

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) [1]

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

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.

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.

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*.



Visit TIA's B2B
Communications Portal



Standards & Technology

[HOME](#) ♦ [MAIN](#) ♦ [POST - CALEA JEM](#) ♦ [CALEA: FAQs](#)

Choose a Sub Category...

CALEA Packet Surveillance Joint Experts Meeting; FAQs

What is CALEA?

The Communications Assistance for Law Enforcement Act, which was enacted on October 24, 1994, as P.L. No. 103-414.

What is CIS?

CALEA Implementation Section formed by FBI to assist CALEA implementation.

What is the purpose of CALEA?

CALEA was intended to preserve the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology. In enacting this statute, however, Congress recognized the need to protect privacy interests within the context of court-authorized electronic surveillance. Thus, in defining the terms and requirements of the Act, Congress sought to balance three important policies:

- "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts;
- (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and
- (3) to avoid impeding the development of new communications services and technologies."

H.R. Rep. No. 103-827, 103d Cong., 2d Sess.(1994), reprinted in 1994 U.S.C.C.A.N. 3489

Who is covered by CALEA?

Telecommunications carriers and providers with the ability to "originate, terminate, or direct communications." - Section 103(a) of CALEA

What are the legal requirements of CALEA?

Section 103 of CALEA establishes four general "assistance capability requirements" that carriers must meet to achieve compliance with CALEA. Section 103(a) requires that 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--

(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.

What is call-identifying information?

CALEA defines call-identifying information as "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."

When is call-identifying information "reasonably available?"

Call identifying information is "reasonably available" to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications.

What is Call Content?

Defined in 18 USC 2510 (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communications."

What is a "safe harbor" under CALEA?

Section 107(a)(2) of CALEA contains a "safe harbor" provision, stating that "[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."

What is J-STD-025?

Subcommittee TR-45.2 of the Telecommunications Industry Association (TIA), along with Committee T1 of the Alliance for Telecommunications Industry Solutions, developed interim standard J-STD-025 to serve as a "safe harbor" for wireline, cellular, and broadband PCS carriers and manufacturers under section 107(a) of CALEA. The standard defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency.

Is J-STD-025 a "safe harbor?"

Yes, for the core CALEA capabilities or features that must be implemented by June, 30, 2000.

Are There Technical Requirements in Addition to J-STD-025?

On August 30, 1999, the FCC found that J-STD-025 was deficient in certain technical respects and remanded the standard to TR-45.2 for revision. The additional requirements (sometimes referred to as punch-list items) are stated in the FCC Report & Order as:

- 1) Provide the content of subject-initiated conference calls supported by the subject's service (including the call content of parties on hold).
- 2) Identify the active parties of a conference call.
- 3) Provide access to all dialing and signaling information available from the subject including a subject's use of features (such as the use of flash-hook and other feature keys).
- 4) Notify law enforcement agency (LEA) when a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy).
- 5) Provide timing information to correlate call-identifying information with the call content of a communications interception.
- 6) Provide digits dialed by a subject after the initial call setup is completed.

Under the Report & Order, these features must be installed by September 30, 2001.

Are packet-mode communication technologies covered by CALEA?

The FCC has concluded 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 JEM does not intend to reach legal conclusions regarding the scope of CALEA and interested contributors to the JEM should consult legal counsel regarding CALEA obligations.

Fcc. CALEA
only

Why was the Joint Experts Meeting (JEM) convened?

Report from May 31, 2000

In the FCC's Third Report and Order regarding implementation of CALEA, it found "that the approach taken with regard to packet-mode communications in J-STD-025 raise[d] significant technical and privacy concerns." Under this standard, law enforcement could be provided with both call-identifying information and call content when only call-identifying information was authorized to be delivered.

The FCC "believe[d] 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." However, the FCC acknowledged that the record before it did not sufficiently address packet technologies and the problems that they may present for CALEA purposes. The FCC noted, for example, "that 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."

Accordingly, the FCC invited TIA to study CALEA solutions for packet-mode technology and report in one year on "steps that can be taken, including particular amendments to J-STD-025, that will better address privacy concerns." To meet the timetable envisioned by the FCC and to build a record based on technical information assimilated from a broad range of industry sources, TIA has convened a JEM.

What is the scope of the JEM?

The scope of the JEM includes reporting on the following packet-mode technologies: TDMA-supported packet (based on evolution of TIA/EIA-136), CDMA-supported packet (based on evolution of TIA/EIA-95), PCS 1900/GSM-supported packet, CDPD, X.25, ISDN, ATM, DSL, Frame Relay, and internet protocol (IP) (including voice over IP). This list of packet technologies is NOT all-inclusive; other packet technologies anticipated to be supported by telecommunications service providers subject to CALEA are welcome to contribute to the JEM.

The scope of the JEM does NOT include: (a) legal issues such as the scope of CALEA, including whether it covers any specific packet-mode communication technology; (b) interpretation of electronic surveillance laws or FCC orders or rules; or (c) the impact of encryption technology on lawfully authorized electronic surveillance other than as it affects the technical issues regarding the feasibility of delivering less than the full content of a packet (i.e., addressing information) to law enforcement in response to a pen register order. The fact that an organization or company contributes to the JEM regarding a particular packet technology is not an admission that CALEA applies to that technology or company.

What packet-mode communication technologies will be addressed at the JEM?

TDMA-supported packet (based on evolution of TIA/EIA-136), CDMA-supported packet (based on evolution of TIA/EIA-95), PCS 1900/GSM-supported packet, CDPD, X.25, ISDN, ATM, DSL, Frame Relay, and IP (including voice over IP).

This list of packet technologies is NOT all-inclusive; those with substantive knowledge of other packet technologies anticipated to be supported by telecommunications service providers subject to CALEA are welcome to contribute to the JEM.

Who may contribute to the JEM and how?

Technical organizations and experts that can add to the empirical body of evidence as it relates to packet-mode communication and CALEA compliance. A link will be provided on this site for contributions.

By what date must CALEA be implemented?

The core requirements of J-STD-025 must be implemented by June 30, 2000.

Additional capabilities required by the FCC as defined in FCC Docket No. 97-213, Third Report & Order, (9/24/99) must be implemented by September 30, 2001.



Association
Membership
Public Policy
Shows & Events

◆ **Standards & Technology**
Press & Publications
Int'l Affairs
Resources

News from TIA
Search/Buy Stds.
Interactive Buyer's Guide
Discussion Forum

FIND **IN** **Regular Documents** back up

<< [HOME](#) | [Advertise with us](#) | [Help Desk](#) | [Office Locations](#) | [Feedback](#)





Visit TIA's B2B
Communications Portal



Press & Publications

[HOME](#) ♦ [MAIN](#) ♦ [PulseOnline Past Issues](#) ♦ May '99

Choose a Sub Category...



TIA's Satellite Division Addresses CALEA Issues

Since the adoption of the Communications Assistance for Law Enforcement Act (CALEA) and publication of an interim industry standard, J-STD-025, CALEA concerns have expanded, impacting paging and satellite communications carriers. Responding to the emerging concerns of the satellite industry about CALEA, on April 1 the TIA Satellite Communications Division (SCD) hosted a CALEA and Critical Infrastructure Protection (CIP) Information session during the EIA/TIA Spring Conference in Washington, D.C.

The CALEA meeting was facilitated by Grant Seiffert, TIA vice president of government relations and Stewart Baker, partner, Steptoe & Johnson (and TIA legal counsel), who provided insightful commentary on the history of CALEA from its inception to current issues. The session focused primarily on CALEA and its impact on the satellite industry.

Distinguished speaker, Stephen R. Colgate, assistant U.S. attorney general for administration at the Department of Justice, remarked that CALEA was not intended to increase the authority of the FBI in the lawful collection of communications beyond reasonably achievable methods. Furthermore, Colgate noted that The Netherlands, South Africa, Ireland, the European Union and this year Australia, are adopting similar legal wiretapping initiatives. Colgate stated that these initiatives create unique international legal issues that will impact the satellite industry's future implementation of CALEA.

Dan Connors, legal advisor to Federal Communications Commission (FCC) Commissioner Ness' Office, explained that the FCC's role with respect to CALEA was primarily to evaluate CALEA cost matters and to mediate when deadlocks occur between communications carriers and the FBI.

CALEA Background

President Clinton signed CALEA into law on October 25, 1994. CALEA defines the duty of telecommunications carriers to assist law enforcement agencies with the lawful interception of communications and the collection of call-identifying information and call content in a constantly changing telecommunications environment. Designed to enable law enforcement agencies to continue to conduct court-authorized surveillance of wire and electronic communications, CALEA states that telecommunications carriers are required to meet the assistance capability requirements set forth in Section 103 of the act. The attorney general

assistance capability requirements set forth in section 103 of the act. The attorney general, by memorandum dated February 24, 1995, delegated management and administration responsibilities of CALEA to the FBI. (For more details, refer to the CALEA section of TIA's Web site at <http://www.tiaonline.org/government/CALEA/>.)

To mediate concerns of the FBI and private-sector telecommunications carriers, manufacturers and others, the FCC was required by law to assist with the implementation of CALEA. After labored discussions among the FCC, FBI and U.S. telecommunications carriers and manufacturers, the FCC reviewed all of the comments submitted concerning the initial CALEA compliance deadline, October 25, 1998. The commission found that compliance with the assistance capability requirements of Section 103 was not reasonably achievable for any telecommunications carrier through the application of technology available before the compliance deadline. Therefore, the October 25, 1998, deadline was extended until June 30, 2000. The FCC's decision to grant an industrywide extension was based primarily upon the agreement of all parties that it should take manufacturers approximately two years from the date on which technical requirements are standardized to develop and begin deploying technology capable of complying with the standard. The FCC added that the June 30, 2000, deadline seemed appropriate for another reason, which was to not have a CALEA compliance deadline that would conflict with the telecommunications industry's efforts to comply with the Year 2000 problem.

"Safe-Harbor Standards"

Working closely with telecommunications carriers and manufacturers, TIA and Committee T1, sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), developed the joint interim industry standard, J-STD-025, which was adopted in December 1997. J-STD-025 defines services and features to support lawfully authorized surveillance and the interfaces to deliver intercepted communications and call-identifying information to law enforcement agencies. This interim industry standard was a "safe harbor," allowing any carrier complying with J-STD-025 to be considered by the FCC to be compliant with the CALEA assistance capability requirements specified in section 103 of the act. Notably, this standard pertained to wireline, cellular and personal communications services (PCS) carriers whose capacity and capability requirements had not been identified at that time.

For more information on this CALEA/CIP information session, contact Benjamin Walston at (703) 907-7749 or email bwalston@tia.eia.org.



Association
Membership
Public Policy
Shows & Events

Standards & Technology
➤ **Press & Publications**
Int'l Affairs
Resources

News from TIA
Search/Buy Stds.
Interactive Buyer's Guide
Discussion Forum

FIND **IN** **Regular Documents**

◀ back ▲ up

[<< HOME](#) | [Advertise with us](#) | [Help Desk](#) | [Office Locations](#) | [Feedback](#)



© 2000 Telecommunications Industry Association
[[Copyright & Disclaimer](#)] [[Privacy Statement](#)]

Last Updated: 12/02/99



Second Joint Experts Meeting (JEM) on CALEA Packet Surveillance

**June 27 (9am start) to June 29 (2pm end)
St. Regis Hotel, 16th St. and K St. NW, Washington, DC**

Meeting Summary

1. Call to Order and Opening Remarks: The chair opened the meeting at 9am on June 27.

- JEM Chair remarks (including purpose and scope of both JEM sessions) The JEM chair reiterated the purpose and scope of the JEM per the initial invite letter (see CALEA JEM link at www.tiaonline.org for a copy of this letter). Three major points were made: (1) the JEM is a fact-finding body, (2) the main purpose of the JEM is to determine the feasibility of delivering less than the full content of a packet to law enforcement under a pen register or trap and trace court order, and (3) the information obtained from the JEM will be submitted to TIA to assist with the TIA report due to the FCC by September 30, 2000.

The scope of the JEM included consideration of all packet technologies (including, but not limited to, IP, TDMA, CDMA, PCS, GSM, CDPD, X.25, ATM, ISDN, Frame Relay, Cable, XDSL). Legal issues, speculative interpretation of FCC orders, and the impact of encryption (other than the effect on technical ability to delivery less than the full content of a packet) were outside the scope of the JEM.

See agenda item 5 below for a summary of the first JEM session.

- Ground Rules for the second JEM session: The JEM chair described the ground rules listed below.
 - A. Run like a TIA standards meeting
 - All contributions numbered and addressed
 - All views explored equally
 - Decisions are consensus (not unanimous) based; JEM chair will use TIA engineering manual definition of consensus
 - Final report will contain items discussed and agreements, as well as minority opinions, if unavoidable
 - B. Deal with technical merit, not emotion
 - C. The subject of cost will not be discussed.
 - D. The goal of the second JEM session is to continue documenting a list of technical alternatives to assist TIA in developing their report to the FCC, with an emphasis on providing details for the technology-specific appendices of the JEM report. In addition, issues associated with each alternative will be identified.

- 2. Introductions and Attendance Registration:** Approximately 80 persons attended the second JEM session. A wide range of companies were represented, as was the FBI and the FCC. The attendance rosters for both JEM sessions are posted on the CALEA JEM website.
- 3. Approve Agenda:** The agenda was approved as is.

4. Distribute, Number, and Assign Contributions:

12 contributions were distributed before or during the meeting, and one contribution from the first JEM session (#105 from Compaq) was discussed. All contributions (including the agendas for both JEM sessions) are posted on the CALEA JEM website. The following illustrates the contribution number, title, and source of each new contribution to the second JEM session:

110: Summary of Wireless Technologies for the Appendix (Rogers Wireless)

111: CDMA2000 Wireless IP Appendix (TIA TR45.6)

112: X.25 over ISDN BRI Technology Appendix (T1)

113: ATM Technology Appendix (T1)

114: Frame Relay Technology Appendix (U S WEST)

115: GPRS Technology Appendix (T1)

116: Call Associated Signaling Reporting (T1)

117: PacketCable Technology Appendix (PacketCable Project of CableLabs)

118: CDPD Technology Appendix (Lucent)

119: IP Technology Appendix (Cisco)

120: Functional Model for Packet Mode Surveillance and Use of Separation Function (FBI CIS)

120a: Information to be added to the IP Appendix (FBI CIS)

5. Background

- Summary of May 3-5 JEM session: JEM chair/vice-chair: Peter Musgrove provided a brief verbal readout. See written meeting summary of the first JEM session on the CALEA JEM website.
- Summary of May 23 Drafting Group meeting: JEM chair/vice-chair: Peter Musgrove pointed out that the drafting group only incorporated comments that were deemed to be within the agreements of the first JEM session. Many comments received via the email reflector were outside that scope and thus were not incorporated by the drafting group. Peter noted that folks are expected to bring up these comments at the second JEM session.
- Update on Legal (CALEA) and Regulatory (FCC R&O) issues since first JEM session: Al Gidari (CTIA), Montgomery Kosma (Gibson, Dunn, and Crutcher LLP): Montgomery Kosma provided a brief overview of recent judicial proceedings with regard to CALEA,

including activity on the pending appeal of the FCC Report and Order before the US Court of Appeals for the District of Columbia.

