ATIS-1000013.v2.2015(R2020)

Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services, Version 2

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000013.v2.2015(R2020), *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services, Version 2*

Is an American National Standard developed by the **Lawfully Authorized Electronic Surveillance (LAES)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000013.v2.2015(R2020)

[Revision and Consolidation of ATIS-1000013.2007 and ATIS-1000013.a.2009]

American National Standard for Telecommunications

Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services, Version 2

Alliance for Telecommunications Industry Solutions

Approved July 21, 2015

American National Standards Institute, Inc.

Abstract

Internet Access and Services can be obtained by establishing a subscription based arrangement. This standard provides capabilities to lawfully intercept communications of subscription-based Internet Access and Services arrangements.

NOTE - Annex A, *ASN.1 Definitions*, of this Standard has also been formatted as a separate plain text file and electronically packaged with this standard.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

This document is entitled *Lawfully Authorized Electronic Surveillance for Internet Access and Services*. This standard is the result of work by members of the Alliance for Telecommunications Industry Solutions (ATIS) Packet Technologies and Systems Committee (PTSC), working within the PTSC Lawfully Authorized Electronic Surveillance (LAES) Subcommittee. This standard defines the interfaces between an Internet Access or Services Provider and a Law Enforcement Agency to assist the Law Enforcement Agency in conducting lawfully authorized electronic surveillance for Internet Access and Services.

This version of the standard provides clarifications, corrections, and enhancements to ATIS-1000013.2007, and adds an informative annex on *Byte Count Reporting in an Internet Access and Services LAES Environment*.

It is not the intent of this document to imply or impact any pending regulatory decisions related to Internet Access and Services. This document provides the mechanisms to perform lawfully authorized electronic surveillance of Internet Access and Services subject to the appropriate legal and regulatory environment.

Future control of this document will reside with ATIS PTSC. This control of additions to the specification, such as ongoing protocol evolution, new applications, and operational requirements, will permit compatibility among U.S. networks. Such additions will be incorporated in an orderly manner with due consideration to the ITU-T layered model principles, conventions, and functional boundaries.

> **NOTE - A buffering solution for use with this standard is addressed in ATIS-1000021, *Technical Report on Data Buffering (Short Term Storage) in an LAES Environment*.**

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Applied Communication Sciences)

G. Myers, PTSC LAES Chair (Counter Link)

N. Rao, PTSC LAES Vice-Chair (Nokia Networks)

The **LAES** Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard for Telecommunications –

Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services

1 Introduction

1.1 Background

This Standard defines the interfaces between a service provider that facilitates subscriber access to the Internet and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance for subscription-based Internet Access and Services (IAS) arrangements. This Standard is provided for purposes of a "safe harbor" as specified in Section 107 of the Communications Assistance for Law Enforcement Act (CALEA) [Ref 1]: "a telecommunications carrier shall be found to be in compliance with the assistance capability requirements under Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with Section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103."[1] [Ref 2, 3, 14, 15].

As used in this Standard, electronic surveillance refers to the interception and delivery of communications for a particular IAS subscriber as lawfully authorized. The said communications may include Communication Identifying Information (CmII) with or without the Communication Content (CmC).

In this Standard, an intercept subject, or more simply a subject, is an IAS subscriber whose communications have been authorized by a legal instrument to be intercepted and delivered to an LEA. The identification of the subject is limited to subject identifiers or subject-related identifiers used by the Internet Access or Services Provider's (IASP) equipment, facility, or communication service – e.g., network address, terminal identity, subscription identity.

As a precondition for an IASP's assistance with Lawfully Authorized Electronic Surveillance (LAES), an LEA must serve an IASP with the necessary lawful authorization identifying the intercept subject, the communications and information to be provided, and service areas where the communications and information are to be provided. Once this lawful authorization is served on an IASP, the IASP shall perform the access, mediation as necessary, and delivery of the identified communications and information to the LEA via LEA-procured equipment, facilities, or services.

1.2 Scope & Purpose

The focus of LAES for IAS is on the network(s) that provide subscriber connectivity to the Internet. IAS may be provided by a set of independent or related entities – e.g., a Digital Subscriber Line (DSL) provider, cable provider, Wireless Fidelity (Wi-Fi®) provider, or a WiMAX®[2] provider and an Internet Service Provider (ISP). This document does not address mobile IP capabilities as defined by the Internet Engineering Task Force (IETF).

---

[1] It is not the intent of this document to imply or impact any pending CALEA regulatory decisions related to IAS. This document provides the mechanisms to perform lawfully authorized electronic surveillance of IAS subject to the appropriate legal and regulatory environment. Where CALEA is found to be applicable to IAS, it is intended that a manufacturer or service provider that is in compliance with this document will have "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. §1001, et seq.

[2] For fixed/nomadic wireless (e.g., as a wireline access alternative).

The scope of this Standard is the set of capabilities to support LAES for IAS and the interface between an IASP and an LEA for delivery of intercepted communication content and communication-identifying information. All other interfaces are outside the scope of this Standard.

Upon publication, this Standard supersedes and replaces ATIS-1000013.2007, ATIS-1000013.a.2009 (Supplement A to ATIS-1000013.2007), and ATIS-1000052 (Technical Report on Byte Count Reporting in an Internet Access and Services LAES Environment).

1.3 Organization

Clause 2, *Normative References*, is a list of references used in the preparation of this Standard.

Clause 3, *Definitions and Acronyms*, defines words and acronyms that are used in this Standard.

Clause 4, *Internet Access and Services Description*, defines IAS and the electronic surveillance model for IAS.

Clause 5, *User Perspective (Stage 1)*, presents the user perspective (Stage 1) requirements for LAES for IAS.

Clause 6, *Network Perspective (Stage 2)*, presents the network perspective (Stage 2) requirements for LAES for IAS.

Annex A, *ASN.1 Definitions (Normative)*, specifies the lawfully authorized electronic surveillance protocol Abstract Syntax Notation One (ASN.1) and associated modules.

Annex B, *Reference Topologies (Informative)*, describes a number of reference network topologies typically used for IAS over various types of access networks.

Annex C, *Optional Messages (Informative)*, provides the network perspective (Stage 2) and abstract syntax for optional IAS lawfully authorized electronic surveillance protocol messages.

Annex D, *IAS Intercept Information Flow Example (Informative)*, provides an example set of IAS events and associated LAES reporting.

Annex E, *IAS Cases and CmII Reporting (Informative)*, identifies the CmII that may be reported for a variety of architecture scenarios.

Annex F, *Byte Count Reporting in an IAS LAES Environment (Informative)*, specifies how byte count of IP packets may be reported in a Packet Data Header Report and a Packet Data Summary Report.

2 Normative References

[Ref 1] *Communications Assistance for Law Enforcement Act (CALEA)*, Public Law 103-414, October 25, 1994.[3]

[Ref 2] *In the Matter of Communications Assistance for Law Enforcement Act, Order on Remand*, CC Docket No. 97-213, 17 FCC Record 6898 (2002).[3]

[Ref 3] *In the Matter of Communications Assistance for Law Enforcement Act, Third Report and Order,* CC Docket No. 97-213, 14 FCC Record 16794 (1999).[3]

[Ref 4] *Wire and Electronic Communications Interception and Interception of Oral Communications*, Title 18 of the United States Code, Chapter 119, Sections 2510 – 2522.[3]

[Ref 5] ITU-T Recommendation X.680, *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation*, July 2002.[4]

[Ref 6] IETF RFC 768, *User Datagram Protocol*, August 1980.[5]

[Ref 7] IETF RFC 793, *Transmission Control Protocol*, September 1981.[5]

---

[3] This document is available from the FCC website at < http://www.fcc.gov/calea >.

[4] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[5] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[Ref 8] Void.

[Ref 9] IETF RFC 791, *Internet Protocol Darpa Internet Program Protocol Specification,* September 1981.[5]

[Ref 10] IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification,* December 1998.[5]

[REF 11] ATIS-1000678.v2.2006(R2013), *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2,* January 2006.[6]

[Ref 12] J-STD-025-B (R2012), *Joint ATIS-TIA Standard on Lawfully Authorized Electronic Surveillance*, August 2006.[7]

[Ref 13] IETF RFC 3339, *Date and Time on the Internet: Timestamps*, July 2002.[5]

[Ref 14] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, *First Report and Order and Further Notice of Proposed Rulemaking*, ET Docket No. 04-295, 20 FCC Rcd 14989 (2005).[3]

[Ref 15] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, *Second Report and Order and Memorandum Opinion and Order*, ET Docket No. 04-295, 21 FCC Rcd 5360 (2006).[3]

[Ref 16] ITU-T Recommendation X.690, *Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguishing Encoding Rules (DER)*, July 2002.[4]

[Ref 17] IETF RFC 2131, *Dynamic Host Configuration Protocol*, March 1997.[5]

[Ref 18] IETF RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*, February 1999.[5]

[Ref 19] IETF RFC 4960, *Stream Control Transmission Protocol*, September 2007.[5]

[Ref 20] IETF RFC 4340, *Datagram Congestion Control Protocol (DCCP)*, March 2006.[5]

3 Definitions & Acronyms

3.1 Definitions

3.1.1 Access-Associated Communications Identifying Information (AACmII): *CmII* associated with communication between the subject and the IAS network for the purposes of login, logout, access authorization, access authentication, or resource allocation caused by the use of, or attempted use of, the IAS network by the subject.

3.1.2 Access Network: See 4.1.

3.1.3 Access Session: The time interval during which the user is authorized to access the networks in the IASP domain.

3.1.4 Communication Content (CmC): The full IP packet streams to and from the subject.

3.1.5 Communication-Identifying Information (CmII): Information that identifies the origin, direction, destination, or termination of each communication generated or received by a subject by means of any equipment, facility, or service of an IASP.

Communications Identifying Information can be one of two types: 1) *Access Associated Communications Identifying Information*; or 2) *Content Associated Communications Identifying Information*.

Communications Identifying Information is “reasonably available” to an Internet Access and Services Provider if it is present at an intercept access point and can be made available without the provider being unduly burdened with network modifications. CmII is delivered by the set of messages defined in this Standard and the set of mandatory and conditional parameters contained therein.

---

[6] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/product.aspx?id=22771 >

[7] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/product.aspx?id=26133>

3.1.6 Communication: Any wire or electronic communication, as defined in [Ref 4].

3.1.7 Content Associated Communications Identifying Information (CACmII): Communication Identifying Information associated with the delivery and routing of the subject's packets in the network (i.e., the headers of the IP packets).

3.1.8 Dynamic IP Address: An IP address that is temporarily assigned to a subscriber's equipment for a limited or specified duration.

3.1.9 Electronic Surveillance: The statutory-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of communication identifying information. As used herein, *surveillance* refers to a single communication intercept, pen register, or trap and trace. Its usage herein does not include administrative subpoenas for obtaining a subscriber's billing records and information about a subscriber's service that an LEA may employ before the start of a communication intercept, pen register, or trap and trace.

3.1.10 IASP Domain: See 4.1.

3.1.11 Intercept: Defined in [Ref 4] section 2510(4) to be "the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

3.1.12 Intercept Access Point (IAP): A point within an Internet and Access Services Provider domain where some of the communications or communications identifying information of an intercept subject's equipment, facilities, and services are accessed.

3.1.13 Intercept Subject: A subscriber whose communications, communications identifying information, or both, have been authorized by a court to be intercepted and delivered to a Law Enforcement Agency. The identification of the intercept subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

3.1.14 Intermediate Network: See 4.1.

3.1.15 Internet Service Provider (ISP) Network: See 4.1.

3.1.16 Law Enforcement Agency (LEA): A government entity with the legal authority to conduct electronic surveillance (e.g., the Federal Bureau of Investigation or a state or local police department).

3.1.17 Packet: An IP packet [Ref 9, 10].

3.1.18 Packet Data Session: The time interval during which the user is granted resources to send or receive packets to or from the Internet.

3.1.19 Session: A set of multimedia senders and receivers and the data streams flowing from senders to receivers.

3.1.20 Static IP Address: An IP address that is permanently assigned to a subscriber's equipment.

3.1.21 Subject: See *intercept subject*.

3.1.22 Subject Domain: See 4.1.

3.1.23 Surveillance: See *electronic surveillance*.

3.2 Acronyms

AAA	Authorization, Authentication, and Accounting
AACmII	Access Associated CmII
AH	Authentication Header
ANSI	American National Standards Institute
A-PDU *or* APDU	Application Protocol Data Unit
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One [Ref 5]

ATIS	Alliance for Telecommunication Industry Solutions
ATM	Asynchronous Transfer Mode
CACmII	Content Associated CmII
CALEA	Communications Assistance for Law Enforcement Act.
CF	Collection Function
CHAP	Challenge Handshake Authentication Protocol
CmC	Communication Content
CmC-APDU	Communication Content Application Protocol Data Unit
CmII	Communication-Identifying Information.
CmII-MF	CmII Mediation Function
CMTS	Cable Modem Termination System
CPE	Customer Premise Equipment
DCCP	Datagram Congestion Control Protocol
DF	Delivery Function
DHCP	Dynamic Host Configuration Protocol
FCC	Federal Communications Commission
GMT	Greenwich Mean Time
GWR	Gateway Router
IAP	Intercept Access Point
IC-APDU	Intercept Content Application Protocol Data Unit
IETF	Internet Engineering Task Force
IAS	Internet Access and Services
IASP	Internet Access or Services Provider
IP	Internet Protocol
IPCP	IP Control Protocol
IPsec	Internet Protocol Security
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
LI	Lawful Intercept
MAC	Media Access Control
MF	Mediation Function
MOC	Mandatory Optional Conditional
NAS	Network Access Server
OSI	Open Systems Interconnect
PADT	PPPoE Active Discovery Terminate
PC	Personal Computer
PDU	Protocol Data Unit
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SA	Security Association
SCTP	Stream Control Transmission Protocol

TCP	Transmission Control Protocol [Ref 7]
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VPN	Virtual Private Network

3.3 Definitions for "Mandatory," "Optional," & "Conditional" Parameters

The value in the Mandatory/Optional/Conditional (MOC) column in the Message Parameter tables in this document indicates whether inclusion of the indicated parameter in the indicated message is *Mandatory* (M), *Optional* (O), or *Conditional* (C).

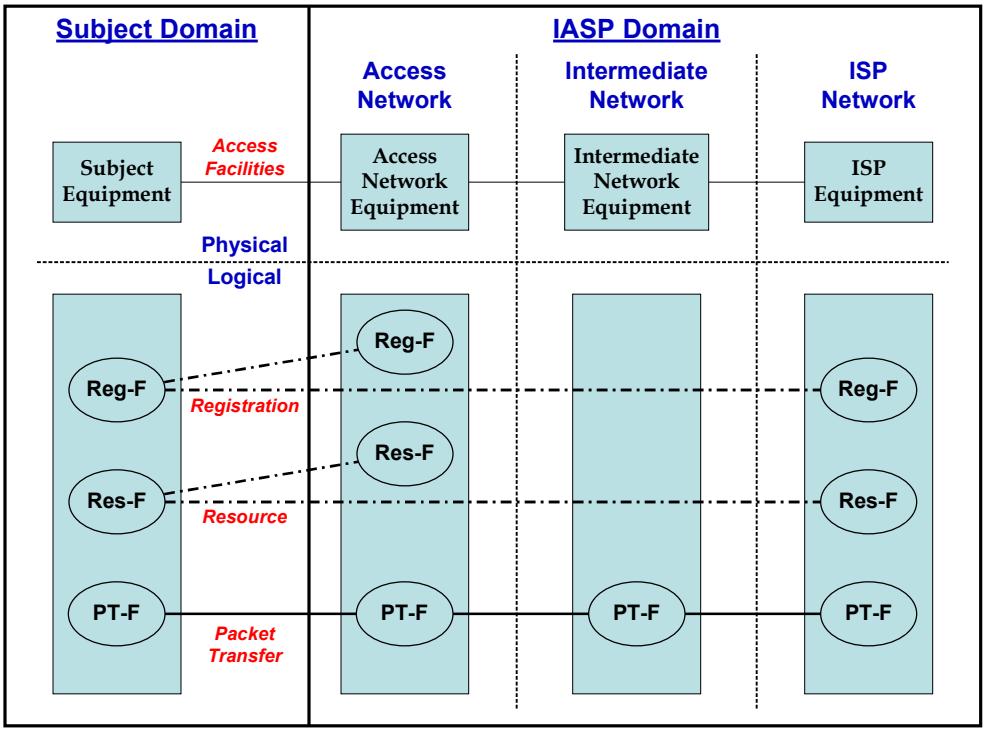
- A *Mandatory (M)* value means that the sender of the message shall always include this parameter in the message.
- An *Optional (O)* value means that the sender of the message may include this parameter in the message.
- A *Conditional (C)* value means that the sender of the message shall include this parameter in the message when the criteria specified in the *Conditions* column are met.

4 Internet Access & Services Description

4.1 Internet Access & Services Model

The general IAS Model describes a framework within which an intercept subject has, gains, or is granted access to physical facilities provided by the Access Network (e.g., fixed DSL) and the subject uses those physical facilities to invoke and utilize services provided by a service provider. The services could be provided by the Access Network provider or a third party service provider (e.g., ISP).

Figure 1 depicts the IAS physical and functional model. The physical and functional components are separated into two domains: the *Subject Domain* and the *IASP Domain*. The IASP Domain consists of the *Access Network*, the *Intermediate Network*, and the *ISP Network*.



