**FOIA Number:** 2008-1524-F

# FOIA MARKER

**This is not a textual record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.**

---

**Collection/Record Group:** Clinton Presidential Records

**Subgroup/Office of Origin:** Office of Science and Technology

**Series/Staff Member:**

**Subseries:**

---

**OA/ID Number:** 43311

**FolderID:**

---

**Folder Title:**
Communications Assistance for Law Enforcement Act (CALEA) [3]

| Stack: | Row: | Section: | Shelf: | Position: |
|---|---|---|---|---|
| S | 1 | 1 | 7 | 3 |

Network Working Group IAB
Request for Comments: 2804 IESG
Category: Informational May 2000

# IETF Policy on Wiretapping

## Status of this Memo



## Copyright Notice



## Abstract

The Internet Engineering Task Force (IETF) has been asked to take a position on the inclusion into IETF standards-track documents of functionality designed to facilitate wiretapping.

This memo explains what the IETF thinks the question means, why its answer is "no", and what that answer means.

## 1. Summary position

The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards.

It takes this position for the following basic reasons:

- The IETF, an international standards body, believes itself to be the wrong forum for designing protocol or equipment features that address needs arising from the laws of individual countries, because these laws vary widely across the areas that IETF standards are deployed in. Bodies whose scope of authority correspond to a single regime of jurisdiction are more appropriate for this task.

- The IETF sets standards for communications that pass across networks that may be owned, operated and maintained by people from numerous jurisdictions with numerous requirements for privacy. In light of these potentially divergent requirements, the IETF believes that the operation of the Internet and the needs of its users are best served by making sure the security properties of



connections across the Internet are as well known as possible. At the present stage of our ignorance this means making them as free from security loopholes as possible.

- The IETF believes that in the case of traffic that is today going across the Internet without being protected by the end systems (by encryption or other means), the use of existing network features, if deployed intelligently, provides extensive opportunities for wiretapping, and should be sufficient under presently seen requirements for many cases. The IETF does not see an engineering solution that allows such wiretapping when the end systems take adequate measures to protect their communications.

- The IETF believes that adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost inevitably jeopardizes the security of communications even when it is not being tapped by any legal means; there are also obvious risks raised by having to protect the access to the wiretap. This is in conflict with the goal of freedom from security loopholes.

- The IETF restates its strongly held belief, stated at greater length in [RFC 1984], that both commercial development of the Internet and adequate privacy for its users against illegal intrusion requires the wide availability of strong cryptographic technology.

- On the other hand, the IETF believes that mechanisms designed to facilitate or enable wiretapping, or methods of using other facilities for such purposes, should be openly described, so as to ensure the maximum review of the mechanisms and ensure that they adhere as closely as possible to their design constraints. The IETF believes that the publication of such mechanisms, and the publication of known weaknesses in such mechanisms, is a Good Thing.

## 2. The Raven process

The issue of the IETF doing work on legal intercept technologies came up as a byproduct of the extensive work that the IETF is now doing in the area if IP-based telephony.

In the telephony world, there has been a tradition of cooperation (often mandated by law) between law enforcement agencies and telephone equipment operators on wiretapping, leading to companies that build telephone equipment adding wiretapping features to their telephony-related equipment, and an emerging consensus in the



industry of how to build and manage such features. Some traditional telephony standards organizations have supported this by adding intercept features to their telephony-related standards.

Since the future of the telephone seems to be intertwined with the Internet it is inevitable that the primary Internet standards organization would be faced with the issue sooner or later.

In this case, some of the participants of one of the IETF working groups working on a new standard for communication between components of a distributed phone switch brought up the issue. Since adding

features of this type would be something the IETF had never done before, the IETF management decided to have a public discussion before deciding if the working group should go ahead. A new mailing list was created (the Raven mailing list, see http://www.ietf.org/mailman/listinfo/raven) for this discussion. Close to 500 people subscribed to the list and about 10% of those sent at least one message to the list. The discussion on this list was a precursor to a discussion held during the IETF plenary in Washington, D.C.

Twenty-nine people spoke during the plenary session. Opinions ranged from libertarian: 'governments have no right to wiretap' - to pragmatic: 'it will be done somewhere, best have it done where the technology was developed'. At the end of the discussion there was a show of hands to indicate opinions: should the IETF add special features, not do this or abstain. Very few people spoke out strongly in support for adding the intercept features, while many spoke out against it, but a sizable portion of the audience refused to state an opinion (raised their hands when asked for "abstain" in the show of hands).

