- Redirection (to identify the redirection event and the redirected-to party),
- CCClose (downstream, of the old connection, if communication interception order),
- CCClose (upstream, of the old connection, if communication interception order),
- Release (of the old connection),
- TerminationAttempt (of the new connection at the redirected-to party),

- CCOpen (downstream, of the new connection, if communication interception order),
- CCOpen (upstream, of the new connection, if communication interception order),
- Answer (if redirected call is answered by redirected-to party),
- CCChange (downstream, of the new connection, if communication interception order),
- CCChange (upstream, of the new connection, if communication interception order)

When a blind transfer of a call under surveillance is performed by a subscriber not under surveillance, the following sequence of call-identifying messages is an example of what may be sent to the LEA:

- CCClose (downstream, of the old connection, if communication interception order),
- CCClose (upstream, of the old connection, if communication interception order),
- Release (of the old connection),
- CCOpen (downstream, of the new connection, if communication interception order),
- CCOpen (upstream, of the new connection, if communication interception order),
- Answer (if redirected call is answered by redirected-to party,
- CCChange (downstream, of the new connection, if communication interception order),
- CCChange (upstream, of the new connection, if communication interception order)

A consultative transfer results in the same sequence of call-identifying messages as three-way calling, as is described in the next section, up until the point where the initiator disconnects.

For example, consider party A being a surveillance subject, and establishing the three-way call with parties B and C.

When the MTA performs the bridging function, and the initiator disconnects, the following sequence of call-identifying messages is an example of what may be sent to the LEA:

- CCClose (downstream, of the call between A and B, if communication interception order),
- CCClose (upstream, of the call between A and B, if communication interception order),
- Release (of the call between A and B),
- Redirection (of the call between A and C, redirected-from A, redirected-to B),
- CCClose (downstream, of the call between A and C, if communication interception order),
- CCClose (upstream, of the call between A and C, if communication interception order),
- Release (of the call between A and C),
- TerminationAttempt (at C, of the new call between B and C),
- CCOpen (downstream, of the new call between B and C, if communication interception order),
- CCOpen (upstream, of the new call between B and C, if communication interception order),
- Answer (of the new call between B and C),
- CCChange (downstream, of the new call between B and C, if communication interception order),
- CCChange (upstream, of the new call between B and C, if communication interception order)

When a bridge service is used, the initiator disconnects, and the bridge is removed from the connection, the following sequence of call-identifying messages is an example of what may be sent to the LEA:

- CCClose (downstream, of the call between A and bridge, if communication interception order),
- CCClose (upstream, of the call between A and bridge, if communication interception order),
- Release (of the call between A and bridge),
- CCClose (downstream, of the call between B and bridge, if communication interception order),
- CCClose (upstream, of the call between B and bridge, if communication interception order),
- Release (of the call between B and bridge),
- Redirection (of the call between C and bridge, redirected-from bridge, redirected-to B),
- CCClose (downstream, of the call between C and bridge, if communication interception order),
- CCClose (upstream, of the call between C and bridge, if communication interception order),
- Release (of the call between C and bridge),
- TerminationAttempt (at B, of the new connection between C and B),
- CCOpen (downstream, of the new call between B and C, if communication interception order),
- CCOpen (upstream, of the new call between B and C, if communication interception order),
- Answer (of the new call between B and C),
- CCChange (downstream, of the new call between B and C, if communication interception order),
- CCChange (upstream, of the new call between B and C, if communication interception order)

6.3.5 Three-Way Calling

Three-way calling, or ad-hoc conferencing, is implemented in two different ways in a PacketCable network, by either the MTA performing the bridging function itself, or through the use of a bridge service. 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 both cases, 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.

Note that the sequence of messages depends on how the feature is implemented within the PC/TSP's network. The messages may vary with different implementations.

When the MTA 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.

