ATIS-1000021

DATA BUFFERING (SHORT TERM STORAGE) IN AN INTERNET ACCESS AND SERVICES LAES ENVIRONMENT

TECHNICAL REPORT

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

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.

ATIS-1000021, *Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment*

Is an ATIS 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-1000021

Technical Report on

DATA BUFFERING (SHORT TERM STORAGE) IN AN INTERNET ACCESS AND SERVICES LAES ENVIRONMENT

Secretariat

Alliance for Telecommunications Industry Solutions

Approved October 2007

Abstract

Reliable collection of intercepts is of paramount importance to Law Enforcement. An option for ensuring reliable collection of intercepts by Law Enforcement is the use of buffering (short term storage) as an adjunct function to the intercept process.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) -- formerly T1S1 -- develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

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

At the time it approved this document, ATIS PTSC, which is responsible for the development of this Technical Report, had the following members:

B. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
C.A. Underkoffler, ATIS Chief Editor
M. Bilca, PTSC LAES Technical Editor

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel-Lucent	Stuart Goldman
AT&T	George Stanek Will Chorley (Alt)
Avici Systems	Esmeralda Swartz
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt)
Cisco Systems	Rajiv Kapoor Mike Hammer (Alt)
Consultant	Bob Hall
Department of Defense	Chris Fitzgerald Ryan Kuseski (Alt)
Embarq Corporation	John Heinz Bill Wiley (Alt)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt)
ETI Connect	Peter Dyrholm David Cooke(Alt)
ETRI	Shin Gak-Kang Wook Hyun (Alt)
FBI ESTS	Marybeth Paglino Edward Ignacio (Alt)
Hewlett-Packard	Steve Mills
Intel Corporation	Walt Brown
Intelsat	Mark Neibert
IP Fabrics	Glen Myers Kevin Graves (Alt)
Microsoft Corporation	Wendy Fong

Organization Represented	Name of Representative
Motorola Inc.	Syed Husain
National Communications Systems	Nicholas Andre An Nguyen (Alt)
NEC Corporation of America	John McDonough Milorad Cvijetic (Alt)
NeuStar	Peggy Rehn Tom McGarry (Alt)
Nokia Siemens Networks	David Francisco Nagaraja Rao (Alt)
Nokia Telecommunications Inc.	Joyabrata Mukherjee Ed Ehrlich (Alt)
Nortel	Joseph Zebarth
PSEP Canada	Sim Simanis Sean Pope (Alt)
Qwest	Steve Showell Andrew White (Alt)
Sprint Nextel	Steve Oliva
SS8 Networks	Cemal Dikmen Scott Coleman (Alt)
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt)
Tellabs Operations	William A. Walker
Tridea Works	Selvan Rengasami Ken Coon (Alt)
VeriSign, Inc.	Anthony M. Rutkowski
Verizon Communications	Thomas Helmes Dave Morris

TABLE OF CONTENTS

TABLE OF FIGURES

Technical Report on

Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment

1 SCOPE, PURPOSE, AND APPLICATION

The topic of Data Buffering (Short Term Storage) in an Internet Access and Services Lawfully Authorized Electronic Surveillance (LAES) Environment was first introduced to the PTSC-LAES Subcommittee in August of 2006 as part of the standards development process that resulted in the publication of ATIS-1000013.2007 [1]. Law enforcement introduced it as a stated need. The PTSC-LAES Subcommittee subsequently proposed, and ATIS/PTSC agreed, to create a separate PTSC Issue (or committee work item) to address the matter. This Technical Report (TR) is the result of that work item. Subsequent to the initiation of the PTSC Issue (i.e., Issue S0049) that resulted in this TR, the FCC submitted a request for comments related to Law Enforcement's *Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act*, requesting among other things functionality/standards consistent with Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment. At the time of publication of this document, the FCC was in the process of comment review. The creation of this document was not in response to the Law Enforcement petition to the FCC.