- Update on J-STD-025 and revisions since first JEM session: Terri Brooks, Chair, TR45.2 Lawfully Authorized Electronic Surveillance (LAES) AdHoc Group: Terri Brooks reported that July 24 is the deadline for ballot comments on the ANSI version of J-STD-025, and August 4 is the deadline for ballot comments on the ANSI version of J-STD-025A. The T1 ballot comment deadline on the ANSI version of J-STD-025 is June 28. The TR45.2 LAES adhoc group ballot review meeting is currently targeted for August 22-24 in Montreal.
- Today's Methods for Separating Pen Register Data from Content on Packet Surveillances, Presentation and Demonstration by FBI Engineering Research: Greg Kesner and Eddie Hill (from the FBI's Engineering Research Facility in Quantico, VA) provided the FBI presentation of their so-called "Carnivore" software which is purportedly able to filter specific information for packet sessions for pen register orders. This software apparently screens IP data fields at various levels in the full packet stream containing the subject's communications. The presentation was used as a basis for the FBI contribution #120 regarding the proposed introduction of a separation function into a TSP network that would filter identifying information from a particular packet stream (see discussion of that document below).

6. Industry contributions on CALEA Packet Surveillance (Main Body of JEM Report)

- Standards Development Organization (SDO) contributions: none.
- Industry Forum contributions: none.
- Individual company contributions on CALEA Packet Surveillance Issues

#120 (Functional Model for Packet Mode Surveillance and Use of Separation Function from the FBI Calea Implementation Section) was presented by Lou Degni and Ken Coon. The recommendations in this contribution were not accepted; however, the task of incorporating a description and a list of issues associated with the separation function was remanded to the drafting group.

(Encourage presenting contribution only if substantively different from SDO or industry contributions above)

7. Industry contributions on CALEA Packet Surveillance (Technology-Specific Appendices)

- Standards Development Organization (SDO) contributions

#111 (Draft appendix for CDMA2000 Wireless IP from TR45.6) was presented by Mark Munson. The group accepted the content of this document and remanded to the drafting group the task of incorporating into the JEM report. AT&T brought up the issue of IP overlap with this and other technologies in the JEM report appendices. The drafting group can consider splitting IP considerations out of each technology-specific appendix, if needed. Some folks commented that overlap with IP text is necessary to maintain logical flow of appendices.

#112 (Draft X.25 over ISDN BRI Technology Appendix for TIA JEM II on Packet Data Surveillance Capabilities from Committee T1S1) was presented by Jay Hilton. This document was accepted and remanded to the drafting group for incorporation into the JEM report.

#113 (Draft ATM Technology Appendix for TIA JEM II on Packet Data Surveillance

Terri
Association

Capabilities from Committee T1S1) was presented by Jay Hilton, who attributed the input to David Hoffman of U S WEST. This document was accepted and remanded to the drafting group for incorporation into the JEM report. Jay commented that the drafting group may want to consider accepting only a subset of this text for eventual incorporation into the JEM report.

#115 (GPRS Specific Information for TIA JEM Report Appendices from T1P1) was presented by John Menard on behalf of Ron Ryan. This document was accepted and remanded to the drafting group for incorporation into the JEM report. The drafting group was asked to remove the ASN.1 encoding without losing any of the pertinent information contained therein.

#116 (Call Associated Signaling Reporting for TIA JEM Report Appendices from T1P1) was presented by John Menard on behalf of Ron Ryan. This document was accepted and remanded to the drafting group for incorporation into the JEM report. The drafting group was asked to decide whether this should be a separate appendix or added to the appendix that is the subject of document #115.

- Industry Forum contributions

#117R1 (PacketCable Technology-Specific Subchapter from the PacketCable project of CableLabs) was presented by Bill Marshall. The drafting group should change “should” to “could” or provide explanatory text stating that suggested IAP locations in this appendix are examples only and are not mandated implementations. Bill asked that three different appendices should be used: one for Cable (physical media), one as an add-on to the appendix on IP, and one devoted to a CMS-controlled VOIP appendix. Handle ASN.1 material same as document #115. Change “we” to “Cablelabs” in reference to 5% capacity number. This document was accepted with modifications noted above and remanded to the drafting group for incorporation into the JEM report.

- Individual company contributions on CALEA Packet Surveillance Issues
(Encourage presenting contribution only if substantively different from SDO or industry contributions above)

#110 (CALEA Packet Data JEM: Appendix Summary from Rogers Wireless) was presented by the chair (Peter Musgrove) on behalf of Ed O’Leary. Peter asked if an advocate would be willing to come forward to push for the recommendation in this document. As no advocate was identified, the recommendation in this contribution was not accepted.

#114 (Draft Frame Relay Technology Appendix for TIA JEM II on Packet Data Surveillance Capabilities from U S WEST) was presented by Jay Hilton (on behalf of David Hoffman). Jay commented that T1S1 had not approved this document, and that they will review output of second JEM session at mid-July T1S1 meeting. This document was accepted and remanded to the drafting group for incorporation into the JEM report

#118 (Draft CDPD appendix for TIA JEM on Packet Data Surveillance Capabilities from Lucent) was presented by William Waung. This document was accepted and remanded to the drafting group for incorporation into the JEM report. It was pointed out that the JEM

(near the end of the meeting) should develop a plan for this and some other appendices to fill in the technical feasibility section before the completion of the JEM report.

#119 (Proposed IP Appendix for FCC Report from Cisco) was presented by Chip Sharp. This document was accepted and remanded to the drafting group for incorporation into the JEM report.

7.5. New Business

#105 (Approach to CALEA Packet to Surveillance from Compaq) was presented by Mark Montz. The recommendations in this document were determined to be closely related to those in the FBI documents #120 and #120a. The largest difference is the provider of the separation function (filtering) software. The Compaq contribution says that open source code should be used in the CALEA sniffer box (i.e., same as the FBI's "separation function"). There were comments for and against the idea of having source code open to the public. The recommendations in this contribution were not accepted; however, the group agreed to remand to the drafting group the task of incorporating a description and a list of issues associated with the separation function and the software code associated with it. These recommendations were discussed in conjunction with those in document #120 and #120a.

#120a (FBI contribution on suggested changes to the IP appendix) was presented by Ken Koon (spelling????). The scalability of the separation function was raised as an issue by AT&T, as well as the feasibility of providing weekly updates to separation function software. SBC raised security and legal issues of the FBI's code or a neutral group's code going into the TSP's network as a separation function. The group agreed to remand the FBI document #120a to the drafting group and encouraged a new section to be added that describes the separation function and the issues associated with it.

8. **Identification of Technical Issues and Alternatives:** This item was handled during the discussion of each of the contributions (see discussion above).
9. **BREAK: Allow Breakout Drafting Group to Refine Key Elements of JEM Report:** The JEM broke at 12:15pm on Wednesday to allow the drafting group to convene at 2pm to revise the JEM report based on the resolution of each of the contributions.
10. **Review JEM Report:** On Thursday morning, Brye Bonner (editor) led discussion describing the output of the drafting session. Many changes were made in real time to the draft JEM report. Other changes not added in real time were remanded to the editor for incorporation after the meeting: (1) The group agreed to add footnote in section 5.2.1 to say that limitation of packet stream to one user's information due to J-STD-025 is an improvement over the current state of the art used by the FBI in which their Carnivore software performs a filtering function on an information pipe from an ISP (with information for multiple users). It was pointed out that privacy groups should understand this improvement afforded by the existing J-STD-025 method for packet surveillance. (2) In GPRS appendix, the editor was asked to use the T1P1 text from the first JEM session as input to creating an introduction section. The JEM steering committee was remanded the task of preparing an overview of "JEM 2 Output" for the JEM report.

11. Clarification of Post-JEM Process for Finalizing JEM Report for forwarding to TIA:

- (1) The editor will provide a revised draft JEM report by June 30, 2000 to the JEM email reflector.
 - (2) Email comments on this revised draft JEM report are due Monday, July 24.
 - (3) Drafting session will be held July 27 (9am start) and July 28 (noon end) in the Washington, DC area. The work of the drafting session is to be conducted in the context of existing JEM agreements.
 - (4) Revised draft JEM report will be sent to the reflector by August 4.
 - (5) Final JEM participant comments on the draft JEM report are due to the reflector by August 16.
 - (6) JEM Steering committee will finalize report and send to reflector (with courtesy copy to TR45, T1, and other SDOs/organizations) and to TIA. Finalization will be done in the context of existing JEM agreements.
 - (7) TIA will use JEM report to create the TIA report due to the FCC on September 30, 2000.
12. **Closing Statements/Adjourn:** The chair thanked the vice-chair and editor for their work on JEM activities. The chair thanked all JEM participants for their contributions and for the resulting enlightening discussion. The second JEM session adjourned around 11:45am on Thursday, June 29, 2000.

TIA COMMITTEE TR-45 MOBILE & PERSONAL COMMUNICATIONS STANDARDS (TR-45)

TITLE: CALEA Packet Surveillance Draft JEM Report

ABSTRACT: This contribution contains the current draft report resulting from the first JEM session.
A second JEM session is planned for June 27-29 to complete the report for TIA.

DATE: May 31, 2000

SOURCE: Peter Musgrove (JEM chair)
AT&T Wireless Services
425-580-6875
peter.musgrove@attws.com

RECOMMENDATION: This document is provided for information only to TR45 to illustrate the
progress achieved at the initial JEM session.

COPYRIGHT STATEMENT:

The contributor grants a free, irrevocable license to the Telecommunications Industry Association (TIA) to incorporate text or other copyrightable material contained in this contribution and any modifications thereof in the creation of a TIA standards publication; to copyright and sell in TIA's name any TIA standards publication even though it may include portions of this contribution; and at TIA's sole discretion to permit others to reproduce in whole or in part such contributions or the resulting TIA standards. This contributor will also be willing to grant licenses under such copyrights to third parties on reasonable, non-discriminatory terms and conditions, if appropriate

NOTICE:

Permission is granted to TIA Committee participants to copy any portion of this document for the legitimate purposes of the TIA. Copying for monetary gain or other non-TIA purposes is prohibited.

Report to TIA on Surveillance of Packet Data

1 References

- TIA /ATIS Interim Standard (Trial Use Standard): Lawfully Authorized Electronic Surveillance, J-STD-025, December 1997.
- Federal Communications Commission, Third Report and Order, CC Docket 97-213, FCC 99-230 released August 31, 1999.
- Packet Cable Standard

2 Definitions and Acronyms

CMS: Call Management Server

H.323: ITU-T Standard for Multimedia call establishment

SIP: Session Initiation Protocol (IETF)

VoP: Voice over Packet

3 Introduction and Executive Summary

3.1 Convening the JEM

In its Third Report and Order regarding implementation of the Communications Assistance for Law Enforcement Act (CALEA), the FCC finds "that the approach taken [by industry] with regard to packet-mode communications in J-STD-025 raises significant technical and privacy concerns." Under J-STD-025 for packet mode communications, law enforcement could be provided with call content when only call-identifying information was authorized to be delivered.

The FCC "believe[s] 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." However, the FCC acknowledges that the record before it does not sufficiently address packet technologies and the problems that they may present for CALEA purposes. The FCC notes, for example, "that 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."

1 Accordingly, the FCC invited TIA to study CALEA solutions for packet-mode
2 technology and report in one year on "steps that can be taken, including
3 particular amendments to J-STD-025, that will better address privacy concerns."
4 To meet the deadline imposed by the FCC, and to build a record based on
5 technical facts, the Telecommunications Industry Association (TIA) has
6 sponsored two Joint Experts Meetings. Lists of JEM invitees and attendees are
7 attached as Appendix A and B, respectively.

8
9 The JEM has served as a technical fact-finding body across the spectrum of
10 packet-mode communication technologies regarding the feasibility of delivering
11 less than the full content of a packet to law enforcement in response to a pen
12 register order. While the scope of the JEM included reporting on the broadest
13 number of packet mode communications technologies, contributions were
14 received only on the following technologies: CDMA2000, GPRS, and IP.

15
16 Prior to meeting in person, contributions from various entities were made
17 available through posting on the TIA website (see CALEA JEM link at
18 www.tiaonline.org). A publicly available mailing list was also maintained. A two-
19 hour question and answer session covering the scope of the JEM was conducted
20 on March 20, 2000. The JEM then convened on May 3-5, 2000, in Las Vegas,
21 NV. Following opening remarks updates were provided on the status of Revision
22 A of J-STD-025, the legal purpose of the JEM, and the status of CALEA
23 activities. Presentations on technical issues followed. A copy of the JEM agenda
24 is attached.

26 **3.2 JEM I Output**

27
28 The first JEM (JEM I) established a framework for preparing this report. A copy
29 of the JEM 1 meeting report to TIA TR45 is attached as appendix C.

30
31 First, JEM I concluded that, based on current FCC guidance, it could not define
32 "call-identifying information" for packet services. Several contributors noted that
33 the term "call-identifying information" is ambiguous with regard to packet
34 communications. Instead, JEM 1 concluded that it could only attempt to identify
35 what information may be available about the packet communication. Once
36 identified, JEM I concluded that it could then best report on the technical impact
37 and feasibility of making that information available to a law enforcement agency
38 (LEA). This decision was consistent with the purpose and scope of the JEM,
39 which did not include discussion of legal issues.

40
41 Second, JEM I noted CALEA requirements apply to telecommunication services
42 but not information services. JEM I recognized, however, that from a packet
43 point of view, the two may be indistinguishable. JEM I determined that it is not
44 technically advisable to determine, on a packet by packet basis, the application
45 or communication service that is being provided. JEM I also concluded that, the

1 application or communication service that is being provided can not be
2 determined even by observation of the complete stream of packets. The point of
3 call setup may be the only time that a telecommunication service can be
4 distinguished from an information service.