This is the background on the basis of which the Internet Engineering Steering Group (IESG) and the Internet Architecture Board (IAB) was asked to formulate a policy.

## 3. A definition of wiretapping

The various legal statutes defining wiretapping do not give adequate definitions to distinguish between wiretapping and various other activities at the technical level. For the purposes of this memo, the following definition of wiretapping is used:

Wiretapping is what occurs when information passed across the Internet from one party to one or more other parties is delivered to a third party:



1. Without the sending party knowing about the third party

2. Without any of the recipient parties knowing about the delivery to the third party

3. When the normal expectation of the sender is that the transmitted information will only be seen by the recipient parties or parties obliged to keep the information in confidence

4. When the third party acts deliberately to target the transmission of the first party, either because he is of interest, or because the second party's reception is of interest.

The term "party", as used here, can refer to one person, a group of persons, or equipment acting on behalf of persons; the term "party" is used for brevity.

Of course, many wiretaps will be bidirectional, monitoring traffic sent by two or more parties to each other.

Thus, for instance, monitoring public newsgroups is not wiretapping (condition 3 violated), random monitoring of a large population is not wiretapping (condition 4 violated), a recipient passing on private email is not wiretapping (condition 2 violated).

An Internet equivalent of call tracing by means of accounting logs (sometimes called "pen registers") that is a feature of the telephone network is also wiretapping by this definition, since the normal expectation of the sender is that the company doing the accounting will keep this information in confidence.

Wiretapping may logically be thought of as 3 distinct steps:

- Capture - getting information off the wire that contains the information wanted.

- Filtering - selecting the information wanted from information gathered by accident.

- Delivery - transmitting the information wanted to the ones who want it.

The term applies to the whole process; for instance, random monitoring followed by filtering to extract information about a smaller group of parties would be wiretapping by this definition.

In all these stages, the possibility of using or abusing mechanisms defined for this purpose for other purposes exists.





This definition deliberately does not include considerations of:

- Whether the wiretap is legal or not, since that is a legal, not a technical matter.

- Whether the wiretap occurs in real time, or can be performed after the fact by looking at information recorded for other purposes (such as the accounting example given above).

- What the medium targeted by the wiretap is - whether it is email, IP telephony, Web browsing or EDI transfers.

These questions are believed to be irrelevant to the policy outlined in this memo.

Wiretapping is also sometimes called "interception", but that term is also used in a sense that is considerably wider than the monitoring of data crossing networks, and is therefore not used here.

## 4. Why the IETF does not take a moral position

Much of the debate about wiretapping has centered around the question of whether wiretapping is morally evil, no matter who does it, necessary in any civilized society, or an effective tool for catching criminals that has been abused in the past and will be abused again.

The IETF has decided not to take a position in this matter, since:

- There is no clear consensus around a single position in the IETF.

- There is no means of detecting the morality of an act "on the wire". Since the IETF deals with protocol standardization, not protocol deployment, it is not in a position to dictate that its product is only used in moral or legal ways.

However, a few observations can be made:

- Experience shows that tools which are effective for a purpose tend to be used for that purpose.

- Experience shows that tools designed for one purpose that are effective for another tend to be used for that other purpose too, no matter what its designers intended.

- Experience shows that if a vulnerability exists in a security system, it is likely that someone will take advantage of it sooner or later.



- Experience shows that human factors, not technology per se, is the biggest single source of such vulnerabilities.

What this boils down to is that if effective tools for wiretapping exist, it is likely that they will be used as designed, for purposes legal in their jurisdiction, and also in ways they were not intended for, in ways that are not legal in that jurisdiction. When weighing the development or deployment of such tools, this should be borne in mind.

## 5. Utility considerations

When designing any communications function, it is a relevant question to ask if such functions efficiently perform the task they are designed for, or whether the work spent in developing them is not, in fact, worth the benefit gained.

Given that there are no specific proposals being developed in the IETF, the IETF cannot weigh proposals for wiretapping directly in this manner.

However, as above, a few general observations can be made:

- Wiretapping by copying the bytes passed between two users of the Internet with known, static points of attachment is not hard. Standard functions designed for diagnostic purposes can accomplish this.

- Correlating users' identities with their points of attachment to the Internet can be significantly harder, but not impossible, if the user uses standard means of identification. However, this means linking into multiple Internet subsystems used for address assignment, name resolution and so on; this is not trivial.