It should be noted that this TR is intended to provide the results of the initial study into the topic of *Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment* by the PTSC-LAES Subcommittee, as well as to provide for a specification for *Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment* should interested parties voluntarily choose to implement such functionality. Any requirements/standards language (i.e., "shall," "should", etc.) is used strictly in the context of ensuring that this TR is inherently sound and provides appropriate guidance to voluntary implementers. This TR is not intended to be considered a "safe harbor standard" under the Communications Assistance for Law Enforcement Act (CALEA). Further, this TR is not intended to imply that the topic *of Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment* falls under CALEA.

1.1 Scope

The scope of this TR is buffering of intercepted Communication Content (CmC) data packets and Communication Identifying Information (CmII) event reports, and the transfer of the buffered CmC and CmII to Law Enforcement Agencies (LEA).

1.2 Purpose

The purpose of this TR is to identify a method to improve the reliability (i.e., increase the probability that intercepted information is not lost over the interface to the LEA(s) due to factors such as link congestion or failure) of transferring CmC and CmII to the LEA(s).

1.3 Application

This technical report on buffering describes an ancillary function that may be utilized to increase the reliability of intercepted Internet Access and Services (IAS) data being transferred to law enforcement. ATIS-1000013.2007 [1] is an industry standard that was developed for the CALEA-based lawful intercept of IAS data. This technical report was developed with the assumption that buffering was outside the scope of the ATIS-1000013.2007 standard. It is an optional function that can be implemented between the Delivery Function (DF) and the Collection Function (CF). The addition of a Buffering Function (BF) does not alter the IAS Surveillance Model as defined in ATIS-1000013.2007.

A BF can either be provided by an LEA or an Internet Access or Service Provider (IASP). An LEA may request an IASP to assist in setting up a buffering solution. If an IASP agrees to provide a buffering solution to an LEA, the IASP determines how buffering will be deployed based on its networking environment and current implementation of supporting Lawfully Authorized Electronic Surveillance (LAES) for IAS.

There may be alternative solutions beyond those discussed in this document that an IASP may propose in order to meet law enforcement's need for increased reliability. The buffering solution to be implemented will be determined based on the result of negotiations between the LEA and the IASP.

2 NORMATIVE REFERENCES

[1]. ATIS-1000013.2007, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*, April 2007.[1]

[2]. IETF RFC 4521, *The Secure Shell (SSH) Protocol Architecture*, January 2006.[2]

[3]. IETF RFC 4252, *The Secure Shell (SSH) Authentication Protocol*, January 2006.[2]

[4]. FIPS Pub 180-2, *Secure Hash Signature Standard*. National Institute of Standards and Technology (NIST), August 2002.[3]

[5]. IETF, *SSH File Transfer Protocol*, draft-ietf-secsh-filexfer-13.txt, July 10, 2006.[4]

[6]. IETF RFC 791, *Internet Protocol*, September 1981.[2]

[7]. IETF RFC 2460, *Internet Protocol*, version 6 (IPv6), December 1998.[2]

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS

3.1 Definitions

3.1.1 Access Function (AF): As used herein, the AF consists of one or more intercept access points that intercept an intercept subject's CmC and CmII unobtrusively. The intercept access points may vary between IASPs [1].

---

[1] 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/default.aspx >

[2] RFC text is available at < http://www.freesoft.org/CIE/RFC/index.htm >.

[3] This document is available from the National Institute of Standards and Technology (NIST) at < http://csrc.nist.gov/publications/fips/ >..

[4] This document is available from the Internet Engineering Task Force (IETF). < http://www3.tools.ietf.org/wg/secsh/ >

3.1.2 Authentication Mechanism: As used herein, refers to any of the mechanisms provided by SSH[2][3] for LEA access to the BF, such as password authentication and public-key authentication.

3.1.3 Buffering Function (BF): The short term storage of the CmC and CmII.

3.1.4 Collection Function (CF): Collection and analysis of the CmC and CmII received from the DF. It is defined to be the location where lawfully authorized intercepted CmC and CmII are collected by a LEA [1].

3.1.5 Delivery Function (DF): Delivery of intercepted communications to one or more CFs. The DF shall deliver intercepted communications in the form of CmC and CmII [1].

3.1.6 Communication Content (CmC): The full Internet Protocol packet streams to and from the subject [1].

3.1.7 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 [1].

