Report to the

Federal Communications Commission

on Surveillance of

Packet-Mode Technologies

(September 29, 2000)

Prepared by the Joint Experts Meeting convened by Committee TR 45 of the Telecommunications Industry Association

Report on Surveillance of Packet-Mode Technologies

Table of Contents 1

1 Introduction

In 1997, an industry specification, TIA/EIA/J-STD-025 Lawfully Authorized Electronic Surveillance, was published in response to the Communications Assistance for Law Enforcement Act (CALEA) released in 1994. Privacy concerns have been raised against the packet data solution contained in this specification.

Accordingly, in its Third Report and Order regarding implementation of CALEA, 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 deadline imposed by the FCC, and to build a record based on technical facts, the Telecommunications Industry Association (TIA) has sponsored two Joint Experts Meetings (JEM). This report represents the findings of these meetings.

1.1 Purpose and Scope

The purpose and scope of this report is to assist the Telecommunications Industry Association (TIA) to prepare a mandated report to the Federal Communications Commission (FCC) regarding certain technical and privacy concerns in packet-mode communications associated with lawfully authorized electronic surveillance under the Communications Assistance for Law Enforcement Act.

1.2 Organization

Section 2 "References" is a list of references used in the preparation of this report.
Section 3 "Acronyms" defines those acronyms that are used in this report.
Section 4 "Introduction and Executive Summary" summarizes the reasons for convening the JEM and the output of JEM I and JEM II.
Section 5 "Packet Communication Sessions established by a Call Management Server" discusses Pen Register and Trap and Trace surveillance of packet-mode communication using a Call Management Server (CMS).
Section 6 "Packet Communication Sessions established without a Call Management Server" discusses Pen Register and Trap and Trace surveillance of packet-mode communication where a CMS is not deployed.
Appendix A "Technical Specific Information" is specific to the technologies discussed in the JEM and includes greater details on surveillance capability of cdma2000, GPRS, CDPD, Packet Cable, X.25, IP, ATM, and Frame Relay.
Appendix B "CALEA JEM Invited and/or Participating Groups List".
Appendix C "JEM I Meeting Agenda".
Appendix D "JEM I Meeting Summary".
Appendix E "JEM II Meeting Agenda".
Appendix F "JEM II Meeting Summary".

2 References

References may be made to specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply, or publications without mention of a specific version, in which case the latest version applies.

American National Standards Institute (ANSI):

[ANSI-95] ANSI/TIA/EIA-95, *800-MHz & 1800MHz CDMA.*

Cable Television Laboratory:

[DOCSIS] SP-RFIv1.1-I05-000714, *Data Over Cable Service Interface Specifications, Radio Frequency Interface Specification*, Cable Television Laboratories, Inc., July 14, 2000.

[PKT-PCES] PKT-SP-ESP-I01-991229, *PacketCable Electronic Surveillance Specification*, Cable Television Laboratories, Inc., December 29, 1999.

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

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

[PKT-SEC] PKT-SP-SEC-I01-991201, *PacketCable Security Specification*, Cable Television Laboratories, Inc., December 1, 1999.

European Telecommunications Standards Institute (ETSI):

[GPRS-1] TS 101 113. 3G TS 22.060, *Digital Cellular Telecommunications System* (Phase 2+) *General Packet Radio Service (GPRS), Service Description; Stage 1* (GSM 02.60*).*

[GPRS-2] 3G TS 23.060, *General Packet Radio Service Description, Stage 2.*

[ETSI-LI] TS 101 509, *Digital Cellular Telecommunications System (Phase 2+); Lawful Interception; Stage 2,.* (GSM 3.33).

[3GPP-LI] 3G TS 33.107, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Architecture and Functions.*

[GSM-1] GSM 02.33 V7.1.0 (1999-07); *Digital Cellular Telecommunications System (Phase 2+); Lawful Interception - stage 1*.

[GSM-2] GSM 03.60 V6.2.0 (1998-10); *Digital Cellular Telecommunication System (Phase 2+); General Packet Radio Service (GPRS); Service Description*.

Federal Communications Commission (FCC):

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

International Standards Organization:

[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.

[ISO8348] ISO 8348: *Information processing systems - data communications - network service definition*.

International Telecommunications Union (ITU):

[X.25] ITU-T Recommendation X.25: *Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet-mode and connected to public data networks by dedicated circuit*.

[Q.931] ITU-T Recommendation Q.931, *ISDN User-network Interface Layer 3 Specification for Basic Call Control.*

Internet Engineering Task Force (IETF):

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

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

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

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

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

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

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

[RFC1958] Carpenter, B., *Architectural Principles of the Internet*, June 1996.

[RFC2775] Carpenter, B., *Internet Transparency*, February 2000.

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

[RFC2804] IAB, *IETF Policy on Wiretapping*, May 2000

[RFC2138] Rigney, C. et. al., *Remote Authentication Dial In User Service (RADIUS*), April 1997.

[RFC1541] Droms, R., *Dynamic Host Configuration Protocol*, October 1993.

[RFC2139] Rigney, C., *RADIUS Accounting*, April 1997.

[RFC1332] McGregor, G., *The PPP Internet Protocol Control Protocol (IPCP)*, May 1992.

[RFC1918] Rekhter, Y., et. al., *Address Allocation for Private Internets*, February, 1996.

[RFC1631] Egevang, K., et. al., *The IP Network Address Translator (NAT)*, May 1994.

[RFC2663] Srisuresh, P. and M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, August 1999.

[RFC1702] Hanks, S., et. al., *Generic Routing Encapsulation over IPv4 networks*, October, 1994.

[RFC1853] Simpson, W., *IP in IP Tunneling*, October 1995.

[RFC2661] Townsley, M., et. al., *Layer Two Tunneling Protocol 'L2TP'*, August 1999.

[RFC2406] Kent, S. and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, November 1998.

[RFC2002] Perkins, C., *IP Mobility Support*, October 1996.

[RFC1661], Simpson, W., *The Point-to-Point Protocol (PPP)*, July 1994.

Telecommunications Industry Association:

[IS-835] TIA/EIA/IS-835, *Wireless IP Network Standard for cdma2000*,

[IS-707-A] TIA/EIA/IS-707-A, *Service Options for CDMA, Revision A*,

[IS-2000-A] TIA/EIA/IS-2000-A. *Spread Spectrum Systems*,

[J-STD-025] TIA/ATIS, *Lawfully Authorized Electronic Surveillance*, December, 1997.

[J-STD-025A] TIA/ATIS, *Lawfully Authorized Electronic Surveillance, Revision A*, May, 2000.

[IS-732] TIA/EIA/IS-732 *Cellular Digital Packet Data*.

Other:

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

3 Acronyms

AAA:	Authentication, Authorization and Accounting
AALs	ATM Adaptation Layers
AF:	Access Function
APN:	Access Point Name Data
ASN.1	Abstract Syntax Notation One
ATIS:	Alliance for Telecommunication Industry Solutions
ATM:	Asynchronous Transfer Mode
BRI:	Basic Rate Interface (ISDN)
CDMA:	Code Division Multiple Access
CDPD:	Cellular Digital Packet Data
CF:	Collection Function
CLAMN:	Called Line Address Modification Notification
CLNP:	Connectionless Network Protocol
CM:	Connection Management
CMS:	Call Management Server
CMTS:	Cable Mobile Termination System
DF:	Delivery Function
DHCP:	Dynamic Host Configuration Protocol
DLCI:	Data Link Connection Identifier
DNS:	Domain Name System
DOCSIS:	Data Over Cable Service Interface Specification
DS0:	Digital Signal Level 0
DTMF:	Dual Tone Multifrequency signaling
FDDI:	Fiber Distributed Data Interface
FR:	Frame Relay
GPRS:	General Packet Radio Service
HFC:	Hybrid Fiber-Coax
HPPI:	Hybrid Performance Parallel Interface
HTTP:	Hypertext Transfer Protocol
H.248/megaco	Media Gateway Control - IETF Working Group
H.323:	A standard approved by the International Telecommunication Union (ITU) that defines how conferencing data is transmitted across networks
IANA:	Internet Assigned Numbers Authority
IAP:	Intercept Access Point
IETF:	Internet Engineering Task Force
IMEI:	International Mobile Equipment Identifier
IMSI:	International Mobile Station Identifier
IP:	Internet Protocol
IPSEC:	Internet Protocol Security
IPv4:	Internet Protocol Version 4
IPv6:	Internet Protocol Version 6
ISDN:	Integrated Services Digital Network

ISP:	Internet Service Provider
JEM:	Joint Experts Meeting
L2TP:	Layer 2 Tunneling Protocol
LAN:	Local Area Network
LATA:	Local Access Transport Area
LAES:	Lawfully Authorized Electronic Surveillance
M-ES:	Mobile End System
MAC:	Medium Access Control
MD-IS:	Mobile Data Intermediate System
MDBS:	Mobile Data Base Station
MG:	Media Gateway
MGC:	Media Gateway Controller
MGCP:	Media Gateway Control Protocol
MS:	Mobile Station
MSID:	Mobile Station Identifier
MSISDN:	Mobile Station International Station Directory Number
MT:	Mobile Terminal
MTA:	Multimedia Terminal Adapter
NAI:	Network Access Identifier
NAS:	Network Access Server
OSI:	Open System Interconnection
PBX:	Private Branch Exchange
PC:	Packet Cable
PDP:	Packet Data Protocol
PDSN:	Packet Data Serving Node
PHY:	Physical Access
PINT:	PSTN and Internet Interworking - IETF WG
POP:	Point Of Presence
PPP:	Point to Point Protocol
PSTN:	Public Switched Telephone Network
PVC:	Permanent Virtual Circuit
QoS:	Quality of Service
RADIUS:	Remote Authentication Dial In User Service protocol
RAS:	Registration, Administration, and Status
RSVP:	Resource Reservation Protocol
SCTP:	Stream Control Transmission Protocol
SFID:	Service-Flow-ID
SG:	Signaling Gateway
SID:	System Identification Number
SIP:	Session Initiation Protocol
SNA:	Systems Network Architecture
SONET:	Synchronous Optical Network
SVC:	Switched Virtual Circuit
TIA:	Telecommunication Industry Association
TCP:	Transmission Control Protocol
TDM:	Time Division Multiplexing

TE:	Terminal Equipment
TSP:	Telecommunications Service Provider
UDP:	User Datagram Protocol
VCI:	Virtual Circuit Indicator
VFRAD:	Voice over Frame Relay Access Device
VoFR:	Voice over Frame Relay
VoP:	Voice over Packet
VoIP:	Voice over Internet Protocol
VPI:	Virtual Path Indicator

4 Introduction and Executive Summary

4.1 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 access to the full call content stream when only Pen Register or Trap and Trace 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."

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 deadline imposed by the FCC, and to build a record based on technical facts, the Telecommunications Industry Association (TIA) convened a Joint Experts Meeting.

The JEM was intended to serve as a technical fact-finding body across the spectrum of packet-mode communication technologies regarding the feasibility of delivering less than the full content of a packet to law enforcement in response to a pen register order. Invitations were sent to a broad range of packet-mode communications expert organizations. The invitation list is attached as Appendix B.

To facilitate discussion at the JEM, contributions from various entities were made available through posting on the TIA website prior to meeting in person (see CALEA JEM link at http://www.tiaonline.org/standards/calea_jem). A publicly available mailing list was also maintained. A two-hour question and answer session covering the scope of the JEM was conducted on March 20, 2000.

The first JEM session was conducted on May 3-5, 2000, in Las Vegas, NV. Based on the results of the first JEM, a second JEM session was conducted in Washington D.C., on June 26-29, 2000. The output from those meetings is described below.

4.2 JEM I Output

Following opening remarks, updates were provided on the status of Revision A of J-STD-025, the legal purpose of the JEM, and the status of CALEA activities. Presentations on technical issues followed. A copy of the JEM I meeting agenda is attached as Appendix C.

While the scope of the JEM included reporting on the broadest number of packet-mode communications technologies, contributions were received only on the following technologies: cdma2000, GPRS, and IP. There was broad discussion across many technologies however.

JEM I established a framework for preparing this report. A copy of the JEM I meeting report to TIA TR45 is attached as Appendix D.

First, JEM I concluded that, based on current FCC guidance, it could not define “call-identifying information” for packet services. Several contributors noted that the term “call-identifying information” is ambiguous with regard to packet communications. Instead, JEM I concluded that it could only attempt to identify what information may be available about the packet communication without regard to whether it might be characterized as "call identifying information" under CALEA. . Once the information was identified, JEM I concluded that it could then report on the technical impact and feasibility of making that information available to a law enforcement agency (LEA). This decision was consistent with the purpose and scope of the JEM, which did not include discussion of legal issues.

Second, JEM I noted that CALEA requirements apply to telecommunication services not information services. JEM I recognized, however, that from a packet point of view, the two may be indistinguishable. JEM I determined that it is not technically advisable to determine, on a packet by packet basis, the application or communication services that is being provided. JEM I also concluded that, the application or communication services that is being provided can not be determined even by observation of the complete stream of packets. The point of communications setup may be the only time that a telecommunication service can be distinguished from an information service.

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

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

Accordingly, the framework for this report reflects this two-pronged approach. In each category, JEM I decided to report on the information available and the technical impact of providing it. Because further information was necessary, a second JEM meeting was scheduled to accept contributions for technologies and assignments were taken to prepare appendices of technologies for this report.