- An adversary has several simple countermeasures available to defeat

wiretapping attempts, even without resorting to encryption. This includes Internet cafes and anonymous dialups, anonymous remailers, multi-hop login sessions and use of obscure communications media; these are well known tools in the cracker community.

- Of course, communications where the content is protected by strong encryption can be easily recorded, but the content is still not available to the wiretapper, defeating all information gathering apart from traffic analysis. Since Internet data is already in digital form, encrypting it is very simple for the end-user.



These things taken together mean that while wiretapping is an efficient tool for use in situations where the target of a wiretap is either ignorant or believes himself innocent of wrongdoing, Internet-based wiretapping is a less useful tool than might be imagined against an alerted and technically competent adversary.

## 6. Security Considerations

Wiretapping, by definition (see above), releases information that the information sender did not expect to be released.

This means that a system that allows wiretapping has to contain a function that can be exercised without alerting the information sender to the fact that his desires for privacy are not being met.

This, in turn, means that one has to design the system in such a way that it cannot guarantee any level of privacy; at the maximum, it can only guarantee it as long as the function for wiretapping is not exercised.

For instance, encrypted telephone conferences have to be designed in such a way that the participants cannot know to whom any shared keying material is being revealed.

This means:

- The system is less secure than it could be had this function not been present.

- The system is more complex than it could be had this function not been present.

- Being more complex, the risk of unintended security flaws in the system is larger.

Wiretapping, even when it is not being exercised, therefore lowers the security of the system.

## 7. Acknowledgements

This memo is endorsed by the IAB and the IESG.

Their membership is:

IAB:

Harald Alvestrand
Randall Atkinson
Rob Austein
Brian Carpenter
Steve Bellovin
Jon Crowcroft
Steve Deering
Ned Freed
Tony Hain
Tim Howes
Geoff Huston
John Klensin

IESG:

Fred Baker
Keith Moore
Patrik Falstrom
Erik Nordmark
Thomas Narten
Randy Bush
Bert Wijnen
Rob Coltun
Dave Oran
Jeff Schiller
Marcus Leech
Scott Bradner
Vern Paxson
April Marine

The number of contributors to the discussion are too numerous to list.

## 8. Author's Address

This memo is authored by the IAB and the IESG.

The chairs are:

Fred Baker, IETF Chair
519 Lado Drive
Santa Barbara California 93111

Phone: +1-408-526-4257
EMail: fred@cisco.com

Brian E. Carpenter, IAB Chair
IBM
c/o iCAIR
Suite 150
1890 Maple Avenue
Evanston IL 60201
USA

EMail: brian@icair.org

## 9. References

[RFC 1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", RFC 1984, August 1996.