When a bridge service is used, the CDC will indicate a new call placed by party A to a bridge service, generating the sequence of call-identifying messages as described in Section 6.2.1. The two previous calls (between A and B, and between A and C) are redirected from A to the bridge service. The following sequence of call-identifying messages is an example of what may be sent to the LEA:

- ServiceInstance (to identify that the three-way call service has been invoked),
- CCClose (downstream, of the call between A and B, if communication interception order),
- CCClose (upstream, of the call between A and B, if communication interception order),

- Release (of the call between A and B),
- CCClose (downstream, of the call between A and C, if communication interception order),
- CCClose (upstream, of the call between A and C, if communication interception order),
- Release (of the call between A and C),
- Redirection (of the call between A and B, redirected-from A, redirected-to bridge),
- TerminationAttempt (at bridge, of call from B to bridge),
- CCOpen (downstream, of the new call between B and bridge, if communication interception order),
- CCOpen (upstream, of the new call between B and bridge, if communication interception order),
- Answer (of the new call between B and bridge),
- CCChange (downstream, of the new call between B and bridge, if communication interception order),
- CCChange (upstream, of the new call between B and bridge, if communication interception order),
- Redirection (of the call between A and C, redirected-from A, redirected-to bridge),
- TerminationAttempt (at bridge, of call from C to bridge),
- CCOpen (downstream, of the new call between C and bridge, if communication interception order),
- CCOpen (upstream, of the new call between C and bridge, if communication interception order),
- Answer (of the new call between C and bridge),
- CCChange (downstream, of the new call between C and bridge, if communication interception order),
- CCChange (upstream, of the new call between C and bridge, if communication interception order).

There are now three separate calls. In this particular implementation, under an interception order, there may now be three separate call content packet streams delivered to LEA, and all will contain the mixed conversations. If the initiator of a three-way call disconnects, all three calls to the bridge terminate. When one participant of a three-way call disconnects, a redirect may result, causing one of the two calls to be redirected to the remaining party, and the other call released. If party C were the one to disconnect, the following sequence of call-identifying messages is an example of what would be sent to LEA:

- CCClose (downstream, of the call between C and bridge, if communication interception order),
- CCClose (upstream, of the call between C and bridge, if communication interception order),
- Release (of the call between C and bridge),
- CCClose (downstream, of the call between A and bridge, if communication interception order),
- CCClose (upstream, of the call between A and bridge, if communication interception order),
- Release (of the call between A and bridge),
- CCClose (downstream, of the call between B and bridge, if communication interception order),
- CCClose (upstream, of the call between B and bridge, if communication interception order),
- Release (of the call between B and bridge),
- Redirection (of the call between A and bridge, redirected-from bridge, redirected-to B),
- TerminationAttempt (at B, of new call between A and B),
- CCOpen (downstream, of the new call between A and B, if communication interception order),
- CCOpen (upstream, of the new call between A and B, if communication interception order),

- Answer (of the new call between A and B),
- CCChange (downstream, of the new call between A and B, if communication interception order),
- CCChange (upstream, of the new call between A and B, if communication interception order).

6.3.6 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 ServiceInstance 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.

6.3.7 Repeat Call

For the Repeat Call feature, the code dialed by the subscriber to invoke the feature and the resulting called party number are delivered to the LEA in an Origination message. A ServiceInstance may be generated when the service is invoked. Typically, this call does not complete, due to the destination being busy.

Implementation of repeat call is done two ways in a PacketCable network, either by the CMS or the MTA performing the function. In either case, repeated call attempts are made to the called party until he answers, or a time limit is exceeded. Each of these call attempts to the terminating party will be treated as a basic originating call, as described in Section 6.2.1, therefore no unique interactions exist for the resulting calls.

6.3.8 Return Call

For the Return Call feature, the code dialed by the subscriber to invoke the feature and the resulting called party number (the last incoming calling number) is delivered to the LEA in an Origination message. The new call originated by the CMS to the last calling party is a basic call as described in Section 6.2.1, therefore no unique interactions exist for the resulting call, except that a ServiceInstance may be generated when the service is invoked.

6.3.9 911 Emergency and N11 Services

911 emergency and N11 service calls are viewed as normal call originations and the description in Section 6.2.1, 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.

6.3.10 Mid-Call CODEC Change

During a call established by the PacketCable CMS, the endpoints may decide (based on recognition of a modem or fax tone, or other conditions) that the previously negotiated coding style 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 [8] of the media flows.

6.3.11 Post-Cut-Through Dialing

When a call is connected to a TSP’s service for processing and routing, the surveillance subject could dial or signal 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.

6.4 CDC Message Descriptions

The messages that identify the call events, described in Section 5.1, 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 Optional. Required fields MUST always be included. Optional fields MUST be included when available.

6.4.1 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
- 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 include the following information.

Table 3 - Answer Message

Attribute Name	Required or Optional	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	O	Include to identify the destination of the call, if different that the called party id, when known. 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.

6.4.2 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 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 Optional	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	O	The Session Descriptor Protocol (SDP) information for the subject endpoint (downstream direction), if it is changed.
Associate_SDP	O	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. MUST be present value of CCC_ID.
Resource_State	O	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).