Finally, JEM I agreed that if a change to the current standard (J-STD-025) were deemed necessary by the Federal Communications Commission, a court or the industry, as a result of this process, the JEM recommends that the open, joint ATIS T1/TIA activity currently underway in TIA TR45.2 LAES Ad Hoc be responsible for completing this task. In its simplest form, this change may just be the inclusion of appropriate references to other standards. Nothing in this process, however, was intended to or should preclude any standards setting or industry organization from adopting their own "safe harbor" standard for their particular technology (e.g., satellite or cable standards).

4.3 JEM II Output

Contributions to JEM II were received in advance of the meeting and made available on the TIA website. Technologies covered in the contributions included: cdma2000 Wireless IP, X.25 over ISDN, ATM, Frame Relay, GPRS, PacketCable, CDPD, and IP.

Following opening remarks, updates were provided on the status of Revision A of J-STD-025 as well as the pending appeal before the U.S. Court of Appeals for the District of Columbia of the FCC Report and Order. Presentations on technical issues followed.

A copy of the JEM II meeting agenda is attached as Appendix E and a copy of the JEM II meeting report to TIA TR45 is attached as Appendix F.

In addition to the contributions based on assignments from JEM I, the CALEA Implementation Section (CIS) of the Federal Bureau of Investigation (FBI) submitted a contribution that proposed a functional approach to separating packet content from packet identifying information. Further, the FBI requested the opportunity to present technology it currently uses to separate identifying information from content known as "Carnivore."

The Carnivore presentation was provided by law enforcement's Data Intercept Technology Program at the FBI's Engineering Research Facility from Quantico, Virginia. The presenters described the current law enforcement techniques for separating identifying information from content to comply with lawfully authorized surveillance orders. In summary, law enforcement, in cooperation with a service provider pursuant to legal authorization, gains access to a packet stream in which the target's communications reside. The access is made on the service provider's premises using law enforcement equipment.

According to the presenters, the target's communications are identified through use of a filtering program developed by law enforcement. In a Pen Register or Trap and Trace Order only the relevant information from the target's packets are stored to disk. The filter

program separates the relevant information from the target's content and law enforcement then collects the information.

The presenters informed JEM II that development of the filter protocol was intensive and fluid because of the ever changing nature of packet protocols and the constant introduction of new protocols; the Carnivore software or filters may need to be updated almost weekly to stay current. Carnivore has not been proven effective, as yet, in cases where the subject's communications are part of a high bandwidth transmission. The presenters acknowledged that to require service providers to develop and maintain similar Carnivore-like software would be extremely burdensome.

CIS then presented its contribution, which suggested "examining the full packet stream from the subject in order to gather the relevant call-identifying information for delivery to the LEA." CIS acknowledged in its contribution, however, that "examine[ing] the full packet stream and examine protocol layers higher than layer 3 would place a high load on existing network elements in most architectures." Accordingly, using the J-STD-025 functional approach to surveillance, CIS suggested that "the access function unobtrusively captures the complete subject packet stream (including all call content and call-identifying information) and distributes it to the delivery function." The delivery function in the contribution contains a new "sub function" referred to as a Separation Function. The Separation Function would remove "any information the LEA may not be entitled to based on the court order [so that in] the case of Title I court orders, all communication content information would be removed." The delivery function would then deliver the identifying information to the LEA's collection function.

CIS did not recommend any specific implementation or ownership of the Separation Function. CIS acknowledged that "development of separation capabilities (i.e. filtering capabilities) within a service provider's network may be unrealistic as it would be highly resource intensive, very inefficient, and potentially inconsistent between providers". For these and other reasons described below there was industry consensus in subsequent discussions that it would not be feasible developing such a Separation Function independently or through a standards based process. To address these issues while also addressing privacy concerns, it was discussed that Carnivore-like software could be made available to service providers so that the Separation Function occurred under service provider management.

JEM II agreed that Carnivore, as presented by CIS, constitutes a potential technical solution for separating content from packet information and therefore is included within the JEM report. However, numerous industry concerns were raised about the introduction of government-provided product into the service provider network. Concerns were acknowledged regarding (a) potential liability for failure of the product, (b) uncertain impact on the network, (c) terms and conditions to obtain the product from government, (d) administrative and operational impacts from constant upgrades to the filter, (e) scalability, (f) privacy, (g) certification or testing of the product, and (h) uncertainty about the scope of the filter (i.e., whether the filter produces information

that is coextensive with call identifying information and who establishes the criteria for separation).

A Compaq contribution recommended that a similar filtering technology be developed by an independent, third party entity as open source code. This solution attempts to (1) overcome potential privacy concerns with a solely law enforcement-developed filter, and (2) take advantage of the opportunity provided by an open source model to receive rapid input on new packet protocols as they are developed. As with the FBI-proposed filter, there are many industry concerns regarding the implementation of an open source solution.

Nonetheless, JEM II recognized CIS and Compaq contributions as valuable additions to the process. There was consensus that the technological solution would be included in the report but that the legal, policy and implementation issues would not be addressed and were beyond the scope of the report. For example, JEM II does not address the potential impact of a Carnivore solution being implemented within the delivery function. The potential solution would require additional study. It was also noted that the current packet-mode solution in J-STD-025 is less intrusive from a privacy perspective than law enforcement's current Carnivore implementation because under the existing standard only the packet stream known by the service provider to be associated with the subject will be delivered to the LEA collection function in contrast to law enforcement's current practice of attaching Carnivore to a packet stream that will contain packets from a number of different users.

JEM II expressed its appreciation to CIS for arranging the Carnivore presentation and for its technical contribution to the JEM, which was incorporated into the report.

In addition to the CIS contribution, contributions regarding other technologies were reviewed, accepted, and incorporated as appendices to the report. It was agreed that the report would be posted on the TIA website for further review and comment before completion of the JEM process and forwarding to TIA.

5 Packet Communication Sessions established by a Call Management Server

This section describes the environment in which call based services are provided using a Call Management Server (CMS). A CMS facilitates the establishment of end-to-end protocols such as H.323 or SIP. The following material in this section assumes that the CMs is capable of providing call events. If the CMS does not provide call events then the discussion in section 6 applies.

5.1 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 Pen Register or Trap and Trace information, to identify the content stream, and to identify the timing requirements). Other standards may address other technologies and networks.

5.2 Technical Impacts

The provider will indicate to law enforcement the negotiated service (e.g. user's session negotiation), however, the user may use the service differently than negotiated. For example, in a voice over packet call the user may be using the service to send or receive other than voice information. Thus, law enforcement may be expecting information regarding a voice call but receive some other content.

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.

6 Packet Communication Sessions established without a Call Management Server

This section describes the environment for service providers that provide packet-mode transport, without the involvement of a CMS.

6.1 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.

6.2 Technical Impacts

For all of the delivery options discussed below, the following comments apply:

- the consensus is that in many technologies the duplication of a packet stream requires significant resources. 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 or Trap and Trace. 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;

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

6.2.1 Delivering the Entire Packet Stream

Currently J-STD-025 specifies delivery of the entire packet stream or just the Source and Destination address information for a user under surveillance. While delivery of the entire packet stream guarantees that authorized Pen Register and Trap and Trace information will be delivered to the LEA, it does not remove content prior to delivery. This places the responsibility on the LEA to retain only the authorized information, which has been raised as a potential issue by the privacy groups. The JEM noted that under this method, only the packets for the user under surveillance are delivered, and not

those for other users on the system. Since the LEA has no access to the packets from other users on the system, this does represent an improvement from the current state of the art .[1]

6.2.2 Delivery of Header routing information

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

6.2.3 Extraction of Pen Register or Trap and Trace information

Relevant Pen Register or Trap and Trace information may be located in different layers of the protocol depending on the specific service used and the application of the packet (e.g., a POP e-mail packet vs. a connection setup packet for H.323 or SIP service). The variability of applications therefore makes it difficult for a service provider to extract such information. New services (and therefore application layer protocols) are developed on a continual basis within the IP environment making isolation of Pen Register or Trap and Trace information within an IP data field even more complicated. If a separation capability were to be developed, maintaining accurate and up-to-date separation capabilities (i.e., filtering capabilities) will require rapid, continuous development which will be highly resource intensive. This process does not lend itself to the current standards development process due to the process' sometimes lengthy, consensus driven nature. It is also expected that the industry resources for this work would be significantly greater than the resources that are currently committed for surveillance standards development.

The JEM did not have sufficient information to determine whether or not an extraction solution would be scalable in the quantity deployments anticipated under CALEA, especially as the filtering becomes more complex and the network speeds increase. Additionally, there may be significant administrative and operational challenges to keeping the extraction function useful and accurate once all of the complications outlined in the IP Appendix (e.g. encapsulation, fragmentation, independent packet routing, and encryption) are taken into consideration. Further, because implementation issues were beyond the scope of the JEM, technical issues with respect to functional implementation such as capacity needs and impact on other Network elements (i.e., whether the extraction function is located within the service provider network) were not identified.

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.

[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.

Delivery of the FCC mandated timing requirement of eight seconds needs to be reviewed and may need to be specified for each technology and each solution discussed above.

Appendix A: Technology Specific Information

This section contains technology-specific information for each packet-mode technology discussed in the JEM. The JEM did not receive contributions for all possible packet technologies; therefore, not all packet technologies are represented in this section. The section is broken into two parts:

- Access Networks: this section and its subsections contain descriptions of information that can be delivered for various types of networks used to access packet-mode networks. This includes the following technologies:

  - cdma2000
  - GPRS
  - CDPD
  - Packet Cable

It was recognized that dial-up access to the Internet was the main method for accessing the Internet for most users, but there were no contributions for this method.

- Network Protocols: this section contains descriptions of information that can be delivered for various packet-mode protocols. The following protocols were covered:

  - X.25
  - IP
  - ATM
  - Frame Relay

A.1 Access networks

A.1.1 Call Associated Signaling Reporting

A.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

With this method, call associated signaling such as SIP/H.323 would be mapped to the J-STD-025 call events.[2] 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.[3]

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 following information could be reported:

- Call Session ID (e.g., Call ID);
- Call Session Information Type (e.g., H.323 family signaling, SIP signaling); and
- Call Session Information.

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

[3] 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).

A.1.2 cdma2000

A.1.2.1 Overview

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

Network elements that are specific to the cdma2000 Wireless IP Network are the Packet Data Serving Node (PDSN), the RADIUS servers [RFC2138], and the Home Agent (HA). The PDSN and local RADIUS server are part of the serving wireless network, while the home and broker RADIUS servers and HA may be part of another IP network (e.g., another wireless network, or private network). The RADIUS servers provide the authentication, authorization and accounting functions and use a Network Access Identifier (NAI) of the form user@realm to identify subscribers. Separate authentication, authorization and accounting are provided via the Radio Network using standard wireless Visitor Location Register (VLR) and Home Location Register (HLR). This information, however, is not communicated with the Wireless IP network elements.

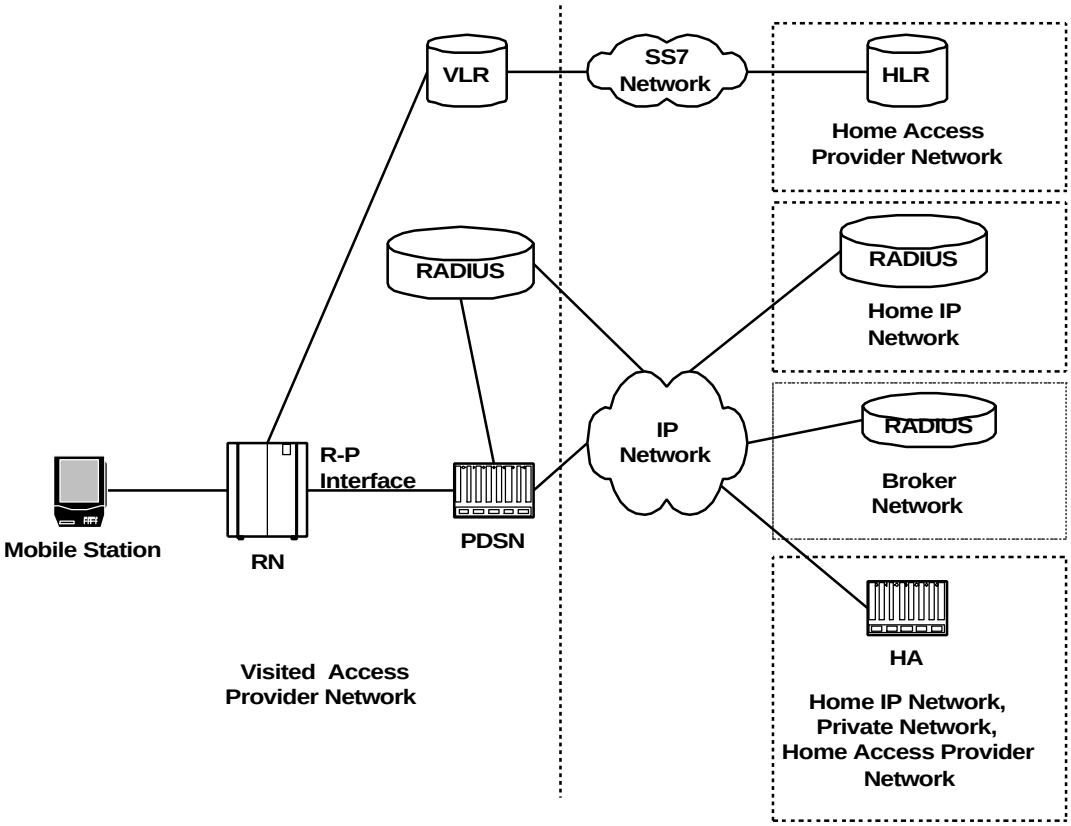


Figure 1: Reference Model (HA only for with Mobile IP service)

A.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 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.

