

Data-Over-Cable Service Interface Specifications

Cable Broadband Intercept Specification

CM-SP-CBI2.0-I06-131003

Issued

Notice

This DOCSIS® specification is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs®. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

© Cable Television Laboratories, Inc., 2006 - 2013.

DISCLAIMER

This document is published by Cable Television Laboratories, Inc. ("CableLabs®").

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various agencies; technological advances; or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein. CableLabs makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the document or any information or opinion contained in the report. Any use or reliance on the information or opinion is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any cable member to purchase any product whether or not it meets the described characteristics. Nothing contained herein shall be construed to confer any license or right to any intellectual property, whether or not the use of any information herein necessarily utilizes such intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

| | | | | |
|-----------------------------------|---|----------------------|-----------------------------|-------------------|
| Document Control Number: | CM-SP-CBI2.0-I06-131003 | | | |
| Document Title: | Cable Broadband Intercept Specification | | | |
| Revision History: | I01 – Released 06/11/07 I02 – Released 12/6/07 I03 – Released 1/21/09 I04 – Released 2/24/11 I05 – Released 05/07/13 I06 – Released 10/03/13 | | | |
| Date: | October 3, 2013 | | | |
| Status: | Work in Progress | Draft | Issued | Closed |
| Distribution Restrictions: | Authors Only | CL/Member | CL/Member/Vendor | Public |

Key to Document Status Codes:

| | |
|-------------------------|--|
| Work in Progress | An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration. |
| Draft | A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process. |
| Issued | A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing. |
| Closed | A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs. |

Trademarks:

CableLabs® is a registered trademark of Cable Television Laboratories, Inc. Other CableLabs marks are listed at <http://www.cablelabs.com/certqual/trademarks>. All other marks are the property of their respective owners.

Contents

| | | |
|----------|--|-----------|
| 1 | SCOPE..... | 1 |
| 1.1 | INTRODUCTION AND PURPOSE | 1 |
| 1.2 | REQUIREMENTS | 1 |
| 2 | REFERENCES | 2 |
| 2.1 | NORMATIVE REFERENCES | 2 |
| 2.2 | INFORMATIVE REFERENCES..... | 2 |
| 2.3 | REFERENCE ACQUISITION..... | 3 |
| 3 | TERMS AND DEFINITIONS | 5 |
| 4 | ABBREVIATIONS AND ACRONYMS | 8 |
| 5 | OVERVIEW..... | 10 |
| 5.1 | LAW ENFORCEMENT'S HIGH-LEVEL REQUIREMENTS | 10 |
| 5.1.1 | <i>Intercept Categories</i> | 10 |
| 5.1.2 | <i>Transparency</i> | 10 |
| 5.1.3 | <i>Confidentiality / Access Control</i> | 10 |
| 5.1.4 | <i>Chronology of an Intercept</i> | 10 |
| 5.1.5 | <i>Correlation</i> | 11 |
| 5.1.6 | <i>Isolation</i> | 11 |
| 5.1.7 | <i>Proportionality</i> | 11 |
| 5.1.8 | <i>Completeness</i> | 11 |
| 5.1.9 | <i>Compression</i> | 11 |
| 5.1.10 | <i>Encryption</i> | 11 |
| 5.1.11 | <i>Performance</i> | 11 |
| 5.1.12 | <i>Availability and Reliability</i> | 12 |
| 5.2 | CABLE BROADBAND INTERCEPT ARCHITECTURE | 12 |
| 6 | ACCESS FUNCTION | 14 |
| 6.1 | OUT OF BAND INTERFACE | 14 |
| 6.2 | PACKET STREAM INTERFACE | 14 |
| 6.3 | PLANNING FOR FUTURE REQUIREMENTS | 14 |
| 7 | MEDIATION FUNCTION REQUIREMENTS | 16 |
| 7.1 | TRANSPARENCY | 16 |
| 7.2 | DATA INTEGRITY..... | 16 |
| 7.3 | ISOLATION..... | 16 |
| 7.4 | PROPORTIONALITY | 17 |
| 7.5 | COMPLETENESS | 17 |
| 7.6 | COMPRESSION | 17 |
| 7.7 | ENCRYPTION..... | 17 |
| 7.8 | PERFORMANCE | 17 |
| 7.9 | CONNECTIVITY REQUIREMENTS | 18 |
| 7.10 | AVAILABILITY, PERFORMANCE AND RELIABILITY..... | 18 |
| 7.11 | TIMING | 19 |
| 7.12 | INTERCEPT CATEGORIES..... | 19 |
| 7.12.1 | <i>Full IP Stream Intercept (For Full Content Broadband Intercept Orders)</i> | 19 |
| 7.12.2 | <i>Limited IP Stream Intercept (For Limited Broadband Intercept Orders)</i> | 19 |
| 7.13 | XML REQUIREMENTS | 20 |
| 7.13.1 | <i>Surveillance Event Messages</i> | 20 |
| 7.13.2 | <i>Packet Data Summary Report (For Limited Broadband Intercept Order Only)</i> | 22 |
| 7.13.3 | <i>Surveillance Status Report</i> | 22 |