3.1.8 Law Enforcement Agency (LEA): A government entity with the legal authority to conduct electronic surveillance [1].

3.1.9 Packet: An Internet Protocol packet [6][7].

3.2 Acronyms & Abbreviations

AF	Access Function
ASN.1	Abstract Syntax Notation Number 1
BF	Buffering Function
CALEA	Communications Assistance for Law Enforcement Act
CF	Collection Function
CmC	Communication Content
CmII	Communication Identifying Information
DF	Delivery Function
IAS	Internet Access and Services
IASP	Internet Access or Services Provider
ID	Identifier
IP	Internet Protocol
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
MAC	Media Access Control
PCAP	Packet CAPture
PDU	Protocol Data Unit
SCTE	Society of Cable Telecommunications Engineers
SFTP	SSH File Transfer Protocol
SHA-256	Secure Hash Algorithm 256
SSH	Secure Shell Protocol, version 2
TR	Technical Report

4 FUNCTIONAL ARCHITECTURE

A BF is an optional capability that may be implemented between the DF and the CF. The buffering function defined in this document is responsible for buffering the CmC and CmII received from the DF. The addition of a BF creates a new interface between the BF and the LEA collection site, which is defined in this TR as the *e′* interface.

The IASP may choose to implement the BF and the *e′* interface. If an IASP chooses to deploy buffering, the functions associated with buffering may be considered as logical functions and do not imply that these functions require separate physical devices. The final configuration will be a tactical deployment decision by the IASP.

The figures in the following two clauses present the intercept data buffering functional models for IAS where both CmC and CmII are intercepted and delivered from the IASP to the LEAs.

There are two buffering functional models:

- LEA-provided
- IASP-provided

4.1 LEA-Provided Buffering Functional Model

The LEA domain includes the following functions:[5]

- *Buffering Function (BF)*: A function responsible for buffering the CmC and CmII, received from the DF via the *e* interface.
- *Buffering-Specific Collection Function (CF′)*: A function responsible for retrieving and collecting CmII and CmC from the BF.

The interface between the DF and the BF is the *e* interface defined in ATIS-1000013.2007. The DF initiates the connection and transmits the CmII and CmC to the BF. The physical connection type, protocols, and bandwidth on the *e* interface are the subject of negotiation between LEA and the IASP. See the checklist in Annex A for deployment considerations. The interface between the BF and the CF′ is inside the LEA domain, and may use a wide area network (WAN).

[5] The Access Function (AF), DF, and the *e* interface shown in Figure 1 are defined in ATIS-1000013.2007.