Notes:
- the Subject may Register in the Access Network and/or with the ISP
- the Resources may be dynamically allocated or fixed at the Access Network (e.g., fixed DSL)
- the ISP allocates resources (e.g., a logical session)

Figure 4.1 – IAS Model

Figure 4.1 contains the following two domains:

1. The *Subject Domain* is composed of the intercept subject and the intercept subject's equipment and facilities. The intercept subject's equipment may include, but is not limited to: personal computers, personal digital assistants (PDAs), gaming equipment, hubs, routers, switches, firewalls, local wireless access points, and any other equipment used by the subject to access the Internet. The subject's facilities, whether owned by the subject or provider, include, but are not limited to, all customer premise wiring and customer premise equipment (CPE) – e.g., DSL or cable modems.

   The physical equipment and facilities in the subject domain support the logical functions of registration (when required), reservation, and packet transfer to and from the Internet. The registration function may be a fixed capability between the CPE and provider equipment for some access capabilities.

2. The *IASP Domain* consists of the Access Network, the Intermediate Network, and the ISP Network. These networks may be provided by one or more providers.

   a. The *Access Network* is composed of the physical and logical facilities that provide the intercept subject access to the Internet. The physical facilities may include, but are not limited to: the physical plant between the subject's customer premise equipment and the access provider, the physical plant and equipment of the access provider, and any equipment and facilities both logical and physical between the access provider and the intermediate network, if an intermediate network exists. The logical facilities may include the registration, reservation, and packet transfer functions, or the access network may provide only the physical and logical facilities for packet transfer, and the registration and reservation functions may reside in the ISP network.

   b. The *Intermediate Network* is a network that may exist between the Access Network and Internet Service Provider Network. The Intermediate Network provides transport to and from the ISP

network. Routing between the Access and ISP Networks may be asymmetrical and be carried across different Intermediate Networks.

c. The *Internet Service Provider (ISP) Network* provides connectivity to the Internet. The ISP may also provide the packet transfer function. The registration and reservation functions may reside in the ISP Network.

The following logical functions are presented in Figure 4.1:

- R*egistration Function (Reg-F)* – Registration for the purposes of this document is defined as any login or authentication process required of the subject by the service provider (either access or ISP) to gain access to the Internet.
- *Resource Function (Res-F)* – Resource reservation for the purposes of this document is defined as reserving resources (e.g., bandwidth) as necessary for access, and granting the subject access to the Internet. Resource reservation is recognized by providing the subject with one or more valid IP addresses, or IP subnet address ranges that allow the subject to access the Internet. Quarantined addresses, or addresses assigned for the purposes of registration are not included as resources assigned in the network.
- *Packet Transfer Function (PT-F)* – For the purposes of this document the packet transfer function is defined as the process of transferring Layer 3 IP packets to and from the Internet. For packet transfer to occur, the subject needs to have completed Reg-F and Res-F if required. For the network to perform PT-F, the network elements need to be able to recognize the Layer 3 packet structure and be able to handle the packets. Only those network elements that recognize the Layer 3 packet structure (i.e., IP header fields) and handle the packets can perform the packet transfer function. A Layer 2 network (e.g., an Asynchronous Transfer Mode (ATM) network) or a Layer 1 network (e.g., a Time Division Multiplexing network) may be used to transport the Layer 3 packets from the customer premise to the ISP network. Network elements in Layer 1 and Layer 2 networks cannot recognize the Layer 3 packet structure and do not use the Layer 3 packet header information. These Layer 1 or Layer 2 networks do not perform PT-F.

In gaining access to the services, the subject – or equipment, e.g., Personal Computer (PC) – may be required to register for service. This registration for service may occur in the Access Network, the ISP Network, or both. In some cases (e.g., fixed DSL), no registration for service may be required in the Access Network as the service is fixed or pre-defined and associated with the subject.

In addition to the subject registration, physical or logical resources may be dynamically allocated to the subject's equipment. This dynamic allocation of resources may occur at the Access Network (e.g., assign physical facilities), the ISP Network (e.g., assign logical session), or both.

The Subject Domain, Access Network, Intermediate Network, and ISP Network may be using IPv4, IPv6, or any combination of IPv4 and IPv6 involving translation or tunneling.

4.2 General Surveillance Model

4.2.1 Electronic Surveillance Model

The functions needed to perform LAES are broadly categorized as access, delivery, collection, service provider administration, and law enforcement administration [Ref 12]. These functions are described herein without regard to their implementation. The relationship between these functional categories is shown in Figure 4.2. As shown, the Access Function (AF), Delivery Function (DF), and IASP Administration Function are the responsibility of the IASP, and the Collection Function (CF) and Law Enforcement Administration Function are the responsibility of the LEA. The use of these functions to perform an interception is initiated by receipt of a specific lawful authorization.

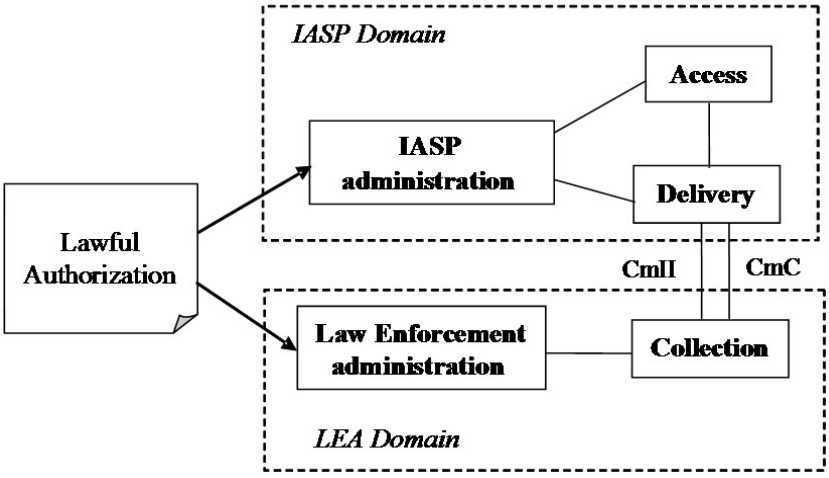


Figure 4.2 – Electronic Surveillance Model

The *Access Function*, consisting of one or more Intercept Access Points (IAPs), accesses and intercepts an intercept subject's CmC and CmII unobtrusively. The IAPs may vary between IASPs.

The *Delivery Function* delivers intercepted communications to one or more CFs. The DF shall deliver intercepted communications in the form of CmC and CmII.

The *Collection Function* collects and analyzes the CmC and CmII received from the DF. It is defined to be the location where lawfully authorized intercepted CmC and CmII is collected by a LEA.

The *IASP Administration Function* controls the IASP's AF and DF.

The *Law Enforcement Administration Function* controls the LEA's CF.

4.2.2 Intercept Access Points

With respect to IAS, IAPs are places in the network where lawful intercept IAS CmII and CmC are intercepted. There are two fundamental types of IAS IAPs:

1. IAS Communication Identifying Information IAPs (CmII-IAPs); and
2. IAS Communication Content IAPs (CmC-IAPs).

CmII-IAPs and CmC-IAPs are associated with CmII and CmC intercept functions respectively that perform the actual interception of CmII and CmC. These CmII and CmC intercept functions are incorporated into one or more network elements. CmII and CmC intercept functions may be collocated within the same network element, or may be distributed among many network elements. See 4.4 for examples of distributions of the IAPs in various network providers within the IASP domain.

4.2.2.1 CmII-IAPs

A CmII-IAP captures the information necessary to generate CmII. CmII may be categorized as Access Associated CmII (AACmII) or Content Associated CmII (CACmII).

a. *Access Associated CmII*: CmII associated with communication between the subject and the IASP domain for the purposes of login, logout, access authorization, access authentication, or resource allocation caused by the use of, or attempted use of, the IAS network by the subject. All AACmII signaled to and from the network shall be reported to law enforcement.

b. *Content Associated CmII*: CmII associated with the delivery and routing of the subject's content in the network, derived from specific fields in the Layer 3 IP headers and Layer 4 headers of the IP packets, as defined 5.2.11 and 5.2.12. Two options exist for delivering CACmII:

- Delivering the records for the specified header fields of each intercepted packets to law enforcement; or
- Delivering summary records.

4.2.2.2 CmC-IAPs

A CmC-IAP intercepts the full packets to and from an intercept subject.

The CmC-IAP intercepts the required content and presents it to the DF or to the Mediation Function (MF). The CmC-IAP can reside in a number of places. The CmC-IAP used in a particular network is an IASP design decision.

4.2.3 Functional Electronic Surveillance Architecture

Figure 4.3 shows a general functional Lawful Intercept (LI) architecture for IAS where both CmC and CmII are intercepted and delivered to LEAs. This functional architecture assumes that one IASP is providing IAS. Three domains are identified:

1. *Subject Domain*: Consists of the subject's equipment, network access equipment-facilities, and associated functions.
2. *IASP Domain*: Consists of the IASP's network equipment-facilities and associated functions. This could be one or more of the networks in the IASP domain discussed in 4.1.
3. *LEA Domain*: Consists of LEAs' LI collection equipment-facilities and associated functions.

The IASP Domain includes the following functions:

- *CmII Access Functions*: One or more functions responsible for isolating and presenting CmII to the CmII MF or DF.
- *CmC Access Functions*: One or more functions responsible for isolating and presenting CmC to the CmC MF or DF.
- *CmII Delivery Function*: A function responsible for delivering the CmII, which is specified in a lawful authorization, to the LEAs. The CmII DF contains a CmII Application Protocol Data Unit (APDU) Demarcation Point. The CmII APDU Demarcation Point is the point in the DF where a CmII APDU is presented to the delivery method for delivering CmII over the 'e' interface to the LEAs' CF.
- *CmC Delivery Function*: A function responsible for delivering the CmC, which is specified in a lawful authorization, to the LEAs. The CmC DF contains a CmC APDU Demarcation Point. The CmC APDU Demarcation Point is the point in the DF where CmC is presented to the Delivery Method for delivering CmC over the 'e' interface to the LEA's Collection Function.
- *CmII Mediation Function*: A function responsible for the presentation[8] of the CmII. This function maps or encapsulates IAS subject access and network signaling messages onto 'e' interface messages.
- *CmC Mediation Function*: A function responsible for the presentation[9] of the CmC.

---

[8] *Presentation*, as used here, means the form and style of the CmII information and includes the conversion or mapping of information from one form or style to another.

[9] *Presentation*, as used here, means the form and style of the CmC and includes the conversion of CmC from one form or style to another.

As discussed in 4.1, the IASP domain consists of the access network, the intermediate network, and the ISP network. The above functions may be performed by one or more networks in the IASP domain.

The following physical demarcation point(s) appear at the boundary between the IASP Domain and the LEA Domain:

- *CmII Physical Demarcation Point*: Point where CmII is presented to the LEA's procured functions and facilities for delivering CmII over the 'e' interface to the LEA's Collection Function.
- *CmC Physical Demarcation Point*: Point where CmC is presented to the LEA's procured functions and facilities for delivering CmC over the 'e' interface to the LEA's Collection Function.

CmII and CmC physical demarcation points may be one and the same, allowing CmII and CmC to be delivered over the same physical interface.

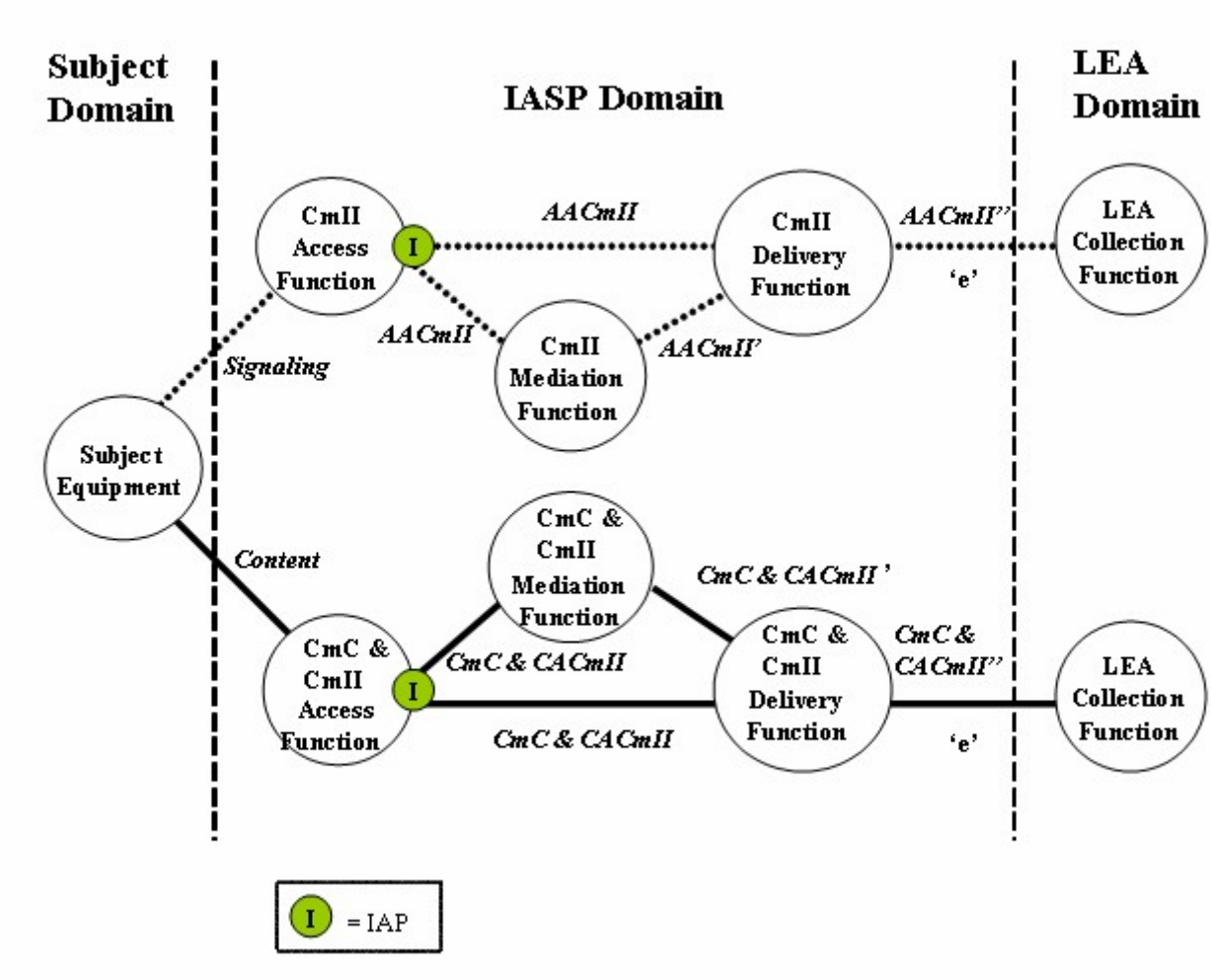


Figure 4.3 – Functional LI Architecture for IAS

Note that the LI architecture presented in Figure 3 is functional in nature and the functions may be distributed and grouped into various network elements and nodes.

In Figure 4.3, the prime (') and double prime ('') symbols indicate that the format of the CmII and CmC may be different.

The MF and DF are logical functions, not physical entities. They may be implemented in separate physical entities or in a single physical entity.

4.2.4 Demarcation

Figure 4.4 shows the A-PDU Demarcation Point to be that point in the DF where the LI-formatted CmII and CmC (i.e., the CmII or CmC A-PDUs) are presented to the Delivery Method at Open Systems Interconnect (OSI) Application Layer 7[10]. The Delivery Method then delivers the A-PDUs to the LEA's Collection Function. The DF Application function formats the CmC and CmII into A-PDUs according to the 'e' interface requirements and presents the formatted A-PDUs to the Delivery Method. The Delivery Method, via the selected protocols (e.g., TCP/IP), sends the encapsulated A-PDUs to the CF.

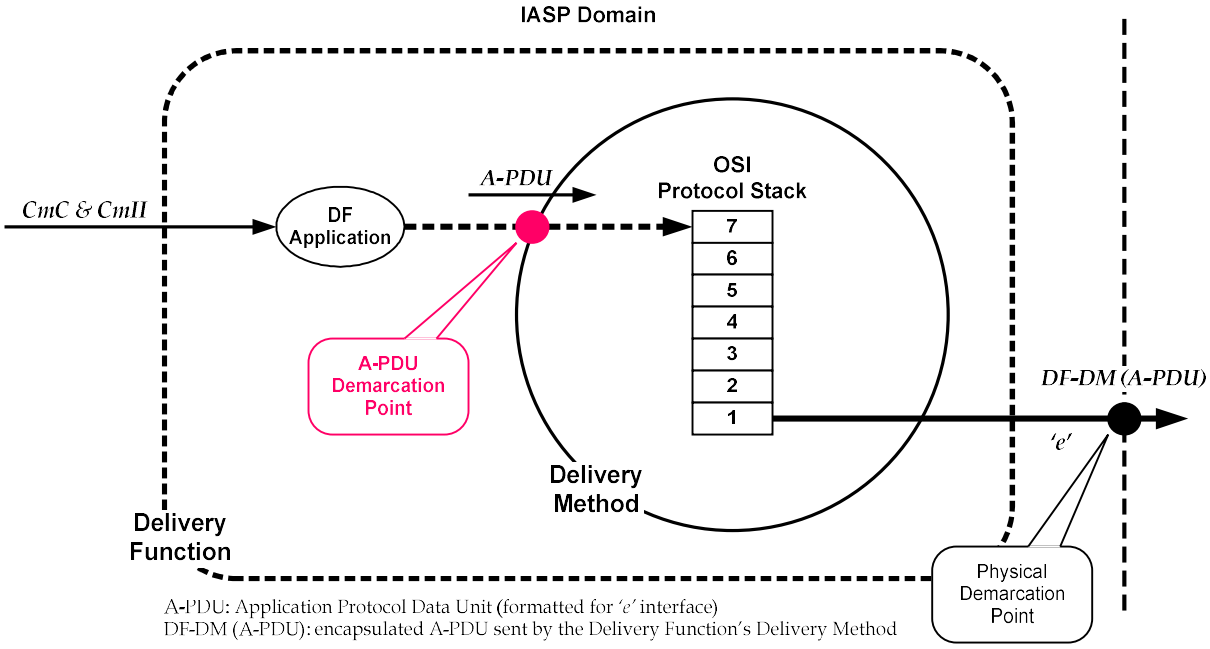


Figure 4.4 – A-PDU Demarcation Point at Delivery Method in Delivery Function

Figure 4.5 shows a more complete picture with the LEA CF receiving the LI-formatted A-PDUs. The Delivery Method of the LEA's CF is a peer protocol stack of the Delivery Method of the IASP's DF. The DF-CF Delivery Method is agreed upon between the IASP and LEA.