5
6 JEM I further concluded that the possibility of encapsulation or encryption of
7 packets outside of the service provider's control makes identifying the application
8 or service even more unlikely.

9
10 The JEM addressed the issues related to packet mode services in two main
11 categories: (1) packet communication sessions established by a Call
12 Management Server (CMS), and (2) transport services, i.e. packet
13 communication sessions established without a CMS. The CMS may, for
14 instance, be an H.323 GateKeeper, or a SIP proxy, or something conceptually
15 equivalent. Typically an access service provider that offers a CMS also provides
16 transport.

17
18 Accordingly, the framework for this report reflects this two-pronged approach. In
19 each category, the JEM decided to report on the information available and the
20 technical impact of providing it. A second JEM was scheduled to be held in
21 Washington, D.C., on June 27-29, 2000, to accept contributions for each
22 technology. Assignments were taken to prepare appendices of technologies for
23 this report.

24
25 Finally, JEM I agreed that if a change to the current standard (J-STD-025) were
26 deemed necessary by the Federal Communications Commission, a court or the
27 industry, as a result of this process, the JEM recommends that the open, joint
28 T1/TIA activity currently underway in 45.2 LAES Ad Hoc be responsible for
29 completing this task. In its simplest form, this change may just be the inclusion of
30 appropriate references to other standards. Nothing in this process, however,
31 precludes any standards setting or industry organization from adopting their own
32 "safe harbor" standard for their particular technology (e.g., satellite or cable
33 standards).

34 35 **3.3 JEM 2 output [editor's note - placeholder]**

36 37 38 **4 Packet Communication Sessions established by a Call** 39 **Management Server**

40
41 The service provider that provides a call service via a call management server,
42 e.g., an H.323 GateKeeper or a SIP proxy. The following discussion assumes
43 that the CMS is providing call events. If the CMS does not provide call events
44 then the discussion in section 5 applies.

4.1 Information that can be reported

Information available is analogous to J-STD-025 call events, but with respect to each technology, enhancements may need to be made to J-STD-025. For example, with respect to Voice-over-Packet (VoP) services, the JEM notes that additional enhancements are needed to J-STD-025 (e.g., to report VoP calls and associated call identifying information, to identify the content stream, and to identify the timing requirements). Other standards may address other technologies and networks.

4.2 Technical Impacts

The type of call content delivered to the LEA may differ from that negotiated with the provider (i.e., the call-identifying packet stream can not guarantee the user is using the packet stream as negotiated).

Interception of packet services also does not guarantee that the packets have been received by the terminating system.

H.323 and SIP call events may not map directly to those call events established in J-STD-025 (e.g., triggering events may be different). Impacts associated with development of a protocol to support reporting packet data communication call events have not yet been investigated and there may be unforeseen issues.

Timing requirements need to be reviewed and may need to be specified for each technology.

The JEM did not address possible difficulties in associating call events with call content as required by CALEA.

5 Packet Communication Sessions established without a Call Management Server

This section describes the service providers that provide packet mode transport, but do not provide access service via a CMS.

5.1 Information that can be reported, subject to technical impact analysis

Establishment of a communication path across an accessing system from the subject's device to a network (not the endpoint) may be required before communication between the subject and associate can begin. If so, the establishment and release of this path could be reported. The information provided may be technology-dependent.

Reporting of information beyond establishment and release requires access to the individual packets, which may yield further information such as non-encapsulated routing information. Alternatively, the entire packet could be

delivered. It must be noted that either may be difficult and not feasible for some existing systems and architectures, as discussed below.

5.2 Technical Impacts

5.2.1 Delivering the Entire Packet Stream

If the service provider is required to deliver the entire packet to provide call-identifying information for a pen-register, the following issues have been identified.

The consensus is that duplication of a packet stream requires significant resources. This may be technology dependent. These resources compete with the Title III resources as well as capacity requirements.

The subscriber under surveillance, and their associates, may detect performance degradation resulting from the impact of duplication of a packet stream for every Pen Register. Other customers using the packet data services of the TSP may also detect the degradation of performance. The JEM notes that a single subscriber to the packet transport service may utilize excessive packet capacity.

5.2.2 Investigating the Packet Stream

Consensus is that examining beyond the outermost routing header of a packet, e.g., IP header, ATM cell header, Frame Relay header, X.25, etc., to identify call-identifying information is not technically advisable (i.e., due to technical complexity, extreme processor load, encryption, unknown protocols, and inability to identify the target).

Consensus is that the information gained from examining the outermost header may not yield useful call-identifying information (e.g. the actual identity of the subject and associate endpoints).

The above considerations are magnified as access speeds increase to gigabit/sec and faster. High-speed technologies may not permit time to investigate the packet.

Timing requirements need to be reviewed and may need to be specified for each technology.

¹ Vendor studies in one technology (PacketCable) determined that packet duplication of over 5% would have such an impact, and that requirements for duplication capacity in excess of 5% would require redesign of the network.

6 Technology Specific Information

Editor's note:

Guide to appendices.

Bullet list of what protocols will have appendices.

Note that we did not receive contributions for all possible packet technologies and not all packet technologies were represented at JEM.

Framework of the Technology Specific Information Subchapter (approx.1-5 pages).

- Architecture overview (diagram)
- Protocol type supported (e.g. IPv4/IPv6, connection/connectionless)
- Performance of the system based on expert opinion.
 - Performance when providing call events.
 - Performance when providing full packet.
- Preferred delivery format.
- Technical feasibility/infeasibility – (reference body of doc).
- Complexity of various solutions.
- How do you map the target identity to the technology address?
- How do you identify the associate?
- What information can be provided to law enforcement (be specific as to whether CMS is used or not)?
 - Do you have a CMS, if so, what information can be provided?
 - If you do not have a CMS what information can be provided?
- Where are the possible points of intercept and their impacts to existing architecture?
- List of relevant standards.
- Possibilities for delivering serving system message.

6.1 Access networks:

6.1.1 CDMA2000

SDO Lead: TR45.6

Contact: Mark Munson (GTE Wireless)

6.1.2 GPRS/UMTS/TDMA

SDO/Org Lead: T1/ETSI/TIA/UWCC.

Contact: Ron Ryan (Nortel), Bernie McKibben (Motorola), Bill Marshall (AT&T)

6.1.3 CDPD

SDO Lead: TR45.6

1 Contact: Dean Anderson (Lucent)

2

3 6.1.4 Packet Cable

4 SDO Lead: CableLabs

5 Contact: Bill Marshall (AT&T)

6

7 6.1.5 xDSL

8 SDO/Org Lead: DSL Forum

9 Contact:

10 6.1.6 X.25

11 SDO Lead: ITU

12 Contact:

13

14 6.1.7 ISDN

15 SDO Lead: T1S1

16 Contact:

17 **6.2 Network layer protocols:**

18 6.2.1 ATM

19 SDO/Org Lead: ATM Forum

20 Contact David Hoffman dwhoffm@uswest.com, Jay Hilton (Telcordia)

21

22 6.2.2 IP, Ipv4, Ipv6

23 SDO Lead: IETF

24 Contact: Chip Sharp (Cisco)

25

26 6.2.3 Frame Relay

27 SDO/Org Lead: Frame Relay Forum

28 Contact: Dave Hoffman (U S WEST)

29

30

31 **6.3 Application layer protocols:**

32 6.3.1 SIP

33 SDO Lead: IETF

34 Contact:

The Drake Hotel
Chicago, IL

TR45/00.05.31.26

- 1 6.3.2 H.323
- 2 SDO Lead: ITU
- 3 Contact:
- 4

TIA COMMITTEE TR-45 MOBILE & PERSONAL COMMUNICATIONS STANDARDS (TR-45)

TITLE: CALEA Packet Surveillance JEM Meeting Summary

ABSTRACT: This contribution contains a summary of the first CALEA Packet Surveillance JEM session held in Las Vegas, NV May 3-5, 2000.

DATE: May 31, 2000

SOURCE: Peter Musgrove (JEM chair)
AT&T Wireless Services
425-580-6875
peter.musgrove@attws.com

RECOMMENDATION: This meeting summary is provided for information to TR45. There was consensus among JEM participants that a second JEM session is needed to allow for appropriate completion of the JEM report to TIA. Because of the need for timely delivery of the JEM report to TIA (which must then deliver a report to the FCC by September 30), the JEM steering committee requests that TR45 remand to the steering committee the tasks of (1) conducting the second JEM session, (2) conducting the appropriate drafting group sessions, and (3) delivering a final JEM report to TIA.

COPYRIGHT STATEMENT:

The contributor grants a free, irrevocable license to the Telecommunications Industry Association (TIA) to incorporate text or other copyrightable material contained in this contribution and any modifications thereof in the creation of a TIA standards publication; to copyright and sell in TIA's name any TIA standards publication even though it may include portions of this contribution; and at TIA's sole discretion to permit others to reproduce in whole or in part such contributions or the resulting TIA standards. This contributor will also be willing to grant licenses under such copyrights to third parties on reasonable, non-discriminatory terms and conditions, if appropriate

NOTICE:

Permission is granted to TIA Committee participants to copy any portion of this document for the legitimate purposes of the TIA. Copying for monetary gain or other non-TIA purposes is prohibited.

Joint Experts Meeting (JEM) on CALEA Packet Surveillance May 3-5, 9am – 5pm PT, Las Vegas, NV

Meeting Summary

<<Note that the documenting convention used throughout this report is that **boldface** print represents agenda items, and non-boldface print represents the meeting summary.>>

1. **Call to Order and Opening Remarks:** Peter Musgrove, JEM chair, opened the meeting at 9am on May 3.

- **JEM Chair remarks (including purpose, scope, acknowledgement of JEM-related work in email discussions and March 20 Q&A call):** The JEM chair reiterated the purpose and scope of the JEM per the initial invite letter (see CALEA JEM link at www.tiaonline.org for a copy of this letter). Three major points were made: (1) the JEM is a fact-finding body, (2) the main purpose of the JEM is to determine the feasibility of delivering less than the full content of a packet to law enforcement under a pen register or trap and trace court order, and (3) the information obtained from the JEM will be submitted to TIA to assist with the TIA report due to the FCC by September 30, 2000.

The scope of the JEM included consideration of all packet technologies supported by Telecommunications Services Providers (TSPs) subject to CALEA (including, but not limited to, TDMA, CDMA, PCS, GSM, CDPD, X.25, ATM, ISDN, Frame Relay, Cable, XDSL). Legal issues, speculative interpretation of FCC orders, and the impact of encryption (other than the effect on ability to delivery less than the full content of a packet) were outside the scope of the JEM.

The JEM chair summarized the most significant pre-JEM activities. There was very limited email reflector discussion of a technical nature before the JEM. On the March 20 Q&A conference call, the following topics were covered in depth: CALEA history and background, a review of regulatory and judicial proceedings, and an update on the status of J-STD-025 and its revisions. A summary of the March 20 Q&A session is available on the CALEA JEM website.

- **Ground Rules for JEM:** The JEM chair described the ground rules listed below.
 - A. Run like a TIA standards meeting**
 - All contributions numbered and addressed
 - All views explored equally
 - Decisions are consensus (not unanimous) based; JEM chair will use TIA engineering manual definition of consensus
 - Final report will contain items discussed and agreements, as well as minority opinions, if unavoidable
 - B. Deal with technical merit, not emotion**
 - C. The subject of cost will not be discussed.**

D. The goal of the JEM is to document a list of technical alternatives to assist TIA in developing their report to the FCC. In addition, issues associated with each alternative will be identified.

2. **Introductions and Attendance Registration:** Approximately 70 persons attended the JEM. A wide range of companies were represented, as was the FBI, the FCC, and the Center for Democracy and Technology (CDT). The attendance roster is posted on the CALEA JEM website.
3. **Approve Agenda:** The JEM agenda was approved without modifications.
4. **Distribute, Number, and Assign Contributions:** 9 contributions were distributed during the meeting. All contributions (including the agenda) are posted on the CALEA JEM website. The following illustrates the contribution number, title, and source of each contribution:

100: TIA/EIA/IS-J-STD-025 Lawfully Authorized Electronic Surveillance Standard: TIA and T1

101R1: Method for Identifying Telecommunications Services and Information Services for Packet-Mode Communications Subject to Surveillance Under CALEA: Universal Wireless Communications Consortium (UWCC)

102 Part 1: Lawful Interception Stage Two document: ETSI/3GPP Joint Working Group

102 Part 2: Liaison statement from ETSI SMG 10 WPD/3GPP SA3 LI WG to TIA TR45 on Harmonized Packet Data Intercept Standards: ETSI/3GPP Joint Working Group

103: Liaison from TR45.2 including two sections of J-STD-025 relevant to packet: TIA TR45.2

104: Packet Mode Communication Call Identifying Information Reporting: T1

105: Approach to CALEA Packet Surveillance: Compaq

106: TR45.6 Report to TIA JEM on Packet Data Surveillance Capabilities: TIA TR45.6

107: Comments on Technical Aspects of Electronic Surveillance of Packet Mode Communication: Cisco Systems

108: Comments on J-STD-025A in regards to packet-mode communication using IP: Cisco Systems

109: CTIA Liaison Report: CTIA

5. Background

- **Legal (CALEA) and Regulatory (FCC R&O) framework for JEM:** Al Gidari, Ed Hall (CTIA): Al Gidari, CTIA, provided a brief overview of the legal and regulatory framework regarding CALEA. See Frequently Asked Questions (FAQs) on the CALEA

JEM website for a detailed summary. Al also pointed out that TSPs may file petitions with the FBI by May 31, 2000 to seek an extension of the CALEA compliance date to March 2001. See FBI website for more information about the flexible deployment plan that must accompany any such filing. Al also indicated that wiretap statistics can be found at www.uscourts.gov/wiretap99.pdf. Ed Hall briefly presented contribution 109 (CTIA Liaison report) for information only; this document indicated CTIA's continued support and interest in the topics to be addressed at the JEM.