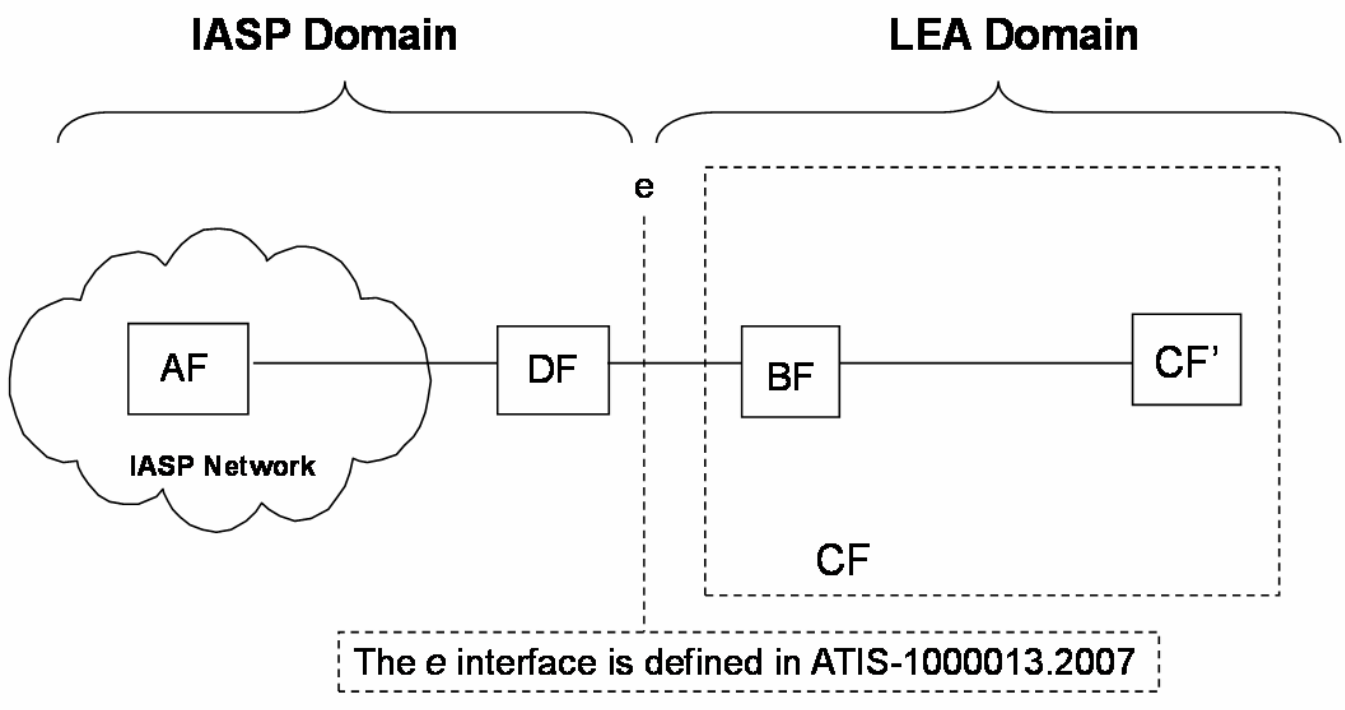

Figure 1: LEA Provided BF

Note that the above is a functional model and does not dictate any specific network architecture or equipment arrangement.

4.2 IASP Provided Buffering Functional Model

The interface between the DF and BF is internal to the IASP network. The *e* interface as defined in ATIS-1000013.2007 [1] may be used. The IASP Domain includes the following functions:[6]

- *Delivery Function (DF)*: A function responsible for delivering the CmII and CmC to the BF.
- *Buffering Function (BF)*: A function responsible for receiving the CmC and CmII from the DF and buffering the information in the file format specified in this document. This function interfaces with the CF′ in the LEA domain through the *e′* interface.

The LEA domain includes the following functions:

- *Collection Function (CF′)*: A function responsible for retrieving and collecting the buffered CmII and CmC from the BF.

The *e′* interface is specified in this document.

[6] The AF, DF and *e* interface shown in Figure 2 is defined in ATIS-1000013.2007