[10] The use of the phrase "Open Systems Interconnect Application Layer 7" is not intended to imply that OSI protocols must be used.

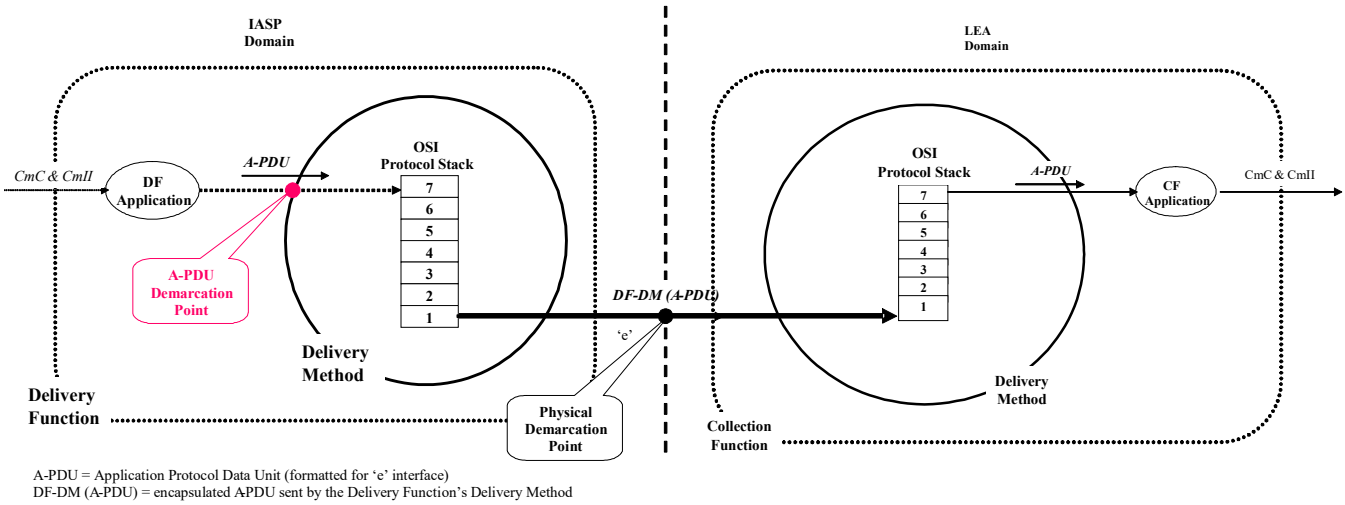


Figure 4.5 – A-PDU Demarcation Point and DF-CF Delivery Method

Figure 4.6 shows a Time T1 for delivering the A-PDU from the AF to the A-PDU Demarcation Point in the DF and a Time T2 for the DF Delivery Method to present the A-PDU to the peer protocol of the CF Delivery Method. Time T2 is dependent on the Delivery Method agreed upon between the IASP and LEA. The IASP has control over time T1. The IASP and the LEA have joint control over Time T2, which is dependent on the IASP-LEA agreed-upon facilities and delivery protocols over the 'e' interface.

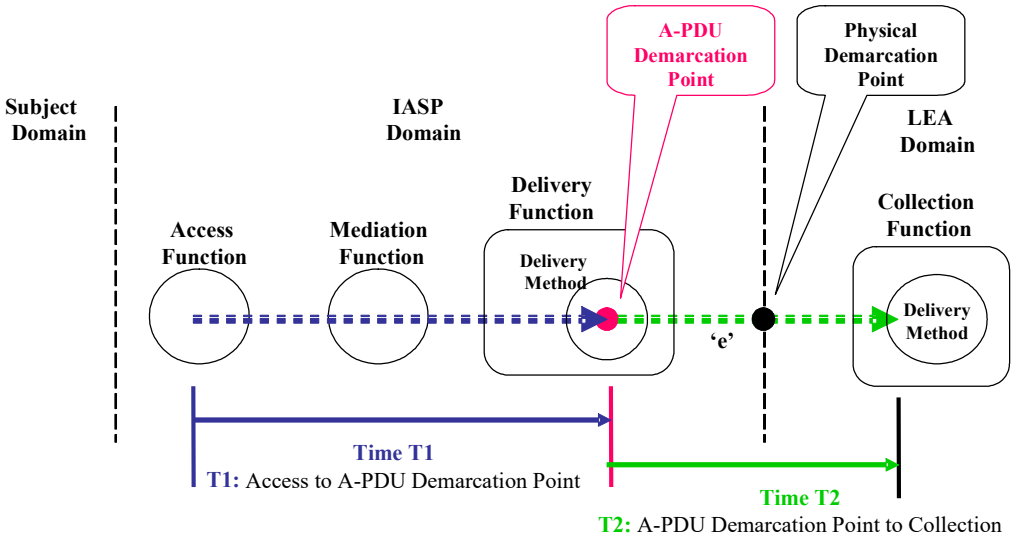


Figure 4.6 – CmII and CmC Delivery Times

The CmC and CmII delivery times are dependent upon the Delivery Method protocols selected and the associated physical facilities utilized during transmission. Establishment of the A-PDU Demarcation Point allows T1 to be determinant. T2 is dependent on the characteristics of the Delivery Method – e.g., protocols, buffering, reliable delivery, security – and the characteristics of the delivery facilities procured by the LEA – e.g., Quality of Service (QoS), bandwidth.

4.2.5 Subject Identification

The subject's access to the IASP domain can be divided into two categories defined by the way the subject activity is identified in the network.

4.2.5.1 Login Identifier

The subject is uniquely identified through a login process. As a result of a successful login process, an intercept may be based on information, such as:

- A single IP address, a set of IP addresses, or an IP subnet assigned to the subject at login; or
- Account-session-id assigned to the subject's session at login.

Note that in the case of multiple logins by the subject, multiple cases of the above conditions may be required for the same subject.

When subject activity is identified in the network through login identification, the subject (or subject's equipment) may be required to transmit and receive "signaling" packets – e.g., Challenge Handshake Authentication Protocol (CHAP) packets and IP Control Protocol (IPCP) packets – to perform Registration Function (Reg-F) and Reservation Function (Res-F) in order to gain access (e.g., authentication and authorization) to the network and to receive resources (e.g., a dynamic IP address). Interception of the subject CmII and CmC is available only after the subject has been identified in the network. Signaling prior to the identification of the subject in the network, or during the period when a subject's equipment has been placed in this "quarantine" state, cannot be intercepted as the subject has not been identified in the network.

4.2.5.2 Equipment Identifier

The subject is identified through an address or interface that uniquely identifies the subject's equipment or session. The intercept resulting from equipment identification may be based on information such as:

- MAC address or set of MAC addresses associated with the subject's equipment;
- Static IP addresses, which could be a single IP address, a set of IP addresses, or an IP subnet assigned to the subject's equipment;
- A physical or logical interface in the access provider's equipment assigned for the subject's equipment (e.g., circuit ID); or
- An ATM or Frame Relay Permanent Virtual Circuit assigned for the subject's equipment.

Note that in some cases the subject may be associated with multiple equipment identifiers.

When subject activity is identified in the network through equipment identification, login AACmII may not be available.

4.3 IAS Surveillance Model

Figure 4.7 depicts the IAS physical and functional surveillance model for addressing lawful intercept capabilities. The physical and functional components are separated into two domains: Subject Domain, IASP Domain. The IASP domain consists of the access network, intermediate network, and ISP network as discussed in 4.1. The figure indicates that one (or more) of the networks in the IASP domain may perform lawful intercept.

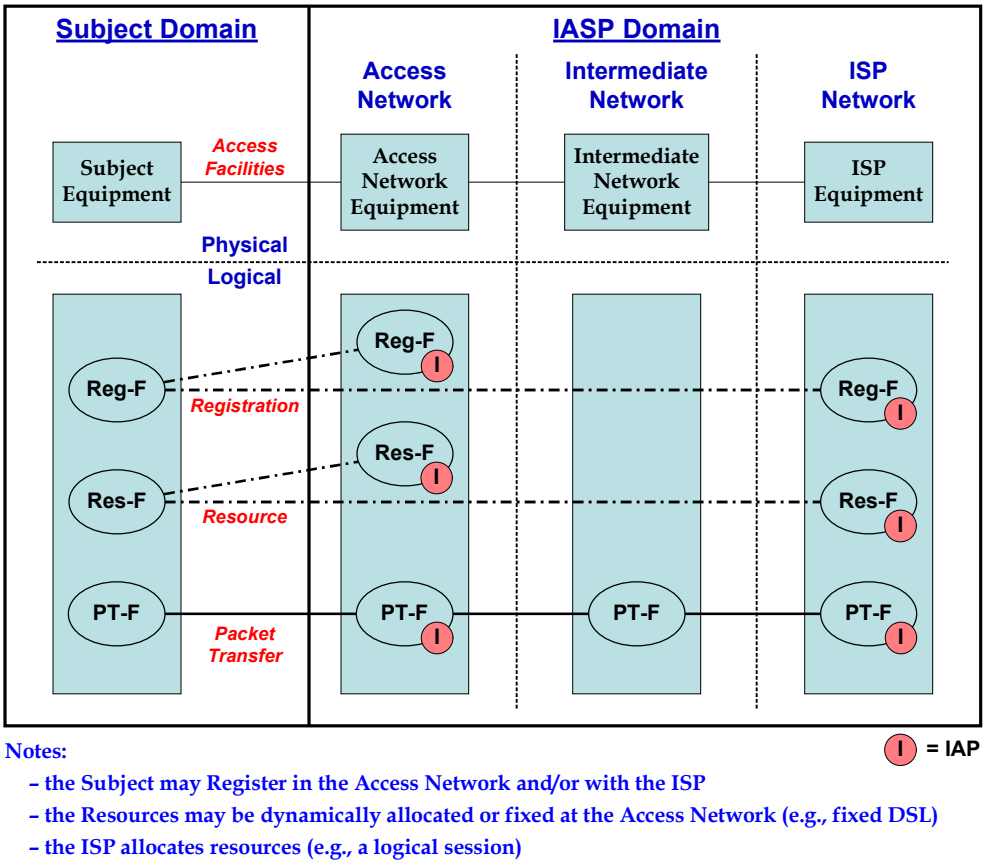


Figure 4.7 – IAS Surveillance Model

The domains consist of both physical and functional components which are of interest in determining and specifying the CmII and CmC to be reported and delivered to the law enforcement agencies.

Within the domains the following functions, described in 4.1 are of interest in providing the LI solution for IAS:

- Reg-F
- Res-F
- PT-F

A table showing a mapping of the LAES events defined in this document to the above functions can be found in 5.4.

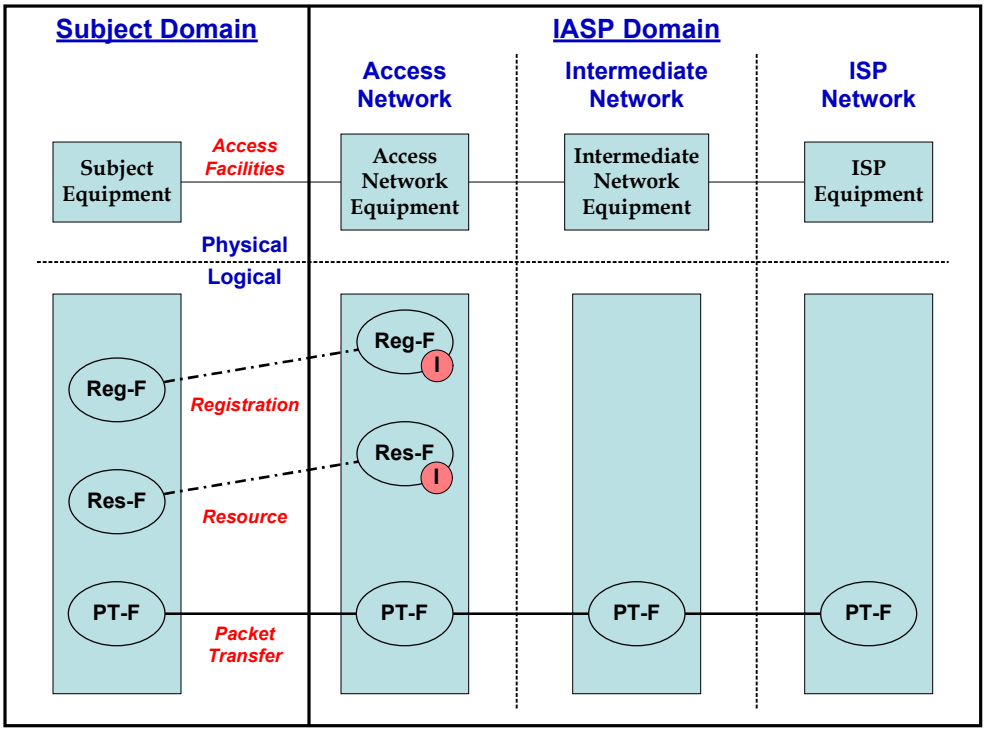
4.4 Intercept Scenarios

The following clauses depict availability of AACmII for various scenarios of Reg-F and Res-F deployment (i.e., whether the Access Network or the ISP Network performs the function).

In the following scenarios, CACmII and CmC are available in an Access Network or ISP Network that performs the PT-F.

4.4.1 Reg-F & Res-F Performed in the Access Network

In Figure 4.8, the Access Network performs the registration, resource reservation, and packet transfer functions. AACmII that may be reported by the Access Network includes both registration and resource reservation information. It should be noted the registration and resource reservation functions may be fixed, in which case no AACmII can be reported.

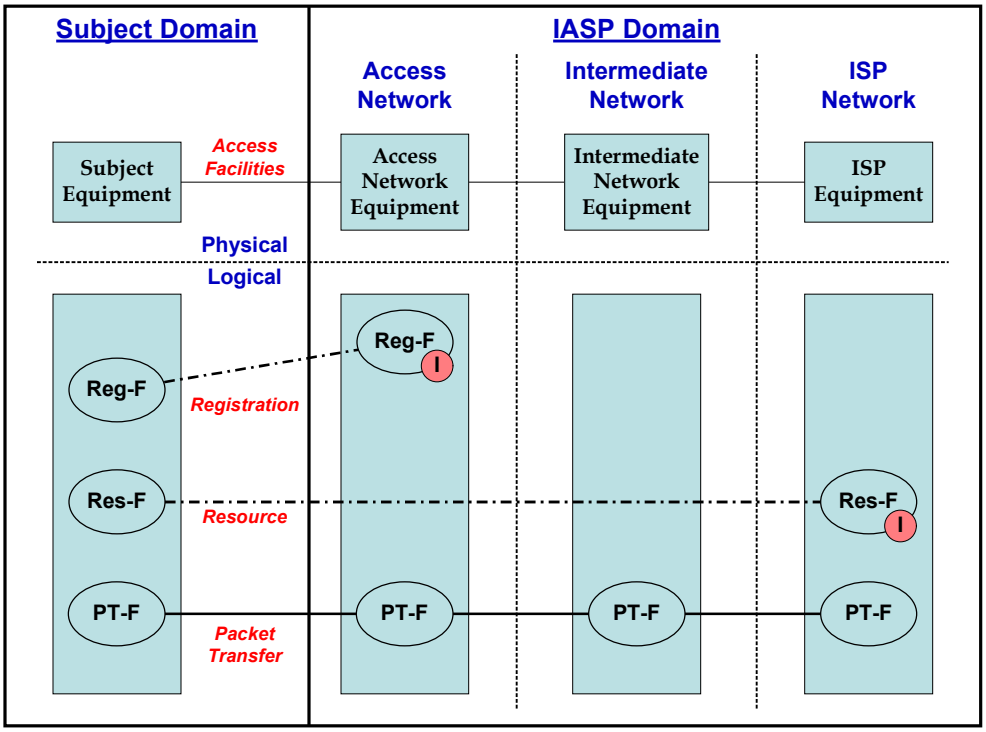


	Access Network	Intermediate Network	ISP Network
Access Associated CmII	Reg-F and Res-F related events		

Figure 4.8 – Registration and Resource Reservation in the Access Network

4.4.2 Reg-F Performed in the Access Network, Res-F Performed in the ISP Network

In Figure 4.9, the Access Network performs the registration function. The resource reservation function is performed by the ISP network. In this scenario the Access Network may provide AACmII associated with registration. It should be noted that registration may be fixed at installation of the service, and therefore cannot be reported. The ISP network performs the resource reservation function, and can report AACmII associated with the resource reservation function.