## 9. Full Copyright Statement

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

# PacketCable™ Electronic Surveillance Specification

## PKT-SP-ESP-I01-991229

**Interim**

### Notice

# 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™ 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.

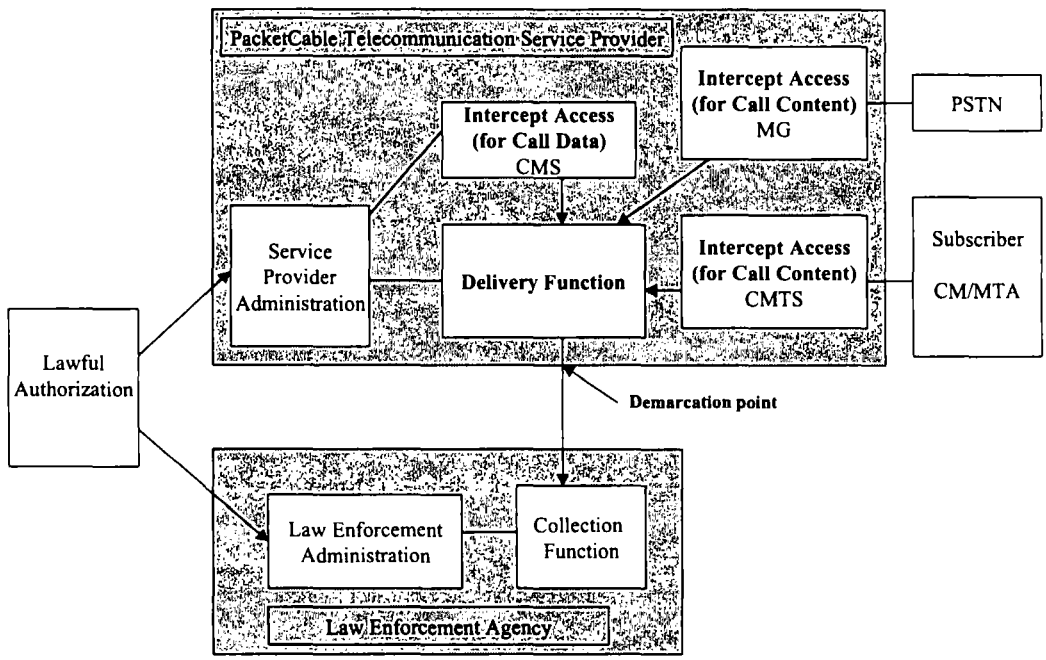


***Figure 1: Electronic Surveillance Model***

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 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.

## 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.

# CALEA JEM Invited and/or Participating Groups List

(Rev. 3.28.00--*In no specific order*)

**Telecommunications Industry Association (TIA):**

☞ *CALEA JEM Web Page:*
http://www.tiaonline.org/standards/CALEA_JEM/
*Note: Scroll down for link to purchase the "safe harbor" Interim Standard J-STD-025*

**ATM Forum:** http://www.atmforum.com/

**CableLabs, PacketCable Project:** http://www.packetcable.com/

☞ *Electronic Surveillance Specification:*
http://www.packetcable.com/specs/pkt-sp-esp-I01-991229.pdf

**GSM North America:** http://www.gsm-pcs.org/northamerica/gsmna.html

**ETSI:** http://www.etsi.org/

☞ Lawful Interception: http://www.etsi.org/technicalactiv/li.htm

**T1S1:** http://www.t1.org/t1s1/t1s1.htm

**T1P1:** http://www.t1.org/t1p1/t1p1.htm

☞ *Working Document on Packet Mode Communication Interception:*
ftp://ftp.t1.org/pub/t1p1/2000/0p100092.doc

☞ *A Method for Reporting Access Control Call Identifying Information:*
ftp://ftp.t1.org/pub/t1p1/2000/0p100860.doc

☞ *A Method for Reporting SIP/H.323 Signaling:*
ftp://ftp.t1.org/pub/t1p1/2000/0p100870.doc

☞ *A Method for Reporting IP Addressing Information:*
ftp://ftp.t1.org/pub/t1p1/2000/0p100880.doc

**3GPP:** http://www.3gpp.org/

☞ *Lawful Interception Architecture and Functions Specification (33.107):*
http://www.3gpp.org/ftp/Specs/March_00/33_series/

**3GPP2:** http://www.3gpp2.org/

**DSL Forum Technical Committee:** http://www.adsl.com/

☞ *Framing and Encapsulation Standards for ADSL: Packet Mode:*
http://www.adsl.com/TR-003.doc

**Frame Relay Forum, Worldwide Technical Committee:** http://www.frforum.com/8000/8004.html

**Wireless Data Forum:** http://www.wirelessdata.org/

**PCIA:** http://www.pcia.com/

☞ *CALEA Suite of Standards for Traditional Paging, Advanced Messaging and Ancillary*

*Services Version 1.2 February 19, 1999:*
http://www.pcia.com/advocacy/Calea_su.pdf

☞ *CALEA Specification for Traditional Paging, Version 1.0, May 4, 1998:*
http://www.pcia.com/advocacy/trad_pgg.pdf

☞ *CALEA Specification for Advanced Paging, Version 1.0, August 1998:*
http://www.pcia.com/advocacy/adv_msg.pdf

☞ *CALEA Specification for Ancillary Services Version 1.0 February 19, 1999:*
http://www.pcia.com/advocacy/Anc_svcs.pdf

☞ *CALEA, Flexible Deployment Assistance Guide (FBI), January 2000:*
http://www.pcia.com/advocacy/pdf/flexgide.pdf