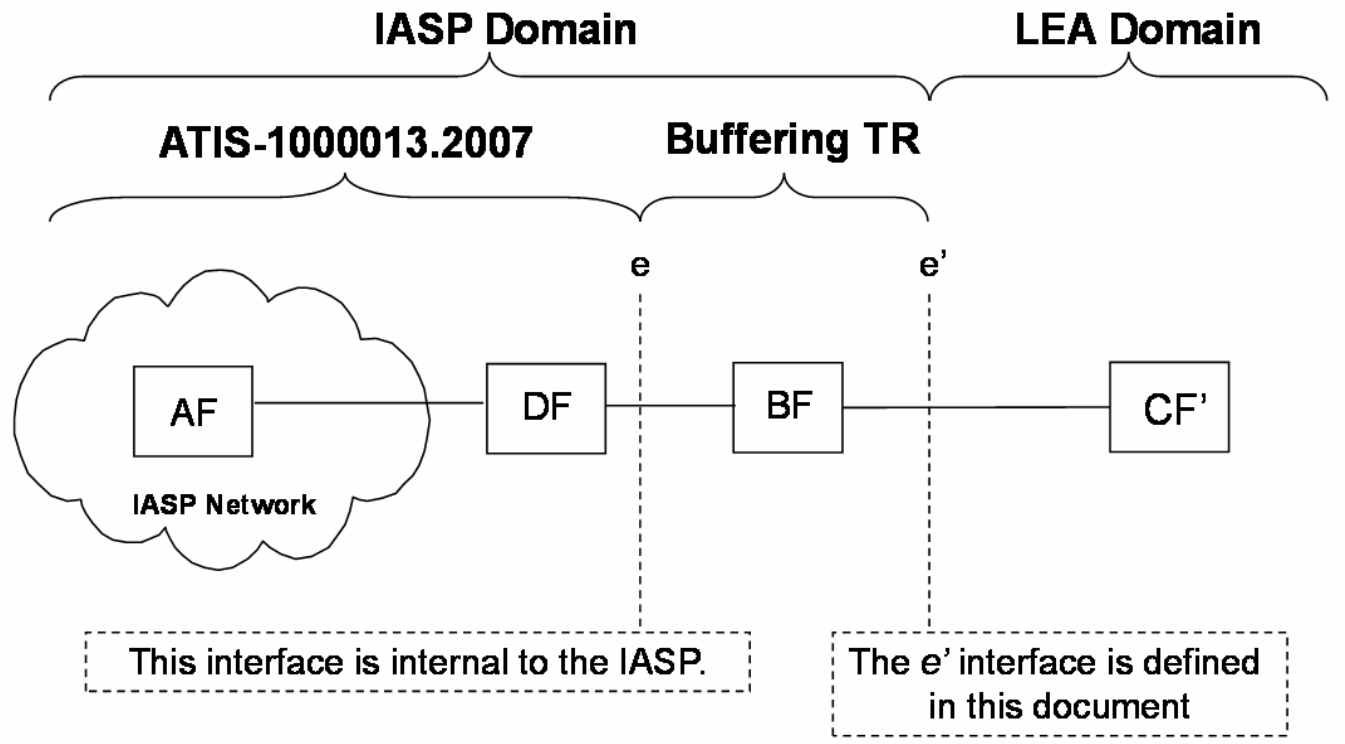

Figure 2: IASP Provided BF

Note that the above is a functional model and does not dictate any specific network architecture or equipment arrangement.

5 BUFFERING FUNCTION

5.1 Overview

The BF creates a set of files for each intercept and makes those files available to the CF' via the *e'* interface. Unlike the *e* interface, in which intercept information is pushed from the DF to the CF in real time, the *e'* interface intercept information is pulled by the CF' from the BF – though, not necessarily in real time. The term "buffering" is used to denote that the intercept information is spread over a number of files created in sequence such that law enforcement may be pulling a completed file across the *e'* interface while the BF is creating subsequent files.

5.2 File and Directory Structure

The BF shall provide a directory structure such that each LEA desiring buffering shall have a case directory for each provisioned intercept. Each case directory corresponds to a single Secure Shell (SSH) [2][3] user name, and should be the home directory for the user identified by the SSH user name. Within the case directory, there are buffer files for CmII information, buffer files for CmC information, and one intercept log.

For example, the directory structure would be:

```
Case a
     CmII files
     CmC files
     Intercept log
Case b
     CmII files
     CmC files
     Intercept log
Case c
     CmII files
     CmC files
     Intercept log
```

5.2.1 Directory Naming

The BF shall have an administrative function that permits its administrator to name and create case directories and to define SSH authorization credentials for each case directory. The BF shall also have an administrative function to denote which cases are to be managed by the BF. In the case where the DF and BF are combined, this may be part of the delivery administration of a case.

The name of a case subdirectory is the case identifier (ID) which is used in the intercept standard (e.g., ATIS-1000013.2007).

5.2.2 Directory Protection Over the e′ Interface

Over the *e′* interface, only the case directory whose name and authentication credentials are known to the BF may be accessed; there shall be no access to directories and files outside of a case directory for a particular access session. The BF shall provide the option of using the same authentication credentials (e.g, password, SSH public key) for multiple case directories. Over the e′ interface, the only permissible actions are to

(1) Gain access to a particular case directory;

(2) Read the attributes of the files;

(3) Read CmII or CmC files;

(4) Delete CmII or CmC files; and

(5) Read the intercept log.

5.3 Buffer Files

This clause defines the characteristics of the CmII and CmC buffer files.