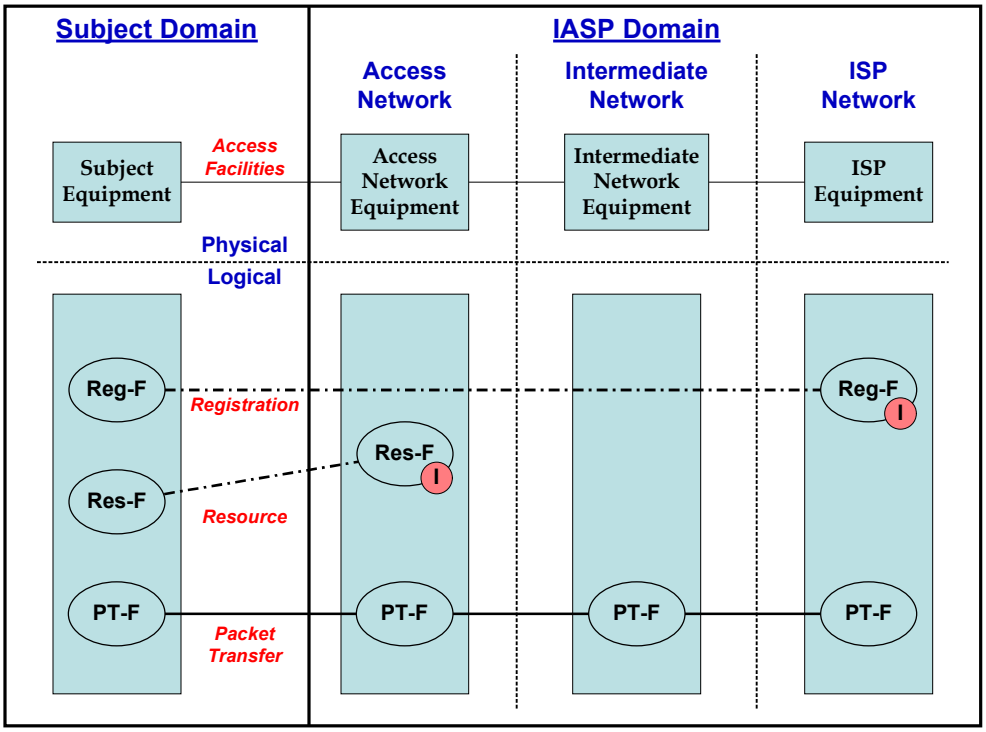


	Access Network	Intermediate Network	ISP Network
Access Associated CmII	Reg-F related events		Res-F related events

Figure 4.9 – Registration in the Access Network, Resource Reservation in the ISP Network

4.4.3 Res-F Performed in the Access Network, Reg-F Performed in the ISP Network

In Figure 4.10, the Access Network performs the resource reservation function. The registration function is provided by the ISP network. In this scenario, the Access Network may provide AACmII associated with the resource reservation function. The ISP network provides the registration function, and can report AACmII associated with the registration function. It should be noted that registration may be fixed at installation of the service, in which case registration AACmII cannot be reported.

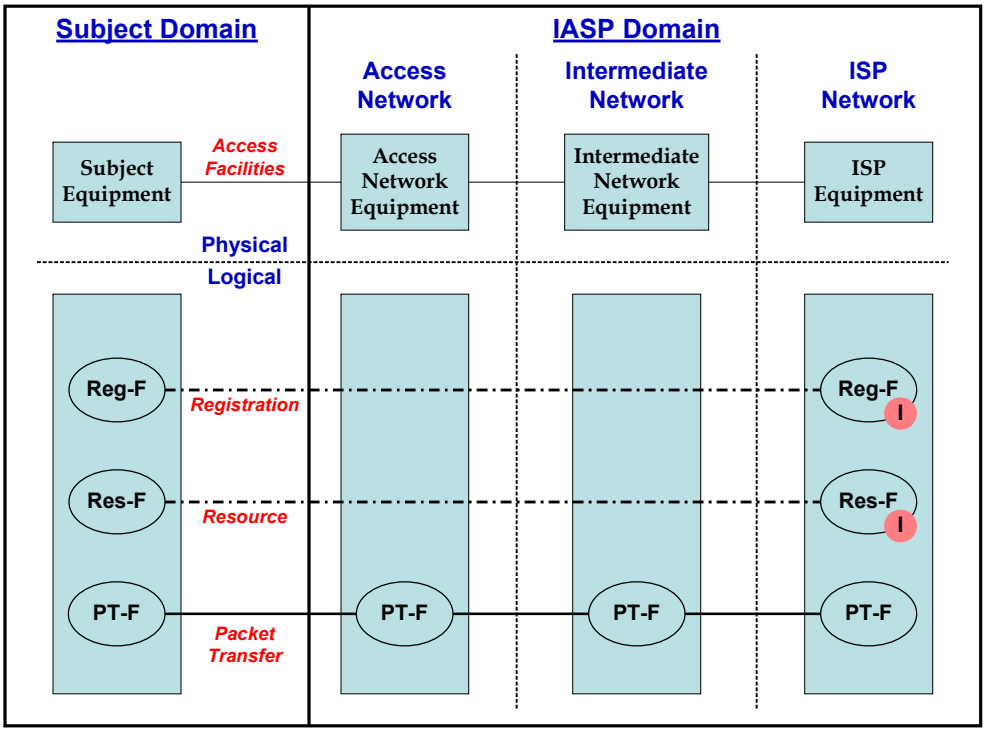


	Access Network	Intermediate Network	ISP Network
Access Associated CmII	Res-F related events		Reg-F related events

Figure 4.10 – Registration in the ISP Network, Resource Reservation in the Access Network

4.4.4 Reg-F & Res-F Performed in the ISP Network

In Figure 4.11, the Access Network performs only the packet transfer function. The registration function and resource reservation functions are provided by the ISP network. The ISP network performs the registration function, and can report AACmII associated with the registration function. It should be noted that registration may be fixed at installation of the service, in which case registration AACmII cannot be reported. The ISP network performs the resource reservation function, and can report AACmII associated with the resource reservation function.



	Access Network	Intermediate Network	ISP Network
Access Associated CmII			Reg-F and Res-F related events

Figure 4.11 – Registration and Resource Reservation Functions in the ISP Network

5 User Perspective (Stage 1)

5.1 Introduction

Clause 5 presents the user perspective (Stage 1) requirements for LAES for IAS. The user in this case is the LEA.

Clause 5.2 presents communication-related events that represent or generate communication-identifying information (termed "surveillance events"). Clause 5.3 presents general capabilities needed for LAES for IAS. Clause 5.4 describes the mapping of surveillance events to functions.

5.2 Surveillance Events

This clause presents surveillance events that cause CmII to be reported. These events support fixed wired access methods (e.g., DSL) as well as fixed wireless access methods (e.g., Wi-Fi®).

5.2.1 Access Attempt

This event occurs when a network registration has been attempted, as in the following case:

- The intercept subject or associated CPE network device – e.g., cable/DSL modem – successfully provides an appropriate form of unique identifying information – e.g., userID/password, Media Access Control (MAC) address – to an IASP's Authentication, Authorization, and Accounting (AAA) server (or other

equivalent functional entity). Access session parameters are negotiated. If the IASP allows multi-login, where the same user identity and password is used multiple times to establish multiple concurrent and distinct access sessions, separate Access Attempt events shall be reported for each session. Also, if users connect to the network using multi-link protocols[11] – e.g., Point-to-Point Protocol (PPP) multi-link protocol – where the same user identity and password are used to authenticate each channel, separate Access Attempt events shall be reported with an indication of a multi-link related login, if each channel is to be authenticated separately.

5.2.2 Access Accepted

This event occurs when the intercept subject or associated CPE network device has successfully authenticated with the network AAA (or functional equivalent) server, as in the following case:

- The intercept subject or associated CPE network device (e.g., cable/DSL modem) successfully provides some form of unique identifying information (e.g., userID/password, MAC address) that is verified and validated by an IASP's AAA server.

If the IASP allows multi-login, where the same user identity and password is used multiple times to establish multiple concurrent and distinct access sessions, separate Access Accepted events shall be provided for each session. Also, if users connect to the network using multi-link protocols (e.g., PPP multi-link protocol) where the same user identity and password are used to authenticate each channel, separate Access Accepted events shall be provided, with an indication of a multi-link related login, if each channel is authenticated separately.

5.2.3 Access Failed

This event occurs when network authentication has failed and an access session has not been successfully established, as in the following case:

- The user (the intercept subject or another person utilizing the CPE network device [e.g., cable/DSL modem] attributed to the intercept subject) provides incorrect identification or authentication information (e.g., userID/password combination, MAC address) to the IASP domain and is rejected by the IASP's AAA server. An access session is not established.

5.2.4 Access Session End

This event occurs when the intercept subject's access to the IASP domain has been disconnected and the access session is terminated, as in the following cases:

- The intercept subject initiates a disconnect request to the network; or
- The subscriber equipment experiences a loss of power.

5.2.5 Access Rejected

This event occurs when an intercept subject's login procedure (authentication or authorization) to the network is successfully completed, but the intercept subject's access attempt is rejected for other reasons, as in the following case:

[11] Multi-link protocols allow the user to establish several different physical connections to the IASP while allowing the IASP to correlate these sessions and treatment as "one" aggregate session.

- The Access Rejected message would be generated when a subject is already logged on, attempts a second login with a valid ID and password, but the network does not allow multiple logins.

5.2.6 Access Signaling Message Report

This event occurs when the IP network receives a signaling message from the intercept subject, sends a signaling message to the intercept subject, or sends or receives a signaling message on behalf of the intercept subject. This message is used to encapsulate and send these access signaling messages – e.g., Remote Authentication Dial In User Service (RADIUS[12]), Diameter[13] – detected in the network.

The Access Signaling Message Report is used in lieu of the access messages described in 5.2.1 through 5.2.5 and shall be triggered when any of the events are detected.

Appropriateness of the use of the Access Signaling Message Report for reporting AACmII depends on the interception and service architectures of the network.

5.2.7 Packet Data Session Start

This event occurs when a subject, or the subject's equipment, successfully completes any login process required by the network and whenever one or more IP addresses or subnets are assigned to the subject's equipment.

5.2.8 Packet Data Session Failed

This event occurs when an intercept subject's login procedure to the network is successfully completed, but the intercept subject is denied access to the network. An example of this is:

- When the IP addresses or other network resources to accommodate the subject's use of the network are not available.

5.2.9 Packet Data Session End

This event occurs when an intercept subject's equipment ends a packet data session with the network.

In cases in which the intercept is based on a subject's IP addresses or subnets that are allocated dynamically (see Clause 5.3.10), the Packet Data Session End event is considered to occur in the following cases:

- The IP address associated with a packet data session is explicitly released (e.g., by a DHCPRELEASE [Ref 17], PPPoE Active Discovery Terminate (PADT) [Ref 18], IPCP Terminate-ACK).
- The IP address associated with a packet data session is no longer assigned to the subject. This may include the following situations:
  - The IASP domain automatically drops a subject's session after a pre-established time period or inactivity period (e.g., DHCP lease expiration).
  - The IASP domain terminates the subject's session for other reasons (e.g., resource condition or administrative controls).
  - The device connected to the network experiences a power failure for a duration long enough that is sufficient to disrupt the subject's session.

---

[12] For more information, see IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*. This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[13] For more information, see IETF RFC 3588, *Diameter Base Protocol*. This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

- The intercept subject's equipment experiences disruption of connectivity (e.g., loss of physical layer or data link layer) for a sufficient time to cause termination of the subject's packet data session.

5.2.10 Packet Data Session Already Established

This event occurs when surveillance begins on an intercept subject's communications for any packet data session of the intercept subject that is already established[14], regardless of whether the intercept subject is actively transmitting or receiving packets, as in the following examples:

- Lawful electronic surveillance commences on an intercept subject who already has an established IAS session with the subscribed-to IASP (e.g., the login event may have occurred prior to surveillance starting), whether or not the intercept subject is actively transmitting or receiving packets at the time.
- Lawful electronic surveillance commences on an intercept subject who is identified by an equipment identifier (as described in 4.2.5.2).

5.2.11 Packet Data Header Report

This event is used to provide CACmII packet header reports on a per packet basis (non-summarized reporting). The event is triggered by each packet sent or received by the subject. The report provides source and destination information derived from the packet headers for each packet. IP addresses and the IP next-layer protocol are always reported. The flow label is reported if the packet is IPv6, and the layer-4 ports are reported if the IP protocol is TCP, UDP, SCTP [Ref 19], or DCCP [Ref 20].

5.2.12 Packet Data Summary Report

This event is used to provide CACmII summary reports. The event is triggered by the Packet Data Session End event and is triggered on an interim basis subsequent to the Packet Data Session Start event or Packet Data Session Already Established event. The report provides source and destination information derived from the packet headers and summary information for the number of packets transmitted or received by the subject for the source and destination pairs. IP addresses and the IP next-layer protocol are always reported. The flow label is reported if the packet is IPv6, and the layer-4 ports are reported if the IP protocol is TCP, UDP, SCTP, or DCCP.

When reported on an interim basis (i.e., prior to the interception of all packets of a packet data session), the reporting may be time-based (e.g., expiration of a timer), packet-count-based, report-size based (i.e., reaching a maximum number of source and destination pairs), or some combination of the above. Reports shall not be cumulative; that is, if an interim report is provided, the information in the next report begins at the time of the previous report.

Each summary item also contains the timestamps of the earliest (first) packet and last packet seen fitting the remainder of the description of the summary item. In the situation where only one packet is seen, both timestamps have the same value. By definition, a summary item would always have a packet count of one or more.

A Packet Data Summary Report should not be sent when there are no packets to report (i.e., no summary items).

The Packet Data Summary Report and Packet Data Header Report are mutually exclusive. At most, one is used per intercept. The Packet Data Summary Report is the alternative preferred by law enforcement.

Packet Data Summary Reports are reported per IAP.

---

[14] There are a number of approaches to determine whether the subject's packet data session has already been established. One approach is to obtain the subject's session status by contacting service provider's user login database (e.g., RADIUS log records). In this approach, the determination of Packet Data Session Already Established relies on the completeness of Res-F. In another approach, the IAP uses the equipment identification to identify the subject and intercepts the subject's packets.

5.3 General Capabilities

5.3.1 Subject Communications

The IASP shall insure that the complete communications (i.e., full packet stream to and from the subject's equipment under a full content order, or packet headers to and from the subject's equipment under an order that requires only the delivery of CmII) of the subject are intercepted.

5.3.2 Communications Delivery

Various delivery methods and associated technologies can be used to support the 'e' interface between an IASP and law enforcement. TCP is the protocol preferred by law enforcement for CmII and CmC delivery over the 'e' interface. If TCP is available, its use is assumed unless a different protocol is agreed to by the LEA and the TSP. If the DF and CF are not local to each other and if high-bandwidth CmC delivery is needed, the DF and CF may support multiple parallel TCP flows.

The format for delivery of CmII across the 'e' interface is specified in Annex A.1. The format for delivery of CmC across the 'e' interface is specified in Annex A.2.

Timing information includes two elements:

a) *Event Time-stamp*: Each surveillance message shall contain a time-stamp that is recorded within a specific amount of time from when the event triggering the surveillance message was detected (i.e., the time difference between the time the CmII triggering event was detected and the time recorded in the time-stamp).

b) *Event Timing*: Surveillance messages shall be sent to the LEA within a defined amount of time after the information pertaining to the CmII triggering event is available at the IAP.

The following timing requirements shall apply to the delivery of CmII:

- Each surveillance message shall be sent by the DF to the CF within eight (8) seconds of receipt by the IAP of the information pertaining to the CmII triggering event at least 95% of the time.
- Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CmII event triggering the surveillance message was detected. The time-stamp shall include a Greenwich Mean Time (GMT) offset, if available.

The following timing requirements shall apply to the delivery of CmC:

- Time-stamps shall be provided with encapsulated intercepted packets delivered to the CF.

5.3.3 Performance & Quality

The IASP shall be capable of performing multiple access intercepts per subject (e.g., two DSL connections).

The IASP shall be capable of performing intercepts on multiple subjects.

The IASP shall be capable of performing intercepts for multiple LEAs for the same subject. The intercepts shall not be detectable among LEAs.

The quality of the 'e' interface is driven by the negotiation between the IASP and the LEA.

5.3.4 Security & Reliability over the 'e' Interface

The equipment, facilities, or services for delivering CmII and CmC over the 'e' interface are procured by the LEA, and their specifications are outside the scope of this Standard. Security and reliability are a function of the equipment, facilities, or services procured (e.g., private line, public internet, point-to-point). The IASP shall offer a method (appropriate for the equipment, facilities, or services procured) to provide a high level of confidence that the intercepted CmII and CmC are delivered to the LEA securely and reliably.

5.3.5 Encryption & Compression

If the IASP uses encryption in the network, the IASP shall deliver the intercepted data to the LEA in unencrypted form or provide the encryption keys and specify the encryption method. If the intercepted data is available at the IAP in both encrypted form and unencrypted form, the IASP shall always provide it to the LEA in unencrypted form.

If the IASP uses compression in the network, the IASP shall deliver the intercepted data to the LEA in uncompressed form, or identify the means to decompress. If the intercepted data is available at the IAP in both compressed form and uncompressed form, the IASP shall always provide it to the LEA in uncompressed form.

5.3.6 Isolation

The IASP shall ensure that only authorized communications are intercepted, according to the surveillance order served.