**UWCC:** http://www.uwcc.org/
☞ *See "Contributions" under TIA CALEA Link*

**CDMA Development Group:** http://www.cdg.org/

**NCTA:** http://www.ncta.com/home.html

**IETF:** http://www.ietf.org/
☞ *Position on Wiretapping:* http://www.ietf.org/internet-drafts/draft-iab-raven-01.txt

**USTA, Technical Disciplines:** http://www.usta.org/

**CTIA:** http://www.wow-com.com/

**3Com:** http://www.3com.com/

**USWest:** http://uswest.com

**Nokia:** http://nokia.com

**Agilent Technologies:** http://www.agilent.com/Top/English/index.html

**NeuStar:** http://www.neustar.com/

**Motorola:** http://www.Motorola.com/

**Deutsche Telekom:** http://www.telekom.de/dtag/ipl2/cda/t1/

**Nortel Networks:** http://www.nortelnetworks.com/index.html
*See T1P1 Links*

**Cisco:** http://www.cisco.com/

**SBC:** http://www.sbc.com/

**Ericsson:** http://www.Ericsson.com/

**Lucent:** http://www.Lucent.com/

**Bell Atlantic Mobile:** http://www.bam.com/

**Pen-Link:** http://www.PenLink.com/
☞ *Downloadable Pen-Link v6.0 Tour:*
http://www.penlink.com/html/tourform.html

**Rogers Wireless:** http://www.rogers.com/wireless/english/index.html

**Siemens:** http://www.siemens.de/ic/index.htm

**AT&T Wireless Services:** http://www.attws.com/

**GTE Wireless:** http://www.gte.com/

**Alcatel USA:** http://www.usa.alcatel.com/

**Telcordia Technologies:** http://www.Telcordia.com/

**ITU-T:** http://www.itu.int/ITU-T/index.html

**ITU-R:** http://www.itu.int/ITU-R/index.html

**FCC:** http://www.fcc.gov/
*Office of Engineering and Technology:* http://www.fcc.gov/oet/
*Wireless Telecom Bureau:* http://www.fcc.gov/wtb/
☞ *Information and Links:* http://www.fcc.gov/wtb/csinfo/calea.html

**FBI:** http://www.fbi.gov/
☞ *CALEA Implementation Section:* http://www.fbi.gov/programs/calea/calea.htm

# Attachment

To: Lt. Col. Terry Kelly

From: Mitchell S. Baxter

Date: July 11, 2000

Re: Relevant Sections of CALEA

---

**TITLE I--INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS**

**SEC. 101. <47 USC 1001 note> --SHORT TITLE.**

This title may be cited as the "Communications Assistance for Law Enforcement Act".

**SEC. 102. <47 USC 1001> DEFINITIONS.**

For purposes of this title--

(2) The term "call-identifying information" means 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.

(4) The term "electronic messaging services" means software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.

(6) The term "information services"--

(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

(B) includes--

[**4280] (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.

(8) The term "telecommunications carrier"--

(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and

(B) includes--

(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332 (d))); or

(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the 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; but

(C) does not include--

(i) persons or entities insofar as they are engaged in providing information services; and

(ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General.

**SEC. 103. <47 USC 1002> ASSISTANCE CAPABILITY REQUIREMENTS.**

(a) Capability Requirements.--Except as provided in subsections (b), (c), and (d) of this section and sections 108(a) and 109(b) and (d), a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of--

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--

[**4281] (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) in a manner that allows it to be associated with the communication to which it pertains,

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall 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);

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information.

(b) Limitations.--

(1) Design of features and systems configurations.-- This title does not authorize any law enforcement agency or officer--

(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or

(B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

(2) Information services; private networks and interconnection services and facilities.-- The requirements of subsection (a) do not apply to--

(A) information services; or

(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

**SEC. 107. <47 USC 1006> TECHNICAL REQUIREMENTS AND STANDARDS; EXTENSION OF COMPLIANCE DATE.**

(a) Safe Harbor.--

(1) Consultation.-- To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representatives of users of telecommunications equipment, facilities, and services, and with State utility commissions.

(2) Compliance under accepted standards.-- A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103.

(3) Absence of standards.-- The absence of technical requirements or standards for implementing the assistance capability requirements of section 103 shall not--

(A) preclude a telecommunications carrier, manufacturer, or telecommunications support services provider from deploying a technology or service; or

(B) relieve a carrier, manufacturer, or telecommunications support services provider of the obligations imposed by section 103 or 106, as applicable.

(b) Commission Authority.--If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that--

(1) meet the assistance capability requirements of section 103 by cost-effective methods;

(2) protect the privacy and security of communications not authorized to be intercepted;

(3) minimize the cost of such compliance on residential ratepayers;

(4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and

(5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

(c) Extension of Compliance Date for Equipment, Facilities, and Services.--

(1) Petition.-- A telecommunications carrier proposing to install or deploy, or having installed or deployed, any equipment, facility, or service prior to the effective date of section 103 may petition the Commission for 1 or more extensions of the deadline for complying with the assistance capability requirements under section 103.

