PacketCable™ Electronic Surveillance Specification

PKT-SP-ESP-I01-991229

Interim

Notice

This PacketCable specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

Document Status Sheet

Document Control Number:	PKT-SP-ESP-I01-991229			
Document Title:	PacketCable™ Electronic Surveillance Specification			
Revision History:	I01-991229: Initial Interim Release			
Date:	December 29, 1999			
Reference:	PacketCable Electronic Surveillance Specification			
Responsible Author:	PacketCable Electronic Surveillance Focus Team			
Status:	~~Work in Progress~~	~~Draft~~	Interim	~~Released~~
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.
Interim	A document which has undergone rigorous Member and vendor review, suitable for use by vendors to design in conformance to and for field testing. For purposes of the “Contribution and License Agreement for Intellectual Property" which grants licenses to the intellectual property contained in the PacketCable Specification, an "Interim Specification" is a "Published” Specification.
Released	A stable document, reviewed, tested and validated, suitable to enable cross-vendor interoperability.

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^{TM} 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 Specification 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 included 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.

CableLabs® is an industry association that, in addition to research and development related to cable technologies, may sponsor technical requirements and standards. The Telecommunications Industry Association has promulgated a standard [J-STD-025] for lawfully authorized electronic surveillance for traditional voice telephony. However, the electronic surveillance features and capabilities for traditional voice telephony provided for in J-STD-025 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.

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.

[1] Although the specifications and requirements of J-STD-025 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 J-STD-025, employing different parameters and being triggered by different events.

[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)).

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.

A subject's call content and call data is transmitted to the LEA over one or more logical channels known as CCC and 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 DF, (2) the number of surveillance orders required to be supported for any single subject, (3) the availability of resources to transport call content and call data information from the DF to the CF, (4) the availability of resources to transport call content and call data information from the IAP to the DF, and (5) the availability of resources to transport redirected call content and call data information between DF's within the PC/TSP network.

Capacity requirements are fundamental to the design and development of any technical standard or specification (as well as for the equipment developed in compliance with such standards). Several technical considerations, pivotal to the design process, are affected by capacity requirements. However, so far, the Attorney General has not identified capacity requirements for 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)." As interpreted by this specification: ***destination*** is the number of the party to which a call is being made (e.g. called party); ***direction*** is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g. redirected-to-party or redirected-from-party); ***origin*** is the number of the party initiating a call (e.g. calling party); and ***termination*** is the number of the party ultimately receiving a call (e.g. answering party). In traditional telephone networks, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization. Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information.

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

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: the number of the party to which a call is being made (e.g. called party). See Call-Identifying information.

DF: Delivery Function.

Direction: the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g. redirected-to party or redirected-from party). See Call-Identifying information.

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: the number of the party initiating a call (e.g. calling party). See Call-Identifying Information.

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 which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer or 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 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 (FCC 99-230, released August 31, 1999). 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

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: the number of the party ultimately receiving a call (e.g. answering party). See Call-Identifying Information.

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 which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.”

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 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.