The IASP shall ensure that only communications associated with the subject's equipment are intercepted. Communications not associated with the subject's equipment, facilities, or services shall not be delivered to the LEA.

5.3.7 Privacy & Authentication

The IASP shall not monitor or permanently record the subject communications.

The IASP shall ensure that the captured communication originates from or is directed to the subject's equipment, facilities, or service.

5.3.8 Transparency

The IASP shall perform the intercept in such a manner that the subject or the subject's terminal equipment cannot reasonably detect that the intercept is being performed. The subject's service parameters (bandwidth, latency, availability, reliability, etc.) shall not be impacted by the intercept in such a way that the surveillance is detectable. Note that replication of packets may cause some latency, but this latency should not be reasonably detectable by the subject.

5.3.9 Dynamic IP Address Management

This section applies to situations where packets are isolated based on IP addresses.

It is essential to track the assignment and release of dynamic IP addresses so the communications of the intercept subject are not missed and only the communications of the intercept subject are captured.

The Packet Data Session Already Established event (Clause 5.2.10) can report the current dynamic IP addresses of an intercept subject when the IASP determines that the subject has already been assigned dynamic IP addresses prior to the start of the intercept.

If the intercept subject is assigned multiple dynamic IP addresses from the network that can be released or reassigned individually, each such IP address should be treated as a separate packet data session.

5.4 Mapping of Surveillance Events to Functions

Table 5.1 depicts events which may be reported for each function.

Table 5.1 – LAES Events and Associated Functions

IAS Functions	LAES Events Reported when LI is enabled
Registration Function (Reg-F) (reports AACmII)	***Access Attempt*** ***Access Accept*** ***Access Reject*** ***Access Session End*** ***Access Failed*** ***Access Signaling Message Report***
Resource Function (Res-F) (reports AACmII)	***Packet Data Session Start*** ***Packet Data Session Failed*** ***Packet Data Session End*** ***Packet Data Session Already Established***
Packet Transfer Function (PT-F) (reports CACmII)	***Packet Data Header Report*** ***Packet Data Summary Report***

6 Network Perspective (Stage 2)

6.1 Introduction

This clause identifies messages, identifies and describes the information to be reported with each IAS CmII message, and also describes the application level CmC delivery format and associated delivery information.

6.1.1 Information Element Definitions for CmII Surveillance Messages

The following information elements appear in the tables:

6.1.1.1 Access Method: When known, identifies the method (e.g., cable modem, xDSL) used to gain access to the network resources, the connection-related CmII elements of the access session (e.g., subscriber interface equipment identification), and whether a multi-link login has occurred.

6.1.1.2 Access Session Characteristics: Identifies characteristics of the intercept subject's access session (e.g., bandwidth limits).

6.1.1.3 Access Session Identity: Uniquely identifies the intercept subject's network access session (e.g., PPP session) for a given surveillance.

6.1.1.4 Intercepted Signaling Message: The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject, which stimulated the sending of the Access Signaling Message Report message.

6.1.1.5 Case Identity: Identifies the intercept subject (remains constant for entire surveillance period). The value of the Case ID parameter is negotiated between the IASP and the LEA.

6.1.1.6 IAP System Identity: Identifies the system with the IAP.

6.1.1.7 IP Address Set: Identifies a set of IP addresses or IP subnets, and allocation method bound to the intercept subject's device for the duration of the IAS session.[15]

6.1.1.8 LEA CmC Delivery: If applicable, identifies the delivered content, the address of the LEA delivery interface where CmC associated with this event will be delivered, the protocol used to deliver the content, and the format of the content being delivered. The LEA CmC Delivery Interface Address includes a Correlation Identifier for correlating CmII to CmC.

6.1.1.9 Location Information: Location information identifies the location of the subject's terminal. When reasonably available and covered by the lawful authorization, location type and actual content of the location field shall be delivered to Law Enforcement.

The IASP shall provide all reasonably available geographical location information of the subject's terminal that is available in the network.

6.1.1.10 MOC: Mandatory, Optional, or Conditional.

6.1.1.11 Network Access Node Identity: Identifies the network node providing access to the intercept subject's equipment.

6.1.1.12 Packet Data Session Identity: Uniquely identifies the packet data session. This is used to correlate CACmII messages with each other, CmC messages with each other; and to correlate CACmII messages with AACmII messages pertaining to Res-F (Clause 5.4), or CmC messages with AACmII messages pertaining to Res-F.

6.1.1.13 Protocol Signal: The actual protocol signal stimulating the event (e.g., a RADIUS signal).

6.1.1.14 Reason for Termination: Identifies:

- The reason the intercept subject's access session was disconnected or terminated (e.g., normal/user-initiated logout, inactivity period threshold exceeded, access session duration limit or account access time limit exceeded, loss of access session) and whether it was initiated by the intercept subject or IASP, when known;
- The reason the AAA server denied access (e.g., incorrect password, invalid or suspended account, invalid subscriber interface equipment identification, unavailable resource);
- The reason the session establishment failed; or
- The reason the session was released.

6.1.1.15 Stream Set: Describes a set of IP packet stream properties.

6.1.1.16 Subscriber Identity: Uniquely identifies the subscriber to the service. This is the alias used by the IASP to identify the intercept subject (e.g., user ID, Service Account ID). There can be more than one form of identity used.

6.1.1.17 Time Stamp: Identifies the date and time that the event was detected.

6.1.1.18 Content Identifier: Correlates CmC to a packet data session. The content identifier and Packet Data Session Identity should be assigned the same value by using the same ASN.1 type (e.g., octet string).

6.1.1.19 Header Set: Describes the CACmII values of one intercepted packet.

[15] The allocation method may be reported as "not applicable" in cases in which the reporting IASP did not assign the IP address(es).

6.1.2 Correlating CmII

The Access Session Identity is used for correlating access session CmII. The Packet Data Session Identity is used for correlating packet data session CmII. When the Access Session Identity is present in a Packet Data message, it is used to correlate packet data session CmII to the access session CmII. See D.2 for correlating CmII with CmC.

6.2 CmII Messages

NOTE - In the following tables, the third column (Conditions) is only populated if the information element is Conditional (C).

6.2.1 Access Attempt Message

The *Access Attempt* message reports Access Associated CmII.

Table 6.1 – Information for Access Attempt Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Access Method	C	Provide when known.
Network Access Node Identity	C	Provide when known.
Protocol Signal	O	

6.2.2 Access Accepted Message

The *Access Accepted* message reports Access Associated CmII.

Table 6.2 – Information for Access Accepted Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Access Method	C	Provide when known.
Network Access Node Identity	C	Provide when known.
IP Address Set	C	Provide when known.
Access Session Identity	M	
Access Session Characteristics	C	Provide when known.
Location Information	C	Provide when reasonably available and lawfully authorized.
Protocol Signal	O	

6.2.3 Access Failed Message

The *Access Failed* message reports Access Associated CmII.

Table 6.3 – Information for Access Failed Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
IP Address Set	C	Provide when known.
Reason for Termination	C	Provide when known.
Protocol Signal	O	

6.2.4 Access Session End Message

The *Access Session End* message reports Access Associated CmII.

Table 6.4 – Information for Access Session End Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
IP Address Set	C	Provide when known.
Access Session Identity	M	
Reason for Termination	C	Provide when known.
Protocol Signal	O	
Location Information	C	Provide when reasonably available and lawfully authorized.

6.2.5 Access Rejected Message

The *Access Rejected* message reports Access Associated CmII.

Table 6.5 – Information for Access Rejected Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
IP Address Set	C	Provide when known.
Reason for Termination	C	Provide when known.
Protocol Signal	O	

6.2.6 Access Signaling Message Report Message

The *Access Signaling Message Report* message reports Access Associated CmII.

Table 6.6 – Access Signaling Message Report Parameters

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Access Session Identity	C	Include when possible.
Intercepted Signaling Message	M	

6.2.7 Packet Data Session Start Message

The *Packet Data Session Start* message reports Access Associated CmII. If there are multiple IP addresses to be reported, they should be reported as separate messages (separate packet data sessions).

Table 6.7 – Information for Packet Data Session Start Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Access Session Identity	C	Provide when known.
Packet Data Session Identity	M	
IP Address Set	M	
Access Session Characteristics	C	Provide when appropriate.
Location Information	C	Provide when reasonably available and lawfully authorized.
LEA CmC Delivery	C	Provide for content intercept.

6.2.8 Packet Data Session Failed Message

The *Packet Data Session Failed* message reports Access Associated CmII.

Table 6.8 – Information for Packet Data Session Failed Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Access Session Identity	C	Provide when known.
Reason for Termination	C	Provide when known.

6.2.9 Packet Data Session End Message

The *Packet Data Session End* message reports Access Associated CmII.

Table 6.9 – Information for Packet Data Session End Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Access Session Identity	C	Provide when known.
Packet Data Session Identity	M	
IP Address Set	M	
Reason for Termination	C	Provide when known.
Location Information	C	Provide when reasonably available and lawfully authorized

6.2.10 Packet Data Session Already Established Message

The *Packet Data Session Already Established* message reports Access Associated CmII. If there are multiple dynamically-assigned IP addresses to be reported, they should be reported as separate messages.

Table 6.10 – Information for Packet Data Session Already Established Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Access Session Identity	C	Provide when known.
Packet Data Session Identity	M	
IP Address Set	C	Provide when known.
Access Session Characteristics	C	Provide when known.
Location Information	C	Provide when reasonably available and lawfully authorized.
LEA CmC Delivery	C	Provide for content intercept.

6.2.11 Packet Data Header Report Message

The *Packet Data Header Report* message reports CACmII.

Table 6.11 – Information for Packet Data Header Report Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Header Set	M	

6.2.12 Packet Data Summary Report Message

The *Packet Data Summary Report* message reports CACmII.

Table 6.12 – Information for Packet Data Summary Report Message

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Stream Set	M	

6.3 CmC Delivery APDU

The CmC APDU encapsulates an individual communications content packet to or from an intercept subject for transfer to the LEA collection system on the delivery interface. It consists of a CmC Delivery Header followed by the content packet.

The CmC APDU contains the following parameters:

Table 6.13 – CmC APDU Parameters

Parameters	MOC	Usage
Correlation Information	M	Enables correlation of CmC and CmII.
Case Identity	M	Identifies the Intercept Subject, corresponding to the Case Identity parameter in the Packet Data Session Start or Packet Data Session Already Established message for the packet session.
IAP System Identity	M	Identifies the system containing the IAP.
Content Identifier	M	Identifies the packet session.
Time Stamp	M	The date and time that the content packet was intercepted.
Packet Direction	O	Indicates the direction of the intercepted packet (from the intercept subject, or to/toward the intercept subject).
Sequence Number	O	Provides sequencing of the CmC APDUs. See Clause 6.3.1.
Payload	M	The intercepted content packet. The payload shall contain the packet's bits at the network layer and above.

6.3.1 CmC Delivery APDU Sequence Number

The SequenceNumber parameter shall be used in the following way:

- The sequence number is initialized to zero for the first CmC APDU for each packet session of an Intercept Subject;
- The sequence number increases by one for each subsequent CmC APDU for the packet session.

The implementation may use a fixed size for the sequence number (e.g., 32-bit integer) and reset it to zero when it reaches its maximum positive value.

Annex A ASN.1 Definitions

(normative)

This annex provides the Abstract Syntax Notation One (ASN.1) [Ref 5] definitions for this Standard. CmII and CmC corresponding to ASN.1 definitions shall be encoded according to Basic Encoding Rules (BER) [Ref 16].

NOTE - This Annex has also been formatted as a separate plain text file and electronically packaged with this standard.

A.1 IAS CmII Abstract Syntax Module

```
IAS-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2015(2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CaseIdentity, TimeStamp
FROM Laesp-j-std-025-b
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-b(2) version-1(0)};

iAS-LAES-CmII-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2015(2)}

IasProtocol ::= SEQUENCE {
    iAS-LAES-CmII-Abstract-Syntax-Module-OID        OBJECT IDENTIFIER,
    iasMessage                                      IasMessage
}

IasMessage ::= CHOICE {
    access-Attempt                  [0] Access-Attempt,
    access-Accepted                 [1] Access-Accepted,
    access-Failed                   [2] Access-Failed,
    access-Session-End              [3] Access-Session-End,
    access-Rejected                 [4] Access-Rejected,
    access-Signaling-Message-Report [5] Access-Signaling-Message-Report,
    session-Start                   [6] Packet-Data-Session-Start,
    session-Failed                  [7] Packet-Data-Session-Failed,
    session-End             [8] Packet-Data-Session-End,
    session-Already-Established     [9] Packet-Data-Session-Already-Established,
    data-Header-Report              [10] Packet-Data-Header-Report,
    data-Summary-Report             [11] Packet-Data-Summary-Report
}

-- Message Definitions

Access-Attempt ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    accessMethod                    [4] AccessMethod                    OPTIONAL,
    networkAccessNodeIdentity       [5] NetworkAccessNodeIdentity       OPTIONAL,
    protocolSignal                  [6] ProtocolSignal                  OPTIONAL,
    ...
}

Access-Accepted ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
```

```
    accessMethod                    [4] AccessMethod                    OPTIONAL,
    networkAccessNodeIdentity       [5] NetworkAccessNodeIdentity       OPTIONAL,
    iPAddressSet                    [6] IpAddressSet                    OPTIONAL,
    accessSessionID                 [7] AccessSessionID,
    accessSessionCharacteristics    [8] AccessSessionCharacteristics    OPTIONAL,
    location                        [9] Location                        OPTIONAL,
    protocolSignal                  [10] ProtocolSignal                 OPTIONAL,
    ...
}

Access-Failed ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    iPAddressSet                    [4] IpAddressSet                    OPTIONAL,
    reasonForTermination            [5] ReasonForTermination            OPTIONAL,
    protocolSignal                  [6] ProtocolSignal                  OPTIONAL,
    ...
}

Access-Session-End ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    iPAddressSet                    [4] IpAddressSet                    OPTIONAL,
    accessSessionID                 [5] AccessSessionID,
    reasonForTermination            [6] ReasonForTermination            OPTIONAL,
    protocolSignal                  [7] ProtocolSignal                  OPTIONAL,
    location                        [8] Location                        OPTIONAL,
    ...
}

Access-Rejected ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    iPAddressSet                    [4] IpAddressSet                    OPTIONAL,
    reasonForTermination            [5] ReasonForTermination            OPTIONAL,
    protocolSignal                  [6] ProtocolSignal                  OPTIONAL,
    ...
}

Access-Signaling-Message-Report ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    accessSessionID                 [3] AccessSessionID                 OPTIONAL,
    signalingMsg                    [4] SET OF InterceptedSignalingMessage,
    ...
}

Packet-Data-Session-Start ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    accessSessionID                 [4] AccessSessionID                 OPTIONAL,
    packetDataSessionID             [5] PacketDataSessionID,
    iPAddressSet                    [6] IpAddressSet,
    accessSessionCharacteristics    [7] AccessSessionCharacteristics    OPTIONAL,
    location                        [8] Location                        OPTIONAL,
    deliveryInformation             [9] LEA-CmC-Delivery                OPTIONAL,
    ...
}

Packet-Data-Session-Failed ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    accessSessionID                 [4] AccessSessionID                 OPTIONAL,
```

```
    reasonForTermination            [5] ReasonForTermination            OPTIONAL,
    ...
}

Packet-Data-Session-End ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    accessSessionID                 [4] AccessSessionID                 OPTIONAL,
    packetDataSessionID             [5] PacketDataSessionID,
    iPAddressSet                    [6] IpAddressSet,
    reasonForTermination            [7] ReasonForTermination            OPTIONAL,
    location                        [8] Location                        OPTIONAL,
    ...
}

Packet-Data-Session-Already-Established ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriberIdentity              [3] SubscriberIdentity,
    accessSessionID                 [4] AccessSessionID                 OPTIONAL,
    packetDataSessionID             [5] PacketDataSessionID,
    iPAddressSet                    [6] IpAddressSet                    OPTIONAL,
    accessSessionCharacteristics    [7] AccessSessionCharacteristics    OPTIONAL,
    location                        [8] Location                        OPTIONAL,
    deliveryInformation             [9] LEA-CmC-Delivery                OPTIONAL,
    ...
}

Packet-Data-Header-Report ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    headerSet                       [3] HeaderSet,
    ...
}

Packet-Data-Summary-Report ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    streamSet                       [3] StreamSet,
    ...
}

-- Parameter Definitions

AccessMethod ::= SET OF SEQUENCE {
    accessType              [0] CHOICE
                            {
                                dialUp     [0] NULL,
                                dsl        [1] NULL,
                                lan        [2] NULL,
                                cable      [3] NULL,
                                wiFi       [4] NULL,
                                wiMax      [5] NULL,
                                other      [6] UTF8String
                            }                                           OPTIONAL,
    accessEquipmentID       [1] UTF8String                              OPTIONAL,
    partOfMultipleLogin     [2] NULL                                    OPTIONAL
}

IpAddressSet ::= SET OF SEQUENCE {
    address                 [0] IpAddress,
    allocationMethod        [1] CHOICE
                            {
                                static     [0] NULL,
                                dynamic    [1] NULL,
                                unknown    [2] NULL,
                                notApplicable [3] NULL
                            },
    prefixLen               [2] INTEGER                                 OPTIONAL
```

```
}

AccessSessionID ::= Value

AccessSessionCharacteristics ::= Value

ContentIdentifier ::= OCTET STRING

HeaderSet ::= SEQUENCE {
    packetDataSessionID       [0] PacketDataSessionID,
    sourceIPaddress           [1] IpAddress,
    destinationIPaddress      [2] IpAddress,
    protocol                  [3] INTEGER,
    sourcePortNumber          [4] INTEGER                                   OPTIONAL,
    destinationPortNumber     [5] INTEGER                                   OPTIONAL,
    iPv6FlowLabel             [6] INTEGER                                   OPTIONAL
    -- byteCount              [30] INTEGER                                  OPTIONAL
               -- Reserved - This value is reserved for use by Annex G of this Standard.
}

InterceptedSignalingMessage ::= SEQUENCE {
    messageType       [0] MessageType,
    message                   [1] Value
}

IAPSystemIdentity ::= VisibleString

IpAddress ::= CHOICE {
    ipV4                      [1] OCTET STRING(SIZE(4)),
    ipV6                      [2] OCTET STRING(SIZE(16))
}

LEA-CmC-Delivery ::= ContentIdentifier

Location ::= SET OF SEQUENCE {
    locationType              [0] UTF8String,
    location                  [1] UTF8String
}
MessageType ::= ENUMERATED {
    radius     (0),
    diameter   (1),
    xml        (2),
    asndot1    (3),
    other      (4)
}

NetworkAccessNodeIdentity ::= Value

PacketDataSessionID ::= Value

ProtocolSignal ::= SEQUENCE {
    protocol                  [0] Protocol,
    signal                    [1] SET OF Value
}

Protocol  ::=  CHOICE {
    radius                    [0] NULL,
    other                     [1] UTF8String
}

ReasonForTermination ::= Value

StreamSet ::= SET OF  SEQUENCE {
    packetDataSessionID       [0] PacketDataSessionID,
    sourceIPaddress           [1] IpAddress,
    destinationIPaddress      [2] IpAddress,
    packetCount       [3] INTEGER,
    protocol                  [4] INTEGER,
    sourcePortNumber          [5] INTEGER                                   OPTIONAL,
    destinationPortNumber     [6] INTEGER                                   OPTIONAL,
    iPv6FlowLabel             [7] INTEGER                                   OPTIONAL,
    firstPacketTimestamp      [8] TimeStamp,
    lastPacketTimestamp       [9] TimeStamp
    -- byteCount              [30] INTEGER                                  OPTIONAL
```

```
            -- Reserved - This value is reserved for use by Annex G of this Standard.
}

SubscriberIdentity ::= Value

Value ::= CHOICE {
    stringVS                [0] VisibleString,
    stringUTF8              [1] UTF8String,
    integer                 [2] INTEGER,
    octets                  [3] OCTET STRING,
    numeric                 [4] NumericString
}

END  -- of IAS-LAES-CmII-Abstract-Syntax-Module
```