(2) Grounds for extension.-- The Commission may, after consultation with the Attorney General, grant an extension under this subsection, if the Commission determines that compliance with the assistance capability requirements under section 103 is not reasonably achievable through application of technology available within the compliance period.

(3) Length of extension.-- An extension under this subsection shall extend for no longer than the earlier of--

(A) the date determined by the Commission as necessary for the carrier to comply with the assistance capability requirements under section 103; or

(B) the date that is 2 years after the date on which the extension is granted.

(4) Applicability of extension.-- An extension under this subsection shall apply to only that part of the carrier's business on which the new equipment, facility, or service is used.

**Attachment**

To: Lt. Col. Terry Kelly

From: Mitchell S. Baxter

Date: July 11, 2000

Re: Relevant Excerpts from FCC CALEA Order discussing Packet-Mode Communications

---

Before the
**Federal Communications Commission** Washington, D.C. 20554

| | | |
|---|---|---|
| In the Matter of: | ) | |
| | ) | |
| Communications Assistance for | ) | CC Docket No. 97-213 |
| Law Enforcement Act | ) | |
| | ) | |

# THIRD REPORT AND ORDER

Adopted: August 26, 1999 Released: August 31, 1999

**2. Packet-Mode**

47. Background. J-STD-025 provides for LEA access to call-identifying information and the interception of wire and electronic telecommunications, regardless of whether the telecommunications are carried in circuit-mode or in packet-mode. It further states that the "call-identifying information associated with the circuit-mode content surveillance is provided on the [call data channel]," but does not specifically address whether call-identifying information, if any, associated with packet-mode surveillance must be provided over a call data channel.

48. The Further NPRM noted that packet data and packet-switching technology are potentially usable for both information services and telecommunications services, but that such technology is subject to CALEA requirements only to the extent it is used to provide telecommunications services, and not for information services. The Further NPRM also noted that privacy concerns could be implicated if carriers were to give to LEAs packets containing both call- identifying and call content information when only the former was authorized. The Further NPRM tentatively concluded that the record is not sufficiently developed to support any particular technical requirements for packet-mode communications, and therefore did not propose technical requirements for such communications. However, the Further NPRM sought comment on a wide range of issues to develop a sufficient record.

49. Comments. EFF, EPIC, and ACLU state that our cautious approach regarding packet-mode communications is correct, and that it is critical that we adequately protect the privacy of communications carried on packet-mode systems. They state that the interim standard's

requirement to deliver the entire packet data stream associated with a given communication violates the privacy provisions of section 103. Therefore, according to EFF, EPIC, and ACLU, until carriers are able to protect the privacy of communications carried over packet-mode systems, we should refrain from adopting capability requirements for such systems.

50. CDT states that carriers using packet technologies have an obligation under CALEA to protect privacy by distinguishing between call content and call-identifying information, so that a LEA does not intercept the former when it has only the narrower authority for the latter. CDT contends that DoJ/FBI acknowledge that protecting privacy by distinguishing between call content and call-identifying information is technically trivial, but states that DoJ/FBI believe there is no obligation on carriers to protect privacy. CDT states that we should not wait until packet technologies are more fully deployed to clarify that carriers have an obligation to protect individual privacy.

51. AT&T supports our tentative conclusion that packet-mode technologies may require differing CALEA solutions. AT&T states that it believes that if we defer setting packet-mode communications standards in this proceeding, industry associations will take up the issue on their own.

52. TIA states that the telecommunications network is rapidly evolving toward a packet- based architecture. TIA cautions that the Commission not stifle the continued development of packet-mode technologies by imposing a solution that could require the redesign (or even abandonment) of certain technologies. TIA recommends that we consider establishing a separate packet-mode standard-setting effort within it.

53. US West argues that risks to advanced services and the Internet support the deferral of any CALEA requirements on packet networks, at least until CALEA can be implemented without inhibiting the development of advanced telecommunications services. It further states that because many packet-mode communications will avoid the circuit-switched network altogether, carriers and manufacturers will have to develop and install CALEA solutions for different network elements from those used in circuit-switched networks. Additionally, US West asserts that separating the header from content in packet-mode communications is not feasible because packet data is delivered in a layered stack structure, and carriers have neither the ability nor any business reason to monitor packet data streams and then decipher the various protocols.