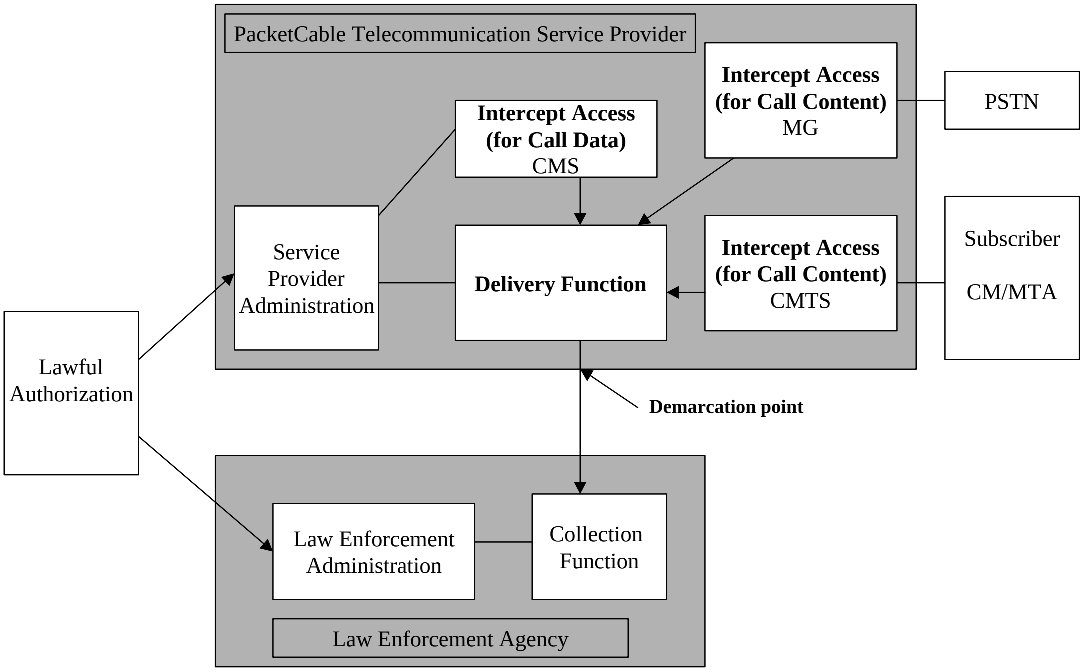
PacketCable Telecommunication Service Provider
Intercept Access (for Call Content) MG
PSTN
Intercept Access (for Call Data) CMS
Service Provider Administration
Delivery Function
Intercept Access (for Call Content) CMTS
Subscriber
CM/MTA
Lawful Authorization
Demarcation point
Law Enforcement Administration
Collection Function
Law Enforcement Agency

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.

2.1 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 1.1 [DOCSIS] 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.

2.2 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).

2.3 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:

a) collect and deliver call content and reasonably available call-identifying information for each intercept subject over the procured law enforcement facilities.

b) ensure that the call content and call-identifying information delivered from the Delivery Function is authorized for a particular LEA;

c) 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;

d) ensure that delivery of surveillance information is only available for the time stated in the lawful authorization;

e) deliver call content and reasonably available call-identifying information using the PCESP protocol.

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.

2.4 Service Provider Administration Func tion (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.

2.5 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.

2.6 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.

3 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.

3.1 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.

3.2 Network Layer Interface

The network layer protocol for delivery of both CDC and CCC information MUST be as defined by the Internet Protocol (IP) [RFC0791]. The transport protocol for CDC information is as specified in Section 5, while transport of CCC information is as specified in Section 4. 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.

3.3 Link-layer Interface

The default link-layer protocol between the DF and CF MUST be as defined by the Ethernet protocol [RFC0894, RFC0826]. However, alternate link-layer protocols MAY be used at the discretion of the PC/TSP based on negotiated agreements with the LEA.

3.4 Physical Interface

The default type of physical interconnect provided by the PC/TSP at the demarcation point MUST be an RJ45 10/100BaseT [ISO8802-3] connection. However, alternate physical interconnects MAY be provided at the discretion of the PC/TSP.

3.5 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.

4 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).

Call Content MUST be delivered as a stream of UDP/IP datagrams, as defined in [RFC0768, RFC0791], sent to the port number at the CF as provided during provisioning of the interception. The UDP/IP payload is of the following format:

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

Table 1: Payload of Call Content Channel Datagrams

Intercepted information originating from a conformant PacketCable MTA will be of the following format:

Original IP Header (20 bytes)
Original UDP Header (8 bytes)
Original RTP Header (variable length, 12-72 bytes)
Original Payload (arbitrary length)

Table 2: Intercepted Information from a Conformant PacketCable MTA

4.1 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) [RFC2327] information provided to the LEA as part of the CCOpen message.

4.2 Original IP Header

This is the IP header [RFC0791], 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.

4.3 Original UDP Header

This is the User Datagram Protocol (UDP) header [RFC0768], 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.

4.4 Original RTP Header

This is the Real-Time Transport Protocol (RTP) header [RFC1889], 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 [RFC1890], and is referenced in the Session Description (SDP) [RFC2327].

4.5 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 [PKT-SEC]. Keying material is contained in the Session Description (SDP) [PKT-NCS], and the algorithm to generate the actual key is described in [PKT-SEC].

Encoding of the voice may be done through use of one of the IETF’s defined CODEC algorithms (as defined in [RFC1890]) or through a dynamic payload type defined in the Session Description (SDP) [RFC2327]. Definition of CODEC algorithms is contained in [PKT-CODEC].