A.1.2.3 Reporting of Call Information

The cdma2000 packet data architecture as described in IS-835 “Wireless Packet Data Standard” provides informational services and as such may act as a bearer service for communication services. The standard does not describe the applications that are supported in the network, nor does it describe how to interpret the packet data information based on the application since this varies widely between different applications. This information is unnecessary and beyond the scope of the standards since the intent is to provide packet data "access." It is not technically feasible to determine, either on a packet

by packet basis or on a stream basis, the application or communication service being used. Furthermore, the possibility of encapsulation or encryption of packets outside of the network makes identifying the application or service even more unlikely. Therefore, the level of complexity required of the network to attempt to extract Pen Register or Trap and Trace information from information services is not feasible.

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

A.1.2.4 Reporting of Access Control Information

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

The following events could be reported:

- packet data service establishment;
- packet data service termination;
- start of interception with packet data service active ; and
- PCF handoff.

A.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 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 whom 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 assigned address, and the true associates may only be identified by additional information in the payload of the packet and not the corresponding IP address.

A.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 a 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 section. Note however, that the home AAA server may reside in a network other than one belonging to a telecommunications service provider.

A.1.2.7 Serving System Message

In the LAES for CALEA 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 roaming 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.

A.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 tunnel.

A.1.3 General Packet Radio Service

A.1.3.1 Overview

General Packet Radio Service (GPRS) is a packet-mode access technique for mobile subscribers providing the transfer of high and low speed data and signaling. Interworking is defined with IP and X.25 networks. Point-to-Point (PTP) and Point-to-Multi-point (MTP) applications are supported along with multiple quality of service profiles for the subscriber. The GPRS allows the service subscriber to send and receive data in an end-to-end packet transfer mode, without utilizing network resources in circuit switched mode.

The following are a number of possible PTP interactive teleservices:

- retrieval services, which provide the capability of accessing information stored in data, base centers. The information is sent to the user on demand only. An example of one such service in the Internet's World Wide Web (WWW);

- messaging services, which offer user-to-user communication between individual users via storage units with store-and-forward mailbox, and/or message handling (e.g., information editing, processing and conversion) functions;

- conversational services which provide bi-directional communication by means of real-time (no store-and-forward) end-to-end information transfer from user to user. An example of such a service is the Internet's Telnet application;

- tele-action services which are characterized by low data-volume (short) transactions, for example credit card validations, lottery transactions, utility meter readings and electronic monitoring and surveillance systems.

Some examples of teleservices that may be supported by a PTM bearer service include:

- distribution services, which are characterized by the unidirectional, flow of information from a given point in the network to other (multiple) locations. Examples may include news, weather and traffic reports, as well as product or service advertisements;

- dispatching services which are characterized by the bi-directional flow of information from a given point in the network (dispatcher) and other (multiple) users. Examples include taxi and public utility fleet services;

- conferencing services which provide multi-directional communication by means of real-time (no store-and-forward) information transfer between multiple users.

Capabilities that may be offered together with the PTM bearer services include:

- geographical routing capability, which provides the ability to restrict message distribution to a specified geographical area;

- scheduled delivery capability, allowing store-and-forward type services to specify a future delivery time and a repetition rate.

It is possible to include these capabilities as part of the service request (i.e., as part of the packet). Some operators may offer PTM services only together with these capabilities.

GPRS defines two new interconnected network nodes:

a) A Serving GPRS Support Node (SGSN) which keeps track of the individual Mobile Station's (MS's) location and performs security functions and access control. The SGSN performs authentication and cipher setting procedures.

b) A Gateway GPRS Support Node (GGSN) which provides interworking with external packet-switched networks.

The GSM Home Location Register (HLR) is enhanced with GPRS subscriber information and the Short Message Service (SMS) Gateway MSC (GMSC) and SMS Interworking MSC (SMS-IWMSC) are upgraded to support SMS transmission via the SGSN. GPRS security functionality is equivalent to the existing GSM security.

The MS informs the network when it re-selects another cell or group of cells known as a routing area.

In order to access the GPRS services, an MS must first make its presence known to the network by performing a GPRS attach. This operation establishes a logical link between the MS and the SGSN and makes the MS available for SMS over GPRS, paging via SGSN, and notification of incoming GPRS data.

In order to send and receive GPRS data, the MS must activate the packet data address that it wants to use. This operation makes the MS known in the corresponding GGSN and interworking with external data networks can commence.

User data is transferred transparently between the MS and the external data via encapsulation and tunneling techniques. This transparent transfer method lessens the requirement to interpret external data protocols and enables easy introduction of additional interworking protocols in the future.

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

- an activation reference identity;
- the target identity which has been intercepted (e.g., MSISDN, IMSI, IMEI if applicable);

- type of protocol activated (e.g., Internet Protocol or X.25);
- PDP address used by the target (e.g., IP Address);
- location information of the target (Cell Global Identity);
- time of event;
- Access Point Name (APN).

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

- GPRS attach;
- GPRS detach;
- PDP context activation;
- start of interception with PDP context active;
- PDP context deactivation;
- Call and/or Routing Area update;
- SMS

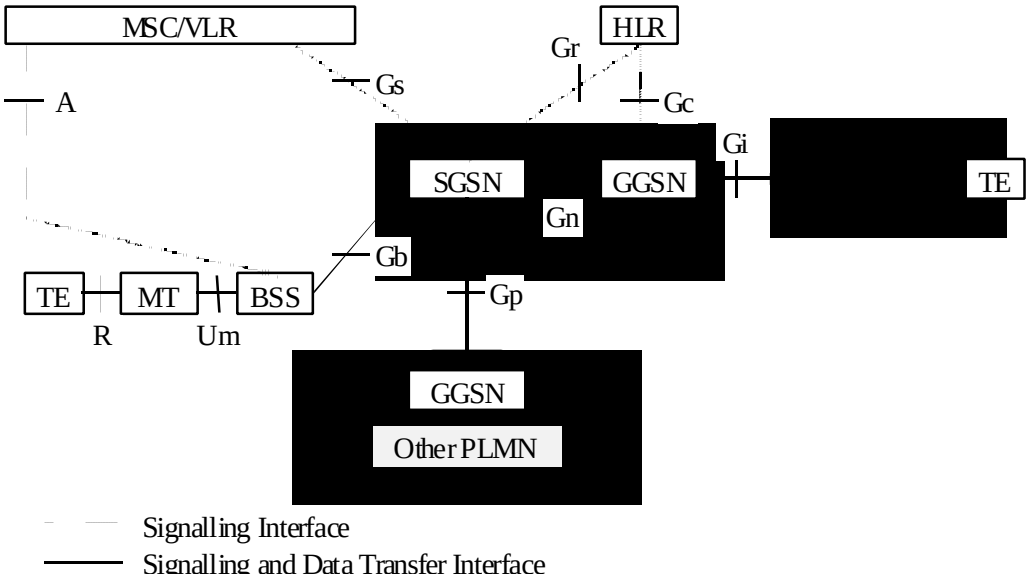


Figure 1. GPRS Simplified GPRS Architecture

The following areas where Call Identifying Information for Packet-mode Communication could be reported to assist Law Enforcement Agencies (LEAs) have been identified.

A.1.3.2 Reporting of Access Control Information

Similar to wireline, wireless systems establish a communication path across the accessing system from the subject's device to a network before communication between subject and associate can begin. The establishment and release of this path could be reported to identify when an intercept subject has established communication ability.

Specific to the issue of reporting information for Access Control as discussed above, the following specific information from the entire list of information available could be reported to law enforcement separately from the content to report the access event:

- access path ID (e.g., a PDP Context path);
- network access address (e.g., Access point Name);
- intercept subject address (e.g., IP address);
- either path establishment or path release (e.g., PDP Context Activation/Deactivation).

A.1.3.3 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[4]. 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.

Specific to the issue of reporting information for identifying the parties to the communication as discussed above, the following specific information from the entire list of information available could be reported to law enforcement separately from the content to identify the addresses of the parties to the communication:

- access path ID (e.g., PDP Context path[5]);
- source address (e.g., IP Source Address[6]);
- destination address (e.g., OP Destination Address).

Access path ID is used to correlate path, source, and destination addresses.

[4] 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.

[5] Correlates Network Address Information to Access Path Events (e.g., PDP Context Activation/Deactivation).

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

A.1.4 Cellular Digital Packet Data

A.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.

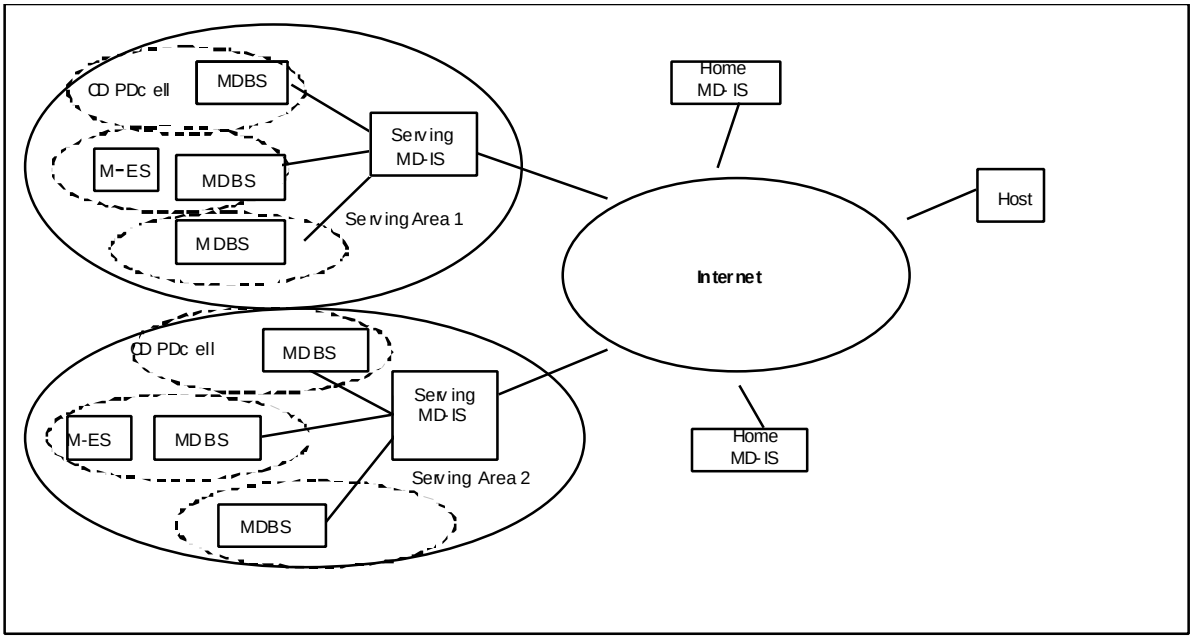


Figure 2. CDPD Network Architecture Model - functional elements

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

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

- Mobile End System
  The Mobile End System (M-ES) is the means by which CDPD Network subscribers gain access to wireless communications. Each M-ES is aware of its location based on

broadcast information. When an M-ES powers up in a CDPD cell, it informs the network of its location using the registration process. When the M-ES moves to another cell, it notifies the network by indicating a change to new cell. When the M-ES moves to another cell in a new serving area, it performs a new registration.

- Mobile Data Base Station
  The MDBS provides Layer 2 data link or media access relay functions for a set of radio channels serving a cell. The MDBS does not participate in the wide area mobility management task.

- Home MD-IS
  Every M-ES address is logically a member of a fixed home area. The home area provides the anchor or mobility-independent routing destination area for routers and hosts that are not mobile aware (*i.e.*, routers and hosts on the general internet). The home MD-IS is responsible for transparently redirecting and forwarding data packets. The redirection and forwarding function is based on the principle of encapsulating M-ES addressed packets and forwarding them to the Serving MD-IS in each serving area the M-ES visits. In other words, data packets destined for the M-ES are routed through the general internet to the Home MD-IS. The Home MD-IS then encapsulates the packet and forwards the encapsulated packet to the appropriate Serving MD-IS. The Home MD-IS does not need to be involved in the routing of packets originated at the M-ES.

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

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

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

A.1.4.2 Network Service

The CDPD network provides wireless mobile routing of network layer data packets. The CDPD System Specifications specifies support for two connectionless network layer

protocols – Internet Protocol (IP) and Connectionless Network Protocol (CLNP). However, the currently deployed systems all support only IPv4.

The CDPD network has been defined to support the network protocol without any modification, as such the identity managed by mobility management is the IPv4 address. In other words, the subscriber identity is the IPv4 address, and is used for all routing purposes. There is no mapping of the target identity to the CDPD technology address.

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

A.1.4.3 Information Provided

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

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

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

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

- Case identity
- Service provider identifier of the serving system.
- Date and time of deregistration of the intercept subject.
- IP address of the intercept subject.