5.3.1 Buffer File Format

5.3.1.1 CmC Files

The two categories of buffer files have different representations. For CmC, the Packet CAPture (PCAP) file format (see Annex C) shall be used, since CmC messages are Internet Protocol (IP) [6][7] packets

encapsulated within a CmC message. The BF will strip away the CmC encapsulation and create the CmC files which will contain the IP packets that were originally intercepted.

The PCAP format requires representation from the data-link layer outward, and since this is almost always Ethernet, an artificial Ethernet header needs to be constructed for each IP packet in the CmC messages. The Ethertype field shall be set to describe the packet as IPv4 [6] or IPv6 [7]. The destination Media Access Control (MAC) address will be set to 0xFFFFFF (Broadcast). The source MAC address shall be the first 6 octets of the correlation ID contained in the CmC message, or the correlation ID padded with zeros if the correlation ID is fewer than 6 octets.

The PCAP timestamp shall contain the timestamp originally stored in the CmC message.

The type of ATIS-1000013.2007 messaging -- e.g., Society of Cable Telecommunications Engineers (SCTE) Datagram, ATIS-1000678.2006, or IAS Datagram Format -- a BF receives shall be provisionable.

5.3.1.2 CmII Files

For CmII buffer files, the representation is different since these are messages with no meaningful layer two through layer four information. CmII buffer files will be sequential files that contain variable-length entities, which are the CmII messages.

5.3.2 File Naming

Buffer files are named by the BF when they are created. CmII files have the name 'caseid_seqnum.cmii', where 'caseid' is the case ID (same name as the case directory) and 'seqnum' is a sequence number. The sequence number starts at 00000000 when the buffering function is activated for an intercept. CmC files have the name 'caseid_seqnum.pcap' following the same conventions.

CmII and CmC files having the same sequence number in the same case directory cover the same period. The BF shall create these files on an event-driven basis (i.e., for a given sequence number in use, there could be a pair of files, just the CmII file, or just the CmC file).

A new CmII file shall use: (1) the sequence number of the corresponding CmC file that is currently open; or (2) the next sequential number if no CmC file is currently open.

A new CmC file shall use: (1) the sequence number of the corresponding CmII file that is currently open; or (2) the next sequential number if no CmII file is currently open.

5.3.3 Buffer File Granularity

An administrative function shall exist for specifying the size granularity for file creation during an intercept. File size granularity limits the maximum amount of data that can be written to a buffer file until it is closed and made available to the LEA.

It shall be possible, per intercept, to provision the maximum:

a) Number of CmII messages and CmC packets buffered per file;
b) Amount of time over which the CmII messages and CmC packets are buffered within a file; and
c) Size of a file.

When a CmII or CmC file is closed due to the above, the corresponding file of other type (i.e., CmC if CmII, CmII if CmC) is also closed.

5.3.4 Buffer File Deletion

The BF shall be able to store buffer files for at least 24 hours after the time they are closed and made available in the case directory. The maximum buffer file storage time should be configurable per case directory.

Buffer files that are deleted by the CF' over the *e'* interface shall be deleted immediately. The BF is permitted to delete CmII and CmC files if they have not been deleted by the CF' after 24 hours. Buffer files shall be deleted by the BF on a first-in, first-out basis.

The event of a file deletion by the BF shall be placed in the intercept log and the event of a file deletion by the CF' may be placed in the intercept log.

5.4 Intercept Log

There is certain information that is useful for an intercept that may not be communicated in CmII and CmC messages. This information is placed in a file per case called the intercept log. The intercept log file is named 'caseid.ilog'.

The intercept log has an initial record defining the product or platform serving as the BF, the software version, and the BF identity.

When a CmII or CmC file is closed, a Secure Hash Algorithm (SHA-256) [4] hash is performed of the file contents. The hash digest and name of the file is placed in the intercept log.

If a CmII or CmC file is deleted by the BF or the CF', the name of the file, a timestamp of when it was deleted, and the reason for deletion are placed in the intercept log entry associated with the deleted file.

If the BF has access to statistics about the *e* interface, the statistics are placed in the intercept log at an administrator-specified interval. The dropped packet statistic is currently the only statistic defined in the log file, and represents *e* interface Protocol Data Units (PDU)s dropped due to parsing errors.