5 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 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 contain a timestamp, with a 200 millisecond accuracy, which identifies the time the event was detected by the IAP. The PCESP message will be available at the DF for delivery to the collection function within eight seconds of its detection by the Intercept Access Point 95% of the time. 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.

5.1 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:

[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.

Answer

A two-way connection has been established for a call under surveillance.

CCChange

A change in the description of call content delivery for a call under interception

CCClose

End of call content delivery for a call under interception

CCOpen

Beginning of call content delivery for a call under interception

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.

TerminationAttempt

The IAP detects a call attempt to a surveillance subject.

5.2 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

5.2.1 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, five call-identifying messages are generated for delivery to LEA - Origination, CCOpen, Answer, CCClose, and Release.

For completed calls originating from a surveillance subject under a Pen Register and Trap and Trace surveillance order, three call-identifying messages are generated for delivery to LEA - Origination, 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.

5.2.2 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, five call-identifying messages are generated for delivery to LEA - TerminationAttempt, CCOpen, Answer, CCClose, and Release.

For completed calls terminating to a subject under a Pen Register and Trap and Trace surveillance order, three call-identifying messages are generated for delivery to LEA - TerminationAttempt, Answer, and Release.

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

5.3 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.

5.3.1 Call Hold

Information about held calls is not available in the PacketCable environment. 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. Therefore, there will not be any CDC messages sent to LEA.

5.3.2 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),
- Redirection (to identify the redirection event and the redirected-to party),
- CCOpen (if communication interception order)
- Answer (if redirected call is answered by redirected-to party),
- CCClose (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 (for the original call, if communication interception order),
- CCClose (for the original call, if communication interception order),
- Redirection (to identify the redirection event and the redirected-to party),
- CCOpen (if communication interception order),
- Answer (if redirected call is answered by redirected-to party),
- CCClose (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.

[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.

5.3.3 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 5.2.1 and 5.2.2, as appropriate.

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 5.3.1.

5.3.4 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 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 (of the old connection, if communication interception order),
- Release (of the old connection)
- TerminationAttempt (of the new connection at the redirected-to party),
- CCOpen (of the new connection, if communication interception order),
- Answer (if redirected call is answered by redirected-to party).

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

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 (of the call between A and B, if communication interception order),
- Release (of the call between A and B)
- Redirect (of the call between A and C, redirected-from A, redirected-to B)
- CCClose (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 (of the new call between B and C, if communication interception order),
- Answer (of the new call between B and C).

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 (of the call between A and bridge, if communication interception order),
- Release (of the call between A and bridge)
- CCClose (of the call between B and bridge, if communication interception order),
- Release (of the call between B and bridge)
- Redirect (of the call between C and bridge, redirected-from bridge, redirected-to B)
- CCClose (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 (of the new call between B and C, if communication interception order),
- Answer (of the new call between B and C).

5.3.5 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 channels 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 5.2.1. 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:

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

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

5.3.6 Call Block

A blocked call will follow the same procedures for a basic call up to the point that it is blocked. 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 LEA prior to the time that the blocking resulted in the call being aborted, then a CCClose message will be sent to the LEA. Up to the point of blocking, the relevant messages and call content will be delivered to the LEA. No specific information is sent to the LEA to identify the blocking of a call.

5.3.7 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. 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 5.2.1, therefore no unique interactions exist for the resulting calls.

5.3.8 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 5.2.1, therefore no unique interactions exist for the resulting call.

5.3.9 911 Emergency and N11 Services

911 emergency and N11 service calls are viewed as normal call originations and the description in Section 5.2.1 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.

5.3.10 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. When the modified SDP descriptions [RFC2327] are known at an IAP for a call under interception, a CCChange message is generated for delivery to LEA. Contained in the CCChange message are updated SDP descriptions of the media flows.

5.4 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.

5.4.1 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:

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.

Table 3: Answer Message

5.4.2 CCChange

The CCChange message is generated for calls under interception prior to or coincident with a change in the Session Description information for either the originating or terminating endpoint. The CCChange message is triggered for surveillances that require the delivery of call content, and its main purpose is to provide LEA with updated information necessary to decode the voice packets for the call.