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

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

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

- 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.

A.1.4.4 Feasibility and Performance

The TIA Interim Standard 732 (IS-732) has no provisions for the capabilities described in this report. Implementation feasibility of these capabilities will depend on each product's design. However, the industry believes that current CDPD products can be modified to supply the information described in this Appendix. These modifications would have limited impact on performance when the percentage of packets being intercepted is low.

A.1.5 Packet Cable

A.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. This section is derived from Packet Cable Labs published standard for implementation of CALEA [PKT-PCES]. The JEM takes no position on any legal conclusions in this standard.. 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 costs, 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.

Note that from time to time this section refers to the voice communications capabilities of a PacketCable network in terms of “telephony” or “IP Telephony.” The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined. Nothing in this section is addressed to, or intended to affect, those legal/regulatory issues. In particular, while this section uses standard terms such as “call,” “call signaling,” “telephony,” “telephone number,” etc., it should be recalled that while a PacketCable network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, and that these differences may be significant for legal/regulatory purposes. Moreover, while reference is made here to “IP Telephony,” it should be recognized that this term embraces

a number of different technologies and network architecture, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this or any other term derived from usage within the traditional circuit-switched telephone industry.

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

A.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.

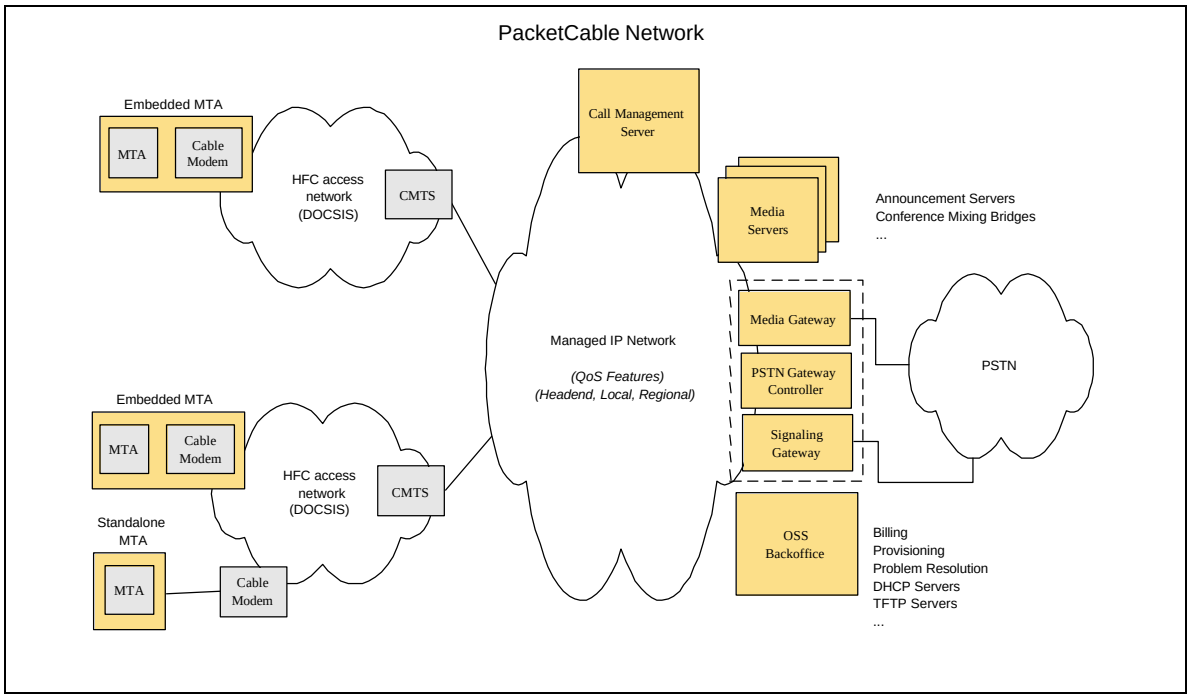


Figure 1. PacketCable™ Reference Architecture

The HFC DOCSIS access network as shown in Figure 2, provides the access to the managed IP 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.

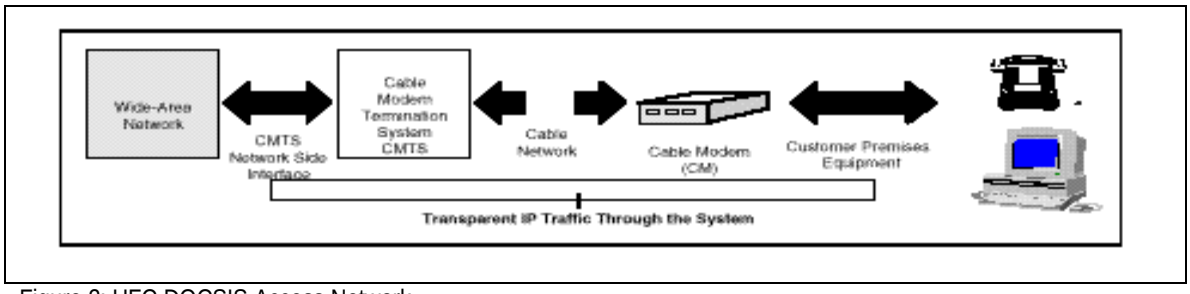


Figure 2: HFC DOCSIS Access Network

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 a 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.

A.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
- Provides multiple audio indicators to phones, such as ringing tones, call waiting tones, stutter dial tone, dial tone, etc.
- Provides standard PSTN analog line signaling for audio tones, voice transport, caller-id signaling, and message waiting indicators.

The PacketCable system design places much of the session control intelligence at the endpoints, where it can easily scale with technology and provides new and innovative services. While this "future-proofing" is a goal of the design, we recognize that it leaves open a wide range of security threats. The basic assumption is that the MTA is not immune to customer tampering, and that the significant incentive for free service will lead to some very sophisticated attempts to thwart any network controls placed on the MTA.
Under these circumstances, it is important to realize that an MTA under customer control will likely not cooperate with electronic surveillance, and methods are therefore described here that do not depend in any way on cooperation with the MTA.

A.1.5.4 Subscriber Identification

A subscriber for electronic surveillance purposes is identified by a telephone number, and the telephone number is reported to Law Enforcement Agency (LEA) in the Pen Register and Trap and Trace information. Other identity information of the subscriber equipment, e.g. a provisioned security certificate, is used by the CMS to dynamically determine the identity of the subscriber and the telephone number for a particular call. The CMS includes, as part of the authorization of network resources, the packet stream identification (source and destination IP addresses, destination port number) and an indication that the packet stream is subject to surveillance.
Other mechanisms of subscriber identification are too dynamic and transient to be used as subscriber identification for surveillance.

Cable Modems (CMs) are manufactured with a unique MAC address (48-bits). This MAC address is used by DOCSIS to identify the CM during the registration process, and identifies a particular configuration file containing further provisioning information for the subscriber. The MAC address only appears on the HFC network, and is often suppressed by the Payload Header Suppression feature of DOCSIS. It is therefore not usable as a subscriber identifier for a 'snooping' function attached to the HFC network. Packet streams generated by the CM are identified by DOCSIS Service Flows. Each Service Flow has a dynamic identifier assigned, the Service-Flow-ID (SFID); while active it also has a Service-ID assigned (SID). The SID is used in the DOCSIS media access layer to control access to the shared upstream resources. The dynamic and transient nature of SIDs makes them unusable as subscriber identifiers for surveillance.

The CM uses DHCP to obtain an IP address. This resulting address is likely to change every time the CM is initialized. Use of a 'snooping' function on the IP links of the network would require dynamic configuration based on DHCP requests. This may be technically feasible, but has not been attempted in the PacketCable environment.

A.1.5.5 Intercept Access Points

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

In a PacketCable network, the following elements are possible Intercept Access Points:

- The Cable Modem Termination System (CMTS) which controls the set of cable modems attached to the shared medium of the DOCSIS network. The CMTS is responsible for intercepting the Call Content, and certain Pen Register and Trap and Trace information.
- The Call Management Server (CMS) which provides service to the subscriber. The CMS is responsible for intercepting the Pen Register and Trap and Trace information.

- The Media Gateway (MG) is designated as an Intercept Access Point for purposes of intercepting Call Content for redirected calls to the PSTN.
- The Media Gateway Controller (MGC) is designated as an Intercept Access Point for purposes of intercepting the Pen Register and Trap and Trace information for redirected calls to the PSTN.

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

A.1.5.6 Information Available to Law Enforcement

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

The following call events are defined, and convey information to an LEA for Pen Register and Trap and Trace events: Answer (a two-way connection has been established for a call under surveillance), Change (a change in the description of call content delivery for a call under interception), Close (end of call content delivery for a call under interception), Open (beginning of call content delivery for a call under interception), Origination (IAP detects that the surveillance subject is attempting to originate a call), Redirection (call under surveillance is redirected, e.g. via termination special service processing, or via a call transfer), and Termination Attempt (IAP detects a call attempt to a surveillance subject).
In most cases, a PC/TSP should be able to intercept calls redirected by a surveillance subject to other locations either in its own network or in the networks of other telecommunications carriers. However, where a subject has redirected incoming calls to a location served by another PC/TSP, the resulting connection may be established without touching the equipment or facilities of the subject's PC/TSP. Instead, the connections will be made directly from the PC/TSP originating the incoming call to the PC/TSP serving the location to which the subject redirected incoming calls. Because the subject's original PC/TSP will not be aware of these resulting connections, access to these connections will have to be obtained from the PC/TSP serving the location to which calls have been redirected.

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

A.1.5.6.1. Reporting Access Control Information

For Packet Cable managed IP network the following information could be reported:

- subject identity;
- target identity;
- access element identity;
- time of event;
- call identity unique to this call;
    - originating Session Descriptor Protocol information;
    - terminating Session Descriptor Protocol information;
    - call content connection identifier for Title lll warrants;
    - redirected information;
    - origination digits
    - termination digits and
    - the transit carrier used to transport the session;

A.1.5.7 Preferred Delivery Format

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

Call Content is delivered as a stream of UDP/IP datagrams, as defined in [RFC0768, RFC0791], sent to the port number at the Collection Function (CF) as provided during provisioning of the interception. The format of the UDP/IP payload is given in the PacketCable Electronic Surveillance Specification.

The Call Data Connections in PacketCable are implemented as TCP/IP connections, established by the Delivery Function (DF), to the Collection Function designated by the LEA in the surveillance provisioning.

Contained in the IP header is the source IP address, which is the address of the DF, and the destination IP address, which is the address of the CF provided during interception provisioning.

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

The default link-layer protocol between the DF and CF is as defined by the Ethernet protocol [RFC0894, RFC0826]. However, alternate link-layer protocols may be used at the discretion of the PC/TSP based on negotiated agreements with the LEA.
The default type of physical interconnect provided by the PC/TSP at the demarcation point is an RJ45 10/100BaseT [ISO8802-3] connection. However, alternate physical interconnects may be provided at the discretion of the PC/TSP.

A.1.5.8 Capacity Limitations

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

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

A.2 Network Layer protocols:

A.2.1 X.25 over ISDN Basic Rate Interfaces (BRI) technology

ATIS committee T1S1 has completed its investigation into the Packet-Mode Communications issues identified by the FCC Report and Order 99-230[i]. The activity was addressed under T1S1's scope and charter to participate in the development of a joint T1-TIA standard on surveillance.

The T1S1 investigation specifically addresses the issues in FCC 99-230 and the request to identify capabilities which can be used to report Pen Register and Trap and Trace information for Packet-Mode Data Communications separately and distinctly from call or communication content. The focus of the investigation was on the X.25 over ISDN Basic Rate Interfaces (BRI) technology. The investigation was conducted on a technical merit basis and made no judgment with respect to legal issues regarding the applicability of the Communications Assistance for Law enforcement Act (CALEA).

A.2.1.1 Information that could be reported

A.2.1.1.1. Pen Register and Trap and Trace Information

For the X.25 Switched Virtual Circuits (SVCs) over ISDN Basic Rate Interfaces (BRI) technology, the packet handler will receive connection setup messaging from the subject. In these cases, the setup messaging exchanged between the subject and packet handler can be used as triggers for monitoring and reporting surveillance events. The following Pen Register and Trap and Trace information is available for X.25 SVC calls and could be provided to the Law Enforcement Agencies (LEAs) separately from the call content:

- Calling Party Number
- Called Party Number
- Answering Party Number
- Call Redirection/Call Deflection information
- Network User Identification (NUI)
- Recognized Private Operating Agency (RPOA)
- Called Line Address Modification Notification (CLAMN)

For the X.25 SVCs over ISDN Basic Rate Interfaces (BRI) technology, the existing J-STD-025 set of Call Data Channel (CDC) messages can be used to report surveillance events of packet-mode data communications during call setup, call progress, and call clearing (i.e., Origination, Termination Attempt, Redirection, Answer, Release). The J-STD-025 parameter set does not support the reporting of the Reverse Charging and Reason for Redirection information.

For X.25 PVC service, the ISDN packet handler uses a pre-provisioned connection across the packet network to deliver all transmitted packets between the subject and associate. In these cases, no connection establishment signaling is involved and, therefore, no end-

to-end routing information is available to the X.25 layer at the packet handler. The packet handler only maps the incoming ISDN connection from the subject to an X.25 PVC across the packet network. Therefore, Pen Register and Trap and Trace information for a PVC is not available at the X.25 layer.