6.4.3 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.

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

Table 5 - CCClose Message

Attribute Name	Required or Optional	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).

6.4.4 CCOpen

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

- resources are reserved on the HFC access network
- in the case of an off-net call, either the send or send/receive 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 Optional	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	O	The Session Descriptor Protocol (SDP) information for the subject endpoint (downstream).
Associate_SDP	O	The Session Descriptor Protocol (SDP) information for the associate endpoint (upstream).
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).

6.4.5 ConferencePartyChange

The ConferencePartyChange message reports a change to the status of the parties in a subject-initiated conference call, when this information is known at the IAP. The ConferencePartyChange message reports the following conditions:

1. when the subject adds a third, or additional parties, to an existing call to form a conference call (regardless of whether the subject initiated or terminated the existing call),
2. when a party in a subject-initiated conference call is placed on hold, or retrieved from hold,

Note that the Release message is used to indicate when a party in a subject-initiated conference call is dropped, released, or otherwise disconnects from the conference call.

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

- The subject adds a third, or additional parties, to an existing to call to form a conference call
- A party in a subject-initiated conference call is placed on hold
- A party in a subject-initiated conference call is retrieved from hold

The ConferencePartyChange message MUST include the following information,

Table 7 - ConferencePartyChange Message

Attribute Name	Required or Optional	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.
Communicating	O	Included when known, to identify all communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service. This parameter may appear independently or in combination with other parameters.
Removed	O	Included when known, to identify a previously communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service; the identity(ies) is removed (e.g., hold service) from a call. This parameter may appear independently or in combination with other parameters.
Joined	O	Included when known, to identify a new communicating call identity(ies), party identity(ies), or both on the identified conference call established by the intercept subject's service; the joined identity(ies) has begun communicating on the call. This parameter may appear independently or in combination with other parameters.

6.4.6 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 filled, 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.

Only digits dialed by a surveillance subject are subject to Dialed Digit Extraction. Digits dialed by the associate(s) are not subject to Dialed Digit Extraction.

The DialedDigitExtraction message MUST be generated when the surveillance subject dials or signals digits after a call is connected to a 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 is performed and the first 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 8 - DialedDigitExtraction Message

Attribute Name	Required or Optional	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".

6.4.7 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 channel.
- New SDP is received for an open media channel.

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

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

Table 9 - MediaReport Message

Attribute Name	Required or Optional	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	O	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	O	The call identifying information from the SDP for the associate endpoint (upstream direction), if an associate's SDP is being reported in the message.

6.4.8 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 Appendix A for PacketCable-specific requirements.

The NetworkSignal message MUST include the following information.

Table 10 - NetworkSignal Message

Attribute Name	Required or Optional	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.
Signaled_To_Party_ID	R	Include to identify the signaled-to party.
Signal	R	AlertingSignal, SubjectAudibleSignal, terminalDisplayInfo, and/or Other.
One or more of the following:		

Attribute Name	Required or Optional	Comment
AlertingSignal	O	
SubjectAudibleSignal	O	
TerminalDisplayInfo	O	
Other	O	

6.4.9 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. 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 include the following information.

Table 11 - Origination Message

Attribute Name	Required or Optional	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 translation was completed.
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	R	Include to identify the originating party.
Called_Party_ID	O	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.
User_Input	O	The digits input by the user.
Translation_Input	O	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	O	Include when a transit carrier is used to transport the call.

6.4.10 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, or by his initiating a call transfer.

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 by the subject's service to another destination
- an incoming call to a surveillance subject is transferred by the subject's action to another destination
- a call originated by a surveillance subject is transferred by the originating surveillance subject to another destination

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

The Redirection message MUST include the following information.

Table 12 - Redirection Message

Attribute Name	Required or Optional	Comment
Case_ID	R	Identifies the Surveillance subject.
Accessing_System_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	O	Included when the redirected call will be identified by a different Call-ID in future CDC messages.
Redirected_from_Party_ID	O	Identifies the redirected-from party.
Redirected_to_Party_ID	R	Identifies the redirected-to party (redirected-to or transferred-to party).
Transit_Carrier_ID	O	Include when a transit carrier is used to transport the redirected call.

6.4.11 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 TerminationAttempt event, when one of the following events is detected by an IAP:

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

The Release message MUST include the following information.

Table 13 - Release Message

Attribute Name	Required or Optional	Comment
Case_ID	R	Identifies the Surveillance subject.
Accessing_Sytem_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.