A.2 IAS CmCC Abstract Syntax Module

```
IAS-LAES-CmCC-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmcc(1) version-2015(2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CaseIdentity, TimeStamp
FROM Laesp-j-std-025-b
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-b(2) version-1(0)}

IAPSystemIdentity, ContentIdentifier
FROM IAS-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2015(2)};

IAS-CC-APDU ::= SEQUENCE {
    cmcDeliveryHeader       [0] CMCDeliveryHeader,
    payload                 [1] OCTET STRING
}

CMCDeliveryHeader ::= SEQUENCE {
    correlationInfo         [0] SEQUENCE
                            {
                                caseId            [0] CaseIdentity,
                                iAPSystemId[1] IAPSystemIdentity,
                                contentIdentifier  [2] ContentIdentifier
                            },
    timestamp               [1] TimeStamp,
    packetDirection         [2] PacketDirection                         OPTIONAL,
    sequenceNumber          [3] INTEGER                                 OPTIONAL
}

PacketDirection ::= ENUMERATED {
    fromSubject(0),
    toSubject         (1)
}

END  -- of IAS-LAES-CmCC-Abstract-Syntax-Module
```

Annex B Reference Topologies

(informative)

This clause describes a number of reference network topologies, typically used for IAS over various types of access networks.

B.1 Dial-up Access

IAS over a switched telephony network is typically referred to as dial-up access. Figure B.1 shows the principal equipment involved in this kind of IAS. Note that the intercept in Figure B.1 is applied at the ISP Network, not at the Access Network[16].

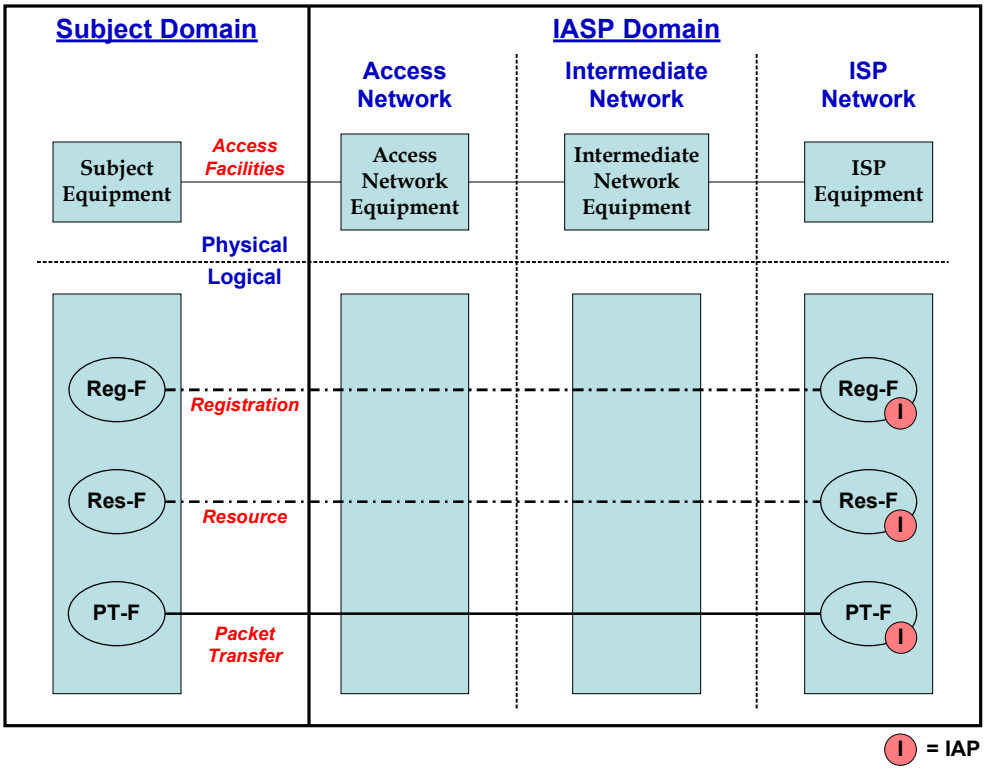


Figure B.1 – Dial-up Access

The CPE for dial-up access typically consists of a computer, laptop, or PDA that is equipped with a modem connected to the telephone network. Via this modem, the telephone number of the Network Access Server (NAS) of the IASP is dialed. The NAS answers the call and the NAS and the end-user typically establish a Point-to-Point Protocol (PPP) connection. Due to the distributed nature of dial-up access, a user may dial into any NAS in the network.

Once the PPP connection is established, the NAS will request the user to identify himself and to provide a password. The NAS will then request the AAA server in the IASP infrastructure (for dial-up access typically a RADIUS server) to perform the authentication based on the provided username and password.

[16] Note that dial-up surveillance solutions in Access Networks are not affected by this solution.

Additionally, the AAA server will check whether the user is authorized to use IAS. If so, the AAA server may provide the NAS with an IP address that is to be used by the subscriber. In other cases, the NAS allocates the IP address from a locally configured pool of addresses and the AAA server does not know the IP address at the time of authentication.

Next, the NAS informs the subscriber about the assigned IP address and other network configuration information, such as the address of the DNS server and/or the address of the gateway to the Internet. The CPE can now set-up its IP protocol stack and establish IP based communication with the Internet.

After the NAS has established a PPP session with the CPE, the NAS may provide the Accounting Server with information indicating the start of the session and the parameters in use for the session (e.g., IP address, NAS address).

The Accounting Server may be a physically separate server from the Authentication/Authorization server. In the case in which the NAS assigns IP addresses from a local pool, this is the first time the IP address assigned to the subject is known externally to the NAS.

At the end of the session, either when the subscriber logs off or when the connection to the NAS is lost, the NAS will provide the Accounting server with details regarding usage of the Internet connection (e.g., duration, bytes sent and received).

This information can be used for accounting purposes. From an LI perspective, the assignment of IP addresses, in relation to the subscriber they are assigned to, as well as the moment of release – i.e., the exchange of accounting information – are of interest.

> NOTE - Many IAPs also support tunneling the PPP session from the NAS to a home gateway either at another location within the IAP or residing on another network (e.g., another IAP or an enterprise). The standard protocol used to support this is Layer 2 Tunneling Protocol which tunnels the PPP frames from the NAS to the home gateway. Proprietary tunneling techniques may also be used based on the service provider. Many of the technologies described in the present document may be used to support the tunneling service (e.g., RADIUS); however, since this service is not an IAS as defined in the present document, it is outside the scope of the present document.

B.2 DSL Access

B.2.1 Example DSL Interception

Figure B.2 below shows example network architectures used in Broadband DSL markets. The example architectures depicted are based on the architectures in TR-59 from the DSL Forum[17]. The diagram has also been enhanced to show probable locations where lawful interception can take place.

In most cases it may be assumed that a *Broadband Remote Access Server (BRAS)* capable device is available in the network where interception can be done. According to the DSL Forum TR-59, a BRAS is defined as the aggregation point for the subscriber traffic. It provides aggregation capabilities (e.g., IP, PPP, ATM) between the Regional or Access Network and the ISP. Beyond aggregation, it is also the injection point for policy management and IP QoS in the Regional or Access Networks.

With regards to Figure B.2:

In the top Access Network, only ATM is available, and there are no BRAS capable devices in the network. In this case, the DSL connections are hauled straight to the ISP, and LI would have to be performed on the ATM switch in the access network. For LI reporting, this is similar to Case 1 in Annex F where the user is permanently connected to the network, and there is no further dynamic registration or resource allocation.

In the middle Access Network, only ATM is available, but this time there is a BRAS capable device. The ideal place for LI would be on the BRAS capable device. However it could still be done on the ATM switch. For LI, if the BRAS device is used, this is similar to case 2 or 3 in Annex F, depending if the user is in their home network or not. Typically there is at least a registration with the BRAS function, and optionally there may be resource allocation.

---

[17] Technical Report, DSL Forum, TR-059*, DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services,* September 2003. Available at < http://www.dslforum.org/techwork/treports.shmtl >.

In the bottom Access Network, Ethernet is used as the transport, and there is a BRAS capable device available. LI could be performed on this device. For LI, this is the same as the middle Access Network described above.

In each case it is assumed that the switch/BRAS is not capable of minimizing the data and of providing a proper "e" interface, and therefore the lawfully intercepted data is delivered to a Delivery Function. Of course should the ATM/BRAS device be capable of supporting an "e" interface, a Delivery Function device would not be required.

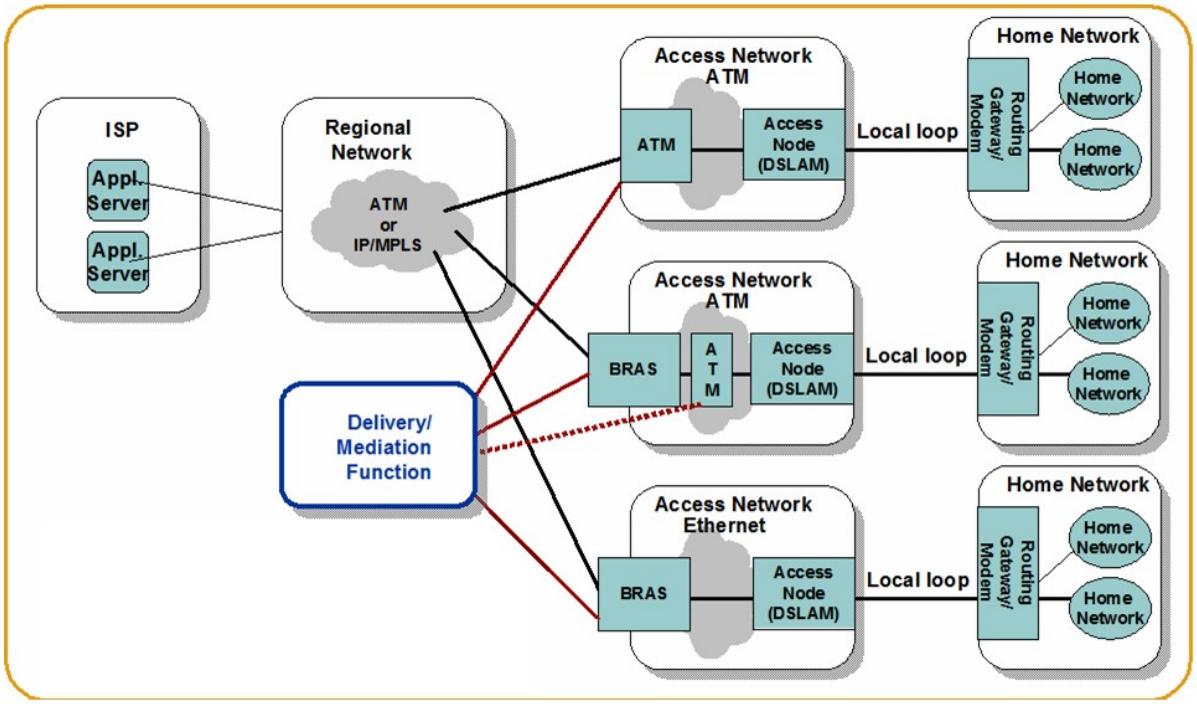


Figure B.2 – Example Interception on Fixed DSL

B.2.2 xDSL Access

IAS over the local loop by means of using specialized equipment for achieving a high bandwidth over copper wire is commonly referred to as xDSL Access. There is great variety of possible architectures and technologies that can be applied for realizing an xDSL network. Therefore, Figure B.3 only shows the principal equipment involved in this kind of IAS.

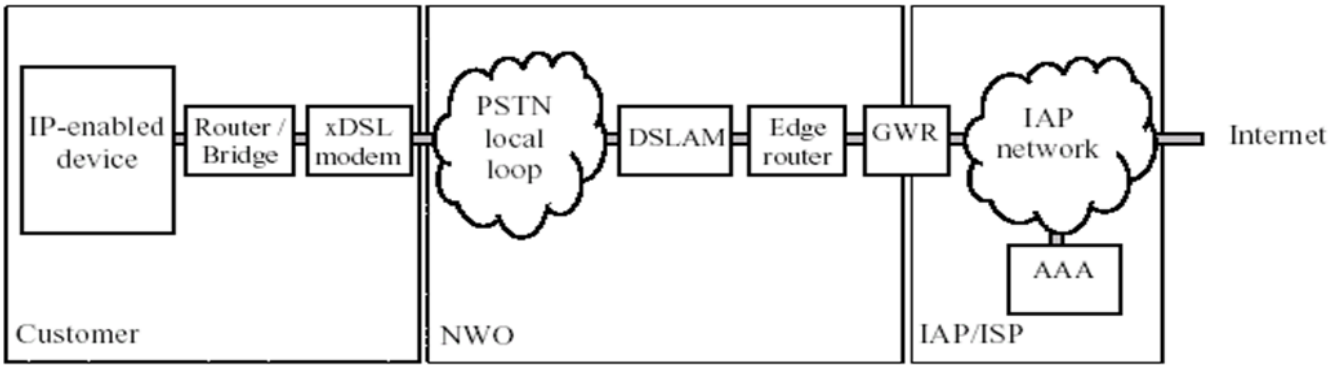


Figure B.3 – Example of xDSL Access

The CPE can consist of a single IP enabled device which is connected to an xDSL modem or, in order to support multiple IP enabled devices to share the xDSL connection, to a router or bridge that is connected to an xDSL modem.

The modem is connected to the copper wire of the telephone network, the local loop. In the telephone switch, this wire and wires from other xDSL lines are connected to the DSL Access Multiplexer (DSLAM). By utilizing frequencies above the telephone bandwidth, the xDSL modem and the DSLAM can encode more data to achieve a higher bandwidth than would otherwise be possible in the restricted frequency range of a PSTN network.

For large scale xDSL infrastructures, two main approaches are used for protocol layering: 1) *PPP over ATM (PPPoA)*; and 2) *PPP over Ethernet (PPPoE)*.

In the *PPPoA architecture*, a CPE router encapsulates IP packets into PPP frames and then segments them into ATM cells. The PPP link is commonly terminated at the Gateway Router (GWR) of the IASP, which concentrates PPP links from multiple Edge routers. The GWR routes the user's IP packets to their final destination. The GWR typically uses a RADIUS server to authenticate and authorize the user. A Dynamic Host Configuration Protocol (DHCP) server may be used to assign the IP address. A PPPoA implementation involves configuring the CPE router with username and password.

In the *PPPoE architecture*, at the user premises an Ethernet-to-WAN bridge is used as opposed to a router and the PPP session is established between the end user's computer and the GWR. PPPoE requires PPP client software to be installed on the user's computer. The client software initiates a PPP session by encapsulating IP packets into PPP frames into a MAC frames and then bridges the frames (over ATM/DSL) via the edge router to the GWR. From this point, PPP sessions can be established, authenticated, etc. As well as in the PPPoA architecture, the GWR typically uses a RADIUS server to authenticate and authorize the user and again DHCP may used to assign the IP address.