| | | |
|---------------------|--|-----------|
| 7.13.4 | Event Parameters..... | 23 |
| 7.14 | CORRELATION | 28 |
| 8 | BROADBAND INTERCEPT FUNCTION, COLLECTION INTERFACE REQUIREMENTS AND FILE FORMAT | 29 |
| 8.1 | BROADBAND INTERCEPT FUNCTION REQUIREMENTS | 29 |
| 8.2 | BROADBAND INTERCEPT FUNCTION DIRECTORY STRUCTURE..... | 29 |
| ANNEX A | LIBPCAP FORMAT [PCAP-FF] (NORMATIVE) | 31 |
| A.1 | GLOBAL HEADER | 31 |
| A.2 | RECORD (PACKET) HEADER | 31 |
| A.3 | PACKET DATA | 32 |
| ANNEX B | MFI FILE TRANSFER FORMATS | 33 |
| B.1 | DATA PACKETS AND DHCP PACKETS | 33 |
| B.2 | HASHES | 33 |
| B.3 | XML ENCODED EVENTS | 33 |
| B.4 | FILE FORMATS FOR INTERCEPT DATA | 33 |
| B.4.1 | XML Instance Documents Format for Limited Intercept..... | 33 |
| B.4.2 | XML Instance Documents Format for OOB Messages..... | 34 |
| ANNEX C | CBI2.0 XML SCHEMA | 35 |
| APPENDIX I | LIMITED INTERCEPT XML INSTANCE DOCUMENT FILE..... | 40 |
| APPENDIX II | OUT OF BAND MESSAGES - XML INSTANCE DOCUMENT FILE | 42 |
| II.1 | OUT OF BAND ACCESS ATTEMPT MESSAGE - XML INSTANCE DOCUMENT FILE | 42 |
| II.2 | OUT OF BAND ACCESS ACCEPTED MESSAGE - XML INSTANCE DOCUMENT FILE..... | 42 |
| II.3 | OUT OF BAND ACCESS FAILED MESSAGE - XML INSTANCE DOCUMENT FILE | 44 |
| II.4 | OUT OF BAND ACCESS SESSION END MESSAGE - XML INSTANCE DOCUMENT FILE | 44 |
| II.5 | OUT OF BAND SURVEILLANCE STATUS REPORT MESSAGE - XML INSTANCE DOCUMENT FILE..... | 44 |
| APPENDIX III | PHYSICAL CONSIDERATION..... | 45 |
| APPENDIX IV | EXAMPLE FLOW CHART IMPLEMENTATION | 46 |
| APPENDIX V | ACKNOWLEDGEMENTS | 52 |
| APPENDIX VI | REVISION HISTORY | 53 |
| VI.1 | ENGINEERING CHANGE FOR CM-SP-CBI2.0-I02-071206. | 53 |
| VI.2 | ENGINEERING CHANGES FOR CM-SP-CBI2.0-I03-090121. | 53 |
| VI.3 | ENGINEERING CHANGE FOR CM-SP-CBI2.0-I04-110224. | 53 |
| VI.4 | ENGINEERING CHANGE FOR CM-SP-CBI2.0-I05-130507. | 53 |
| VI.5 | ENGINEERING CHANGE FOR CM-SP-CBI2.0-I06-131003. | 53 |