The intercept log is a sequential file. Its Abstract Syntax Notation Number 1 (ASN.1) definition appears in clause 7.

5.5 Buffering Capacity

The default buffering capacity shall be a minimum of 24 hours per intercept.

The number of cases a BF can simultaneously support is limited by the available storage space, the total subject bandwidth of cases which require CmC buffering, and the required time which the buffered data needs to be stored. If an LEA requests an intercept which would exceed the capacity of the BF the LEA may, as mutually agreed with the IASP:

a) Request more buffer storage capacity; or
b) Use the existing capacity for more cases by reducing the required buffer file storage time.

The LEA may reduce the buffer file storage time for any or all of the LEA's active cases.

6. E' INTERFACE

6.1 e' Protocol Stack

The CF' accesses Buffer Function files via SSH File Transfer Protocol (SFTP) [5]. The BF shall provide at least one secure authentication method supported by SSH. The CF' initiates the SFTP connection to the BF to retrieve the buffered CmII, CmC, and intercept log files.

The BF shall not support access to the CmII and CmC buffer files currently open for writing, but it must support access to the intercept log.

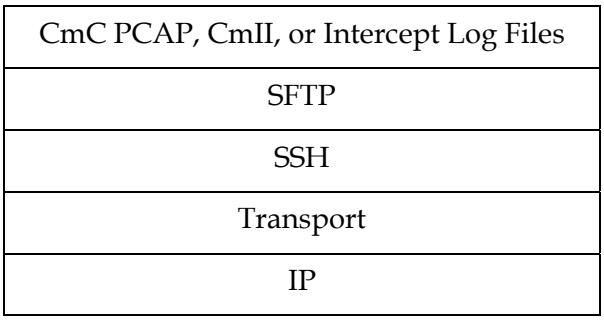

Figure 3: Protocol Stack

Annex A
(informative)

A CHECKLIST FOR DEPLOYING LEA-PROVIDED BUFFERING (SHORT TERM STORAGE) EQUIPMENT

The following checklist of items needs to be considered during negotiations between a LEA and an IASP in developing arrangements that will allow LEA-provided buffering (short term storage) equipment to be deployed as close as practical to the DF. Note that the following is not an exhaustive list, and not all items may apply to every implementation.

1. *Floor Space Requirements*:
    a. Rack Space.
    b. Cage Space.
    c. Shared facility.
2. *Interconnection Requirements*:
    a. From DF to BF, including physical connection, protocols, bandwidth, security.
    b. Interconnection (cross-connects).
    c. From BF to LEA, including physical connection, protocols, bandwidth, security.
3. *Installation Services/Assistance*:
    a. Qualified/Certified Personnel.
4. *Geographic Location of BF*.
5. *Security*:
    a. Building.
    b. Cage Area.
    c. Facilities.
    d. Access/Entrance Procedures.
    e. Identification/Authorization List.
6. *Environmental*:
    a. Fire Suppression.
    b. Lighting.
    c. Heat Dissipation/Ventilation.
    d. Cooling.
    e. Network Equipment Building System (NEBS)7 Compliance.
7. *Power and Grounding Requirements*:
    a. AC Voltage.
    b. DC Voltage.

---

[7] NEBS is the most common set of safety, spatial, and environmental design guidelines applied to telecommunications equipment in the United States. The NEBS equipment design guidelines are described in Telcordia documents:

- GR-63, *NEBS™ Requirements: Physical Protection*.
- GR-1089, *Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*.

   c. Redundant Power Feeds.
   d. Power Backup/ Uninterruptible Power Supply (UPS).
   e. Grounding Bus.

8. *Reliability Factor*:
   a. Alternate Facilities.
   b. Alternate Site.
9. *LEA provided Buffering Equipment*:
   a. NEBS Compliance.
10. *Service Level Agreement*.