For X.25 PVC service, only administrative records and operations personnel have knowledge of the end-to-end connection. This is because the operations personnel used the end-to-end information to provision the connection from the user to the packet handler (via an ISDN Permanent B-Channel Connection or D-Channel Connection) and then from the packet handler to an interoffice facility. At each switch in the PVC's path (which may cross network boundaries), the connection is mapped from one facility to another, until it is connected to the associate. Since the Pen Register and Trap and Trace information for X.25 PVCs cannot be derived by information at a given switch, the delivery of such information to LE over the J-STD-025 delivery interfaces cannot be automated.

A.2.1.1.2. Call Content

While only CDC messages should be sent for Pen Register type surveillances, Title III surveillances will require that call content be delivered over the packet Call Content Channel (CCC).

The call content information is available at the X.25 level. All X.25 packets should be intercepted and Pen Register and Trap and Trace information is not separated from call content before being replicated and transported over the packet CCC to LE.

The existing J-STD-025 set of messages to report the assignment and release of packet CCCs for the delivery of intercepted call content from packet-mode data communications can also be utilized (i.e., CCOpen, CCClose). The existing procedure in the J-STD-025 for reporting call content (Fast Select data) over the CDC can be used to report the transport of call content in X.25 SVC call setup, call progress, and call clearing packets.

The call content monitoring impacts for X.25 PVCs are similar to those described for X.25 SVCs. When monitoring call content for X.25 SVCs, the LEAs receive the necessary call parameters within the signaling packets that are also delivered over the packet CCC. However, for X.25 PVCs there are no signaling packets, and the call parameters are pre-provisioned for the connection. Consequently, when a court order requires call content monitoring for X.25 PVCs, the call parameters will need to be reported separately via a manual process, similar to the process for ascertaining the Pen Register and Trap and Trace information for X.25 PVCs. When call content is to be monitored on a X.25 PVC, certain call parameters may be needed to facilitate the LEAs processing of the call content data packets delivered over the packet CCC delivery interface. These call parameters include the packet modulo sequencing, the packet size, and the window size for the packet call. Without these parameters, it will be difficult or impossible for LEAs to properly extract the call content from the monitored packet-data communication.

A.2.1.2 Technical Impacts

The following Pen Register and Trap and Trace information is available for X.25 SVC calls but can not be reported to the LEAs because the existing J-STD-025 set of Call Data Channel (CDC) messages and parameters do not support the reporting of the information:

- Reverse Charging facility
- Reason for Redirection (as reported in the CLAMN facility)

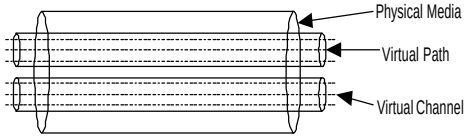
When an X.25 PVC is re-provisioned to a different remote party (where the intercept subject is the local party), it may be problematic to ensure that LEAs receive timely notification. For X.25 PVCs that cross LATA (and usually state) boundaries, the ISDN service provider is not able to provide the identity of the remote party. Although the service provider may have noted the network address of the remote party in their records, this information has only nominal significance. Since the terminating party is in a different network, the local service provider cannot ensure that the X.25 PVC is actually connected to the network address listed in their records because network addresses do not have any real significance for X.25 PVC. The service provider can only confidently report the identification of the interoffice connection that is used to hand-off the X.25 PVC to the interLATA carrier. The LEAs would need to request that the interLATA carrier provide information about the connection; finally, the LEAs could then request that the remote ISDN service provider confirm the identity of the remote party.

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

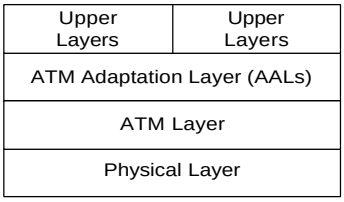
A.2.2 Asynchronous Transfer Mode

This section describes Asynchronous Transfer Mode (ATM) and its use in transporting voice telephony. It concentrates on the public network where ATM is predominately used as the bearer service for other, upper layer protocols that are concerned with the origination and routing of voice telephony calls. Therefore, the use of Switched Virtual ATM Connections is not described in this Appendix.

ATM is a switching method that uses fixed size units, called "cells," to transport information from the source to the destination. It is designed to be a general-purpose transfer mode for a wide range of services including, but not limited to, the transport of voice and data. ATM provides Layer 2 functionality in the Open System Interconnection (OSI) protocol layer model. Each ATM cell consists of a 5-octet header that defines the virtual circuit associated with the cell. Virtual circuits are defined by a combination of a Virtual Path Indicator (VPI) and a Virtual Channel Indicator (VCI). The remainder of the ATM cell consists of a 48-octet payload. In a typical public network, large numbers of virtual circuits are carried on the physical media.



Included in the ATM header is a payload-type indicator that describes the cell as containing either user information or network management data. No information is included in the 5-octet header that defines the type of user data that is being transported.



Separating the ATM layer from the user data is an adaptation layer that adapts the services provided by the ATM layer to those required by the higher layers. There are currently only three ATM Adaptation Layers (AALs) in common use and are described in this Appendix. Each different adaptation layer defines specific services to the upper layer applications that they are designed to transport.

Providing voice telephony over any bearer service requires the use of an Interworking Function to map the user's voice signals into whatever protocol the bearer requires.

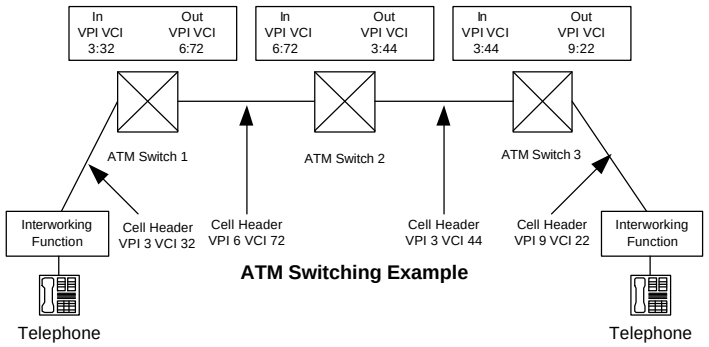
Voice telephony in an ATM network can be provided by AAL1 (Circuit Emulation Service), AAL2 (Voice Over ATM) and AAL5 (Variable Bit Rate).

ATM adaptation Layer AAL1 defines how Time Division Multiplexing (TDM) type circuits can be emulated over an ATM network. AAL1 supports emulation of DS1, DS3, and nxDS0 circuits and is used primarily to provide transport of PBX trunks.

ATM adaptation Layer AAL2 defines a method to provide variable length packet payload multiplexing within a single virtual circuit. One of the major advantages to using AAL2 is that it provides for multiplexing of voice packets into a single ATM cell. Either AAL2

or ATM adaptation Layer AAL5 is used to transport signaling data (DTMF, Common Channel Signaling, etc.) to the Voice Gateway.

ATM adaptation layer AAL5 defines a method to provide variable bit rate services primarily for data applications where the bursty nature of the applications can tolerate variations in delay. Voice over Packet (VoP) may be carried over AAL5, but the information above the ATM Layer appears as data to the ATM Layer.



As ATM cells arrive at the ingress to the network, each cell header is examined to determine if the cell contains network management or user information. If the cell contains user information, the VPI and VCI are looked up in a routing table to determine the outgoing facility to use in transporting the cell. Because the outgoing facility may use a different VPI/VCI combination, the node must replace the VPI/VCI with the new values. Cells continue in this way, moving from node to node until they reach their final destination. At no time during this process of *relaying* cells does the network know anything about the upper layer protocols that are being transported. Note that the VPI/VCI only indicates the association between the adjacent nodes and not the end-to-end connection. Nothing about the VPI/VCI defines the final destination of the cell or the user data that is being transported. Thus, Pen Register and Trap and Trace information is not available. ATM switching nodes are designed to relay the ATM cells as quickly as possible. This design effectively prohibits the ATM switch from reassembling and examining the user information encapsulated in each cell due to the processing demand and implementation that would be required. Within an ATM network, it is not technically feasible to extract the upper layer protocol, which contains the information of interest to the LEA from the ATM cell stream. It may be technically feasible, however, to extract call content information at the ingress and egress service interfaces.

A.2.3 Internet Protocol

The IPv6 RFC 2460 is available and may become widely deployed in the future. However, as its deployment is limited at this time the JEM considered only IPv4 impact on CALEA and did not consider the impact of IPv6.

A.2.3.1 Introduction

This section analyzes the areas identified in the main text of the section as they apply to networks using the Internet Protocol.

This section first discusses architectural principles of the Internet and the Internet Protocol that apply to the analysis of CALEA. It then follows the basic organization of the main text in that it investigates what information can be delivered and the technical issues of delivering that information both for a provider that supports a Call Management System and a provider that only supports IP transport.

Although the Internet (and IP) supports many applications other than Call Management Systems, due to the special consideration given to voice applications in the JEM this section only deals with Call Management Systems.

A.2.3.2 Scope

This section concentrates on the Internet Protocol and related protocols.

While the Internet Protocol can be carried by a multitude of underlying protocol technologies (e.g., leased line, dial-up modem, ATM, Frame Relay, X.25, etc.), this section does not consider the implications of CALEA on the underlying protocols. This is left to the appendix for the specific technology.

In addition, this section does not provide special considerations to any applications other than Call Management Systems that run over IP.

A.2.3.3 Architectural principles related to CALEA

This section briefly describes architectural principles of the Internet that apply to the CALEA analysis.

There are plenty of tutorials and books on IP and routing available. It is assumed the reader is familiar with the operation of the Internet and the suite of Internet protocols. However, discussions of general principles that affect the issue at hand are included.

A.2.3.3.1. End-to-end principle

"The network's job is to transmit datagrams as efficiently and flexibly as possible. Everything else should be done at the fringes." [RFC1958]

The end-to-end principle is simple, but powerful. It recognizes that there are many functions that only make sense to implement in hosts at the edge of the network. Examples are reliability, security (encryption), etc. This is in marked contrast to other protocols and networks that have been developed over the last 100 years which attempt to subsume these functions into the network.

As an example, the Internet assumes that, in general, reliable data transfer is assured by the end systems instead of the network. What this means is that any retransmission due to packet loss is done end-to-end instead of inside the network. As a counterexample, X.25 and similar protocols provide retransmission on a hop-by-hop basis.

Quoting from [Saltzer], "The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete

version of the function provided by the communication system may be useful as a performance enhancement.)"

This does not mean that a service provider cannot offer enhanced services over such a network. What it means is that the enhanced services are either provided as part of the transport mechanism (e.g., Quality of Service) or are enabled on hosts reachable via the Internet. Examples of such systems are DNS, email servers, Web servers, etc. The customer reaches these services just like it would any other service not offered by the service provider (i.e., via IP).

A by-product of this principle is that the IP transport network will not necessarily know what applications are being run over the network since there is no "setup" in which the network participates. In fact, the network is designed not to know what application is being carried. The applications run end-to-end and the network just routes packets. Where the network does provide an application-level service, it is through a host that it manages that communicates end-to-end with the customer's host over the provider's network.

The end result of this is an explosion of innovation in applications. Anyone with a link to the Internet can develop and offer new and innovative services to anyone else on the Internet (e.g., Napster). This applies to voice applications just as much as any other applications.

A.2.3.4 Security

Security encompasses many areas including, but not limited to, encryption. In general, the end-to-end principle applies to security (i.e., end-systems are responsible for their own security). However, service providers can provide assistance in some areas of security. For example, even though two end-systems may have adequate security in their locations and use strong cryptography between them, unless they have the cooperation of their service provider they are susceptible to denial of service attacks from third parties that flood their link to the Internet such that communications is degraded.

As discussed in Section 6 of [RFC2804], the introduction of capabilities for electronic surveillance tends toward making the network itself less secure, even when the capability is not being exercised. Much effort is underway in the industry to make the Internet more secure, not less. Development of specific protocols and methods for delivering an end-user's information to a third party without the knowledge of the end-user does not contribute to making the Internet more secure.

Encryption has been a controversial topic for a long time. However, with the advent of more powerful computing devices and more powerful and available encryption algorithms, strong encryption is now technically available (but possibly not legally or politically available) to most people on the Internet. Following the end-to-end principle, encryption should take place between two hosts, not in the network itself. The network may use encryption for its own purposes, but the hosts using the network ultimately must take care of themselves. The end systems may have a trust relationship with the service provider that enables the service provider to share in the security mechanism and encryption of data; however, the fact that CALEA may require the service provider to provide decrypted information (or keys) to an outside body (i.e., LEA) without the user's

knowledge will force the service provider to implement mechanism that could make the system less secure than it might otherwise be, even if the subject is not under surveillance.

A.2.3.5 Encapsulation

"IP on everything" - Source Unknown

The Internet Protocol is designed to operate over a wide variety of network technologies and protocols. In fact, the term internetwork (thus internet) derives from the fact that it was designed to interwork over multiple networking. Normally, an encapsulation method is defined for how to run IP over a particular networking technology. Encapsulation methods have been defined by the IETF for a wide variety of networking technologies (e.g., HIPPI, X.25, Frame Relay, ATM, FDDI, Ethernet, Token Ring, Arcnet, leased line, dialup, etc.). As IP is routed from one network type (e.g., SONET) to another (e.g., Ethernet) it is encapsulated into a different mechanism that is usually specific to a particular network type.