- **J-STD-025 and revisions (history and current status): Terri Brooks and Gary Pellegrino, Chair and Vice-Chair, respectively, of TR45.2 Lawfully Authorized Electronic Surveillance (LAES) AdHoc Group:** Terri Brooks, chair TR45.2 LAES AdHoc Group, provided a brief overview of the past and ongoing work regarding J-STD-025 and its revisions. Terri pointed out that (1) J-STD-025 was originally published in late 1997, (2) J-STD-025A, which includes support for several FBI "punchlist" items but contained no changes to packet data support, was published in April 2000, and (3) both J-STD-025 and J-STD-025A are slated to be sent out for separate ANSI ballots during May 2000. Terri also provided a brief overview of the packet support methods in J-STD-025.

Contribution 100 (J-STD-025) was introduced by Terri Brooks as "for information only" to the JEM.

Contribution 103 (Liaison from TR45.2) was introduced by Gary Pellegrino, Vice-Chair TR45.2 LAES AdHoc Group. The liaison pointed out that the deployment of an interim packet data solution may be able to be avoided if a long-term standard solution could be achieved quickly (via the JEM process, quick decision-making by the FCC, and quick standardization activity by relevant standards development organizations). The JEM reached consensus on the following sentences: If a change to the current standard (J-STD-025) is deemed necessary by the FCC, a court, or the industry as a result of this process, the JEM recommends that the current joint open TIA/T1 activity currently underway in the TR45.2 LAES AdHoc group be responsible for completing this task. In its simplest form, this change may just be the inclusion of appropriate references to other standards. The resolution of Contribution 103 is contained entirely in the agreement reached above.

6. **Industry contributions on CALEA Packet Surveillance Issue:** The JEM participants agreed to allow the contributors of each document under this agenda item to provide an overview and explain the rationale for their recommendations. However, it was agreed that the JEM would not act on any recommendations in any particular contribution until all contributors under this agenda item received the opportunity to present their respective documents in an initial pass. Subsequently, the JEM would revisit and act upon the individual recommendations in a second pass of each contribution. The summary notes below indicate the results of the first pass discussion. The resolution of the recommendations achieved during the second pass are described under agenda items 7 and 8 below.

- **Standards Development Organization (SDO) contributions:**

Contribution 102, Parts 1 and 2 (ETSI/3GPP JWG Liaison) was presented by Bernie McKibben (Motorola). Bernie indicated that a small adhoc group could address the details in these documents at some point during the JEM. Some concerns were voiced that the harmonization issue would have to be worked by an SDO and not by the JEM.

Bernie indicated that event reporting only could be done to solve the pen register delivery issue for GPRS packet data. The JEM chair requested that the contributor attempt to summarize the key issues relevant to the JEM to ease discussion of this document in the second pass.

Contribution 104 (T1 Liaison) was presented by Wayne Zeuch (T1 Vice-Chair) and Ron Ryan (T1P1 LAES AdHoc Group Chair). This document provided a list of items that could be sent to law enforcement via event reporting, including access control information, packet data communication addresses, and call associated information. Ron indicated that the difficulty of the event reporting described in this document had not been gauged, and that he expected the JEM to perform this function.

Contribution 106 (TIA TR45.6 Liaison) was presented by Mark Munson (TR45.6 Chair). The document stressed issues with reporting user identity, call identifying information, access control, and serving system information.

- **Industry Forum contributions:**

Contribution 101R1 (UWCC position) was presented by Bill Marshall (AT&T). This document stressed the importance of determining when it is feasible for a system to determine and send call identifying data for packet communications to law enforcement for a pen register or trap and trace court order. The document indicated that the establishment of known telecommunications services should be the trigger for sending call identifying information.

- **Individual company contributions on CALEA Packet Surveillance Issues (Encourage presenting contribution only if substantively different from SDO or industry contributions above):**

Contribution 105 (Compaq document) was presented briefly by the JEM chair, as there was no Compaq representative in attendance. This document stressed the feasibility of using a CALEA "sniffer box" attached at strategic signaling points in a system to fulfill the CALEA obligations for packet surveillance. Since there was no Compaq representative available at the JEM, the JEM chair requested that an advocate would be sought from anyone in attendance on the second day (after allowing for overnight review) to push for the recommendations in this document.

Contribution 107 (Cisco Technical Aspects document) was presented by Chip Sharp. This document stressed the differentiation of content and call identifying information for telecommunications services versus information services, delivery of destination address information without the content, delivery of the source address without the content, and delivery of the content of a packet flow to/from a subject.

Contribution 108 (Cisco comments on J-STD-025A) was provided for information only and was not discussed further at the JEM, as this information is relevant to the SDO modifying the standard (i.e., TR45.2).

7. Identification of Technical Issues and Alternatives:

An initial attempt to reach consensus via a straw poll on general methods for providing call identifying information only (without content) for packet surveillance was not successful.

Very high-level straw poll choices for a preferred packet surveillance method for a given packet stream were proposed as follows:

- (1) Send nothing or all of the packet,
- (2) Send headers or the whole packet, or
- (3) "Peel the onion" on a packet to examine multiple layers.

While the highest number of JEM participant organizations preferred option #1 above, it was determined that the JEM could not reach consensus on which of the choices was most appropriate.

The JEM decided to revisit each of the contributions discussed under agenda item 6 and attempt to quickly identify which individual recommendations are agreed and which are not.

In discussion of contribution 102, the JEM agreed that for GPRS, J-STD-025 messages should be the basis for event reporting to satisfy pen register orders. This agreement was remanded to the drafting group for incorporation into the JEM report.

In discussion of contribution 104, the JEM agreed that for call servers utilizing SIP/H.323/similar signaling, a viable solution for satisfying pen register court orders was to map SIP/H.323/similar signaling to J-STD-025 call events. The contribution also included discussions and examples on reporting communication Path Establishment/Release and investigating the layer 3 header for Source and Destination routing addresses. The content of this document was remanded to the drafting group for incorporation into the JEM report.

In discussion of contribution 106, the JEM agreed that the content of this document should be remanded to the drafting group for incorporation into the JEM report.

In discussion of contribution 101R1, the JEM agreed that the content of this document should be remanded to the drafting group for incorporation into the JEM report.

No advocate surfaced for contribution 105 (with the absence of Compaq, the contributing company). Therefore, the JEM agreed that the JEM report would not contain any material from this contribution.

In discussion of contribution 107, the JEM agreed that the content of this document should be remanded to the drafting group for incorporation into the JEM report. The JEM agreed that "target identification" should be added as an issue in the JEM report.

The JEM agreed contribution 108 was not applicable to the JEM report; however, the JEM agreed that "IPV6" should be added as an issue in the JEM report.

8. Identify Key Elements of JEM Report:

A drafting group worked between the second and third days of the JEM and developed a draft report that was reviewed on Friday, May 5 by all participants. Key elements of the main body of the JEM report and of the technology-specific appendices were identified. See TR45/00.05.31.26 for the most up-to-date version of the draft JEM report.

9. Review JEM Summary:

Significant discussion took place on the content of the draft report on May 5. The editor was remanded the task of updating the main body of the draft report after the JEM. The revised report was agreed to be circulated to the JEM email reflector for comments. Email comments on the main body of the draft report are due to the JEM email reflector by May 22. A drafting session was established for May 23 in Washington, DC to review these email comments and incorporate them into a new draft JEM report. The revised report, along with a meeting summary from the chair, will both be presented to the TIA TR45 meeting on May 31-June 1 as the output from the first JEM session.

10. Closing Statements/Adjourn:

The JEM agreed that additional follow-up is required to provide an opportunity to accept contributions to provide details for the technology-specific appendices of the JEM report. The JEM agreed that a second JEM session is needed, and the task of determining a date for this second JEM was remanded to the JEM steering committee (subsequent to the meeting, the steering committee determined the second JEM session would be held June 27-29 in the Washington, DC area). The JEM decided to remove all substantive appendix material in the draft JEM report at this time in favor of soliciting contributions on the technology-specific appendices for the second JEM session. Assignments were taken for each of the technology-specific appendices (see assignments list in the draft JEM report). The JEM agreed that the deadline (to allow for appropriate pre-meeting review by participants) for submission of the technology-specific appendix contributions to the JEM email reflector is June 15. These contributions, and any others, will be reviewed during the second JEM session.

The chair emphasized the importance of follow-up on the action items noted above. The chair thanked everyone for their participation in the first JEM session. The JEM adjourned at approximately 2pm on May 5.



Report to TIA on Surveillance of Packet Data

1 References

- TIA /ATIS Interim Standard (Trial Use Standard): Lawfully Authorized Electronic Surveillance, J-STD-025, December 1997.
- Federal Communications Commission, Third Report and Order, CC Docket 97-213, FCC 99-230 released August 31, 1999.

• Packet Cable Standard

The standards which describe the cdma2000 Wireless IP service are

TIA/EIA/IS-835 Wireless IP Network Standard

ANSI-95

TIA/EIA/IS-707-A

TIA/EIA/IS-2000-A

[DOCSIS] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RF1v1.1-I03-991105, Cable Television Laboratories, Inc., November 05, 1999. <http://www.CableLabs.com/>

[PKT-PCES] PacketCable Electronic Surveillance Specification, PKT-SP-ESP-I01-991229, December 29, 1999, Cable Television Laboratories, Inc., <http://www.PacketCable.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.

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

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

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

7 [RFC2327] Handley, M, and V. Jacobson, SDP: Session Description Protocol, April,
8 1998.

9 [SALTZER] End-To-End Arguments in System Design, J.H. Saltzer, D.P.Reed,
10 D.D.Clark, ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288.

11 [RFC1958] Carpenter, B., "Architectural Principles of the Internet", RFC
12 1958, June 1996.

13 [RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, February
14 2000.

15 [RFC2401] Kent, S. and Atkinson, R., Security Architecture for the Internet
16 Protocol, November 1998

17

18 [RFC2804] IAB, "IETF Policy on Wiretapping", RFC 2804, May 2000

19 [RFC2138] Rigney, C. et. al. " Remote Authentication Dial In User Service
20 (RADIUS)", IETF RFC 2138, April 1997.

21 [RFC1541] Droms, R., "Dynamic Host Configuration Protocol", IETF RFC
22 1541, October 1993.

23 [RFC2139] Rigney, C., "RADIUS Accounting", IETF RFC 2139, April 1997.

24 [RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol
25 (IPCP)", IETF RFC 1332, May 1992.

26 [RFC1918] Rekhter, Y., et. al., "Address Allocation for Private Internets" IETF
27 RFC 1918, February, 1996.

28 [RFC1631] Egevang, K., et. al., "The IP Network Address Translator (NAT)",
29 IETF RFC1631, May 1994.

30 [RFC2663] Srisuresh, P. and Holdrege, M., "IP Network Address Translator
31 (NAT) Terminology and Considerations", IETF RFC 2663, August
32 1999[RFC1702] Hanks, S., et. al., "Generic Routing Encapsulation over IPv4
33 networks", IETF RFC 1702, October, 1994.

34 [RFC1853] Simpson, W., "IP in IP Tunneling", IETF RFC 1853, October
35 1995.

36 [RFC2661] Townsley, M., et. al., "Layer Two Tunneling Protocol 'L2TP' ", IETF
37 RFC 2661, August 1999.

1 [RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload
2 (ESP)", IETF RFC 2406, November 1998.
3 [RFC2002] Perkins, C., "IP Mobility Support", IETF RFC 2002, October 1996.
4 [RFC1661], Simpson, W., "The Point-to-Point Protocol (PPP)", IETF RFC
5 1661, July 1994.
6

7 **2 Definitions and Acronyms**

8 CMS: Call Management Server

9 IPv4:

10 IPv6:

11 H.323:

12 SIP:

13 VoP: Voice over Packet

14 **3 Introduction and Executive Summary**

15 *3.1 Convening the JEM*

16
17 In its Third Report and Order regarding implementation of the Communications
18 Assistance for Law Enforcement Act (CALEA), the FCC finds "that the approach
19 taken [by industry] with regard to packet-mode communications in J-STD-025
20 raises significant technical and privacy concerns." Under J-STD-025 for packet
21 mode communications, law enforcement could be provided with call content when
22 only call-identifying Pen Register and Trap and Trace information was authorized
23 to be delivered.
24

25 The FCC "believe[s] that further efforts can be made to find ways to better
26 protect privacy by providing law enforcement only with the information to which
27 it is lawfully entitled." However, the FCC acknowledges that the record before it
28 does not sufficiently address packet technologies and the problems that they may
29 present for CALEA purposes. The FCC notes, for example, "that some packet
30 technologies (e.g., frame relay, ATM, X.25) are connection oriented i.e., there are
31 call set-up and take-down processes, similar to those used in circuit switched voice
32 networks, whereby addressing information is made available to the carrier
33 separate from and before call content is transmitted. Other packet technologies
34 (e.g., Internet protocol based solutions) would not be processed this way."
35

36 Accordingly, the FCC invited TIA to study CALEA solutions for packet-mode
37 technology and report in one year on "steps that can be taken, including
38 particular amendments to J-STD-025, that will better address privacy concerns."
39 To meet the deadline imposed by the FCC, and to build a record based on
40 technical facts, the Telecommunications Industry Association (TIA) has

1 sponsored two Joint Experts Meetings. Lists of JEM invitees and attendees are
2 attached as Appendix A and B, respectively.

3
4 The JEM has served as a technical fact-finding body across the spectrum of
5 packet-mode communication technologies regarding the feasibility of delivering
6 less than the full content of a packet to law enforcement in response to a pen
7 register order. While the scope of the JEM included reporting on the broadest
8 number of packet mode communications technologies, contributions were
9 received only on the following technologies: CDMA2000, GPRS, and IP.

10
11 Prior to meeting in person, contributions from various entities were made
12 available through posting on the TIA website (see CALEA JEM link at
13 www.tiaonline.org). A publicly available mailing list was also maintained. A two-
14 hour question and answer session covering the scope of the JEM was conducted
15 on March 20, 2000. The JEM then convened on May 3-5, 2000, in Las Vegas,
16 NV. Following opening remarks updates were provided on the status of Revision
17 A of J-STD-025, the legal purpose of the JEM, and the status of CALEA
18 activities. Presentations on technical issues followed. A copy of the JEM agenda
19 is attached.
20

21 *3.2 JEM I Output*

22
23 The first JEM (JEM I) established a framework for preparing this report. A copy
24 of the JEM 1 meeting report to TIA TR45 is attached as appendix C.