Annex B
(normative)

B ASN.1 DEFINITION OF INTERCEPT LOG

```
--  ATIS-0x0000x-YYYY ANNEX B - IAS Buffering Log Abstract Syntax Module

IAS-Buffering-Log-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) buffering-log(3) version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS ;

-- OID for IAS-Buffering-Log-Abstract-Syntax-Module
IAS-Buffering-Log-Abstract-Syntax-Module-OID ::= OBJECT IDENTIFIER


InterceptLogRecord ::= CHOICE {
                sys-def                 [0] SystemDefinition,
                file-complete             [1] FileCompletion,
                file-delete               [2] FileDeletion,
                stat                      [3] Statistic
}
SystemDefinition ::= SEQUENCE {
                mod                       [0] Model,
                vers                      [1] Version,
                bfId                      [2] BfId
}
FileCompletion ::= SEQUENCE {
                file                      [0] FileName,
                digest                    [1] HashDigest
}
FileDeletion ::= SEQUENCE {
                file                      [0] FileName,
                time                      [1] GeneralizedTime,
                delete-reason             [2] FileDeleteReason
}
Statistic ::= CHOICE {
                dropped                   [0] DroppedPackets
}

Model ::= VisibleString
Version ::= SEQUENCE {
                maj                       [0] MajorVersion,
                min                       [1] MinorVersion
}

MajorVersion     ::= INTEGER
MinorVersion     ::= INTEGER
BfId     ::= VisibleString
FileName         ::= VisibleString
HashDigest       ::= OCTET STRING
FileDeleteReason ::= CHOICE {
                deletedbyCF               [0] NULL,
                administrative            [1] NULL
}
DroppedPackets ::= SEQUENCE {
                drops                     [0] Drops,
                timePeriod                [1] GeneralizedTime
}
Drops ::=                                       INTEGER
END  -- of IAS-Buffering-Log-Abstract-Syntax-Module
```

Annex C
(normative)

C LIBPCAP FILE FORMAT

PCAP (also called libpcap) files are a *de facto* industry standard way for software tools to store network packets. The format has been stable and in widespread use for many years, but has not been the subject of a published standard or RFC. Thus, the format used in the BF is documented in this Annex.

A PCAP file consists of a global header followed by zero or more packet records. A *packet record* consists of a fixed-length PCAP packet header followed by the packet.

The global header consists of 24 octets of information, shown below as a C language type definition:

```
struct pcap_hdr_s {
        guint32 magic_number;
        guint16 version_major;
        guint16 version_minor;
        gint32  thiszone;
        guint32 sigfigs;
        guint32 snaplen;
        guint32 network;
};
```

In the above type definition, the following elements are defined:

- **magic_number**: Used to detect the file format itself and the byte ordering. The writing application writes 0xa1b2c3d4 with its native byte ordering format into this field.
- **version_major, version_minor**: The version specified is 2 (major), 4 (minor).
- **thiszone**: The correction time in seconds between Coordinated Universal Time (UTC) and the local time zone of the following packet header timestamps.
- **sigfigs**: In theory, the accuracy of time stamps in the capture; in practice, all tools set it to 0, as does the BF.
- **snaplen**: The maximum size of each packet. Typical use is to set this to 65535, which is what the BF does.
- **network**: Data link layer type of the packets in the packet records. Set to 1 by the BF, denoting that the packet records contain Ethernet frames.

The global header is followed by a sequence of packet records. The header of a packet record consists of 16 octets defined as follows:

```
struct pcaprec_hdr_s {
        guint32 ts_sec;
        guint32 ts_usec;
        guint32 incl_len;
        guint32 orig_len;
};
```

In the above type definition, the following parameters are defined:

- **ts_sec**: The date and time when this packet was captured (in the BF, the timestamp that was represented for the packet on the e interface). This value is in seconds since January 1, 1970 00:00:00 UTC, as adjusted by thiszone from the global header for adjustments. Note that this time representation does not extend beyond the year 2038.
- **ts_usec**: The microseconds when this packet was captured, as an offset to ts_sec. This must have a value < 1,000,000.
- **incl_len**: The number of octets of the packet as actually saved in the file. In the BF, this should always be the same value as the next field.
- **orig_len**: The length of the packet as delivered to the BF. If incl_len and orig_len differ, the actual saved packet size was limited by snaplen.

The second part of the packet record is the actual packet of incl_len octets. In the case of the BF, the packet is an Ethernet frame.