IP also encapsulates upper layer protocols inside its data field. These upper layer protocols are usually transparent to the IP layer and to the Internet between two hosts. IP provides a Protocol ID that identifies the protocol contained in its data field. TCP and UDP are two predominant protocols that run over IP; however, other protocols can be run directly over IP (e.g., IPSEC, IP, RSVP, SCTP, etc.). Over 100 Protocol numbers have been assigned by IANA for use in the IP Protocol ID field. Normally for user data transfer, the Protocol ID does not identify the application the hosts are running. The applications normally run over a transport protocol (e.g., UDP or TCP) that runs on IP. The end systems can identify which application a particular packet is destined for by the TCP (or UDP) port number. There are several thousand port numbers currently registered with IANA for use with TCP or UDP.

Thus the application data is usually encapsulated in UDP or TCP, which is encapsulated in IP, which is encapsulated in a link or network specific mechanism.

A.2.3.6 Connectionless Orientation

The Internet Protocol is a connectionless protocol. In general, each packet contains all the information needed to route the packet from one host on a network to another host on the same or different network. Each packet is routed through the network(s) independent of the previous packet and may take a different path through network(s) than a previous or subsequent packet. There is no explicit setup mechanism between a host and the network to provide communication between two hosts. There is no "call" in IP. Loop Start in the analog telephony world and Q.931 in the ISDN world are examples of signaling protocols between a host (e.g., telephone) and network that set up connections (i.e., calls) between two hosts (e.g., two telephones).

As mentioned earlier, a service provider can provide services by deploying hosts in the network to which customers' hosts can communicate. A customer's host can request service from the provider's host; however, the network provides the connectivity for the

packets. An example of this is DNS. A host wants to communicate with another host, but only knows the host name and not the IP address. The host sends a query to the DNS server via IP and the DNS server responds with the destination host's IP address. This is still a connectionless service.

A.2.3.7 Boundaryless

"There's a freedom about the Internet: As long as we accept the rules of sending packets around, we can send packets containing anything to anywhere." [Berners-Lee]

One by-product of the above principles is that IP inherently has no concept of geopolitical boundaries. While a network's design may provide some loose constraints as to what path a packet may take, there is usually no guarantee a packet will take a particular path at any particular time.

For example, a host in Tuscaloosa, Alabama may download a file from another host in Mobile, Alabama. There is no guarantee that the packets in this download will stay in the state of Alabama. They may transit part of the network in Mississippi, Florida or any nearby state. This is considered part of normal operation of the Internet. Therefore, information that may be reasonably available in a connection-oriented network may not be available in an IP network.

A.2.3.8 Call Management System

The main text contains general information for packet-mode technologies concerning information derived from a call management system. This section contains information specific to the Internet Protocol.

Call Management Systems don't exist for the Internet Protocol. However, call management systems exist for applications that run, end-to-end, over IP. In general on an IP network, a call management system is a host attached to the IP network running call management protocols end-to-end over IP to its clients. For VoIP applications, the encoded voice stream is also carried over UDP/IP. In VoIP, the IP packets carrying voice are usually carried directly between the two endpoints involved in the call. The Call Management System is not involved in transporting the voice packets.

A.2.3.8.1. Information that could be reported

The information discussed in the main text also applies to IP-based Call Management Services. Since the information available from Call Management Services tends to be specific to the application (i.e., Voice) as opposed to IP, the information itself is pretty much the same as the main text. The call events described in J-STD-025 are examples of information that can be reported.

In a network that provides a call management system, only call events that are triggered by messages between the target and CMS are available.

For IP, the call content flow within the immediate network can be characterized by the source and destination IP address and source and destination UDP port numbers negotiated between the CMS and target during call establishment. This only applies to

call control protocols that exchange IP address and port numbers with the CMS. This applies to most VoIP signaling protocols currently defined, but may not apply to future applications.

The following are IP-specific items:

IP information for call management protocol:

IP address used by target
TCP or UDP port number used by target
IP address used by Call Management System
TCP or UDP port number used by Call Management.

IP information for voice packet stream

IP address used by target for voice packet stream
TCP or UDP port number used by target for voice packet stream
IP address used by target's associate for voice packet stream
TCP or UDP port number used by target's associate for voice packet stream

Other call events similar to those defined in J-STD-025 may be available to the extent that the Call Management supports similar services (e.g., Call Forward).

A.2.3.8.2. Technical issues

The issues addressed in the main text also apply to IP. This section discusses issues specific to IP.

A.2.3.8.3. Location and Ownership of Call Management System

Since it runs over IP the Call Management System can be located anywhere on a global IP network. It can be provided by the Service Provider that also provides the Internet access service to a customer, by another Service Provider on the Internet or by a customer on another Internet Service Provider. The CMS may not be within the same jurisdictional boundaries as the client host to which it is providing service even if the two endpoints involved in a call are within the same jurisdictional boundaries. The only real requirement is that the users have reachability via IP to the CMS. In the extreme case, the CMS could be in a different country from the hosts to which it is providing service.

This follows the principle laid out in Section A.2.2.7

Given that Call Management protocols are end-to-end protocols over the Internet, a Service Provider will only have access to call events detected on its Call Management System. This section only discusses issues with what information can be gleaned from a Call Management System operated by the Service Provider.

The Call Management Server in an IP network can only report events based on packets that are terminated on or originated from the Call Management Server. If the target knows the destination address of the person it wants to call or if the target uses a Call Management System not under the control of the service provider, the target can establish a VoIP call without the knowledge of the service provider's Call Management System. Call Events for such calls will not be available to the service provider.

Even when the target uses the provider's Call Management Server, not all call events for call manipulation may go through the Call Management Server. For example in the middle of a call the endpoint under surveillance may exchange call control information with a Call Management Server not under the control of the service provider. These packets will not necessarily go through the Call Management Server, but will be routed normally as data packets.

A.2.3.8.4. Call Management Protocols

The Internet places no restriction on the protocols used between the CMS and client for managing calls. In today's PSTN, the base protocols used for call control are limited to a small number due to the technology and the small number of providers. Each country or network may define its own variant of the base PSTN protocol but they all have the base in common.

The following is a list of some of the protocols defined for call management over IP by various industry groups

- H.323,
- SIP,
- H.248/megaco,
- MGCP,
- PINT (based on SIP)

More protocols are being developed. Each of the above listed protocols is fairly flexible in allowing different services based on the core protocol. Therefore, nailing down a complete, fixed set of call events that are available via each protocol is close to impossible.

In addition, some of these protocols (e.g., SIP) can be used for provision of information services. In fact, the same CMS host could offer information services using the same protocol at the same time as offering VoIP service.

Since the CMS and the client usually run on open computing systems, new call control protocols are usually easily downloaded and installed. The CMS and client don't have to run standard protocols as long as they agree with each other what protocol to use.

The ubiquitous HTTP (i.e., protocol used to support the World Wide Web) is also being used by various entities to offer VoIP services such as "click-to-dial". In this case, there is not necessarily a specific call control protocol and the CMS is a web server.

In some protocols (e.g., SIP, H.323), the information exchanged between the client and the CMS may only be sufficient to resolve an identifier such as an email address to an IP address which the client uses to negotiate the call further. In this case, subsequent call events may not be available to the CMS.

Although the call control protocols have UDP/TCP port numbers assigned to them via IANA, there is no hard requirement in the Internet to use these port numbers. The port numbers used for call control is a bilateral agreement between the CMS and client. Most

of the time, applications will utilize the IANA-assigned port numbers at least for the initial information exchange; however, this is easily changed by agreement.

The port number negotiated between the CMS and the end-systems for the actual voice stream is variable and dynamic. It is assigned to each end of the call on a call-by-call basis. In addition, some call control protocols may use a dynamically assigned port number for negotiating supplementary and other services.

In conclusion:

- There is not a clear, fixed definition of CMS for VoIP.
- There is not a complete, fixed, limited set of services defined for VoIP. However, a limited, fixed set of services can be defined that might be available by most providers (e.g., connect, disconnect, forward, transfer, etc.).
- There are multiple protocols a client can use to communicate to the CMS.
- The UDP or TCP port numbers used between CMS and client for call control are via bilateral agreement. Most of the time they are IANA-assigned.
- The CMS used for VoIP support can also offer Information Services at the same time using the same protocol.

A.2.3.8.5. Service Paradigms

The CMS does not necessarily follow any traditional paradigm in terms of the services it offers. Some Service Providers will use a CMS to offer VoIP services that mimic today's PSTN as closely as possible, thus recreating the current telephone system on IP. In this case, it is reasonable to expect that call events similar to those defined in J-STD-025 or PacketCable(TM) may be available. Other Service Providers, or end-users on the Internet, may provide innovative services that are not possible or available on today's phone system and may not offer many of the services that are available on today's phone networks. In fact, some of the new services may not be recognizable as traditional voice services and could be interpreted as information services. This is the anticipated result of the end-to-end principle, which enables anyone attached to the Internet to develop and offer services.

The distinction between an "electronic messaging service" which as defined by CALEA includes audio (e.g., voice) and is not included in CALEA requirements and a VoIP service will tend to blur as time goes on and the market develops. For example, an end-user could send an email with an audio attachment. The receiver of the email could listen to the attachment and send back an email with an audio attachment as a response. This may fall under the "electronic messaging service" and could also be seen as a voice conversation with a long delay.

The amount of control a Call Management Server exercises over a target's endpoint varies greatly depending on the standard used and how it is used. It can exercise very little control, such as in some SIP or H.323 RAS cases, or detailed control such as in H.248 or MGCP. Thus, the amount of information available will depend on the service offered by the service provider and by the protocols used for providing the service.

If the Service Provider is providing a traditional telephony service over IP, then call events such as those defined in J-STD-025 or the PacketCable specification should be available.

A.2.3.8.6. Redirection of Calls

As discussed previously, packets carrying the call content are not guaranteed to follow a particular path through the Internet. Nor are they guaranteed to stay on the provider's network even if the two endpoints are on the provider's network. If the target is communicating with another endpoint off the provider's network and redirects the call to another endpoint off the provider's network, then most likely all packets involved in the redirected call will not transit the provider's network (although it is possible they will). Therefore, these packets are not available to the original service provider and cannot be provided. In addition, since the call is redirected, the service provider's Call Management Server is no longer involved and may not have access to any call events related to the redirected call.

A.2.3.8.7. Target Identification

In order to provide the information required, the correct target must be identified.

If the service provider has a relationship with the target and the target uses the service provider's CMS, then it will probably be able to identify the target via either a login, pre-assigned IP address or other pre-assigned identifier (e.g., calling party number).

If the IP address of the target is known, it can be used to identify call events from the target. Usage of IP addresses has the same issues discussed below for IP Transport.

However, some services offered on the Internet may not require a specific relationship between the provider and the client. For example, these may be ad-hoc services offered via the World Wide Web. The provider of the service may not know who is using the service, much like a web server today. In this case, the only information it may have about the target is the information the target sends it. The target's IP address would be one constant that could be used to identify the target. Again, correlating the IP address to the target will have the same difficulties as defined below for IP transport.

In traditional PSTN telephony, the telephone number can be used to identify the called and calling party. It is recognized that this usually identifies a physical telephone that anyone can use, including people that are not under surveillance. In VoIP, a telephone number may not be used to identify the caller. For example, SIP allows the use of email-like addresses (e.g., foo@bar.com) to identify the called and calling party. Therefore, existence of telephone numbers is not guaranteed on the CMS.

A.2.3.8.8. Performance and Complexity

The performance impact on the Call Management System will depend on the services offered and the information required. If information similar to J-STD-025 is provided, the performance implications will be similar.

If the protocol used to deliver the information to the LEA is significantly different from the protocol used by the CMS for its other communication, it could have an affect on the complexity and performance of the system. For example, if the CMS is using IP to

provide service but must use X.25 to communicate to the LEA, the separate drivers and software to run X.25 may introduce additional complexity. In addition, if the data formats used to deliver to the LEA are substantially different, then this will also introduce additional complexity (e.g., a CMS that does not use ASN.1 to provide service but must use ASN.1 to provide CALEA information).

A.2.3.8.9. Delivery Format

The various call control protocols listed above utilize different encoding mechanisms. For example, SIP is text encoded with syntax defined in Augmented Backus-Naur Format (ABNF) while H.323 is binary-encoded with syntax defined in ASN.1. H.248 allows both. Thus, it is not possible to define a delivery protocol that is consistent with the encoding mechanism of each protocol.

However, it is possible to define a delivery mechanism for all the identified protocols that run over IP and reduce the complexity of using multiple network protocols for delivery.

A.2.3.8.10. Points of Intercept

For CMS, the point of intercept would most likely be on or near the CMS.