54. DoJ/FBI argue that the interim standard's treatment of packet-mode communications in pen register cases does not conflict with anything in CALEA, and hence that standard is not deficient in this regard. DoJ/FBI state that, as a technical matter, it is perfectly feasible for a LEA to employ equipment that distinguishes between a packet's header and its communications payload and makes only the relevant header information available for recording or decoding. DoJ/FBI further state that the statutory distinction between telecommunications carriers and providers of information services does not correspond to any distinction between packet-mode and circuit-mode communications; therefore, the use of packet-mode protocols does not turn the transmission of a wire or electronic communication by a telecommunications carrier into the provision of information services.

55. Discussion. We find that the approach taken with regard to packet-mode communications in J-STD-025 raises significant technical and privacy concerns. Under this standard, LEAs would be provided with both call-identifying information and call content even in cases where a LEA is authorized only to receive call-identifying information (i.e., under a pen register). We are aware that packet-mode technology is rapidly changing, and that different technologies may require differing CALEA solutions for separating call-identifying information from call content. We also

recognize that we must avoid implementing CALEA requirements that could impede the development of new technologies. We do not believe that the record sufficiently addresses packet technologies and the problems that they may present for CALEA purposes. For example, some packet technologies (e.g., frame relay, ATM, X.25) are connection oriented--i.e., there are call set-up and take-down processes, similar to those used in circuit switched voice networks, whereby addressing information is made available to the carrier separate from and before call content is transmitted. Other packet technologies (e.g., internet protocol based solutions) would not be processed this way. We believe that further efforts can be made to find ways to better protect privacy by providing law enforcement only with the information to which it is lawfully entitled. We note that TIA recommends further study of this matter. Accordingly, we invite TIA to study CALEA solutions for packet-mode technology and report to the Commission in one year on steps that can be taken, including particular amendments to J-STD-025, that will better address privacy concerns. In the interim, we find that packet-mode communications, including call-identifying information and call content, may be delivered to law enforcement under the interim standard. Further, we are herein requiring that packet-mode communications be delivered to LEAs under that standard no later than September 30, 2001. That date is 15 months after the June 30, 2000 CALEA compliance deadline, and will afford manufacturers that have not yet developed a packet-mode capability the time needed to do so.

56. We recognize that the solution we have crafted above is not perfect because a LEA may receive both call identifying information and call content under a pen register. We note, however, that independent legal barriers exist which will protect, to a certain extent, the privacy rights of individuals until a permanent solution is developed. In particular, under this interim arrangement the LEA will be legally prohibited from using any content information in a court proceeding if it has only a pen register or trap and trace authorization. We find, therefore, that in weighing the factors identified under section 107(b) of CALEA--that is, in particular, (1) to meet the assistance capability requirements of section 103 by cost effective methods, (2) to protect the privacy and security of communications not authorized to be intercepted, and (3) to encourage the provision of new technologies and services to the public --we believe that the above solution provides the most suitable temporary remedy available at this time. We emphasize, however, that we intend this solution to be only an interim one. We recognize that, in view of the growing importance of packet-mode communications, a timely permanent solution is essential. Accordingly, we expect that TIA will deliver a report to us no later than September 30, 2000 that will detail a permanent solution, keeping in mind the objectives underlying CALEA which are described in paragraph 2, supra.

**MEMORANDUM**

Re: CALEA/Packet-Mode Networks

Date: July 12, 2000

---

## Summary


- We have been examining the current status of CALEA as it applies to packet switching. As you know, CALEA is the principal authority that law enforcement agencies ("LEA") utilize to gain cooperation from carriers to monitor communication technologies under the law.

- The Federal Communications Commission ("FCC") is authorized under CALEA to interpret and administer the provisions affecting LEA and private telecommunications owners and operators.

- The FCC recognized that packet-mode communications are troublesome, in that they are used for both telecommunications and information services, while CALEA only affects owners and operators of telecommunications facilities – such as wireline, cellular, and broadband PCS.

- At this time, the FCC has interpreted CALEA to allow LEA to monitor packet-switching technologies. Until the FCC approves a final standard, common carriers must be prepared to deliver packet-mode communications (both header and body) to LEA by September 30, 2001, under an interim standard (J-STD-025) developed by an industry trade association.

- Until a workable standard is established, the FCC has the expectation that LEA will use available technology to separate header and body in intercepted packets.

- The various equities (privacy community, industry, LEA) have given the FCC their input, and the FCC has directed industry to propose amendments to the standard by September 30, 2000 addressing the various concerns, especially the privacy issues.