6.4.12 ServiceInstance

The ServiceInstance message reports when an IAP has detected a defined service event.

The ServiceInstance message MUST be generated when an IAP has detected a defined service event unless the information reported would be redundant with the information reported by other CDC messages (e.g., Origination message when the Return Call feature is invoked as described in Section 6.3.8).

The ServiceInstance message MUST include the following parameters:

Table 14 - ServiceInstance Message

Attribute Name	Required or Optional	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.
Related_Call_ID	O	Used to correlate the different calls for Call_Forward, Call_Waiting, and Three_Way_Call.
Service_Name	R	The Service_Name Attribute MUST be present. Class Service_Name: • Call_Block • Call_Forward • Call_Waiting • Repeat_Call • Return_Call • Three_Way_Call
First_Call_Calling_Party_Number	O	Indicates the number of the first calling party for Call_Waiting.
Second_Call_Calling_Party_Number	O	Indicates the number of the second calling party for Call_Waiting.
Called_Party_Number	O	Indicates the number of the called party for Call_Waiting.
Calling_Party_Number	O	Indicates the number of the calling party for Repeat_Call or Return_Call.

6.4.13 SubjectSignal

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, call waiting, call hold, three-way calling).

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 Appendix A for PacketCable-specific requirements.

The SubjectSignal message MUST include the following information.

Table 15 - SubjectSignal Message

Attribute Name	Required or Optional	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	O	Uniquely identifies a call within a system, if the dialing or signaling occurs within a call.
Signaled_From_Party_ID	R	Include to identify the signaled-from party.
Signal	R	SwitchhookFlash, DialedDigits, and/or OtherSignalingInformation
One or more of the following:		
SwitchhookFlash	O	
DialedDigits	O	
OtherSignalingInformation	O	

6.4.14 TerminationAttempt

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

The TerminationAttempt message MUST include the following information.

Table 16 - TerminationAttempt Message

Attribute Name	Required or Optional	Comment
Case_ID	R	Identifies the Surveillance subject.
Accessing_Sytem_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 TerminationAttempt is message is used to correlate the other messages.
Calling_Party_ID	O	Identifies the originating party, when available.
Called_Party_ID	O	Include if more specific than the surveillance subject identity (surveillance subject DN) associated with the Case_ID.
Redirected_From_Info	O	Include if information about previous redirections for the incoming call is available to the IAP

6.5 CDC Messages and Parameter Definitions

This section provides ASN.1 definitions for the CDC Messages and associated parameters. Some of these definitions come from [19]. 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 [10]. This specification uses IMPLICIT tagging for more compact encoding.