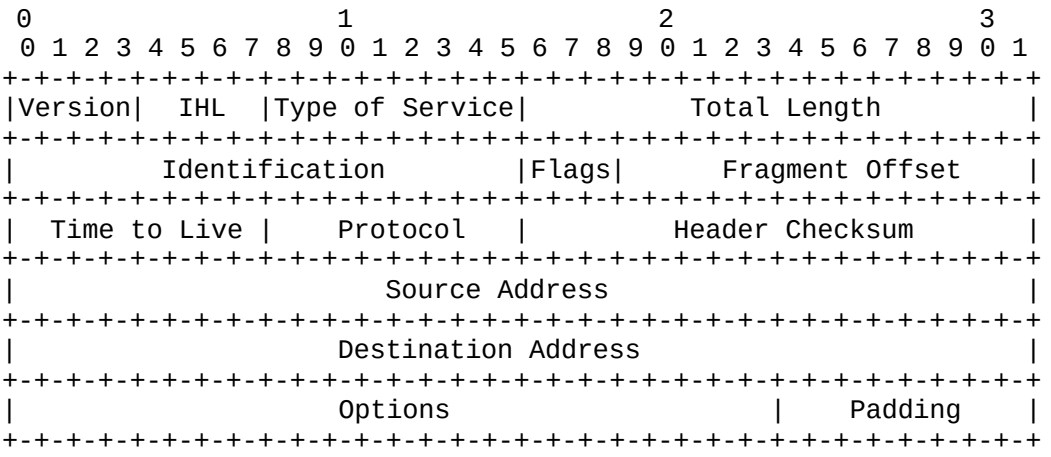
A.2.3.9 IP Transport

This section focuses on information available from a service provider that is offering IP transport. In this case, the subject is not using a Call Management System offered by the service provider.

A.2.3.9.1. Information that can be reported

The IP transport provider utilizes the information in the IP packet for providing service. In general, routers are optimized to operate on the IP header for providing service. Layer 2 switches are optimized to operate on Layer 2 headers to support transmission of IP.

A copy of the IPv4 header is shown below:



The information in this packet header that identifies the source and destination endpoints is the Source and Destination Address fields.

Since the provider in this case does not participate in any call control, it does not have access to information identifying a call. All it does is transport packets. Note that this discussion also applies to a Service Provider that provides a CMS when the target is not using the CMS.

The next layer protocol is identified by the Protocol field. The valid values for the Protocol field are defined by IANA. The next layer protocol could be UDP, TCP or could also be IP. There are several hundred Protocol Numbers defined by IANA for protocols running over IP.

The following three cases were identified at JEM I concerning information that can be provided:

1) Transmission of entire packet stream: In this case, the provider transmits the entire packet stream to and from the target to an LEA and the LEA uses minimization to extract the information to which they are legally entitled. However, it should be noted that this is similar to the original solution, which caused the FCC to request this report. In other words, there is no separation of Pen Register and Trap and Trace information from call content. In this section, transmission of the entire packet stream means transmission of the packets whose source or destination IP address match the target's.
2) IP source and destination address: This is the source and destination address contained in the IP header. In the case of tunneling, this would be the information contained in the outermost IP header. This could also include the Protocol ID field.
3) Extraction of information in the IP data field: This consists of the provider examining the data field of each IP packet in the packet stream to discover "Pen Register and Trap and Trace information." Since IP uses successive encapsulations to carry data, the question of how deep into a packet a Service Provider must go to retrieve the information. Examples of information discussed included:
   - TCP or UDP port numbers; and
   - Call Control (e.g., SIP Invite, H.323 SETUP) information extracted from data field.

A.2.3.9.2. Technical Issues

This section discusses the issues surrounding delivering the information identified above as well as several general issues related to IP technologies.

A.2.3.9.3. IP Packet Fragmentation

The maximum packet sizes supported by the various networks in the path from source to destination may vary. When a router receives a packet on one interface that is larger than the maximum packet size of the interface to which the packet is routed, the router might fragment the large packet into multiple smaller packets. A host might also perform this fragmentation, but it is recommended that the application not generate packets that are too big.

If an IP packet is fragmented, only the first packet will contain the upper-layer protocol headers. For example, only the first packet will contain the TCP header and thus the port numbers. The subsequent packets will not contain the port numbers. Therefore, port numbers may not be available in each IP packet.

A.2.3.9.4. Target Identification

This is a general issue related to all three cases identified in JEM I in addition to the Call Management System case. In any of the above cases, the LEA must identify the target.

There are two general issues involving target identification:

Use of Network Address Translation; and

Use of Dynamic IP Address Assignment.

A.2.3.9.4.1 Use of Network Address Translation

The global Internet uses globally unique IP addresses. However, provision is made [RFC1918] for usage of private addresses. Two non-overlapping private networks may use the same private IP address space.

When end-systems on different networks using private addresses (or an end system on a private network and an end system on a public network) need to communicate, a method called Network Address Translation is used to translate the IP addresses between the two networks. Therefore, the IP address contained in an IP packet in one network may be different from the IP address for the same packet in another network. The address translation between two networks can be fixed (address in one network statically mapped to an address in another network) or dynamic (address in one network dynamically mapped to one of a pool of addresses in the other network). In the case of dynamic mapping, the address seen in one network may be mapped to a different address in the other network depending on time of observation.

A.2.3.9.4.2 Use of Dynamic IP Addresses

IP addresses can be "leased" for a period of time, released and reused. These addresses are usually called "dynamic" IP addresses as opposed to "static" IP addresses, which are

assigned to a user for an extended period of time. A dynamic IP address only identifies an endpoint for the duration of usage by that endpoint. Several mechanisms have been defined to assign IP addresses dynamically. The most common are Dynamic Host Control Protocol (e.g., in LANs and cable networks) [RFC1541] and Internet Protocol Control Protocol (A control protocol used by PPP endpoints, e.g., ., in dialup or xDSL networks) [RFC1332]. Therefore, an IP address may only identify the target or its associate during the duration of a particular connection or session. The target and its associate may have a different IP address at a different time, even if connecting from the same location.

In some of the dynamic addressing schemes, the user authenticates with the network before being assigned an IP address. For example, in dialup Internet access the user usually has to authenticate using PPP before it is assigned an IP address. The user database is stored in a server and the Remote Authentication Dial In User Service (RADIUS) [RFC2138] protocol is used between the network access device and the server to determine if the user is allowed to access the network. However, in many cases the IP address is allocated from a pool on the network access device and not from the RADIUS server. Therefore, even the RADIUS server that authenticates the user may not be aware of address assigned to the user. If the provider uses RADIUS Accounting [RFC2139], then the accounting messages sent from the network access device to the accounting server may contain the address information. RADIUS is an example of an authentication and accounting protocol and is not necessarily the only one used in a network.

A.2.3.10 Transmission of entire packet stream

In the case (case 1) of transmission of the entire packet stream, there is no separation of Pen Register and Trap and Trace information from content since the provider is providing all the data to and from the target.

In order to transmit the entire packet stream to the LEA, the packet stream must be extracted from the aggregate packet stream. There are a several methods for doing this:

- Packet replication: In this method the service-providing equipment (e.g., router) replicates the packet stream to/from the target and transmits the packet stream to the LEA (possibly from a different interface). A simple example of this is to connect to a span port on an ethernet switch.
- "Sniffing" the packet stream: In this method, the provider or LEA connects equipment to the physical medium to extract the packet stream from the aggregate packet flow. A simple example of this is to tap into a coax ethernet cable and copy off packets.

If packet replication is performed on the service-provider equipment, the capacity used for replication will not be available for providing service. This may affect service to the provider's customers including the target. Packet replication may require hardware support that is not available in all equipment.

"Sniffing" the packet stream requires non-obtrusive physical access to the transport medium. Some physical media (e.g., fiber optic) is not conducive to a non-invasive tap unless a tap is preinstalled for such activity.

There are several issues with transporting the entire packet stream. One is based on the service provided. For example, a virtual private dial service encapsulates the PPP packet from the customer into an IP packet (using L2TP) destined for a gateway into another network. In this case, the Network Access Equipment does not normally assign or look at the IP addresses in the customer's packets. In addition, multiple user sessions can be multiplexed into one tunnel to the remote side. Monitoring behind the NAS would require specialized equipment to de-encapsulate the tunneled packet (and possibly de-encrypt) to extract the original IP addresses.

A.2.3.11 Transmission of IP Source and Destination Address

To transmit the IP source and destination addresses (case 2) requires the equipment to read the IP header, extract the source & destination address and deliver that information to the LEA.

Service providing equipment may not be designed to extract IP header information and deliver it to the LEA. Other equipment may be able to do this. In any case, the processing capacity used for delivering the header information is not available for routing packets. The amount of load on the system will depend on the system. There is a multitude of vendor equipment of different types deployed for Internet service and each one would have to be tested to determine what load it would support.

On the other hand, specialized equipment exists today that can extract the IP header information and some other information (e.g., TCP or UDP port number) from a real-time stream.

A.2.3.12 Extraction of Information from Packet Stream

The extraction of information from a packet stream for delivery to the LEA was one option (case 3) discussed at the JEM and other fora. For example, the provider would be required to monitor the packet stream, detect a call control packet containing Pen Register and Trap and Trace information (e.g., for VoIP), extract the Pen Register and Trap and Trace information from the packet and deliver it to the LEA.

Routers supporting service on the Internet typically only make routing decisions based on the IP addressing information. Service providing equipment is not generally designed to look past the IP headers (some may look at TCP or UDP port numbers for filtering) when switching or routing packets. Any processing capacity used for extracting information from a packet stream is not available for routing packets. Given the increase in capacity of Internet connections and that systems generally run at peak load much of the time, there is very little capacity to monitor data fields.

An alternative is to use equipment that is not providing service to the customer but has access to the data stream (e.g., via a port on an ethernet switch). This equipment could acquire the information required and deliver it. This would require extra equipment by the service provider and new operating procedures. In addition, any time new equipment is added to a network it introduces the possibility of errors and misconfiguration and can disturb the functioning of the network.

However, as noted in the main text, there is no reliable method for determining the Pen Register and Trap and Trace information when monitoring a packet stream. If given a specific IP address and port number and if encryption or tunneling isn't used and if the call control protocol is identified then it might be possible to extract the call control information for VoIP calls. However, there is no guarantee that the session is a telecommunications service or an information service. It would be similar to requiring telecommunications carriers to monitor inband communications, detect and demodulate modem tones, detect and decode the information carried in the modem signal and extract Pen Register and Trap and Trace information that may be carried. This is not equivalent to detecting in-band DTMF.

A.2.3.13 Tunneling

One of the issues with identifying the target and providing information is the use of tunneling. In essence, tunneling is the act of encapsulating network protocol packets into IP packets to be routed across the network. In this section, the tunneling of IP packets is considered. The tunneling method defines a mechanism to encapsulate IP packets inside other IP packets. The outer IP header is used to route the packet across the network. The source and destination addresses of the outer IP header identify the tunnel endpoints. The IP addresses in the IP header may not be the IP address of the final endpoints. For example, the tunnel endpoint could de-encapsulate the IP packet and route it onward using the encapsulated IP address information.

There are several methods that can be used for tunneling IP packets across an IP network: Generic Routing Encapsulation [RFC1702], IP-in-IP [RFC1853], Layer 2 Tunneling Protocol [RFC2661], IP Encapsulating Security Payload (ESP) [RFC2406], etc.

The network routes packets based on the outer IP headers and not on the inner headers. In some cases, such as in IPSEC ESP [RFC2406], the encapsulated IP packet is encrypted and isn't available even if the service provider could sniff into the data packet.

For tunnels originated from the target, the destination IP address in the IP packets from the target and the source IP address of IP packets to the target are not necessarily the IP address of its associate. This IP address could be a tunnel endpoint, which will de-encapsulate and route the tunneled packet onward. The source IP address of IP packets from the target and destination IP address of IP packets to the target will normally be the IP address of the target in order for packets to be routed to it properly.

For tunnels originated in the network, the original IP headers may be available. However, in some cases, such as L2TP, the original IP addresses may not be readily available. In L2TP, the network access device encapsulates all PPP frames from the user into IP packets into another IP packet destined for another location. In this case, the IP addresses of the outer IP header will be the IP address of the network access device and the remote tunnel endpoint. The target's IP address will not be in the outer IP header at all. The IP address of the target is assigned by and is only seen by the remote tunnel endpoint. The tunnel from the network access device to the remote tunnel endpoint may be shared by many users including the target.

A.2.3.14 IP Address Spoofing

Another issue that will affect the integrity of the information provided to the LEA is IP address spoofing.

A destination IP address must be authentic or else it cannot be routed to an endpoint. However, a source IP address may or may not be authentic since it is not required for the network to route packets to the destination properly. A valid source IP address is required for the destination to transmit packets properly back to the source. However, there may be cases in which an entity may not care about receiving responses.

Although there are several methods available to do so, in general network access devices do not check for invalid source IP addresses before accepting packets into the network and forwarding them. Therefore, this allows endpoints to spoof the source IP addresses.

There are two cases when dealing with spoofed IP addresses and CALEA:

Target spoofing source IP addresses to a destination

Associate spoofing source IP addresses to the target

In the first case, if the provider is keying on the source IP address in order to provide information to the LEA and the target is using a shared line to access the network, the provider would not necessarily detect and supply information on IP packets with spoofed source IP addresses from the target. A consequence of this is that the target could carry out a Denial of Service attack on a remote host without it being detected by the tap.

In the second case, a remote endpoint could send packets to the target with spoofed source IP addresses. This could result in several things happening:

Under a Trap & Trace order, the remote endpoint could cause the LEA to investigate users who have no relationship with the target by spoofing their IP addresses.