In the PPPoA architecture, the CPE router may keep the connection established, even if the user's computer has been shutdown. Therefore, in this architecture IP address assignment will happen very rarely; only once until either the router is shutdown or, if due to network or equipment failure, the connection is lost and re-established. In the PPPoE architecture, the IP address is assigned every time the user's computer logs on. In some cases the IAP will resort to assigning static IP addresses to xDSL users. When in this case the user establishes an IP connection, the IP address will still be assigned by means of a RADIUS and or DHCP server, but it will always be the same IP address. If this is the case, especially in combination with a PPPoA architecture, for LI purposes it is a lot easier to obtain a user's IP address from the IASP administration, rather than obtaining it from the network by technical means – e.g., capturing and interpreting RADIUS or DHCP traffic. If it is decided to resort to technical means for intercepting the IP address, for a timely start of the interception, it may be considered to bounce the user's connection in order to enforce assignment of a new IP address.

B.3 Cable Access

IAS over the cable network by means of using specialized equipment for achieving a high bandwidth over coaxial wire is commonly referred to as cable modem access. As in the case of xDSL, there is great variety of possible architectures and technologies that can be applied for realizing a cable modem network. Therefore, Figure B.4 only shows the principal equipment involved in this kind of IAS.

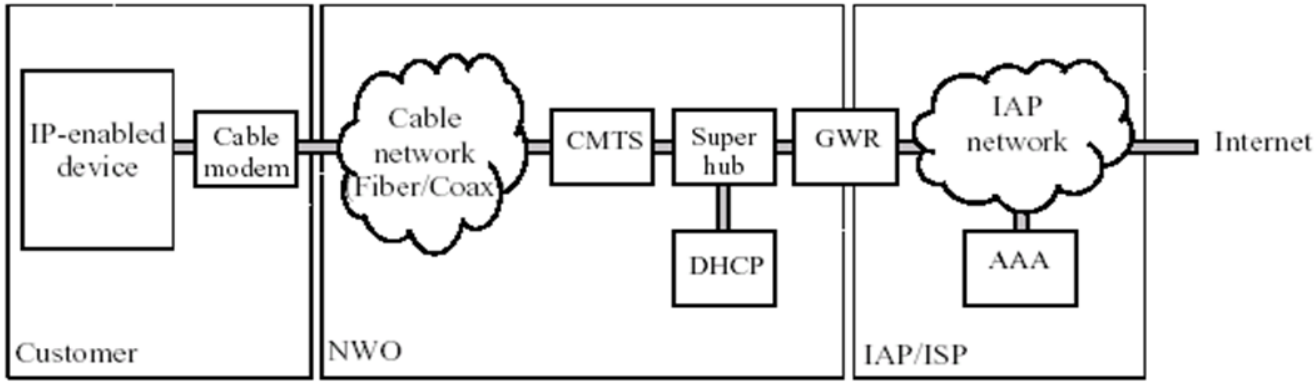


Figure B.4 – Cable Modem Access

The CPE typically consists of an IP enabled device connected to a cable modem via an Ethernet port. The cable modem connects to the Cable network using a coaxial cable. For downstream data, a cable modem is capable of receiving up to 36 Mbps of data. Upstream data is transmitted with data rates from 320 kbps up to 10 Mbps.

At the IASP end, the data channels are terminated at a Cable Modem Termination System (CMTS). This CMTS aggregates multiple cable modem channels and routes the user's IP packets, either over Ethernet or over ATM, into an IP network. Depending on the applied standards, network architecture and geographical factors, multiple CMTSs may be aggregated by a distribution hub, multiple distribution hubs by a super hub, and multiple super hubs by a Gateway Router.

Typically, IP addresses are assigned by means of DHCP based on the MAC address of either the cable modem or the users' computer, depending on applied standards and equipment, where either the computer or the cable modem will broadcast a DHCP request. The DHCP servers are typically distributed at the Super hub level and provisioned from a central location with the MAC addresses of authorized subscribers. Typically, IP addresses are assigned dynamically to most subscribers, but may be fixed for particular users. The latter may be assigned by means of DHCP as well. Also, the IAP may authenticate and authorize subscribers for the access service based on a username and password. Such additional authentication can also be used for the provision process – for example, when a user replaces his computer and therefore changes his MAC address. The AAA protocol used for this may be RADIUS or proprietary.

From an LI perspective, the AAA process is less relevant than the DHCP based IP address assignment. An interception solution in a cable modem environment will typically capture DHCP traffic in an attempt to identify a subscriber based on the MAC address of the equipment. The potential geographical spread of DHCP servers may become an issue, since this implies that the interception solution must therefore be distributed over a potentially large number of locations as well.

In some cases, the IASP may use PPPoE for access. This operation is similar to that described for xDSL.

B.4 Bonding of Multiple Access Links

Figure B.5 is an illustration of a subject with multiple links to the access network “bonded” to provide higher bandwidth. The links between the subject network and the access network can be dial-up, ISDN, xDSL, Cable, or

any other type of media. Bonding of multiple links requires a link layer protocol such as Multilink PPP (RFC 1990[18]) running on both the subject's router and the access provider's router.

Multilink PPP is a link local protocol, and does not pass beyond the access router. The subject's equipment may load balance and prioritize packets across all links in the multilink bundle. Packet fragmentation and priority queuing may also be configured depending upon individual link speeds. Packet re-assembly may be link local, or may be end-to-end. Packets transmitted to the subject may be processed in a similar manner, and distributed across all links in the multi-link bundle.

LI of multilink bundles may require each interface of the access router to be configured to intercept the subject packets to ensure all packets are captured. As re-assembly can be either link local, or end-to-end, fragmented packets must either be re-assembled prior to being passed to the LEA, or the information required to re-assemble the packets in the proper order must be included to allow the LEA to re-assemble the packets.

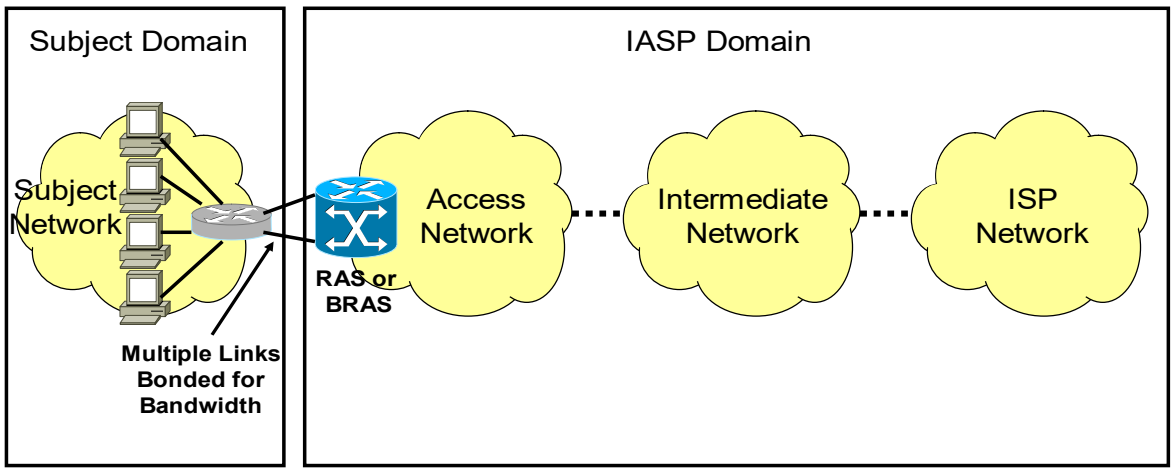


Figure B.5 – Example of multiple links between the Subject and the Access Network

[18] See IETF RFC 1990, *The PPP Multilink Protocol (MP)*. This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

Annex C Optional Messages

(informative)

The following parameters are used in this annex:

Primary Account Subscriber ID – If Subscriber Identity is not the account's primary subscriber, identifies the account number or other administrative identifier uniquely assigned to the primary account and the primary subscriber under whom the account is registered.

Server ID – The server the intercept subject is communicating with to request the change.

Changes Attempted – Identifies all added, deleted, or modified account/service information/attributes.

Result of Change Attempt – Identifies whether the service change request was accepted and implemented or refused. If refused, identifies the reason. If error occurs while processing request, identifies the error that occurred and the result (e.g., no change made).

VPN Security Association ID – Uniquely identifies the VPN Security Association within the public Internet Access and Services session (remains constant for entire VPN Security Association).

VPN Security Association Protocol(s) – Identifies the protocol(s) – e.g., Internet Protocol Security Internet Key Exchange, Point-to-Point Tunneling Protocol, Layer 2 Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE), etc. – and any associated information concerning the protocols (e.g., IPsec AH, etc.) used to establish and maintain the SA.

Local VPN Endpoint IP Address – Identifies the IP address (to include version) of the IASP domain system participating in the VPN SA.

Remote VPN Endpoint IP Address – Identifies the IP address (to include version) of the remote network system participating in the VPN SA.

Local VPN Encryption Algorithm(s) – Identifies the encryption algorithm(s) – e.g., Triple Data Encryption Standard, Encapsulating Security Payload, Rivest Cipher 4, Message Digest 5, Secure Hash Algorithm, etc. – used by the IASP domain system to encrypt the packets traversing the VPN tunnel.

Remote VPN Encryption Algorithm(s) – Identifies the encryption algorithm(s) – e.g., 3DES, ESP, RC4, MD5, SHA-1, etc. – used by the remote network system to encrypt the packets traversing the VPN tunnel.

VPN Encryption Key(s) – Identifies – by protocol(s) and/or algorithm(s) – the actual encryption key(s) the IASP and remote network systems used to encrypt the intercept subject's packets, when content surveillance is authorized and the content is transmitted to an LEA in the encrypted form.

VPN Termination Cause – If the VPN SA cannot be successfully established, identifies the error condition/reason.

Surveillance Status - The following are the possible surveillance statuses:

- *Inactive* – Surveillance is not being performed.
- *Active* – Surveillance is being performed. A surveillance is active between the activation and deactivation of the surveillance. The following are the two possible specific surveillance statuses for an active surveillance:
    - *Partially active* – ***Not all*** of the functionality (e.g., IAPs) needed to fully perform surveillance on an intercept subject is performing surveillance.
    - *Fully active* – ***All*** of the functionality (e.g., IAPs) needed to fully perform surveillance on an intercept subject is performing surveillance.
- *Unknown*.

C.1 Stage 2

C.1.1 Service Change

The Service Change event occurs when a registered account being used by an intercept subject has a service type or other service attribute(s) modified either by the IASP or a user (e.g., registered primary account holder or secondary user authorized to request/enact such service changes for the account) which may impact an intercept subject's ability to access a public IP network.

The Service Change event is considered to occur when either the intercept subject or the IASP:

- Adds a userID (subaccount) to an account.
- Drops a userID (subaccount) from an account.
- Deletes an existing account.
- Alters a userID.
- Modifies passwords or other authentication keys.
- Locks a userID's access for a period of time.
- Modifies the QoS parameters (e.g., service tier and associated Type of Service characteristics [e.g., Precedence of Data, Minimum Delay, Maximum Throughput, Maximum Reliability, Minimum Cost], bandwidth).
- Modifies the set of active or subscribed-to features (e.g., encryption).

Table C.1 – Information for Service Change Event

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Primary Account Subscriber Identity	C	Provide when known
Intercept Subject's IP Address	C	Provide when known
Server Identity	C	Provide when known
Changes Attempted	M	
Result of Change Attempt	M	

C.1.2 Virtual Private Network (VPN) Security Association Establishment

The VPN Security Association Establishment event occurs when a VPN connection is established between an intercept subject host and a destination host using an IASP VPN system as the intercept subject's VPN endpoint.

> NOTE – A VPN connection can be established in a tunneling mode whereby only the endpoints – the intercept subject host and a destination host – participate in the set up of the protected SA and exchange encrypted IP packet payloads. All intermediary network elements (the IASP in this case) see only the source and destination IP addresses of the endpoints in the unencrypted IP headers, but the port addresses remain hidden within the encrypted packet contents. However, if an IASP system participates in the VPN connection establishment (transport mode VPN) on behalf of the intercept subject, the event and associated information can be detected by the IASP.

A VPN Security Association Establishment event is considered to occur in the following case:

- The intercept subject establishes a (transport mode) VPN with participation of an IASP VPN network system.

Table C.2 – Information for VPN Security Association Establishment

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Session ID	C	Provide when known
Subscriber ID	C	Provide when known
Access Session IP Address	C	Provide when known
VPN Security Association ID	M	
VPN Security Association Protocol(s)	M	
Local VPN Endpoint IP Address	M	
Remote VPN Endpoint IP Address	M	
Local VPN Encryption Algorithm(s)	M	
Remote VPN Encryption Algorithm(s)	M	
Local VPN Encryption Key(s)	M	
Remote VPN Encryption Key(s)	M	

C.1.3 Virtual Private Network (VPN) Security Association Release

The VPN Security Association Release event occurs when a VPN connection that was established by an IASP domain system on behalf of the intercept subject supporting protected IP communications with a remote IP address terminates.

The VPN Security Association Release event is considered to occur in the following cases:

- Either the local or remote end of the VPN end the Security Association.
- The VPN SA is terminated due to inactivity or an error.

Table C.3 – Information for VPN Security Association Release

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Session ID	C	Provide when known
Subscriber ID	C	Provide when known
Access Session IP Address	C	Provide when known
VPN Security Association ID	M	
VPN Termination Cause	M	

C.1.4 Surveillance Activation

The Surveillance Activation event occurs when the IASP activates a surveillance for an intercept subject for a particular LEA, based on the authorization submitted to the IASP by the LEA.

When the surveillance activation occurs, the surveillance could have a *fully active or partially active status*.

The Surveillance Activation event is considered to occur in the following case:

- The IASP activates surveillance for a particular intercept subject for a particular LEA.

Table C.4 – Information for Surveillance Activation

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Surveillance Status	M	

C.1.5 Surveillance Continuation

The Surveillance Continuation event occurs when the IASP periodically reports the status of an ongoing, *active* surveillance to an LEA. At the time of reporting, an *active* surveillance could have a *fully active* status (if surveillance is being fully performed) or *partially active* status (if surveillance is being partially performed). This event occurs periodically, and occurs individually for every *active* surveillance (and only for *active* surveillances).

The IASP could perform this reporting at the same time (but individually) for every *active* surveillance or when an independently tracked period ends for each *active* surveillance.

The Surveillance Continuation event is considered to occur in the following case:

- At the end of every period for which the IASP is to report the status of an *active* surveillance. The period shall be provisionable in one hour increments, with an upper bound of 24 hours.

Table C.5 – Information for Surveillance Continuation

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Surveillance Status	M	

C.1.6 Surveillance Change

The Surveillance Change event occurs when a change is made to the status of an active surveillance. Specifically, the event occurs then the status changes from *fully active* to *partially active* or from *partially active* to *fully active*. A variety of conditions (e.g., failure/recovery of an IAP) could cause the change in status.

The Surveillance Change event is considered to occur in the following cases:

- A *fully active* surveillance becomes *partially active*.
- A *partially active* surveillance becomes *fully active*.

Table C.6 – Information for Surveillance Change

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Surveillance Status	M	

C.1.7 Surveillance Deactivation

The Surveillance Deactivation event occurs when the IASP deactivates a surveillance for an intercept subject for a particular LEA (i.e., the status of the surveillance has become *inactive*), based on the authorization submitted to the IASP by the LEA.

The Surveillance Deactivation event is considered to occur in the following case:

- The IASP deactivates surveillance for a particular intercept subject for a particular LEA.