The following defines the PCESP messages:

```
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-4(4)}

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
  ...}

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

Message ::= CHOICE {
  answer                  [1]  Answer,
  ccclose                 [2]  CCClose,
  ccopen                  [3]  CCOpen,
  reserved0               [4]  NULL,                -- Reserved
  origination             [5]  Origination,
  reserved1               [6]  NULL,                -- Reserved
  redirection             [7]  Redirection,
  release                 [8]  Release,
  reserved2               [9]  NULL,                -- Reserved
  terminationattempt      [10] TerminationAttempt,
  reserved                [11] NULL,                -- Reserved
  ccchange                [12] CCChange,
  reserved3               [13] NULL,                -- Reserved
  reserved4               [14] NULL,                -- Reserved
  dialeddigitextraction   [15] DialedDigitExtraction,
  networksignal           [16] NetworkSignal,
  subjectsignal           [17] SubjectSignal,
  mediareport             [18] MediaReport,
  serviceinstance         [19] ServiceInstance,
  confpartychange         [20] ConferencePartyChange,
  ...
}

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

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,
  ...
}

CCClose ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  cCCId               [3] EXPLICIT CCCId,
  flowDirection       [4] FlowDirection,
  ...
}

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,
  ...
}

ConferencePartyChange  ::= SEQUENCE {
  caseId             [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime          [2] EventTime,
  callId             [3] CallId,
  communicating      [4] SEQUENCE OF SEQUENCE {
                         -- include to identify parties participating in the
                         -- communication.
    partyId [0] SEQUENCE OF PartyId OPTIONAL,
                -- identifies communicating party identities.
    cCCId   [1] EXPLICIT CCCId OPTIONAL,
                -- included when the content of the resulting call is
                -- delivered to identify the associated CCC(s).
    ...
                      } OPTIONAL,
  removed            [5] SEQUENCE OF SEQUENCE {
                       -- include to identify parties removed (e.g., hold
                       -- service) from the communication.
    partyId [0] SEQUENCE OF PartyId OPTIONAL,
                -- identifies removed party identity(ies).
    cCCId   [1] EXPLICIT CCCId OPTIONAL,
                -- included when the content of the resulting call is
                -- delivered to identify the associated CCC(s).
    ...
                      } OPTIONAL,
  joined             [6] SEQUENCE OF SEQUENCE{
                         -- include to identify parties newly added to the
                         -- communication.
```

```
    partyId [0] SEQUENCE OF PartyId OPTIONAL,
                -- identifies newly added party identity(ies) to an existing
                -- communication.
    cCCId   [1] EXPLICIT CCCId OPTIONAL,
                -- included when the content of the resulting call is
                -- delivered to identify the associated CCC(s).
    ...
                     } OPTIONAL,
  ...
}

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,
  ...
}

NetworkSignal ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
                      -- Signal
                      -- The following four parameters are used to report
                      -- information regarding network-generated signals.
                      -- Include at least one of the following four
                      -- parameters to identify the network-generated signal
                      -- being reported.
  alertingSignal       [4] AlertingSignal                      OPTIONAL,
  subjectAudibleSignal [5] AudibleSignal                       OPTIONAL,
  terminalDisplayInfo  [6] TerminalDisplayInfo                 OPTIONAL,
  other                [7] VisibleString (SIZE (1..128, ...))  OPTIONAL,
  -- Can be used to report undefined network signals
  signaledToPartyId    [8] PartyId,
  ...
}

Origination ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  calling             [4] PartyId,
```

```
  called              [5] PartyId           OPTIONAL,
  input               CHOICE {
  userinput             [6] VisibleString  (SIZE (1..32, ...)),
  translationinput      [7] VisibleString  (SIZE (1..32, ...)),
  ...
                      },
  reserved0           [8] NULL,             -- Reserved
  transitCarrierId    [9] TransitCarrierId  OPTIONAL,
  ...
}

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,
  ...
}

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

ServiceInstance ::= SEQUENCE {
  caseId              [0] CaseId,
  accessingElementId  [1] AccessingElementId,
  eventTime           [2] EventTime,
  callId              [3] CallId,
  relatedCallId       [4] CallId               OPTIONAL,
  serviceName         [5] VisibleString (SIZE (1..128, ...)),
  firstCallCalling    [6] PartyId              OPTIONAL,
  secondCallCalling   [7] PartyId              OPTIONAL,
  called              [8] PartyId              OPTIONAL,
  calling             [9] PartyId              OPTIONAL,
  ...
}

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.
  switchhookFlash           [0] VisibleString (SIZE (1..128, ...))  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,
  ...
}

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,
  ...
}

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

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
  callWaitingPattern1   (6),   -- normal call waiting tone
  callWaitingPattern2   (7),   -- incoming additional call waiting tone
  callWaitingPattern3   (8),   -- priority additional call waiting tone
  callWaitingPattern4   (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
  ...
}
-- 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).

AudibleSignal ::= ENUMERATED {
  notUsed                  (0),  -- Reserved
  dialTone                 (1),
  recallDialTone           (2),  -- recall dial tone, stutter dial tone
  ringbackTone             (3),  -- tone indicates ringing at called party
                                 -- end
  reorderTone              (4),  -- reorder tone, congestion tone
  busyTone                 (5),
  confirmationTone         (6),  -- tone confirms receipt and processing of
                                 -- request
  expensiveRouteTone       (7),  -- tone indicates outgoing route is
                                 -- expensive
  messageWaitingTone       (8),
  receiverOffHookTone      (9),  -- receiver off-hook tone, off-hook warning
                                 -- tone
  specialInfoTone          (10), -- tone indicates call sent to announcement
  denialTone               (11), -- tone indicates denial of feature request
```

```
  interceptTone             (12), -- wireless intercept/mobile reorder tone
  answerTone                (13), -- wireless service tone
  tonesOff                  (14), -- wireless service tone
  pipTone                   (15), -- wireless service tone
  abbreviatedIntercept      (16), -- wireless service tone
  abbreviatedCongestion     (17), -- wireless service tone
  warningTone               (18), -- wireless service tone
  dialToneBurst             (19), -- wireless service tone
  numberUnObtainableTone    (20), -- wireless service tone
  authenticationFailureTone (21), -- wireless service tone
  ...
}
-- This parameter identifies the type of audible tone 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), ANSI/TIA/EIA-41-D, Cellular Radiotelecommunications
-- Intersystem Operations, and GSM 02.40, Digital cellular telecommunications
-- system (Phase 2+); Procedure for call progress indications.

CallId ::= SEQUENCE {
  sequencenumber  [0] VisibleString (SIZE(1..25, ...)),
  systemidentity  [1] VisibleString (SIZE(1..15, ...)),
  ...
}
-- 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

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.

EventTime ::= GeneralizedTime

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

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..32, ...))  OPTIONAL,
  reserved8            [11] NULL               OPTIONAL, -- Reserved
  trunkId              [12] VisibleString (SIZE(1..32, ...))  OPTIONAL,
  reserved9            [13] NULL               OPTIONAL, -- Reserved
  genericAddress       [14] VisibleString (SIZE(1..32, ...))  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,
  ...
}

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

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

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

TerminalDisplayInfo ::= SEQUENCE {
  generalDisplay         [0] VisibleString (SIZE (1..80, ...))  OPTIONAL,
    -- Can be used to report display-related
    -- network signals not addressed by
    -- other parameters.
  calledNumber           [1] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  callingNumber          [2] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  callingName            [3] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  originalCalledNumber   [4] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  lastRedirectingNumber  [5] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  redirectingName        [6] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  redirectingReason      [7] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  messageWaitingNotif    [8] VisibleString (SIZE (1..40, ...))  OPTIONAL,
  ...
}
-- This parameter reports information that is displayed on the surveillance
-- subject's terminal. See GR-506-CORE, LSSGR: Signaling for Analog
-- Interfaces (A Module of the LATA Switching Systems Generic Requirements
-- [LSSGR], FR-64).

TransitCarrierId ::= VisibleString (SIZE(3..7, ...))

END -- PCESP
```