Under Title III, the remote endpoint could incriminate the target (and other users) by sending illegal material to the target with spoofed source IP address.

Although the information required to carry out the above attack is not necessarily readily available (e.g., the fact the target is under surveillance, the IP address of other endpoints, etc.), it is possible for a sophisticated user with knowledge.

Software to spoof IP packets is readily available on the Internet. Tracing a packet stream with spoofed source IP address back to the originator is extremely difficult to do on the Internet, especially if the packet flow is intermittent.

A.2.3.15 Delivery format

In defining the delivery format for IP, the characteristics of internet connections should be taken into account.

The connection speeds from providers to their customers is continuing to increase. The delivery vehicle for the information collected may have to be substantially different for a customer connected via Gigabit Ethernet to one connected via a dial-in modem.

For delivering IP addresses, the provider could provide large amounts of effectively the same information for large data flows since the IP addresses don't usually change for a data flow. Alternatively, the provider could supply the information once per data flow.

The latter option could reduce the amount of information transmitted to the LEA and the strain on the system.

A.2.3.15.1. Transport Protocol

In defining the protocol used between the POI and the LEA, the following characteristics of the transport protocol must be taken into account:

- Reliability: While TCP will provide a reliable connection between the LEA and the POI, it will also require more processing in the end-systems. If a real-time packet stream is required to the LEA, TCP may not be suitable since it is not designed for real-time transport. A UDP based protocol will require the least processing; however, UDP does not provide reliability.
- Security: If IPSEC is used between the POI and the LEA, the processing requirements of IPSEC must be taken into account.

A.2.3.16 Performance and Complexity

Due to the different types of network access, the different types of equipment and different vendors, acquiring hard performance numbers on the impact of providing information is not possible. It would require testing of each piece of equipment in each scenario.

However, some general principles can be considered.

Introducing new features and new code into a system introduces complexity into the system along with probable errors. For service providing equipment, since monitoring streams is a real-time activity that touches the mainline of packet forwarding, the complexity is added directly to the part of the system that can least afford added complexity. If the monitoring is provided in off-line equipment that is monitoring the communications then the system can be optimized for monitoring and filtering functions without necessarily affecting service to customers.

A.2.3.17 Points of Intercept

The point of intercept for an IP transport provider would preferably be close to the edge of the network. The closer to the core of the network, the heavier the traffic flows and the more random the traffic patterns.

The point of intercept should be flexible based on the provider's network design and equipment capabilities. The following are possibilities:

> One location for the Point of Intercept is the first equipment that routes the target's traffic. Another location is an aggregation router through which the target's traffic flows. However, as discussed previously, performing packet monitoring an delivery from equipment that is providing service to a customer detracts from the resources available to service customers.
>
> Another Point of Intercept is within the access POP for the provider. The raw packet stream can be provided via a port on a POP switch (e.g., ethernet switch) or via a line monitor. Non-service providing equipment can be used to take the raw packet stream as input and provide the required CALEA information as output.

No matter where the Point of Intercept is located, some correlation has to be provided to correlate the target's current IP address with the surveillance stream.

A.2.4 Frame Relay

This section describes Frame Relay (FR) technology and its use in transporting voice telephony. It concentrates on the public network where FR is predominately used to transport packetized data. Traditionally FR has been used to transport LAN to LAN and legacy traffic such as bisync and SNA. Recently, non-traditional uses (Voice over Frame Relay [VoFR]) have begun to materialize.

Early transport of packetized data made use of X.25. X.25 includes considerable overhead that Frame Relay was designed to overcome. The major differences between X.25 and Frame Relay are:

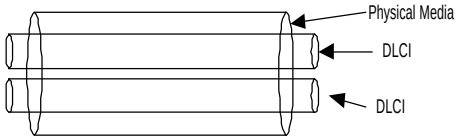
- Logical connection multiplexing and switching takes place at Layer 2 rather than Layer 3;
- Frame Relay leaves end-to-end flow and error control to upper layers; and
- User data and call control signaling are carried on separate connections.

The advantage of Frame Relay lays in the fact that the communication process has been streamlined to take advantage of modern transmission systems that are less prone to error. By lowering the overhead necessary to transport data, increases in throughput and decreases in delay have been realized.

Frame Relay switching is best understood by examining the frame format:

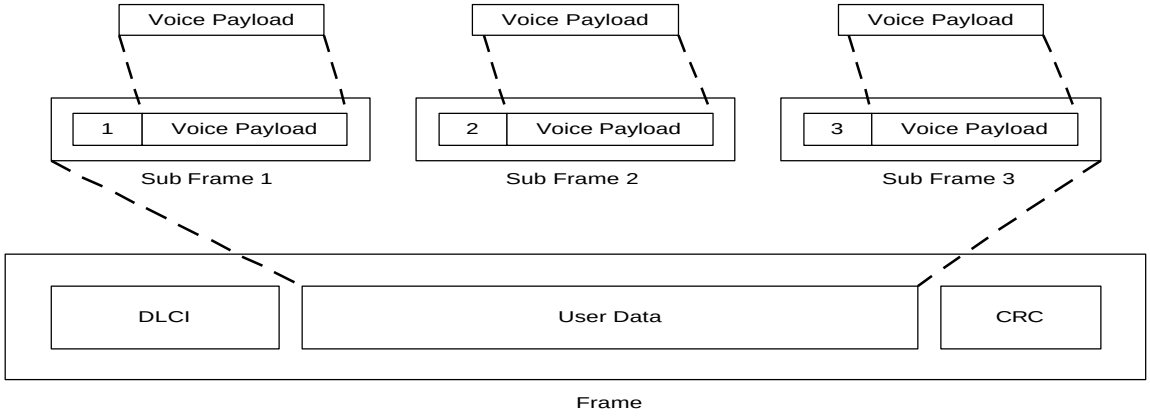
Flag 1 octet	Address 2-4 octets	User Data Variable	FCS 2 octets	Flag 1 octet

The address field has a default length of 2 octets, but can be extended to 3 or 4 octets. Included in the address filed is the data link connection identifier (DLCI) that is used to define the virtual circuit number. This arrangement allows for the multiplexing of many virtual circuits onto a single physical media.



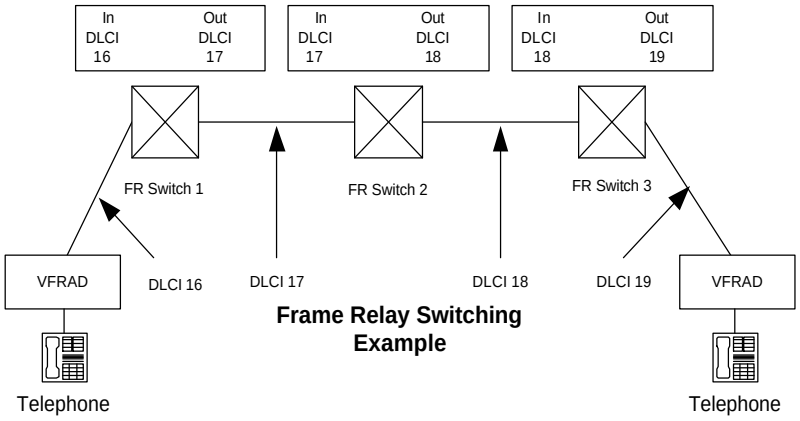
Voice over Frame Relay (VoFR) offers the promise of consolidating data and voice traffic over the same Frame Relay network. Recent advances in Frame Relay features, specifically to support real-time services such as voice, have made Frame Relay an attractive alternative for carrying voice traffic. The Frame Relay Forum introduced the Voice Over Frame Relay Implementation Agreement (FRF.11) in December 1998.

The Voice Over Frame Relay Implementation Agreement (FRF.11) includes features to support real-time transport of voice traffic over a Frame Relay network. Service Multiplexing, defined in FRF.11 is a feature that allows for the multiplexing of many voice circuits onto a single VoFR DLCI. The relationship between voice payload sub-frames and Frame Relay frames is illustrated in the following diagram:



Each sub-frame carries a Sub Channel Identifier that identifies the voice payload sub-frame that is used to carry each individual voice channel.

A Voice Frame Relay Access Device (VFRAD) accomplishes encapsulation of voice traffic into frames. A VFRAD is positioned between a PBX or key set and the Frame Relay network. The VFRAD multiplexes voice, fax, and data from a variety of sources into a common Frame Relay connection. In addition, the VFRAD can provide other services such as compression, encryption, silent suppression, etc. Using voice compression, up to 255 voice sub-channels can be multiplexed within a single Frame Relay DLCI. Addressing is accomplished in VoFR by the transmission of binary representations of dual tone multi-frequency (DTMF). Many aspects of VoFR implementations are left to vendor specific implementations.



Frame Relay Switching Example

As frames arrive at the ingress to the network, the Frame Relay header is examined to determine the DLCI. The DLCI value is mapped to an outgoing facility, which may use a different DLCI. Note that the DLCI value has only local significance. Each end of the Frame Relay connection can, and probably will utilize a different DLCI value. Nothing about the DLCI value at any node in the network identifies the final destination of the frame and the user data that is being transported.

At no time during the transport of user data does the Frame Relay switch examine the user data to determine anything about the nature of the upper layer protocols, including the nature of voice traffic being transported. The voice sub-channels that are being

carried within the DLCI have significance only at the edges, where they are de-multiplexed by the VFRAD.
It is not technically feasible to examine the user data that is being switched by the Frame Relay switch. Switching nodes are designed to relay the frames as quickly as possible. This design effectively prohibits the Frame Relay switch from examining the user information encapsulated within the frame due to the processing and implementation that would be required. Due to the vendor specific implementation of most aspects of VoFR, having the ability to examine the voice payload could be a moot point because of proprietary compression and encryption.

Appendix B: CALEA JEM Invited and/or Participating Groups List

(*In no specific order*)
Rev. 3.28.00

Telecommunications Industry Association (TIA):

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Framing and Encapsulation Standards for ADSL: Packet Mode:

http://www.adsl.com/TR-003.doc

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

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

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

CALEA Suite of Standards for Traditional Paging, Advanced Messaging and Ancillary Services Version 1.2 February 19, 1999:
http://www.pcia.com/advocacy/Calea_su.pdf

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

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

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

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

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

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

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

IETF: http://www.ietf.org/
Position on Wiretapping: http://www.ietf.org/rfc/rfc2804.txt?number=2804

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

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

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

USWest: http://uswest.com

Nokia: http://nokia.com

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FBI: http://www.fbi.gov/

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

Appendix C: JEM 1 Meeting Agenda

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

Joint Experts Meeting (JEM) on CALEA Packet Surveillance

May 3-5, 9am – 5pm PT, Las Vegas, NV

Proposed Agenda

1. **Call to Order and Opening Remarks**
   - JEM Chair remarks (including purpose, scope, acknowledgement of JEM-related work in email discussions and March 20 Q&A call)
   - Ground Rules for JEM
     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**
3. **Approve Agenda**
4. **Distribute, Number, and Assign Contributions**
5. **Background**
   - Legal (CALEA) and Regulatory (FCC R&O) framework for JEM: Al Gidari, Ed Hall (CTIA)
   - 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) Ad Hoc Group
6. **Industry contributions on CALEA Packet Surveillance Issue**
   - Standards Development Organization (SDO) contributions
   - Industry Forum contributions

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

7. **Identification of Technical Issues and Alternatives**
8. **Identify Key Elements of JEM Report**
9. **Review JEM Summary**
10. **Closing Statements/Adjourn**

Appendix D: JEM I Meeting Summary

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

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.

  E. 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.

Appendix E: JEM II Meeting Agenda

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

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

Proposed Agenda

1. **Call to Order and Opening Remarks**
   - JEM Chair remarks (including purpose and scope of both JEM sessions)
   - Ground Rules for the second JEM session
     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.

   F. 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**
3. **Approve Agenda**
4. **Distribute, Number, and Assign Contributions**
5. **Background**
   - Summary of May 3-5 JEM session: JEM chair/vice-chair
   - Summary of May 23 Drafting Group meeting: JEM chair/vice-chair

- Update on Legal (CALEA) and Regulatory (FCC R&O) issues since first JEM session: Al Gidari (CTIA), Montgomery Kosma (Gibson, Dunn, and Crutcher LLP)
- Update on J-STD-025 and revisions since first JEM session: Terri Brooks, Chair, TR45.2 Lawfully Authorized Electronic Surveillance (LAES) AdHoc Group
- Today's Methods for Separating Pen Register Data from Content on Packet Surveillances, Presentation and Demonstration by FBI Engineering Research

6. **Industry contributions on CALEA Packet Surveillance (Main Body of JEM Report)**
   - Standards Development Organization (SDO) contributions
   - Industry Forum contributions
   - Individual company contributions on CALEA Packet Surveillance Issues

   (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
   - Industry Forum contributions
   - Individual company contributions on CALEA Packet Surveillance Issues

   (Encourage presenting contribution only if substantively different from SDO or industry contributions above)
8. **Identification of Technical Issues and Alternatives**
9. **BREAK: Allow Breakout Drafting Group to Refine Key Elements of JEM Report**
10. **Review JEM Report**
11. **Clarification of Post-JEM Process for Finalizing JEM Report for forwarding to TIA**
12. **Closing Statements/Adjourn**

Appendix F: JEM II Meeting Summary

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

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.

G. 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 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 DataSurveillance 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 Coon. 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.