Figures

| | |
|---|----|
| Figure 1 - Logical Network Diagram | 12 |
| Figure 2 - Broadband Intercept Interfaces | 13 |
| Figure 3 - Provisioning the functions with data from the CMTS | 47 |
| Figure 4 - The Access Function, Intercept Access Points, and Out-of-Band Processing | 48 |
| Figure 5 - Packet Processing: full intercepts and limited intercepts | 49 |
| Figure 6 - The file manager | 50 |
| Figure 7 - The Broadband Intercept Function..... | 51 |

Tables

| | |
|---|----|
| Table 1 - DHCP Events of Interest to LE | 20 |
| Table 2 - Information Elements and sub elements in Message Parameter Tables | 23 |
| Table 3 - xml Defined Types | 25 |
| Table 4 - Information for Access Attempt Message | 26 |
| Table 5 - Information for Access Accepted Message | 26 |
| Table 6 - Information for Access Failed Message | 27 |
| Table 7 - Information for Access Session End Message | 27 |
| Table 8 - Information for Packet Data Summary Report Message | 27 |
| Table 9 - Information for Surveillance Status Report Message | 28 |

1 SCOPE

1.1 Introduction and Purpose ¹

This specification defines the interfaces between a cable Multiple System Operator's ("MSOs") network elements that provide Broadband Internet services to the public using a DOCSIS[®] network and a Law Enforcement Agency (LEA) so as to assist the LEA in conducting a lawfully authorized broadband electronic surveillance in accordance with the Communications Assistance for Law Enforcement Act (CALEA), including those provisions of CALEA that address subscriber privacy and security.

Accordingly, a manufacturer or service provider that is in compliance with this specification will have a "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. 1001 et seq for broadband surveillance. The CALEA safe harbor for VoIP communication is covered under the Packet Cable[™] Electronic Surveillance Specification.

This release is specifically directed toward network elements using IPv4 [DHCPv4] and IPv6 [DHCPv6] by means of CableLabs provisioning specifications which rely on Dynamic Host Configuration Protocol (DHCP) protocol for Internet Protocol (IP) address allocation management. Future releases of this specification may update this specification to provide IPv6 SLAAC (Stateless Address Autoconfiguration) or a mixed system of both IPv4 and IPv6 services, such as IP mobility in furtherance of an LEA conducting lawful surveillance under CALEA. Similarly, IP MultiCast and IPTV are to be evaluated for further study.

1.2 Requirements

Throughout this document, the words used to define the significance of particular requirements are capitalized. These words are:

| | |
|--------------|---|
| "MUST" | This word means that the item is an absolute requirement of this specification. |
| "MUST NOT" | This phrase means that the item is an absolute prohibition of this specification. |
| "SHOULD" | This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course. |
| "SHOULD NOT" | This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label. |
| "MAY" | This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product. For example; another vendor may omit the same item. |

¹ Revised per CBI2.0-N-10.0976-1 on 2/2/11 by JB.

2 REFERENCES

2.1 Normative References²

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

| | |
|------------------|--|
| [100Base-X] | ANSI/IEEE Std 802.3-2002 (ISO/IEC 8802-3:2000), IEEE Standard for Information technology--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Section 2, March 8, 2002. |
| [1000Base-X] | ANSI/IEEE Std 802.3-2002 (ISO/IEC 8802-3:2000), IEEE Standard for Information technology--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Section 3, March 8, 2002. |
| [10GBase-X] | IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks -- Specific requirements Part 1-5: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specific. |
| [18 U.S.C. 3127] | 18 U.S.C. § 3127(3) defines Pen Register. 18 U.S.C. § 3127(4) defines Trap and Trace. |
| [18 U.S.C. 2518] | 18 U.S.C. § 2518(7) defines Appropriate Legal Authority. |
| [DHCPv4 Options] | RFC3396 Encoding Long Options in DHCPv4 (updates RFC2131). |
| [DHCPv4] | RFC2131 Dynamic Host Configuration Protocol for IPv4. |
| [DHCPv6] | RFC3315 Dynamic Host Configuration Protocol for IPv6 (stateful). |
| [LIBPCAP] | The libpcap format: http://www.tcpdump.org . |
| [PCAP-FF] | PCAP File Format: http://www.tcpdump.org . |
| [PC-ESP1.5] | PacketCable™ 1.5 Specifications, Electronic Surveillance, PKT-SP-ESP1.5-I02-070412, April 12, 2007, Cable Television Laboratories, Inc. |
| [RFC IPv4] | IETF RFC 0791, Internet Protocol, Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981. |
| [RFC IPv6] | IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification. S. Deering and R. Hinden, December 1998. |
| [RFC 5139] | IETF RFC 5139, Revised Civic Location Format for Presence Information, February 2008 version replaces RFC 4119. |