Appendix A PACKETCABLE-SPECIFIC REQUIREMENTS

This appendix contains 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 corresponding Event Message (i.e., Event_time and Time Zone; refer to [16]).

A.2 DialedDigitExtraction CDC Message

In order to report post-cut-through digits to law enforcement, the CMS MUST instruct the CMTS 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 CMTS MUST then forward the intercepted packets to the DF. However, the CMS MUST instruct the CMTS 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 and decode the received upstream RTP packets, detect and extract any dialed digits that may be reported in the audio stream or as RFC 2833 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.

The DF MUST forward the received RTP packets 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 NetworkSignal CDC Message

The following table contains a mapping between NCS [17] signals and the NetworkSignal message. The CMS (IAP) MUST generate and format a NetworkSignal message according to the following table when the CMS applies any of the following NCS signals to the MTA (subject to section 6.4.8).

Table 17 - Mapping of NCS signals to NetworkSignal message

Code	Description (Name)	Comments	Encoding Requirements
0-9,*,#, A,B,C,D	DTMF tones	The NetworkSignal message is generated when DTMF tones are *signaled toward* the intercept subject (as a Signal). The NetworkSignal message is not generated when DTMF tones are *signaled by* the intercept subject (as an Event). The Origination or SubjectSignal message is generated in the latter case.	Encode in: other Value is the set of signaled tones (e.g., “12013452367”, “*123”).
bz	Busy tone		Encode in: subjectAudibleSignal busyTone
cf	Confirmation tone		Encode in: subjectAudibleSignal confirmationTone

Code	Description (Name)	Comments	Encoding Requirements
ci (ti, nu, na)	Caller Id	The NetworkSignal message contains the calling party number and calling party name, when signaled.	For ci/nu (calling party number) and ci/na (calling party name): If signal includes a calling number, terminalDisplayInfo:callingNumber = number If signal indicates privacy ("P") for calling number, terminalDisplayInfo:callingNumber = "private" If signal indicates unavailability ("O") for calling number, terminalDisplayInfo:callingNumber = "unavailable" If signal does not include anything (number, P or O) for calling number, terminalDisplayInfo:callingNumber is not included in NetworkSignal message If signal includes calling name, terminalDisplayInfo:callingName = name If signal indicates privacy ("P") for calling name, terminalDisplayInfo:callingName = "private" If signal indicates unavailability ("O") for calling name, terminalDisplayInfo:callingName = "unavailable" If signal does not include anything (name, P or O) for calling name, terminalDisplayInfo:callingName is not included in NetworkSignal message
dl	Dial tone	The NetworkSignal message is generated when the *immediate* generation of dial tone is requested. The NetworkSignal message is not generated when the *conditional future* (e.g., upon off-hook transition) generation of dial tone is requested.	Encode in: subjectAudibleSignal dialTone
mwi	Message waiting indicator		Encode in: subjectAudibleSignal messageWaitingTone
ot	Off-hook warning tone		Encode in: subjectAudibleSignal receiverOffHookTone
r0	Distinctive ringing (0)		Encode in: alertingSignal alertingPattern5
r1	Distinctive ringing (1)		Encode in: alertingSignal alertingPattern6