25
26 First, JEM I concluded that, based on current FCC guidance, it could not define
27 "call-identifying information" for packet services. Several contributors noted that
28 the term "call-identifying information" is ambiguous with regard to packet
29 communications. Instead, JEM 1 concluded that it could only attempt to identify
30 what information may be available about the packet communication. Once
31 identified, JEM I concluded that it could then best report on the technical impact
32 and feasibility of making that information available to a law enforcement agency
33 (LEA). This decision was consistent with the purpose and scope of the JEM,
34 which did not include discussion of legal issues.

35
36 Second, JEM I noted CALEA requirements apply to telecommunication services
37 not information services. JEM I recognized, however, that from a packet point of
38 view, the two may be indistinguishable. JEM I determined that it is not
39 technically advisable to determine, on a packet by packet basis, the application or
40 communication service that is being provided. JEM I also concluded that, the
41 application or communication services that is being provided can not be
42 determined even by observation of the complete stream of packets. The point of

1 call setup may be the only time that a telecommunication service can be
2 distinguished from an information service.

3
4 JEM I further concluded that the possibility of encapsulation or encryption of
5 packets outside of the service provider's control makes identifying the application
6 or service even more unlikely.

7
8 The JEM addressed the issues related to packet mode services in two main
9 categories: (1) packet communication sessions established by a Call Management
10 Server (CMS), and (2) transport services, i.e. packet communication sessions
11 established without a CMS. The CMS may, for instance, be an H.323
12 GateKeeper, or a SIP proxy, or something conceptually equivalent. Typically an
13 access service provider that offers a CMS also provides transport.

14
15 Accordingly, the framework for this report reflects this two-pronged approach. In
16 each category, the JEM decided to report on the information available and the
17 technical impact of providing it. A second JEM was scheduled to be held in
18 Washington, D.C., on June 27-29, 2000, to accept contributions for each
19 technology. Assignments were taken to prepare appendices of technologies for
20 this report.

21
22 Finally, JEM I agreed that if a change to the current standard (J-STD-025) were
23 deemed necessary by the Federal Communications Commission, a court or the
24 industry, as a result of this process, the JEM recommends that the open, joint
25 T1/TIA activity currently underway in 45.2 LAES Ad Hoc be responsible for
26 completing this task. In its simplest form, this change may just be the inclusion
27 of appropriate references to other standards. Nothing in this process, however,
28 precludes any standards setting or industry organization from adopting their own
29 "safe harbor" standard for their particular technology (e.g., satellite or cable
30 standards).

31 32 *3.3 JEM 2 output [editor's note – placeholder]*

33 34 35 **4 Packet Communication Sessions established by a Call** 36 **Management Server**

37
38 The service provider that provides a call service via a call management server, e.g.,
39 an H.323 GateKeeper or a SIP proxy. The following discussion assumes that the
40 CMS is providing call events. If the CMS does not provide call events then the
41 discussion in section 5 applies.

4.1 Information that can be reported

Information available is analogous to J-STD-025 call events, but with respect to each technology, enhancements may need to be made to J-STD-025. For example, with respect to Voice-over-Packet (VoP) services, the JEM notes that additional enhancements are needed to J-STD-025 (e.g., to report VoP calls and associated ~~call-identifying information~~ Pen Register and Trap and Trace information, to identify the content stream, and to identify the timing requirements). Other standards may address other technologies and networks.

4.2 Technical Impacts

The type of call content delivered to the LEA may differ from that negotiated with the provider (i.e., the ~~call-identifying~~ Pen Register and Trap and Trace packet stream information ~~can~~ does not guarantee the user is using the packet stream as negotiated).

Interception of packet services also does not guarantee that the packets have been received by the terminating system.

H.323 and SIP call events may not map directly to those call events established in J-STD-025 (e.g., triggering events may be different). Impacts associated with development of a protocol to support reporting packet data communication call events have not yet been investigated and there may be unforeseen issues.

Timing requirements need to be reviewed and may need to be specified for each technology.

The JEM did not address possible difficulties in associating call events with call content as required by CALEA.

5 Packet Communication Sessions established without a Call Management Server

This section describes the service providers that provide packet mode transport, but do not provide access service via a CMS.

5.1 Information that can be reported, subject to technical impact analysis

Establishment of a communication path across an accessing system from the subject's device to a network (not the endpoint) may be required before communication between the subject and associate can begin. If so, the establishment and release of this path could be reported. The information provided may be technology-dependent.

1 Reporting of information beyond establishment and release requires access to the
2 individual packets, which may yield further information such as non-encapsulated
3 routing information. Alternatively, the entire packet could be delivered. It must
4 be noted that either may be difficult and not feasible for some existing systems
5 and architectures, as discussed below.

6 *5.2 Technical Impacts*

7 For all of the delivery options discussed below, the following comments apply:
8 The consensus is that in many technologies the duplication of a packet stream
9 requires significant resources. This may be technology dependent. These
10 resources compete with the Title III resources as well as capacity requirements.

11
12 The subscriber under surveillance, and their associates, may detect performance
13 degradation resulting from the impact of duplication of a packet stream for every
14 Pen Register. Other customers using the packet data services of the TSP may also
15 detect the degradation of performance. The JEM notes that a single subscriber to
16 the packet transport service may utilize excessive packet capacity.

17
18 It is assumed that the subscriber under surveillance can be readily identified
19 within the network by the technology specific identifiers listed in the appendices.
20

21 *5.2.1 Delivering the Entire Packet Stream*

22 Currently J-STD-025 specifies delivery of the entire packet stream for a user
23 under surveillance. While this guarantees that authorized Pen Register and Trap
24 and Trace information will be delivered to the LEA, it does not remove content
25 prior to delivery. This places the responsibility on the LEA to only retain
26 the authorized information, which has been raised as a potential issue by the
27 privacy groups. The JEM noted that under this method, only the packets for the
28 user under surveillance are delivered, and not those for other users on the system.
29 Since the LEA has no access to the packets from other users on the system, this
30 does represent an improvement from the current state of the art .¹~~add footnote~~.

31
32 ~~If the service provider is required to deliver the entire packet to provide call-~~
33 ~~identifying information for a pen register, the following issues have been~~
34 ~~identified.~~

35
36 ~~The consensus is that duplication of a packet stream requires significant~~
37 ~~resources. This may be technology dependent. These resources compete with the~~
38 ~~Title III resources as well as capacity requirements.~~

¹ The packet processing equipment used in most present day Telecommunication Service
Provider networks does not include a capability to extract the packet stream for a particular user.
Therefore, prior to implementation of J-STD-025, lawfully authorized surveillance may necessitate
access to data streams supporting multiple users.

1
2 ~~The subscriber under surveillance, and their associates, may detect performance~~
3 ~~degradation resulting from the impact of duplication of a packet stream for every~~
4 ~~Pen Register. Other customers using the packet data services of the TSP may~~
5 ~~also detect the degradation of performance. The JEM notes that a single~~
6 ~~subscriber to the packet transport service may utilize excessive packet capacity.~~²

7 5.2.2 Delivery of Header routing information

8
9 The JEM agreed that a TSP could extract the packet header routing information
10 from the packet content associated with a user under surveillance. It was noted
11 that only providing this information (i.e. the source and destination address
12 information) may not give LEAs access to all the necessary Pen Register and Trap
13 and Trace information. Specifically, the IP addressing information that could be
14 provided by an IP service provider may not meaningfully identify either the
15 subject or associate due to IP capabilities such as Network Address Translation
16 and dynamic IP addressing. For example, in cases where Pen Register or Trap
17 and Trace surveillance requires information contained in the IP data
18 field such as (e.g. email addresses) would not be, providing with the routing
19 information only the IP addresses is insufficient.

20 5.2.3 Extraction of Pen Register and Trap and Trace information

21
22 Relevant Pen Register and Trap and Trace information may be located in
23 different layers of the protocol depending on the specific service used and the
24 application of the packet (e.g., a POP e-mail packet vs. a connection setup packet
25 for H.323 or SIP service). New services (and therefore application layer
26 protocols) are developed on a continual basis within the IP environment making
27 isolation of Pen Register and Trap and Trace information within an IP data field
28 even more complicated. Therefore, accurate separation capabilities (i.e., filtering
29 capabilities) will require rapid, continuous development which will be highly
30 resource intensive. This process does not lend itself to the current standards
31 development process due to its consensus driven nature. It is also expected that
32 the industry resources for this work would be significantly greater than the
33 resources that are currently committed for surveillance standards development.

34
35 The JEM did express concerns that although such a solution does appear possible
36 today as demonstrated by the FBI, such a solution may or may not be scalable in
37 the quantity deployments anticipated under CALEA, especially as the filtering
38 becomes more complex and the network speeds increase. Additionally, the

² Vendor studies in one technology (PacketCable) determined that packet duplication of over 5% would have such an impact, and that requirements for duplication capacity in excess of 5% would require redesign of the network.

1 challenges of keeping the extraction function useful and accurate may be extreme
2 once all of the complications outlined in the IP Appendix (e.g. encapsulation,
3 fragmentation, independent packet routing and encryption) are taken into
4 consideration.

5
6 Location of this extraction function could be at various locations, including both
7 within the service provider's network, or within the LEA facilities. Each of these
8 options has issues for consideration. If the extraction function were located in
9 the service provider's network, it would mean that a service provider would be
10 deploying equipment which it has neither developed nor tested. This is contrary
11 to current practice, and may impact quality of service and network reliability. If
12 the extraction function is located in the LEA facilities, there may be concerns
13 raised about privacy, although as described in Section 5.2.1, it would be better
14 than the current state of the art.

16 **5.2.2 Investigating the Packet Stream**

17
18 ~~Consensus is that examining beyond the outermost routing header of a packet,~~
19 ~~e.g., IP header, ATM cell header, Frame Relay header, X.25, etc., to identify call-~~
20 ~~identifying information is not technically advisable (i.e., technical complexity,~~
21 ~~extreme processor load, encryption, unknown protocols, and inability to identify~~
22 ~~the target).~~

23
24 ~~Consensus is that the information gained from examining the outermost header~~
25 ~~may not yield useful call identifying information (e.g. the actual identity of the~~
26 ~~subject and associate endpoints).~~

27
28 ~~The above considerations are magnified as access speeds increase to gigabit/sec~~
29 ~~and faster. High speed technologies may not permit time to investigate the~~
30 ~~packet.~~

31
32 Delivery Timing of Delivery of the FCC mandated timing requirement of eight
33 secondss-needs to be reviewed and may need to be specified for each technology
34 and each solution discussed above.

36 **6 Technology Specific Information**

37 Editor's note:

38 Format for Appendix

39 Guide to appendices.

Bullet list of what protocols will have appendices. Note that we did not receive contributions for all possible packet technologies and not all packet technologies were represented at JEM.

~~Framework of the Technology Specific Information Subchapter (approx. 1-5 pages).~~

- ~~—Architecture overview (diagram)~~
- ~~—Protocol type supported (e.g. IPv4/IPv6, connection/connectionless)~~
- ~~—Performance of the system based on expert opinion.~~
 - ~~——Performance when providing call events.~~
 - ~~——Performance when providing full packet.~~
- ~~—Preferred delivery format.~~
- ~~—Technical feasibility/unfeasibility (reference body of doc).~~
- ~~—Complexity of various solutions.~~
- ~~—How do you map the target identity to the technology address?~~
- ~~—How do you identify the associate?~~
- ~~—What information can be provided to law enforcement (be specific as to whether CMS is used or not)?~~
 - ~~Do you have a CMS, if so, what information can be provided?~~
 - ~~If you do not have a CMS what information can be provided?~~
- ~~—Where are the possible points of intercept and their impacts to existing architecture?~~
- ~~—List of relevant standards.~~
- ~~—Possibilities for delivering serving system message.~~

6.1 Access networks

6.1.1 Call Associated Signaling Reporting:

6.1.1.1 Reporting Call Associated Information

Future wireless systems may be supporting Voice Over IP (VoIP) calls via new signaling methods such as SIP and H.323. In these scenarios a call client in the handset communicates with a call server controlled by the accessing system to establish a voice call using packet mode communication. The accessing system may then interwork the VoIP call into the PSTN using signaling and media gateways (e.g., RTP-TDM, SIP-SS7) or deliver the call directly into a network using packet mode communication (e.g., SIP, RTP). Call associated information can be reported in these scenarios. Two methods have been identified:

a) Reporting J-STD-025 Call Associated Events

1 With this method call associated signaling such as SIP/H.323 would be mapped
2 to the J-STD-025 call events.³ The development of this method is required in
3 order to provide backward compatibility for systems that incorporate the J-STD-
4 025 capabilities. This method will require changes and enhancements to J-STD-
5 025.⁴

6 7 b) Reporting SIP/H.323 Signaling

8
9 With this method the actual call associated signaling is reported to the LEAs.
10 This alternate capability may be advantageous to future systems that do not
11 have a backward compatibility issue with the J-STD-025 call events.:
12

13 6.1.16.1.2 CDMA2000

14 SDO Lead: TR45.6

15 Contact: Mark Munson

16 6.1.2.1 Overview

17
18 The cdma2000 Wireless IP service offering is described in TIA/EIA/IS-835. This
19 standard specifies a system that will provide IPv4 service over a cdma2000 radio
20 network. Two types of service are described, namely Simple IP, which provides IP
21 service within a network much like traditional dial-up IP service, and Mobile IP,
22 which provides persistent IP service across all connected networks. The Wireless
23 IP system only provides for transport of IPv4 packets, and does not offer any
24 higher level functions for communication services within the standardized system.
25 High level figures depicting the various network elements for these two services are
26 shown in Figures 1 and 2.

27
28 Network elements that are specific to the cdma2000 Wireless IP Network are the
29 Packet Data Serving Node(PDSN), the RADIUS servers [REF XX], and the Home
30 Agent (HA). The PDSN and local RADIUS server are part of the serving wireless
31 network, while the home and broker RADIUS servers and HA may be part of
32 another wireless network, or part of some private network. The RADIUS servers
33 provide the authentication, authorization and accounting functions and use a
34 Network Access Identifier (NAI) of the form user@realm to identify subscribers.
35 Separate authentication, authorization and accounting are provided via the Radio
36 Network using standard wireless Visitor Location Register (VLR) and Home

³ See J-STD-025 Section 4.4 Call Associated Information Surveillance Service Description - Call Identifying Information IAP (IDIAP) and the listed call events.

⁴ Currently in J-STD-025 the IDIAP call events are defined only for circuit-mode calls. In addition these events may not be able to carry all necessary packet mode VoIP information (e.g., Session Definition Protocol information).