The CCChange message MUST include the following information:

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 change became effective.
Call_ID	R	Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message.
Originating_SDP	O	The Session Descriptor Protocol (SDP) information for the originating endpoint, if it is changed.
Terminating_SDP	O	The Session Descriptor Protocol (SDP) information for the terminating endpoint, if it is changed.
CCC_ID	O	The CCC-ID value that will appear in all intercepted packets for this call. MUST be present only if the DF is assigning a new value of CCC-ID.

Table 4: CCChange Message

5.4.3 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 one of the following events are detected by an IAP:

- a request to release a call and that the resources for the call are released
- an abnormal termination of a call and that the resources for the call are released.

The CCClose message MUST include the following information:

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.

Table 5: CCClose Message

5.4.4 CCOpen

The CCOpen message is generated for calls under interception when the first of either the originating or terminating party is provided voice packet quality of service. The

CCOpen message is triggered for surveillances that require the delivery of call content, and it identifies the beginning of the delivery of call content information. The main purpose of this message is to provide LEA with information necessary to decode the voice packets for the call.

The CCOpen message MUST include the following information:

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 first voice packet QoS was detected.
Call_ID	R	Uniquely identifies a call within a system. Same Call_ID as the related Origination or TerminationAttempt message.
Originating_SDP	R	The Session Descriptor Protocol (SDP) information for the originating endpoint.
Terminating_SDP	R	The Session Descriptor Protocol (SDP) information for the terminating endpoint.
CCC_ID	R	The CCC-ID value that will appear in all intercepted packets for this call.

Table 6: CCOpen Message

5.4.5 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.
- 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:

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.

Table 7: Origination Message

5.4.6 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 MAY be generated when a call under surveillance is forwarded or transferred by a party other than a surveillance subject.

The Redirection message MUST include the following information:

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.
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.

Table 8: Redirection Message

5.4.7 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 Answer 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:

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.

Table 9: Release Message

5.4.8 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:

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	R	Identifies the originating party.
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

Table 10: TerminationAttempt Message

5.5 CDC Messages and Parameter Definitions

CDC messages and parameters shall be encoded to be binary compatible with X.208 Abstract Syntax Notation One (ASN.1) and X.209 Basic Encoding Rules (BER). This specification uses IMPLICIT tagging for more compact encoding. Parameters of the CHOICE type are encoded EXPLICIT to ensure compatibility.

The following defines the PCESP messages:

```
PCESP DEFINITIONS IMPLICIT TAGS ::=
BEGIN

Message ::= CHOICE {
    answer              [1] Answer,
    ccclose             [2] CCClose,
    ccopen              [3] CCOpen,
                        [4] NULL,      -- Reserved
    origination         [5] Origination,
                        [6] NULL,      -- Reserved
    redirection         [7] Redirection,
    release             [8] Release,
                        [9] NULL,      -- Reserved
    terminationattempt  [10] TerminationAttempt,
                        [11] NULL,     -- Reserved
    ccchange            [12] CCChange
}
```

5.5.1 Answer

```
Answer ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] CallId,
    answering           [4] PartyId                   OPTIONAL
}
```

5.5.2 CCChange

```
CCChange ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] CallId,
                        [4] EXPLICIT CCCId            OPTIONAL,
    originating         [5] SDP                       OPTIONAL,
    terminating         [6] SDP                       OPTIONAL
}
```

5.5.3 CCClose

```
CCClose ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] EXPLICIT CCCId,
}
```

5.5.4 CCOpen

```
CCOpen ::= SEQUENCE {
                              [0] CaseId,
                              [1] AccessingElementId,
                              [2] EventTime,
                              CHOICE {
                                      [3] SEQUENCE of CallId,
                                      [4] NULL,                  -- Reserved
                              }
                              [5] EXPLICIT CCCId,
    originating               [6] SDP,
    terminating               [7] SDP
}
```

5.5.5 Origination

```
Origination ::= SEQUENCE {
                              [0] CaseId,
                              [1] AccessingElementId,
                              [2] EventTime,
                              [3] CallId,
    calling                   [4] PartyId,
    called                    [5] PartyId                OPTIONAL,
    input                     CHOICE {
    userinput                         [6] VisibleString (SIZE (1..32)),
    translationinput                  [7] VisibleString (SIZE (1..32))
                              }
                              [8] NULL,                  -- Reserved
                              [9] TransitCarrierId       OPTIONAL
}
```