Table C.7 – Information for Surveillance Deactivation

Information Element	MOC	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	

C.2 IAS CmII Optional Messages Abstract Syntax Module

The same ASN.1 encoding as in Annex A is used.

```
IAS-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii-optional(2) version-2015(2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CaseIdentity, TimeStamp
FROM Laesp-j-std-025-b
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-b(2) version-1(0)}

IAPSystemIdentity, IpAddressSet
FROM IAS-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2015(2)};

iAS-LAES-CmII-Optional-Messages-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii-optional(2) version-2015(2)}

IasOptionalProtocol ::= SEQUENCE {
    iAS-LAES-CmII-Optional-Messages-Abstract-Syntax-Module-OID     OBJECT IDENTIFIER,
    iasOptionalMessage                                             IasOptionalMessage
}

IasOptionalMessage ::= CHOICE {
    serviceChange                   [0] ServiceChange,
    vpnSecurityEstablishment        [1] VPNSecurityEstablishment,
```

```
    vpnSecurityRelease              [2] VPNSecurityRelease,
    surveillanceActivation          [3] SurveillanceActivation,
    surveillanceContinuation        [4] SurveillanceContinuation,
    surveillanceChange              [5] SurveillanceChange,
    surveillanceDeActivation        [6] SurveillanceDeActivation
}

-- Message Definitions

ServiceChange ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    subscriber                      [3] SubscriberIdentity,
    primaryAccountSubscriber        [4] SubscriberIdentity              OPTIONAL,
    interceptSubjectsIPAddressSet   [5] IpAddressSet                    OPTIONAL,
    serverIdentity                  [6] ServerIdentity                  OPTIONAL,
    changesAttempted                [7] ChangesAttempted,
    resultofChangeAttempt           [8] ResultofChangeAttempt,
    ...
}

VPNSecurityEstablishment ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    sessionID                       [3] SessionIdentity                 OPTIONAL,
    subscriber                      [4] SubscriberIdentity              OPTIONAL,
    accessSessionIPAddressSet       [5] IpAddressSet                    OPTIONAL,
    vpnSecurityAssociation          [6] VPNSecurityAssociationIdentity,
    vpnSecurityAssociationProtocols [7] VPNSecurityAssociationProtocols,
    localVPNEndpointIPAddressSet    [8] IpAddressSet,
    remoteVPNEndpointIPAddressSet   [9] IpAddressSet,
    localVPNEncryptionAlgorithms    [10] LocalVPNEncryptionAlgorithms,
    remoteVPNEncryptionAlgorithms   [11] RemoteVPNEncryptionAlgorithms,
    localVpnEncryptionKeys          [12] VPNEncryptionKeys,
    remoteVpnEncryptionKeys         [13] VPNEncryptionKeys,
    ...
}

VPNSecurityRelease ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    sessionID                       [3] SessionIdentity                 OPTIONAL,
    subscriber                      [4] SubscriberIdentity              OPTIONAL,
    accessSessionIPAddressSet       [5] IpAddressSet                    OPTIONAL,
    vpnSecurityAssociation          [6] VPNSecurityAssociationIdentity,
    vpnTerminationCause             [7] VPNTerminationCause,
    ...
}

SurveillanceActivation ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    surveillanceStatus              [3] SurveillanceStatus,
    ...
}

SurveillanceContinuation ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    surveillanceStatus              [3] SurveillanceStatus,
    ...
}

SurveillanceChange ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    surveillanceStatus              [3] SurveillanceStatus,
    ...
```

```
}

SurveillanceDeActivation ::= SEQUENCE {
    caseId                          [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity,
    timestamp                       [2] TimeStamp,
    ...
}

-- Parameter Definitions

ChangesAttempted ::= UTF8String
LocalVPNEncryptionAlgorithms::= UTF8String
RemoteVPNEncryptionAlgorithms ::= UTF8String
ResultofChangeAttempt ::= UTF8String
ServerIdentity ::= UTF8String
SessionIdentity ::= UTF8String
SubscriberIdentity ::= UTF8String
SurveillanceStatus ::= UTF8String
VPNEncryptionKeys ::= SET OF UTF8String
VPNSecurityAssociationIdentity ::= UTF8String
VPNSecurityAssociationProtocols ::= SET OF UTF8String
VPNTerminationCause ::= UTF8String

END  -- of IAS-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
```

Annex D IAS Intercept Information Flow Example

(informative)

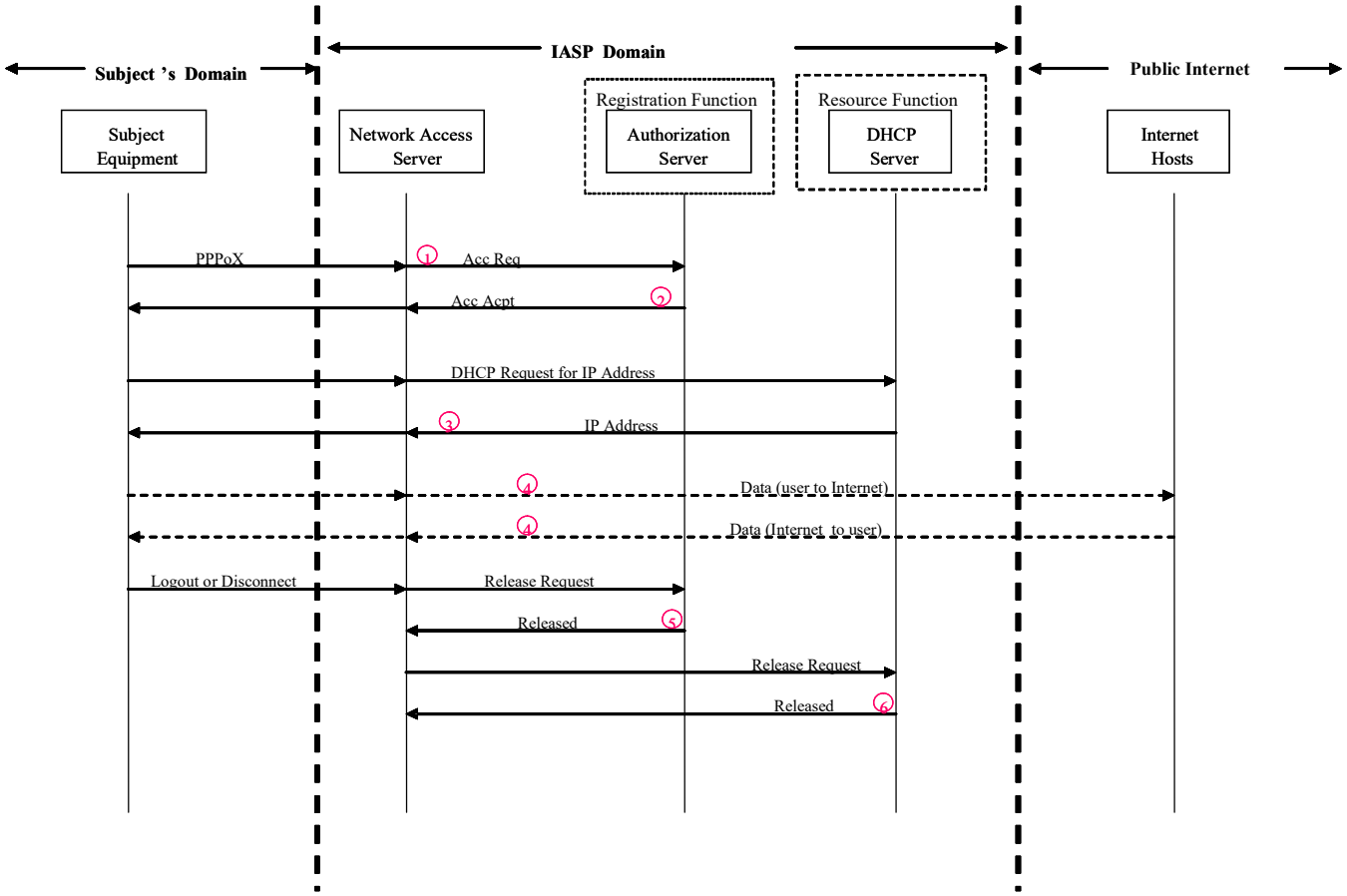


Figure D.1 – Internet Access and Services Events and Associated LAES Reporting

1. The subject establishes a session with the network for purposes of authorization to access network services. An example would be a PPP session established to a broadband access server. An *Access Attempt* LAES message is reported from the DF to the CF.

Not all access methods will require the subject to login. This event and message are applicable only to those methods requiring the subject to login.

2. The subject's access attempt is authorized by the network authorization server. This event triggers the reporting of the *Access Accepted* LAES message from the DF to the CF.

Not all access methods will require the subject to login. This event and message are applicable only to those methods requiring the subject to login.

2a. If the subject's access login attempt fails to be authorized, the *Access Rejected* LAES message is reported from the DF to the CF.

Not all access methods will require the subject to login. This event and message are applicable only to those methods requiring the subject to login.

3. An IP address allowing access to the public Internet is assigned to the subject. This event triggers the reporting of the *Packet Data Session Start* LAES message from the DF to the CF.

3a. If the subject successfully completes the login process, but the process of assigning an IP address is not completed (e.g., IP address pool exhausted, or subject disconnects prior to assignment completion), the *Packet Data Session Failed* LAES message is reported from the DF to the CF.

3b. If the packet data session state has been established (e.g., IP address successfully assigned) prior to the establishment of the surveillance, the *Packet Data Session Already Established* LAES message is reported from the DF to the CF.

4. The subject transmits or receives content packets to or from the public Internet.

4a. If the lawful authorization includes content, the content packets including the IP packet headers, are formatted for delivery, and CmC is sent from the DF to the CF.

4b. If the lawful authorization does not include content, CACmII shall be delivered per 6.2.11, *Packet Data Header Report Message*, or 6.2.12, *Packet Data Summary Report Message*, and sent from the DF to the CF.

5. The subject logs out from the network, or the connection between the subject and the network is interrupted such that the service provider's access equipment views the subject equipment as disconnected or timed out. This event triggers the reporting of the *Access Session End* LAES message from the DF to the CF.

Not all access methods will require the subject to login. This event and message are applicable only to those methods requiring the subject to login.

6. The subject's IP address is released per reasons described in 5.2, *Surveillance Events.* This event triggers the reporting of the *Packet Data Session End* LAES message from the DF to the CF.

Annex E IAS Cases & CmII Reporting

(informative)

Due to a variety of architecture scenarios, the IAS functions listed in this Standard will not always be available within a particular domain and the CmII available will vary. Table E.1 identifies the CmII which may be reported for various cases.

Table E.1 – Example IAS Cases and CmII Reporting

	Case 1	Case 2	Case 3	Case 4
Function	**Access Network Fixed**	**Access Network Fixed Registration**	**Access Network Dynamic Registration**	**ISP Dynamic Registration**
Registration Function (Reg-F)				
Access Attempt	**No**	**Yes**	**Yes**	**Yes**
Access Accept	**No**	**Yes**	**Yes**	**Yes**
Access Reject	**No**	**Yes**	**Yes**	**Yes**
Access Session End	**No**	**Yes**	**Yes**	**Yes**
Access Failed	**No**	**Yes**	**Yes**	**Yes**
Access Signaling Message Report	**No**	**Yes**	**Yes**	**Yes**
Resource Function (Res-F)				
Packet Data Session Start	**No**	**No**	**Yes**	**Yes**
Packet Data Session Failed	**No**	**No**	**Yes**	**Yes**
Packet Data Session End	**No**	**No**	**Yes**	**Yes**
Packet Data Session Already Established	**Yes**	**Yes**	**Yes**	**Yes**
Packet Transfer Function (PT-F)				
Packet Data Header Report	**Yes**	**Yes**	**Yes**	**Yes**
Packet Data Summary Report	**Yes**	**Yes**	**Yes**	**Yes**

Note that the ability to report LI events as shown in Table E.1 is equipment, architecture, and network dependent and the reporting of these events may not be technically feasible in all cases.

Case 1: CmII reported at the Access Network when no Registration or Resource Allocation

In this case the Access Network provides fixed facilities to the subject (e.g., DSL) and there is no dynamic Registration or Resource allocation process at the Access Network. When the intercept is applied at the Access Network, a CmII message is sent to the LEA(s) indicating intercept has started on active facilities of the subject. When the intercept is ended, a message is sent indicating the intercept has stopped on the subject's active resources.

Case 2: CmII reported at the Access Network with Registration but no Resource Allocation

In this case the Access Network provides fixed facilities to the subject (e.g., DSL), and there is a dynamic Registration of the equipment (e.g., PC) with the Access Network. When the intercept is applied at the Access Network, a CmII message is sent to the LEA(s) indicating intercept has started on active facilities of the subject.

When the equipment is activated, the equipment registers with the Access Network. If there is a de-registration, a message is sent indicating the subject (i.e., subject's equipment) has de-registered from the Access Network. When the intercepted is ended, a message is sent indicating the intercept has stopped on the subject's active resources.

Case 3: CmII reported at the Access Network with Registration and Resource Allocation

In this case the Access Network dynamically allocates or associates facilities to the subject (e.g., nomadic), and there is a dynamic Registration of the subject or equipment (e.g., PC) with the Access Network. The intercept is applied at the Access Network before the subject registers for service and resources are allocated and thus there are no active facilities associated with the subject (i.e., no need for reporting intercept started on active resources of the subject). When the subject subsequently registers for service and is allocated resources, CmII messages are sent to the LEA(s) indicating subject registration and resource allocation. When resources are de-allocated a CmII message is sent to the LEA(s). If the subject de-registers, a CmII message is sent to the LEA(s).

Case 4: CmII reported at the ISP with Registration and Resource Allocation

In this case the ISP dynamically allocates or associates facilities to the subject and there is a dynamic Registration of the subject (e.g., Login) with the ISP. The intercept is applied at the ISP before the subject registers for service and resources are allocated and thus there is no active facility associated with the subject (i.e., no need for reporting intercept started on active resources of the subject). When the subject subsequently registers for service and is allocated resources (e.g., a logical session), CmII messages are sent to the LEA(s) indicating subject registration and resource allocation. When resources are de-allocated a CmII message is sent to the LEA(s). If the subject de-registers, a CmII message is sent to the LEA(s).

Annex F Byte Count Reporting in an IAS LAES Environment

(informative)

F.1 Introduction

This Standard specifies two methods for delivering CACmII to the LEA: the Packet Data Header Report and the Packet Data Summary Report. This Annex specifies how byte count of IP packets is to be reported in a Packet Data Header Report and a Packet Data Summary Report (i.e., in addition to the other IP layer-3 and layer-4 information included in these messages).

Events that trigger reporting of the Packet Data Header Report or the Packet Data Summary Report shall instead trigger reporting of the Packet Data Header Report or the Packet Data Summary Report as specified in this Annex.

Creation of this Annex is premised upon the understanding that byte count in the Packet Data Header Report is not currently part of the safe harbor CALEA requirements. This Annex makes no representation regarding byte count information being provided pursuant to a lawful authorization that does not include a full content intercept.

Any requirements or standards language (i.e., “shall”, “should”) is used strictly in the context of ensuring that this Annex is inherently sound and provides appropriate guidance to voluntary implementers.

F.1.1 Scope & Purpose

This Annex specifies LAES capability of reporting byte count in the Packet Data Header Report and Packet Data Summary Report messages in an IAS environment.

F.1.2 Application

An IASP currently provides byte count data as part of a full content intercept. There is an LEA need to obtain byte count information associated with an intercept subject’s electronic communications, pursuant to a lawful authorization that does not include a full content intercept (e.g., a pen-register order). The subject may have engaged in many different types of packet data sessions. Byte counts, together with other Internet Protocol (IP) header information – such as IP addresses and port numbers – could help the LEA in determining the types of sessions in which the subject was engaged to enable the LEA to focus investigations on specific sessions. Therefore, there is a need to incorporate byte count data in packet header information reported to the LEA when lawfully authorized.

F.1.3 Byte Count

The integer value contained in the Total Length field of the IP header if the packet is IPv4 [Ref 9], or Payload Length field of the IP header if the packet is IPv6 [Ref 10].

F.1.3.1 Total Byte Count

The sum of the byte counts for all packets included in the packet count for a packet data session.

F.2 Byte Count Reporting Capability

When byte count reporting is utilized, the Packet Data Header Report (Clause 5.2.11) and Packet Data Summary Report (Clause 5.2.12) shall apply.

Events that trigger reporting of the Packet Data Header Report shall trigger reporting of the Packet Data Header Report with the inclusion of an additional parameter as specified in Clause F.3.1 below.

Events that trigger reporting of the Packet Data Summary Report shall trigger reporting of the Packet Data Summary Report with the inclusion of an additional parameter as specified in Clause F.3.2 below.

F.2.1 Packet Data Header Report

The Packet Data Header Report provides the CACmII on a per packet basis. The Packet Data Header Report is triggered by each packet of a packet stream sent or received by the intercept subject. The Header Set parameter in the Packet Data Header Report message shall include the number of bytes (byte count) that are transferred in each packet. The byte count reported is the number contained in the Total Length field of the packet header if the packet is IPv4 [Ref 3], or Payload Length field of the packet header if the packet is IPv6 [Ref 4]. The byte count is in addition to all the information that is reported in the Packet Data Header Report.

F.2.2 Packet Data Summary Report

The Packet Data Summary Report provides CACmII in a summarized format. The Stream Set parameter in the Packet Data Summary Report message shall include the total byte count for a packet data session. Total byte count is the sum of the byte counts for all packets included in the packet count for a packet data session. The total byte count is in addition to all the information that is reported in the Packet Data Summary Report.

F.3 Byte Count Reporting Abstract Syntax Notation

F.3.1 Byte Count Reporting Abstract Syntax Notation - Packet Data Header Report

In conjunction with the Packet Data Header Report, the “byteCount” shall be inserted into the HeaderSet parameter.

```
    byteCount                [30] INTEGER                                    OPTIONAL
```

The following shows how the “byteCount” is inserted into the HeaderSet parameter:

```
HeaderSet ::= SEQUENCE {
    packetDataSessionID       [0] PacketDataSessionID,
    sourceIPaddress           [1] IpAddress,
    destinationIPaddress      [2] IpAddress,
    protocol                  [3] INTEGER,
    sourcePortNumber          [4] INTEGER                                    OPTIONAL,
    destinationPortNumber     [5] INTEGER                                    OPTIONAL,
    iPv6FlowLabel             [6] INTEGER                                    OPTIONAL,
    byteCount                [30] INTEGER                                    OPTIONAL
}
```

F.3.2 Total Byte Count Reporting Abstract Syntax Notation - Packet Data Summary Report

In conjunction with Packet Data Summary Header Report, the “totalByteCount” shall be inserted into the StreamSet parameter.

```
    totalByteCount            [30] INTEGER                                  OPTIONAL
```

The following shows how the “totalByteCount” is inserted into the StreamSet parameter:.

```
StreamSet ::= SET OF SEQUENCE {
    packetDataSessionID       [0] PacketDataSessionID,
    sourceIPaddress           [1] IpAddress,
    destinationIPaddress      [2] IpAddress,
    packetCount               [3] INTEGER,
    protocol                  [4] INTEGER,
    sourcePortNumber          [5] INTEGER                                   OPTIONAL,
    destinationPortNumber     [6] INTEGER                                   OPTIONAL,
    iPv6FlowLabel             [7] INTEGER                                   OPTIONAL,
    firstPacketTimestamp      [8] TimesStamp,
    lastPacketTimestamp       [9] TimesStamp,
    totalByteCount            [30] INTEGER                                  OPTIONAL
}
```