1 Location Register (HLR). This information, however, is not communicated with
 2 the Wireless IP network elements.

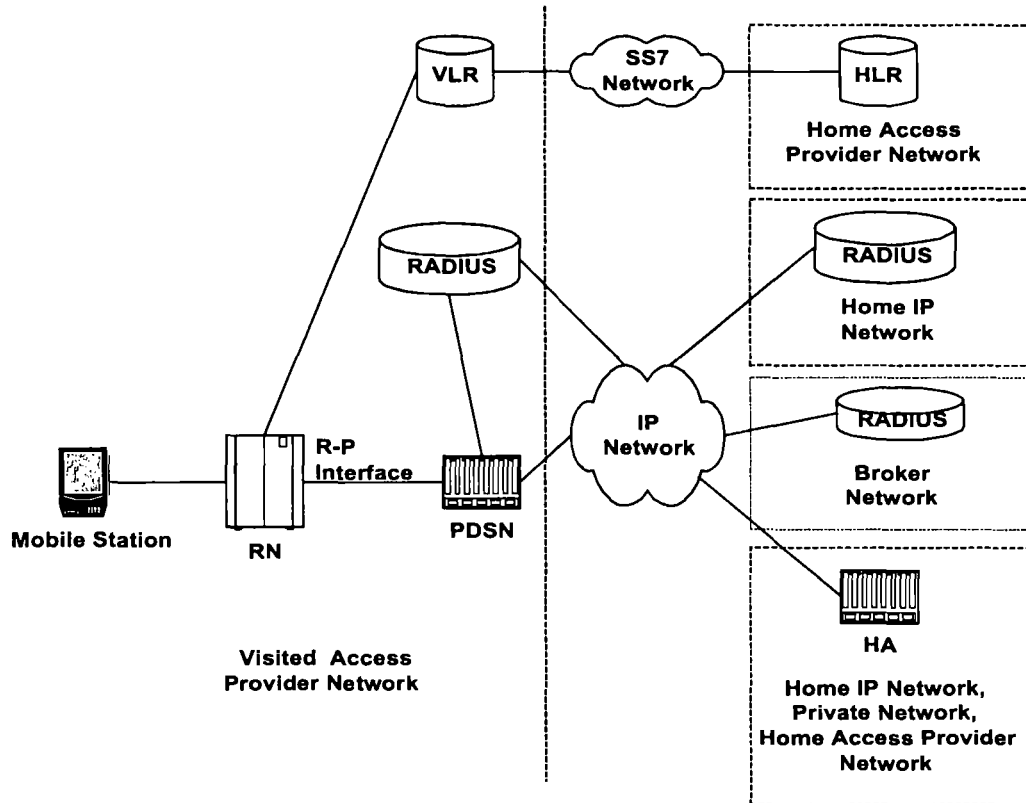


Figure 1: Reference Model (HA only for with Mobile IP service)

6.1.2.2 Technical Capabilities for support of CALEA

Since the cdma2000 Wireless IP system only provides basic transport of IPv4 packets and does not provide communication services such as Voice over IP which require a call management server, it is limited in its ability to report specific call identifying Pen Register and Trap and Trace information. The network is unaware of any underlying services that are running between the user and any correspondent nodes, and as such is unable to report call events. As such, the cdma2000 Wireless IP system capabilities are consistent with those referenced within the JEM report under the section Packet Communication Sessions established without a Call Management Server.

6.1.2.3 Reporting of Call Information

1 The cdma2000 packet data architecture as described in IS-835 "Wireless Packet
2 Data Standard" provides informational services and as such may act as a bearer
3 service for communication services. The standard does not describe the
4 applications that are supported in the network, nor does it describe how to
5 interpret the packet data information based on the application since this varies
6 widely between different applications. This information is unnecessary and beyond
7 the scope of the standards since the intent is to provide packet data "access." It is
8 not technically feasible to determine, neither on a packet by packet basis no on a
9 stream basis, the application or communication service being used. Furthermore,
10 the possibility of encapsulation or encryption of packets outside of the network
11 makes identifying the application or service even more unlikely. Therefore, the
12 level of complexity required of the network to attempt to ~~separate-extract each~~
13 ~~identifying~~ Pen Register and Trap and Trace information from information services
14 is unfeasible.

15
16 The system is capable of providing copies of the full IP packets to law enforcement
17 for a limited number of subjects given the constraints detailed below in the System
18 Performance Impacts section. The system could also provide only the outermost IP
19 routing headers, although which as discussed in the JEM report may not provide
20 any significant value. In either case, however, the system is unable to differentiate
21 those packets which are associated with a communications service from those that
22 are associated with an information service and as such must deliver all or none of
23 the packets associated with a given user. It should be noted that in some loading
24 situations a user may be able to detect performance degradation resulting from this
25 service, and that a single heavy user may occupy a disproportionate amount of
26 system resources.

28 6.1.2.4 Reporting of Access Control Information

29
30 Similar to wireline systems, wireless systems establish a communication path across
31 the accessing system from the subject's device to a network before communication
32 between subject and associate can begin. The establishment and release of this path
33 corresponds to establishment and termination of packet data service and could be
34 reported to assist LEAs in recognizing when an intercept subject has established
35 communication ability.

36
37 The following events could be reported

- 38
- 39 - packet data service establishment;
- 40 - packet data service termination;
- 41 - start of interception with packet data service active ;
- 42 - PCF handoff;
- 43

6.1.2.5 Target and Associate Identity

End users can be identified by either the NAI or their MSID. Since the MSID is not used in the Wireless IP system, the NAI is the most appropriate form of identification. Because the IP address of a target may be either dynamically assigned on a per session basis, it is not practical to just identify the subject by an IP address. The system can determine on a real time basis the IP address that has been assigned to the NAI associated with a subject for that session and then perform further interception based on that IP address. It should be noted that the architecture specified in TIA/EIA/IS-835 allows for multiple users (in the case of externally connected devices) to access the packet data network through a single terminal. It should be further noted that the home network for the NAI may or may not belong to a wireless service provider, that a user may have multiple NAIs which can be used to access the network, and that the NAI is not tied to use on a single terminal.

After a communication path is established by a wireless accessing system between the subject device(s) and network, the subject can communicate directly with many associates over the connecting path. The associates with who the subject is communicating can only be identified within the Wireless IP network by the corresponding IP addresses – no further information is available to the network. These addresses may be of a transitive nature since the associates could have a dynamically address, and the true associates may only be identified by additional information in the payload of the packet and not the corresponding IP address.

6.1.2.6 Point of Interception

There are several points in the network where the user information transiting the system may be intercepted. These include components within the visited access network where the target is being provided packet data transport service, and components within the home network which provide additional services. Due to the nature of communication flows for Simple IP and Mobile IP services, the recommended point of interception is in the visited access network at the Packet Data Serving Node (PDSN). By intercepting at the visited PDSN, all information flowing between an subject and associate for both Simple IP and Mobile IP may be monitored and all relevant user identifying information is readily available. Some serving system information may be obtained from the home network HLR and Home AAA servers as described later in this document. Note however that the home AAA server may reside in a network other than one belonging to a telecommunications service provider.

6.1.2.7 Serving System Message

In the LAES standard, J-STD-025, a non-call associated surveillance service was defined to access information within a telecommunication system. The non-call associated information identified was Serving System information for personal or terminal mobility. The Serving System message in this standard provides information as to the current system assigned to provide service for the mobile subscriber.

The mobile gains access to the cdma2000 network via the CDMA network and the subscription to the packet data service. The home network (HLR) could advise law enforcement of the network where the subscriber is now roaming, but may not have knowledge that the subject is using the packet data service subscription. However, the home AAA could advise law enforcement, in a similar fashion, that the subject is being provided packet data service by a foreign network and the IP address of PDSN providing access. In summary, serving system information for MSID based lawful interception may be obtained at the HLR while serving system information for NAI based lawful interception may be obtained from the Home AAA server.

6.1.2.8 Method of Delivery to Law Enforcement

Given that the PDSN and home AAA servers are network elements in an IP based network, the most logical and preferred method for communicating information to law enforcement is via an IP network connection. Access Control and Serving system information could be standardized for transmission within an IP packet, and if copies of the full packets are provided, the contents of the communication stream could be encapsulated in a standard IP in IP tunnel.

6.1.2.9 System Performance Impacts *(editor's note, place holder for information to come)*

**For providing access information
For providing full copies of packets**

6.1.2.10 Relevant Standards

**The standards which describe the cdma2000 Wireless IP service are
TIA/EIA/IS-835 Wireless IP Network Standard
ANSI-95
TIA/EIA/IS-707-A
TIA/EIA/IS-2000-A**

1
2 **6.1.2 GPRS/UMTS/TDMA**

3 ~~SDO Lead: T1/ETSI/TDMA/UWCC.~~

4 ~~Contact: Ron Ryan, Bernie McKibben, Bill Marshall.~~

5
6 **6.1.3 GPRS Appendix:**

7 *Editor's note: add intro from T1P1 contributions*

8
9 For GPRS the following information could be provided to the LEAs separately
10 from the call content:

- 11
12 - an activation reference identity;
13 - the target identity which has been intercepted (e.g., MSISDN, IMSI, IMEI if
14 applicable);
15 - type of protocol activated (e.g., Internet Protocol or X.25);
16 - PDP address used by the target (e.g., IP Address);
17 - location information of the target (Cell Global Identity);
18 - time of event;
19 - Access Point Name (APN).
20

21 The above information is available when the intercept subject utilizes the GPRS
22 service via the following events at the GPRS Support Nodes (e.g., SSGN, GGSN):
23

- 24 - GPRS attach;
25 - GPRS detach;
26 - PDP context activation;
27 - start of interception with PDP context active;
28 - PDP context deactivation;
29 - Call and/or Routing Area update;
30 - SMS;
31

32 The following areas where ~~Call Identifying Pen Register and Trap and Trace~~
33 Information for Packet Mode Communication could be reported to assist Law
34 Enforcement Agencies (LEAs) have been identified:
35

36 **6.1.3.1 ~~4~~-Reporting of Access Control Information**

37
38 Similar to wireline, wireless systems establish a communication path across the
39 accessing system from the subject's device to a network before communication
40 between subject and associate can begin. The establishment and release of this path
41 could be reported to assist LEAs in recognizing when an intercept subject has

1 established communication ability. The following provides an example of how the
2 information could be reported⁵:

3
4 The following information indicates a packet mode communication path has
5 been either established or released between the intercept subject device(s) and a
6 network:

7
8 ~~IAPSystemIdentity~~ ~~OPTIONAL~~,
9 ~~TimeStamp~~,
10 ~~AccessPathID~~, ~~Uniquely identifies the access path (e.g., a PDP~~
11 ~~Context path)~~
12 ~~Network Access Address~~, ~~Identifies the network address of the path (e.g.,~~
13 ~~APN⁶)~~
14 ~~Intercept Subject Address~~, ~~Identifies the PDP Address of the subject~~
15 ~~(e.g., IP address)~~
16 ~~event~~
17 ~~PathEstablished~~, ~~e.g., PDP Context Activation~~
18 ~~PathReleased~~ ~~e.g., PDP Context Deactivation~~
19

⁵ The events reported are based on the GPRS PDP Context Activation and Deactivation processes.

⁶ Access Point Name (APN) from GPRS

6.1.3.2 2) Reporting Packet Data Communication Addresses

After a communication path is established by a wireless accessing system between the subject device(s) and network, the subject can communicate directly with an associate over the connecting path. In this scenario the packet mode communication, voice or data, bypasses the call server of the accessing system and there would be no J-STD-025 type call events reported to the LEAs.⁷ To assist LEAs in identifying the parties to the communication, the network addresses available to the accessing system could be reported. For example, with an IP network layer the source and destination addresses for the IP packet in the IP Header could be reported. The following ASN.1 encoded message provides an example of how the information could be reported:

The following information contains network source and destination information for the traffic between the subject and associate.

~~Case Identity,~~
~~IAPSystemIdentity~~ OPTIONAL,
~~TimeStamp,~~
~~AccessPathID,~~ Uniquely identifies the access path (e.g., a PDP Context path)⁸—
~~SourceAddress,~~ e.g., IP Source Address⁹
~~DestinationAddress~~ e.g., IP Destination Address

Editor's note: CAS has been moved to the beginning of this section.

Call Associated Signaling Reporting ~~Appendix:~~

~~Reporting Call Associated Information~~

~~Future wireless systems may be supporting Voice Over IP (VoIP) calls via new signaling methods such as SIP and H.323. In these scenarios a call client in the handset communicates with a call server controlled by the accessing system to establish a voice call using packet mode communication. The accessing system may then interwork the VoIP call into the PSTN using signaling and media gateways (e.g., RTP TDM, SIP SS7) or deliver the call directly into a network using packet~~

⁷ When packet mode voice calls involve the accessing system's call server, the call signaling events are reported and the reporting of packet header information would be redundant and unnecessary.