5.5.6 Redirection

```
Redirection ::= SEQUENCE {
                              [0] CaseId,
                              [1] AccessingElementId,
                              [2] EventTime,
    old                       [3] CallId,
    redirectedto              [4] PartyID,
                              [5] TransitCarrierId       OPTIONAL,
                              [6] NULL,                  -- Reserved
                              [7] NULL,                  -- Reserved
    new                       [8] CallId                 OPTIONAL,
    redirectedfrom            [9] PartyId                OPTIONAL
}
```

5.5.7 Release

```
Release ::= SEQUENCE {
```

```
                              [0] CaseId,
                              [1] AccessingElementId,
                              [2] EventTime,
                              [3] CallId
}
```

5.5.8 TerminationAttempt

```
TerminationAttempt ::= SEQUENCE {
                              [0] CaseId,
                              [1] AccessingElementId,
                              [2] EventTime,
                              [3] CallId,
    calling                   [4] PartyId,
    called                    [5] PartyId                  OPTIONAL,
                              [6] NULL,                    -- Reserved
                              [7] RedirectedFromInfo       OPTIONAL
}
```

5.5.9 Message Parameters

```
AccessingElementId ::= VisibleString (SIZE(1..15))
                              --  This is a copy of the Element ID present in the
                              --  Event Message specification [PKT-SP-EM]

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 generates this structure from the
                        -- CCCId contained in the Event Messages 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


PartyId ::= SEQUENCE {
                        [0] NULL                OPTIONAL,   -- Reserved
                        [1] NULL                OPTIONAL,   -- Reserved
                        [2] NULL                OPTIONAL,   -- Reserved
                        [3] NULL                OPTIONAL,   -- Reserved
                        [4] NULL                OPTIONAL,   -- Reserved
                        [5] NULL                OPTIONAL,   -- Reserved
    dn                  [6] VisibleString (SIZE(1..15))     OPTIONAL,
    userProvided        [7] VisibleString (SIZE(1..15))     OPTIONAL,
                        [8] NULL                OPTIONAL,   -- Reserved
                        [9] NULL                OPTIONAL,   -- Reserved
    ipAddress           [10] VisibleString (SIZE(1..32))    OPTIONAL,
                        [11] NULL               OPTIONAL,   -- Reserved
    trunkId             [12] VisibleString (SIZE(1..32))    OPTIONAL,
                        [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
}

SDP ::= VisibleString (SIZE(1..2048))

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

END
```

APPENDIX A 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. In particular, PacketCable wants to recognize the following individuals for their significant involvement and contributions to this specification: Burcak Beser, and Mike Mannette (3Com); Mike St. Johns (Excite@Home); Bill Marshall (primary author) (AT&T); Stephane Proulx (Broadsoft); Bill Foster (Cisco); D.R. Evans (Lucent Cable Communications); Jim Alfieri, Flemming Andreasen, Mario Edini, and Volnie Whyte (Telcordia), and Nancy Davoust (CableLabs). A special thanks to Bill Marshall for his exceptional effort in developing this specification.

APPENDIX B REFERENCES

[DOCSIS] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-I03-991105, Cable Television Laboratories, Inc., November 05, 1999. http://www.CableLabs.com/

[ISO8802-3] ISO/IEC 8802-3, 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, 1996. Available via http://www.iso.ch/projects/ics.html, field 35.110.

[J-STD-025] TIA and ANSI Committee T1, Lawfully Authorized Electronic Surveillance, December, 1997.

[PKT-CODEC] PacketCable Audio/Video Codecs Specification, PKT-SP-CODEC-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[PKT-NCS] PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I02-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[PKT-SEC] PacketCable Security Specification, PKT-SP-SEC-I01-991201, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./

[RFC0768] Postal, J, User Datagram Protocol, August, 1980.

[RFC0791] Postal, J., Internet Protocol, September, 1981.

[RFC0826] Plummer, D, Ethernet Address Resolution Protocol, November, 1982.

[RFC0894] Horning, C, Standard for the Transmission of IP Datagrams over Ethernet Networks, April, 1984.

[RFC1889] Schulzrinne, H, S. Casner, R. Frederick, V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, January, 1996.

[RFC1890] Schulzrinne, H, RTP Profile for Audio and Video Conferences with Minimal Control, January, 1996.

[RFC2327] Handley, M, and V. Jacobson, SDP: Session Description Protocol, April, 1998.