Code	Description (Name)	Comments	Encoding Requirements
r2	Distinctive ringing (2)		Encode in: alertingSignal alertingPattern1
r3	Distinctive ringing (3)		Encode in: alertingSignal alertingPattern2
r4	Distinctive ringing (4)		Encode in: alertingSignal alertingPattern3
r5	Distinctive ringing (5)		Encode in: alertingSignal alertingPattern7
r6	Distinctive ringing (6)		Encode in: alertingSignal alertingPattern8
r7	Distinctive ringing (7)		Encode in: alertingSignal alertingPattern9
rg	Ringing		Encode in: alertingSignal alertingPattern0
ro	Reorder tone		Encode in: subjectAudibleSignal reorderTone
rs	Ringsplash		Encode in: alertingSignal alertingPattern4
rt	Ring back tone		Encode in: subjectAudibleSignal ringbackTone
sl	Stutter dial tone	The NetworkSignal message is generated when the *immediate* generation of stutter dial tone is requested. The NetworkSignal message is not generated when the *conditional future* (e.g., upon off-hook transition) generation of dial tone is requested.	Encode in: subjectAudibleSignal recallDialTone
vmwi	Visual message waiting indicator	A NetworkSignal message is generated when the visual message waiting indicator is turned on and when it is turned off.	Encode in: terminalDisplayInfo messageWaitingNotif Value is “VMWI ON” when the indicator is turned on. Value is “VMWI OFF” when the indicator is turned off.
wt1	Call waiting tones		Encode in: alertingSignal ca1lWaitingPattern1
wt2	Call waiting tones		Encode in: alertingSignal callWaitingPattern2
wt3	Call waiting tones		Encode in: alertingSignal callWaitingPattern3
wt4	Call waiting tones		Encode in: alertingSignal callWaitingPattern4

A.4 SubjectSignal CDC Message

The following table contains a mapping between NCS [17] signals and the SubjectSignal message. The CMS (IAP) MUST generate and format a SubjectSignal message according to the following table when the CMS receives any of the following events from the MTA (subject to section 6.4.13):

Table 18 - Mapping of NCS signals to SubjectSignal message

Code	Description (Name)	Comments	Encoding Requirements
0-9,*,#,A,B,C,D	DTMF tones	When DTMF tones are *signaled by* the intercept subject (as an Event), the Origination message could be generated instead of the SubjectSignal message. The SubjectSignal message is not generated when DTMF tones are *signaled toward* the intercept subject (as a Signal). The NetworkSignal message is generated in this latter case.	Encode in: signal dialedDigits Value is the set of signaled tones (e.g., "12013452367", "*123").
ft	Fax tone		Encode in: signal otherSignalingInformation Value is "FAX TONE".
hf	Flash hook		Encode in: signal switchhookFlash Value is "FLASHHOOK".
mt	Modem tones		Encode in: signal otherSignalingInformation Value is "MODEM TONE".
TDD	Telecomm Devices for the Deaf (TDD) tones		Encode in: signal otherSignalingInformation Value is "TDD TONE".

A.5 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 CMS will provide the CCC_ID to a CMTS as one of the Electronic Surveillance parameters in a DQOS Gate-Set message. This CCC_ID will appear in the content streams if content replication has been enabled (i.e., with the DUP-CONTENT flag in the Electronic Surveillance DQOS Parameters being set). The CCC_ID will also appear in the QoS_Reserve, QoS_Commit and QoS_Release messages sent to the DF (i.e., if the DUP-EVENT flag is set). A CMS will also provide the CCC_ID in Media_Report messages in order to ensure that the DF can correlate the (CCC) content streams with the corresponding (CDC) event messages that relate to content intercepts.

Similarly, an MGC selects the CCC_ID that it sends when it requests content interception at a PSTN Gateway and will use the CCC_ID in event messages that are related to content streams, in order to provide the appropriate correlation between the event messages and content streams.