⁸ Correlates NetworkAddressInfo to AccessPathEvent

⁹ Either the source or destination address is associated with the intercept subject and thus indicates direction of packet flow.

mode communication (e.g., SIP, RTP). Call associated information can be reported in these scenarios. Two methods have been identified:

a) Reporting J-STD-025 Call Associated Events

With this method call associated signaling such as SIP/H.323 would be mapped to the J-STD-025 call events.¹⁰ The development of this method is required in order to provide backward compatibility for systems that incorporate the J-STD-025 capabilities. This method will require changes and enhancements to J-STD-025.¹¹

b) Reporting SIP/H.323 Signaling

With this method the actual call associated signaling is reported to the LEAs. This alternate capability may be advantageous to future systems that do not have a backward compatibility issue with the J-STD-025 call events. The provides an example of how the information could be reported:

—Case Identity,
—IAPSystemIdentity — OPTIONAL,
—TimeStamp,
—CallSessionID, — e.g., Call ID
—CallSessionInfoType, — the type of signaling (e.g., H.323 family, SIP)
—CallSessionInfo

6.1.36.1.4 CDPD

SDO Lead:

Contact: Dean Anderson

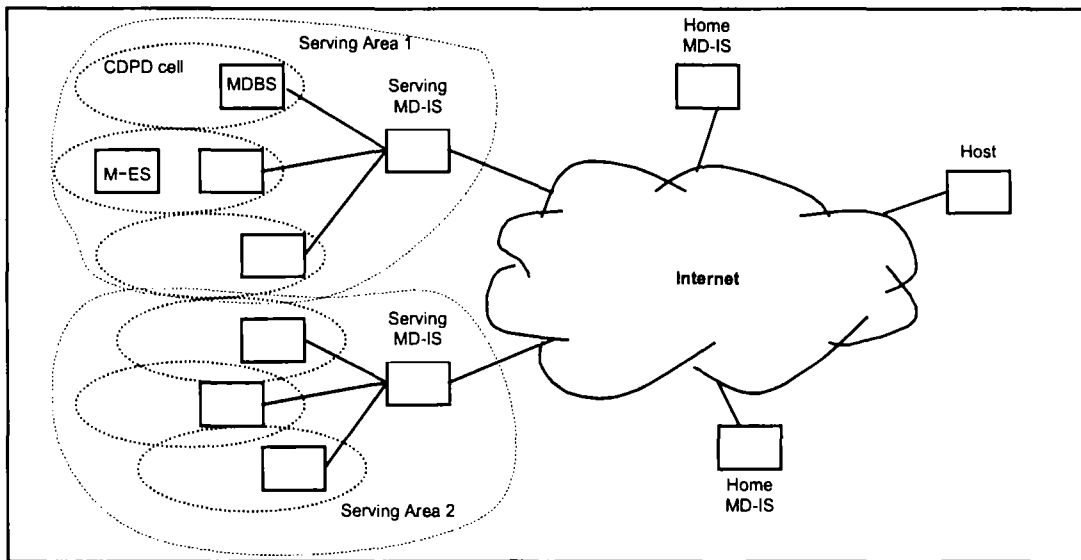
Appendix: Cellular Digital Packet Data (CDPD)

6.26.1.4.1 CDPD Architecture Overview

The CDPD Network operates as a collection of CDPD Service Provider Networks. The network architecture model shown in the diagram identifies the abstract functional elements.

¹⁰ See J-STD-025 Section 4.4 Call Associated Information Surveillance Service Description - Call Identifying Information IAP (IDIAP) and the listed call events.

¹¹ Currently in J-STD-025 the IDIAP call events are defined only for circuit-mode calls. In addition these events may not be able to carry all necessary packet mode VoIP information (e.g., Session Definition Protocol information).



1
 2
 3
 4 The CDPD specific Mobile Data Intermediate System (MD-IS) perform routing
 5 functions based on knowledge of the current location of the Mobile End-System
 6 (M-ES). The geographic grouping of cells connected to an MD-IS defines a
 7 serving area. Each serving area may cover multiple cellular radio coverage regions.
 8 Multiple serving areas may exist in a single CDPD service provider network.
 9 Multiple CDPD service provider networks are interconnected to provide seamless
 10 mobility routing for the mobile subscriber.

11
 12 Mobility Management functions to support routing are localized in the following
 13 network entities:

14
 15 • Mobile End System

16 The Mobile End System (M-ES) is the means by which CDPD Network
 17 subscribers gain access to wireless communications. Each M-ES is aware of its
 18 location based on broadcast information. When an M-ES powers up in a
 19 CDPD cell, it informs the network of its location using the registration
 20 process. When the M-ES moves to another cell, it notifies the network by
 21 indicating a change to new cell. When the M-ES moves to another cell in a
 22 new serving area, it performs a new registration.

23 • Mobile Data Base Station

24 The MDBS provides Layer 2 data link or media access relay functions for a
 25 set of radio channels serving a cell. The MDBS does not participate in the
 26 wide area mobility management task.

27 • Home MD-IS

28 Every M-ES address is logically a member of a fixed home area. The home
 29 area provides the anchor or mobility-independent routing destination area for

1 routers and hosts that are not mobile aware (*i.e.*, routers and hosts on the
2 general internet). The home MD-IS is responsible for transparently redirecting
3 and forwarding data packets. The redirection and forwarding function is
4 based on the principle of encapsulating M-ES addressed packets and
5 forwarding them to the Serving MD-IS in each serving area the M-ES visits.
6 In other words, data packets destined for the M-ES are routed through the
7 general internet to the Home MD-IS. The Home MD-IS then encapsulates the
8 packet and forwards the encapsulated packet to the appropriate Serving MD-
9 IS. The Home MD-IS does not need to be involved in the routing of packets
10 originated at the M-ES.

- 11 • **Serving MD-IS**

12 The Serving MD-IS handles the routing of packets for all M-ESs in its serving
13 area. When an M-ES registers for network access in an MD-IS serving area,
14 the Serving MD-IS provides the Home MD-IS the current location of the M-
15 ES. The serving MD-IS provides readdressing service by decapsulating
16 forwarded data packets from the Home MD-IS and routes them to the correct
17 radio cell. Data packets received from an M-ES and destined for a peer host are
18 routed as in any internetwork, without the requirement of traversing the home
19 MD-IS.

20
21 It should be noted that in the CDPD mobility management architecture, each
22 network entity maintains a component of the complete information. The Home
23 MD-IS maintains information regarding the M-ES to the detail of the serving
24 area. Furthermore, the Home MD-IS does not have visibility to the data packets
25 originated by the M-ES.

26
27 The Serving MD-IS maintains information regarding the location of M-ES to the
28 resolution of a radio cell. The Serving MD-IS also routes all data packets destined
29 to and originated from the M-ES. However, when the M-ES relocates to another
30 serving area, the old Serving MD-IS is not informed of the new serving area.

32 6.1.4.2 Network Service

33
34 The CDPD network provides wireless mobile routing of network layer data
35 packets. The CDPD System Specifications specifies support for two
36 connectionless network layer protocols – Internet Protocol (IP) and
37 Connectionless Network Protocol (CLNP). However, the currently deployed
38 systems all support only IPv4.

39
40 The CDPD network has been defined to support the network protocol without
41 any modification, as such the identity managed by mobility management is the
42 IPv4 address. In other words, the subscriber identity is the IPv4 address, and is

1 used for all routing purposes. There is no mapping of the target identity to the
2 CDPD technology address.

3
4 Furthermore, since the CDPD network provides routing of connectionless
5 network layer protocol data packets, there is no Call Management Service.
6

7 6.1.4.3 Information Provided

8
9 On the CDPD system, a Mobile End System (M-ES) must register with the
10 network prior to establishment of data communications with peer entities.
11 Therefore, at time of registration, the CDPD network shall provide the following
12 information:

- 13 • Case identity
- 14 • Service Provider Network Identity of the serving system.
- 15 • Date and time of registration of the intercept subject.
- 16 • IP address of the intercept subject.

17
18 The CDPD mobility management procedure requires the M-ES to register when
19 moving from one serving area to another. Therefore, if the intercept is provided
20 at the Home MD-IS, the above information is provided whenever an M-ES moves
21 to a new serving area. If the intercept is provided at the Serving MD-IS, the
22 above information shall only be provided on entry of the M-ES into its serving
23 area.

24
25 At the time of deregistration of the intercept subject, the CDPD network shall
26 provide the following information:

- 27 • Case identity
- 28 • Service provider identifier of the serving system.
- 29 • Date and time of deregistration of the intercept subject.
- 30 • IP address of the intercept subject.

31
32 Once a CDPD M-ES has been registered, an intercept point at a Serving MD-IS
33 shall provide the following on each IP packet delivered to, or received from the
34 intercept subject:

- 35 • Case identity
- 36 • Date and time of receipt of the IP packet by the network
- 37 • Source and destination IP addresses of the intercepted packet
- 38 • The Cell Identifier of the location of the intercept subject M-ES (if available).

39
40 Once a CDPD M-ES has been registered, an intercept point at a Home MD-IS
41 shall provide the following on each IP packet delivered to the intercept subject:

- 42 • Case identity

- Date and time of receipt of the IP packet by the network
- Source and destination IP addresses of the intercepted packet
- The Service Provider Network Identity of the serving system.

Technical feasibility and complexity *(editor's note: placeholder for information to follow)*

6.2.16.1.5 Packet Cable

SDO Lead:

Contact: Bill Marshall

76.1.5.1 Introduction

PacketCable™, a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies, is identifying and defining specifications which may be used to implement packet-based telephony, video, and other high speed, multimedia services over hybrid fiber coax (HFC) cable systems utilizing the DOCSIS protocol for access and the Internet Protocol (IP) for end-to-end data transport. PacketCable utilizes a network superstructure that overlays the two-way data-ready broadband cable access network. While it is anticipated that the initial PacketCable service offering will be packet-based residential telephony, the long-term project vision encompasses a large family of packet-based services.

In recent years the growth of a worldwide IP based data network, coupled with the exponential growth in the number of households that have online access, have resulted in an enabling environment for offering integrated voice and data services over a common broadband cable access network and IP transport backbone. While the initial application of IP voice technology was for toll bypass services, the technology has now matured to the point where it is feasible to offer IP based voice services, including services that may substitute for local exchange services offered by traditional local exchange carriers, and even intelligent feature phone service for both voice and video.

With the success of the DOCSIS standardization effort, the QoS enhancements of DOCSIS 1.1, and the acceleration of major cable system upgrades for two way capacity, the infrastructure is in place for development and deployment of packetized voice and video applications. These applications can be deployed at relatively low incremental cost, providing a reasonable alternative to traditional local telephony, as well as a platform for introducing the next generation of telephony and general real time multimedia services.

1 Note that from time to time this document refers to the voice communications
2 capabilities of a PacketCable network in terms of "telephony" or "IP Telephony."
3 The legal/regulatory classification of IP-based voice communications provided
4 over cable networks and otherwise, and the legal/regulatory obligations, if any,
5 borne by providers of such voice communications, are not yet fully defined.
6 Nothing in this document is addressed to, or intended to affect, those
7 legal/regulatory issues. In particular, while this document uses standard terms
8 such as "call," "call signaling," "telephony," "telephone number," etc., it should
9 be recalled that while a PacketCable network performs activities analogous to
10 these PSTN functions, the manner by which it does so differs considerably from
11 the manner in which they are performed in the PSTN by telecommunications
12 carriers, and that these differences may be significant for legal/regulatory
13 purposes. Moreover, while reference is made here to "IP Telephony," it should be
14 recognized that this term embraces a number of different technologies and
15 network architecture, each with different potential associated legal/regulatory
16 obligations. No particular legal/regulatory consequences are assumed or implied
17 by the use of this or any other term derived from usage within the traditional
18 circuit-switched telephone industry.

19 Note also that this document discusses the interface between a
20 telecommunications carrier that provides telecommunications services to the
21 public for hire using PacketCable™ capabilities (a
22 "PacketCable/Telecommunications Service Provider," or "PC/TSP") and a Law
23 Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized
24 electronic surveillance. Companies using PacketCable capabilities will not in the
25 normal case be "telecommunications carriers," either as defined in the
26 Communications Assistance for Law Enforcement Act (CALEA) or otherwise.
27 Instead they will be providers of information services. However, some companies
28 using PacketCable capabilities may, by virtue of other actions, be
29 "telecommunications carriers" for purposes of CALEA with respect to their use of
30 PacketCable capabilities. In this regard, a telecommunications carrier that
31 complies with a publicly available technical requirement or standard adopted by
32 an industry association or standards-setting organization shall be found to be in
33 compliance with the assistance capability requirements of CALEA. As noted,
34 cable operators are not ordinarily telecommunications carriers, but if a cable
35 operator has taken the steps to become a carrier, and uses PacketCable to provide
36 carrier services, then CALEA might apply to the equipment used to implement
37 PacketCable. For this reason, we are providing consideration of CALEA
38 concerns as part of the PacketCable specification, for the benefit of anyone who
39 might use this architecture/technology as part of their carrier activities.
40
41

86.1.5.2 Architecture

The PacketCable reference architecture for PacketCable 1.0 is shown in Figure 1. The architecture can be divided into three phases. The access network on the originating client side, the managed IP Network with an interface to the PSTN and the access network on the terminating client side.

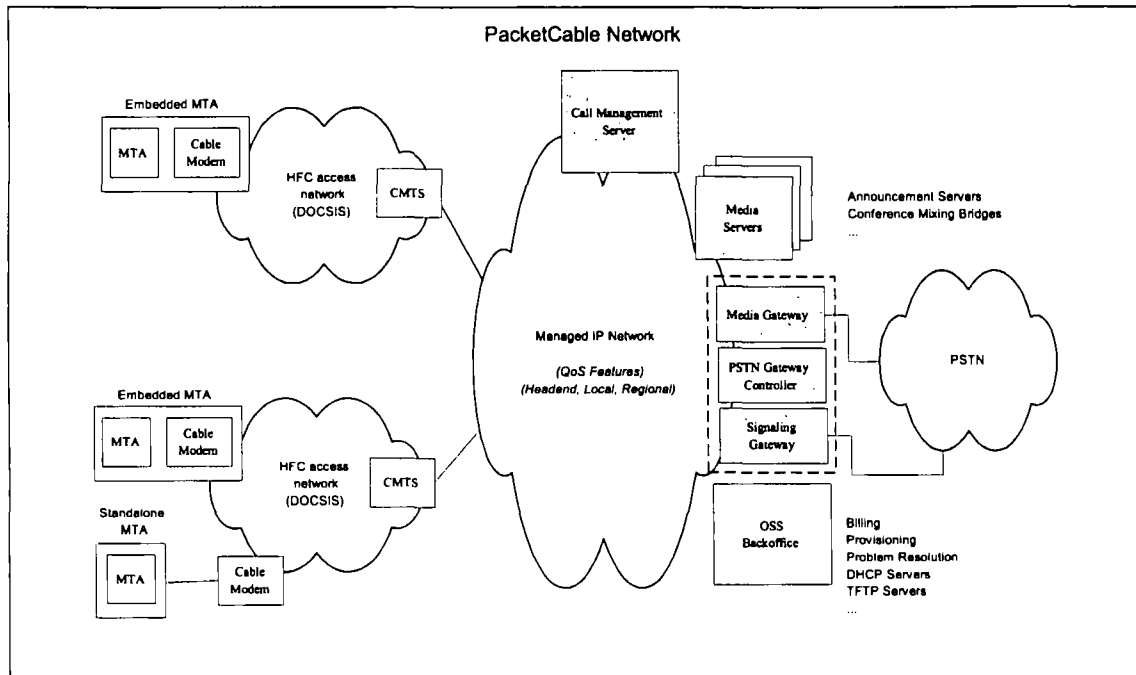


Figure 1. PacketCable™ Reference Architecture

The HFC DOCSIS access network as shown in Figure 2, provides the access to the IP managed network with DOCSIS 1.1 enabled Quality of service. The access network is defined to include the Cable Modem (CM), Multi-media Terminal Adapter (MTA), and the Cable Modem Termination System (CMTS). In PacketCable 1.0 the subscriber equipment consists of an embedded MTA with a DOCSIS CM MAC and PHY. The CMTS resides in the cable head end office and provides provisioning, authorization, and admission control for data communication over the access network.