# Discussion

**Background:**

Congress passed the Communications Assistance for Law Enforcement Act ("CALEA" or the "Act") on the last night of its 1994 session.[1] CALEA mandates that telecommunications carriers must design their systems so as to be accessible by law enforcement agencies ("LEA"). Among other things, the statute requires systems to be capable of enabling the government to intercept all wire and electronic communications carried by a carrier, and to access call-identifying information that is reasonably available to the carrier.

The Act authorizes the Federal Communications Commission ("FCC") to establish, by rule, technical requirements or standards that meet the assistance capability requirements, if industry or standards-setting organizations have failed to set such standards, or if any party believes that an industry standard is deficient.

The Telecommunications Industry Association ("TIA") developed a standard, J-STD-025, to serve as a "safe harbor" for carriers, enabling them to be in compliance with CALEA.

The Equities:

- FBI/DOJ filed a petition for FCC rulemaking, contending that the TIA's standard was deficient, and offered a nine-point "punch list" of items needed to satisfy CALEA requirements.

- The privacy community (EPIC, CDT, EFF, ACLU) filed their own petitions, arguing that the interim standard was *over inclusive*, because it included, among other things, packet-mode communications capabilities. They expressed concern that the FBI was overreaching in seeking the ability to monitor the Internet.[2]

- Many carriers also filed petitions, alleging that the FBI/DOJ standards were onerous, imposing too difficult and costly a burden. They also assert that forcing them to conform would inhibit the development of new technology in this rapidly developing field.

The FCC has released several Orders and Notices of Proposed Rule Making (NPRM), first extending the original deadline for installation of CALEA-compliant equipment based on the J-STD-025 standard until June 30, 2000, ordering that six of the nine "punch list" capabilities requested by FBI/DOJ be implemented by wireline, cellular and broadband PCS carriers, and seeking comments regarding packet-mode communications. While the Orders require that packet-mode capability be implemented, the FCC has not yet adopted technical requirements for packet-mode communications; rather, packet-mode data – both header and content -- will be delivered to law enforcement under the interim standard, pending further study. The FCC extended until September 30, 2000 the deadline for TIA to develop a packet-mode standard.

---

[1] It is significant that it was passed at the last minute under cover of night, because it was (and still is) highly controversial.

[2] This is a visceral issue for the privacy community. One group's website trumpets that the FBI is seeking "KGB-like powers;" several discuss CALEA and the FBI in terms of "Big Brother."

**The Issues:**

Packet switching is troublesome in that it may be used for both telecommunications and information services. It is important to note that CALEA draws a distinction, defining "information services" to include the means for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications.

Significantly, the CALEA definition of "telecommunications carrier" explicitly *excludes* information service providers, which include, for example, AOL and Prodigy. Thus, according to the FCC, packet data and packet-switching technology are subject to the requirements of CALEA only to the extent they are used to provide telecommunications services, and not for information services.

CALEA also requires telecommunications carriers to provide information to LEA "in a manner that protects...the privacy and security of communications... not authorized to be intercepted." This mandate would be violated if the carrier were to give LEA both call-identifying and call-content information.

The parties before the FCC disputed whether the J-STD-025 standard is adequate. The privacy community contends that the FBI seeks to obtain the full content of a subject's packet-mode communications even when the government is authorized only to intercept addressing or signaling information.

FBI/DOJ contends that the distinction between telecommunications carriers and providers of information services does not correspond to any distinction between packet-mode and circuit-mode communications, and asserted that LEA can employ equipment that distinguishes between a packet's header and its communications payload, making only the relevant header information available for recording or decoding.

**The FCC's Ruling:**

Heeding TIA's call for further study, the FCC gave TIA an additional year to study CALEA solutions for packet-mode technology, and to report to the FCC by September 30, 2000, suggesting possible modifications to J-STD-025, taking into account the relevant privacy issues. In the interim, the FCC held that packet-mode communications, including call-identifying information and call content, may be delivered to LEA under the interim standard. Finally, the FCC required that packet-mode communications be delivered to LEA under that standard by September 30, 2001.

The FCC recognized that the solution is imperfect, in that LEA can receive both call identifying information and call content under a pen register. It then noted that independent legal barriers exist which will protect, to a certain extent, the privacy rights of individuals until a permanent solution is developed. In particular, under the interim arrangement, LEA will be legally prohibited from using any content information in a court proceeding if it has only a pen register or trap and trace authorization.

**Note:** While some law reviews on related subjects discuss this issue, I was unable to find any substantive articles directly on point; it may be that the issue is too new. I am attaching excerpts from CALEA, which define key terms, and an excerpt from the latest FCC Order discussing packet-mode communications.