MGC's and CMS's MUST ensure that the CCC_ID is unique for those content channels being intercepted at a given point in time within a given domain. The Element-ID MUST be used to specify the first 17 bits of

the CCC_ID. The remaining 15 bits are selected by the CMS or MGC in such a way as to ensure that CCC_ID is unique for that CMS or MGC at a given point in time.

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 can 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.6 Instructing Components to Perform Electronic Surveillance

A.6.1 COPS Interface Requirements

A CMS MUST include the COPS Electronic-Surveillance-Parameters object in a Gate-Set message when it detects that a call is subject to a Call Content intercept and decides to perform the intercept at the CMTS (as opposed to the MG). The DUP-EVENT flag and the DUP-CONTENT flags MUST be set, and the DF-IP-Address-for-CDC, DF-Port-for-CDC, DF-IP-Address-for-CCC, DF-Port-for-CCC, CCC-ID, and Billing-Correlation-ID fields MUST be filled in when the Electronic-Surveillance-Parameters object is included in a Gate-Set message.

A CMS MUST NOT include the COPS Electronic-Surveillance-Parameters object in a Gate-Set message when a call is not subject to a Call Content intercept.

A CMTS MUST include the Electronic-Surveillance-Parameters object as appropriate when sending a Gate-Info-Ack in response to a Gate-Info message if the CMTS is performing surveillance on the particular Gate.

A.6.2 TGCP Interface Requirements

A MGC MUST include the TGCP parameters “es-cci” and “es-ccd” in the LocalConnectionOptions of a CRCX or MDCX when it detects that a call is subject to a Call Content intercept.

A MGC MUST NOT include the TGCP parameters “es-cci” and “es-ccd” in the LocalConnectionOptions of a CRCX or MDCX if a call is not subject to a Call Content intercept.

A.7 Timing Information

The PacketCable Electronic Surveillance Specification relies on multiple components (CMS, CMTS, MGC, MG, DF) to gather and deliver Call Data and Call Content to the LEA. Once the Call Data and Call Content is 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 (CMS, CMTS, MGC) or timestamp RTP packets (DF) MUST use Network Time Protocol (NTP) time synchronization as defined in [11].

A.8 Filtering CDC Events in Redirected Calls

Using the call-forward or transfer feature, 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, only a subset of call data events should be reported 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. The DF MUST support the ability to disable the filter when provisioning an intercept. This means that the filter will not be activated even in a redirection case that meets the criteria below.

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

- Answer
- CCChange
- CCClose
- CCOpen
- MediaReport
- Release
- TerminationAttempt
- Redirection
- ServiceInstance (Call Forward)

When the filter feature is enabled for a particular intercept, the DF MUST activate the filter under the following conditions:

- When it receives a Service_Instance EM indicating that the Call Forward feature has been invoked and the subject is listed as the party this is forwarding the call.
- When it receives a Redirection EM and the subject is listed as the party that is redirecting the call.

When the filter feature is enabled for a particular intercept, the DF MUST deactivate the filter under the following conditions:

- When it receives a Service_Instance EM indicating that the Call Forward feature has been invoked and the subject is listed as the party that is receiving the forwarded call.
- When it receives a Redirection EM and the subject is listed as the party that is receiving the redirected call.

Appendix B Acknowledgements

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

PacketCable wishes to recognize the following individuals for their significant involvement and contributions to this specification:

Jim Alfieri, Flemming Andreasen, Mario Edini, and Volnie Whyte (Telcordia)
Nancy Davoust (CableLabs).
Burcak Beser, and Mike Mannette (3Com)
Mike St. Johns (Excite@Home)
Bill Marshall (AT&T)
Stephane Proulx (Broadsoft)
Shantnu Sharma (ADC)
Simon Krauss (CableLabs)
Mike Kogut, Kan Wang (Telcordia)
Anthony Rutkowski (VeriSign)
D.R. Evans (Arris)
Bill Foster, Craig Mulholland, Chip Sharp (Cisco)
Dave Flanagan (Motorola)
Mujdat Pakkan (SS8)
Greg Ratta, Jean Trakinat, Ken Coon, and Michael Bilca (Tridea Works)
Ron Franks (Siemens)
Christian Kittlitz (Nortel)

Eric Rosenfeld, CableLabs

Appendix C Revision History

The following ECN was incorporated into PKT-SP-ESP1.5-I02-070412:

ECN	ECN Date	Summary
ESP1.5-N-07.0390-2	3/12/07	Clarification of eCM DOCSIS versions