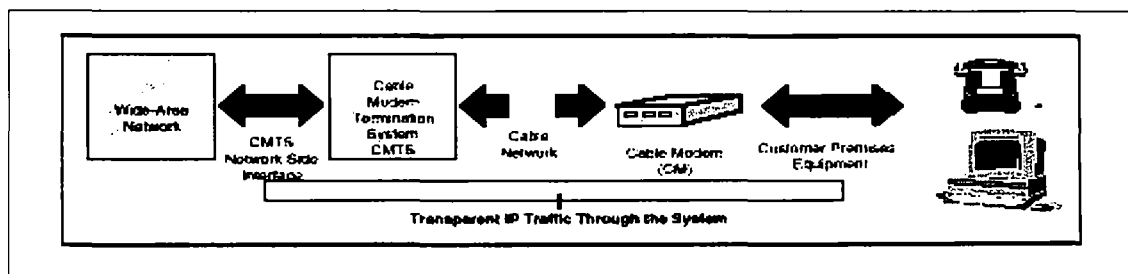


Figure 22: HFC DOCSIS Access Network

The PacketCable managed IP network provides interconnection between PacketCable network elements involved in call signaling, provisioning, and quality of service establishment, as well as long-haul IP connectivity to other PacketCable administrative domains. The managed IP network is defined to include the Call Management Server which contains a Call Agent to provide the telephony signaling services and a Gate controller which is responsible for the admission policy decision. Announcement Server is used to manage and provide all announcements in the network.

The PSTN interface is a vital part of the PacketCable reference architecture. The PSTN interface consists of three main elements, the Signaling Gateway (SG) which translates signaling messages between the PSTN and IP network, the Media Gateway (MG) which translates media between the PSTN and IP network, and the Media Gateway Controller (MGC) which controls the access to the PSTN gateway.

96.1.5.3 Subscriber Equipment

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

1 • Provides multiple audio indicators to phones, such as ringing tones, call
2 waiting tones, stutter dial tone, dial tone, etc.
3 • Provides standard PSTN analog line signaling for audio tones, voice
4 transport, caller-id signaling, and message waiting indicators
5 The PacketCable system design places much of the session control intelligence at
6 the endpoints, where it can easily scale with technology and provide new and
7 innovative services. While this “future-proofing” is a goal of the design, we
8 recognize that it leaves open a wide range of security threats. The basic
9 assumption is that the MTA is not immune to customer tampering, and that the
10 significant incentive for free service will lead to some very sophisticated attempts
11 to thwart any network controls placed on the MTA.
12 Under these circumstances, it is important to realize that an MTA under
13 customer control will likely not cooperate with electronic surveillance, and
14 methods are therefore described here that do not depend in any way on
15 cooperation with the MTA.

16 ~~106.1.5.4~~ Subscriber Identification

17 A subscriber for electronic surveillance purposes is identified by a telephone
18 number, and the telephone number is reported to Law Enforcement Agency
19 (LEA) in the ~~call-identifying~~ Pen Register and Trap and Trace information. Other
20 identity information of the subscriber equipment, e.g. a provisioned security
21 certificate, is used by the CMS to dynamically determine the identity of the
22 subscriber and the telephone number for a particular call. The CMS includes, as
23 part of the authorization of network resources, the packet stream identification
24 (source and destination IP addresses, destination port number) and an indication
25 that the packet stream is subject to surveillance.

26 Other mechanisms of subscriber identification are too dynamic and transient to
27 be used as subscriber identification for surveillance.

28 Cable Modems (CMs) are manufactured with a unique MAC address (48-bits).
29 This MAC address is used by DOCSIS to identify the CM during the registration
30 process, and identifies a particular configuration file containing further
31 provisioning information for the subscriber. The MAC address only appears on
32 the HFC network, and is often suppressed by the Payload Header Suppression
33 feature of DOCSIS. It is therefore not usable as a subscriber identifier for a
34 ‘snooping’ function attached to the HFC network.

35 Packet streams generated by the CM are identified by DOCSIS Service Flows.
36 Each Service Flow has a dynamic identifier assigned, the Service-Flow-ID
37 (SFID); while active it also has a Service-ID assigned (SID). The SID is used in
38 the DOCSIS media access layer to control access to the shared upstream
39 resources. The dynamic and transient nature of SIDs makes them unusable as
40 subscriber identifiers for surveillance.

41 The CM uses DHCP to obtain an IP address. This resulting address is likely to
42 change every time the CM is initialized. Use of a ‘snooping’ function on the IP
43 links of the network would require dynamic configuration based on DHCP

1 requests. This may be technically feasible, but has not been attempted in the
2 PacketCable environment.

3 ~~16.1.5.5~~ Intercept Access Points

4 The Intercept Access Function, performed by the Intercept Access Points (IAPs),
5 isolates an intercept subject's communication or reasonably available call-
6 ~~identifying Pen Register and Trap and Trace~~ information unobtrusively. The
7 Access Function is responsible for the collection of call content and reasonably
8 available call-~~identifying Pen Register and Trap and Trace~~ information and
9 making such information available to the Delivery Function.

10 In a PacketCable network, four elements are designated as Intercept Access
11 Points:

- 12 • The Cable Modem Termination System (CMTS) which controls the set of
13 cable modems attached to the shared medium of the DOCSIS network.
14 The CMTS is responsible for intercepting the Call Content, and certain
15 ~~call-identifying Pen Register and Trap and Trace~~ information.
- 16 • The Call Management Server (CMS) which provides service to the
17 subscriber. The CMS is responsible for intercepting the ~~Call-Identifying~~
18 ~~Pen Register and Trap and Trace~~ information.
- 19 • The Media Gateway (MG) is designated as an Intercept Access Point for
20 purposes of intercepting Call Content for redirected calls to the PSTN.
- 21 • The Media Gateway Controller (MGC) is designated as an Intercept Access
22 Point for purposes of intercepting the ~~Call-identifying Pen Register and~~
23 ~~Trap and Trace~~ information for redirected calls to the PSTN.

24 The equipment and facilities of each subscriber include two Intercept Access
25 Points (CMTS and CMS), and ~~call-identifying Pen Register and Trap and Trace~~
26 information reasonable available at these IAPs is provided to LEA. Redirected
27 calls in the PacketCable network might not utilize the equipment or facilities of
28 the subscriber who initiated the redirection. Accordingly, the Intercept Access
29 point for a call that has been redirected will be either the CMS/CMTS of the new
30 destination (if redirected to another PacketCable endpoint within the same
31 provider's network) or the MGC/Media Gateway of the PSTN interconnection (if
32 redirected to a PSTN endpoint).

33 ~~16.1.5.6~~ Information Available to Law Enforcement

34 For purposes of the PacketCable network's surveillance capabilities, only those
35 packets sent or received by the intercept subject that utilize the capabilities of the
36 Call Management Server to establish the communication, and utilize enhanced
37 Quality of Service as authorized by the Call Management Server, are considered
38 "calls" within the scope of surveillance support obligations set out in CALEA.
39 Cable operators that have deployed PacketCable capabilities may offer a range of
40 other services to their customers that make use of packet-switched
41 communications, such as email and Internet access. Other than the packets

1 identified in the first sentence of this paragraph, packets sent or received by the
2 intercept subject are considered Information Services.

3 The following call events are defined, and convey information to a LEA for each
4 identifying Pen Register and Trap and Trace events: Answer (a two-way
5 connection has been established for a call under surveillance), CCChange (a
6 change in the description of call content delivery for a call under interception),
7 CCClose (end of call content delivery for a call under interception), CCOpen
8 (beginning of call content delivery for a call under interception), Origination (IAP
9 detects that the surveillance subject is attempting to originate a call), Redirection
10 (call under surveillance is redirected, e.g. via termination special service
11 processing, or via a call transfer), and TerminationAttempt (IAP detects a call
12 attempt to a surveillance subject).

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

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

27 The messages that identify the call events convey the basic information that reports the
28 disposition of a call. This section describes those event messages and the supporting information.

29 *(editor's note: the "message" section will be changed to be in line with the other appendices which show information that*
30 *could be reported as bulleted items.)*

31 ~~12.16.1.5.6.1~~ Answer

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

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

- 37 - an outgoing call from a surveillance subject is answered or cut-through in both
38 directions.
- 39 - a surveillance subject answers a previously unanswered call originating from an on-net
40 or off-net associate.
- 41 - a redirected call identified by the PC/TSP as a call under surveillance is answered or
42 cut-through in both directions

1 The Answer message includes 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 than 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.

2 Table 1: Answer Message

3 **12.26.1.5.6.2 CCChange**

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

9 The CCChange message includes 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.

1 Table 2: CCChange Message

2 **12.36.1.5.6.3 CCClose**

3 The CCClose message reports the end of delivery of call content for a call under interception. The
4 CCClose message is generated for calls under interception when a Call Content Channel has been
5 opened (via a CCOpen message) and one of the following events are detected by an IAP:

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

8 The CCClose message includes 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.

9 Table 3: CCClose Message

10 **12.46.1.5.6.4 CCOpen**

11 The CCOpen message is generated for calls under interception when the first of either the
12 originating or terminating party is provided voice packet quality of service. The CCOpen message
13 is triggered for surveillances that require the delivery of call content, and it identifies the

- 1 beginning of the delivery of call content information. The main purpose of this message is to
 2 provide LEA with information necessary to decode the voice packets for the call.
- 3 The CCOpen message includes 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.

4 Table 4: CCOpen Message

5 ~~12.56.1.5.6.5~~ Origination

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

- 8 - call origination signaling by a surveillance subject is detected, and the call is routed
 9 toward an on-net or off-net destination. This may include translation of digits
 10 entered by the subject to another set of digits (e.g. 800-number translation).
- 11 - call origination signaling by a surveillance subject is detected, and the call could not
 12 be completed.
- 13 - call origination signaling by a surveillance subject is detected, and the subject signaled
 14 the call to be abandoned before the call could be routed to its destination.

15 The Origination message includes 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 5: Origination Message

12.66.1.5.6.6 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 is 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 includes 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.

1 Table 6: Redirection Message

2 **12.76.1.5.6.7 Release**

3 The Release message reports the release of resources used for a call under surveillance. The
4 Release message is generated for calls under surveillance that had previously reported an Answer
5 event, when one of the following events is detected by an IAP:

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

9
10 The Release message includes 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.

11 Table 7: Release Message

12 **12.86.1.5.6.8 TerminationAttempt**

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

1 - an incoming off-net or on-net call to a surveillance subject is detected

2 The TerminationAttempt message includes 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

3 Table 8: TerminationAttempt Message

4

5 136.1.5.7 Preferred Delivery Format

6 The network layer protocol for delivery of both Call Data Connection (CDC) and
7 Call Content Connection (CCC) information is as defined by the Internet
8 Protocol (IP) [RFC0791]. Both CCC and CDC information may be provided
9 over the same physical interface. Information is available in the CCC and CDC
10 information packets to identify the type of packet (either CDC or CCC) and the
11 particular case. The identification is provided either directly by the packet
12 containing the surveillance case identifier, or indirectly by the packet containing
13 an identifier that can be correlated with the case identifier.

14 Call Content is delivered as a stream of UDP/IP datagrams, as defined in
15 [RFC0768, RFC0791], sent to the port number at the Collection Function (CF)
16 as provided during provisioning of the interception. The format of the UDP/IP
17 payload is given in the PacketCable Electronic Surveillance Specification.
18 The Call Data Connections in PacketCable are implemented as TCP/IP
19 connections, established by the Delivery Function (DF), to the Collection
20 Function designated by the LEA in the surveillance provisioning.
21 Contained in the IP header is the source IP address, which is the address of the
22 DF, and the destination IP address, which is the address of the CF provided
23 during interception provisioning.

1 All transfer of packets other than those operationally required to maintain the
2 link are from the Delivery Function to the Collection Function only. At no time
3 may the LEA send unsolicited packets from the CF to the DF.
4 The default link-layer protocol between the DF and CF is as defined by the
5 Ethernet protocol [RFC0894, RFC0826]. However, alternate link-layer
6 protocols may be used at the discretion of the PC/TSP based on negotiated
7 agreements with the LEA.
8 The default type of physical interconnect provided by the PC/TSP at the
9 demarcation point is an RJ45 10/100BaseT [ISO8802-3] connection. However,
10 alternate physical interconnects may be provided at the discretion of the PC/TSP.

11 146.1.5.8 Capacity Limitations

12 Capacity requirements are fundamental to the design and development of any
13 technical standard or specification (as well as for the equipment developed in
14 compliance with such standards). Several technical considerations, pivotal to the
15 design process, are affected by capacity requirements. However, so far, the
16 Attorney General has not identified capacity requirements for
17 telecommunications carriers that use PacketCable capabilities to provide
18 telecommunications services. In the absence of these formal capacity
19 requirements, CableLabs has had to make certain reasonable assumptions about
20 capacity in order to proceed with developing this specification. CableLabs
21 believes that these assumptions reflect reasonable estimates based on industry's
22 technical expertise as well as law enforcement's historical requirements on other
23 technologies. However, to the extent that these reasonable assumptions differ
24 from whatever formal capacity requirements the Attorney General eventually
25 identifies, substantial modifications to this specification may be required (with
26 resulting delays and lost effort in the design and development of equipment
27 consistent with this specification).

28 As such, PacketCable has made the following assumptions: (1) the IAP supports a
29 maximum number of intercepts of 5% of its active calls, (2) the DF supports a
30 maximum of five surveillance orders for any single subject, (3) the DF to CF
31 interface must be capable of supporting the maximum number of intercepts times
32 the maximum number of intercepts per subject, (4) it is the responsibility of the
33 PC/TSP to provide adequate resources to transport call content and call data
34 information from the IAP to the DF based on statistical call models, (5) it is the
35 responsibility of the PC/TSP to provide adequate resources to transport
36 redirected call content and call data information between DFs within the PC/TSP
37 network based on statistical call redirection models, (6) when adequate resources
38 are not available, situations may arise where call content and ~~call-identifying Pen~~
39 Register and Trap and Trace information are not delivered to the LEA.