2.2 Informative References

This specification uses the following informative references.

| | |
|---------|---|
| [14FCC] | <i>In the Matter of Communications Assistance for Law Enforcement Act</i> , Third Report and Order, 14 FCC Rcd 16794 (1999): http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1999/fcc99011.txt |
|---------|---|

² Removed T1.IAS per CBI2.0-N-08.0677-1, 12/02/08 by JS, revised per CBI2.0-N-10.0976-1 on 2/2/11 by JB.

| | |
|-----------------|--|
| [20FCC] | <i>In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services</i> , First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989 (2005), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260434A1.doc |
| [47CFR 64.2100] | 47 C.F.R. § 64.2100. Purpose: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2100&YEAR=2000&TYPE=TEXT |
| [47CFR 64.2101] | 47 C.F.R. § 64.2101. Scope: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2101&YEAR=2000&TYPE=TEXT |
| [47CFR 64.2102] | 47 C.F.R. § 64.2102. Definitions: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2102&YEAR=2000&TYPE=TEXT |
| [47CFR 64.2103] | 47 C.F.R. § 64.2103. Policies and procedures for employee supervision and control: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2103&YEAR=2000&TYPE=TEXT |
| [47CFR 64.2104] | 47 C.F.R. § 64.2104. Maintaining secure and accurate records: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2104&YEAR=2000&TYPE=TEXT |
| [47CFR 64.2105] | 47 C.F.R. § 64.2105. Submission of policies and procedures and commission review: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2105&YEAR=2000&TYPE=TEXT |
| [47CFR 64.2106] | 47 C.F.R. § 64.2106. Penalties: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2106&YEAR=2000&TYPE=TEXT |
| [ID Filexfer] | IETF Internet Draft, SSH File Transfer Protocol, draft-ietf-secsh-filexfer-13.txt http://tools.ietf.org/html/draft-ietf-secsh-filexfer-13 |
| [ID sftp] | IETF Internet Draft, Uniform Resource Identifier (URI) Scheme for Secure File Transfer Protocol (SFTP) and Secure Shell (SSH), draft-ietf-secsh-scp-sftp-ssh-uri-04.txt http://tools.ietf.org/html/draft-ietf-secsh-scp-sftp-ssh-uri-04 |
| [IPFIX] | IETF IP Flow Information Export (IPFIX) information: http://www.ietf.org/html.charters/ipfix-charter.html |
| [OSSiv2.0] | Data-Over-Cable Service Interface Specifications, DOCSIS 2.0 Operations Support System Interface Specification, CM-SP-OSSiv2.0-C01-081104, November 4, 2008, Cable Television Laboratories, Inc. |
| [PCAP] | PCAP Man Page. http://www.tcpdump.org/pcap3_man.html |
| [W3C-SCHEMA] | www.w3c.org/XML/Schema World Wide Web Consortium |

2.3 Reference Acquisition

- ATIS, 1200 G Street NW, Ste. 500, Washington DC 20005, USA
Phone: +1-202-628-6380, Fax: +1-202-393-5453, Internet: <http://www.atis.org>.
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: <http://www.cablelabs.com/>.
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, <http://www.ietf.org>.
- Internet Engineering Task Force (IETF), Internet: <http://www.ietf.org>.
Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>. Internet-Drafts may also be accessed at <http://tools.ietf.org/html/>.

- Institute of Electrical and Electronics Engineers (IEEE), IEEE Operations Center, 445 Hoes Lane, Piscataway, New Jersey 08854-1331, USA, Phone: +1-732 981 0060, Fax: +1-732 981 1721, Internet: <http://standards.ieee.org>.
- U.S. Code, <http://www.access.gpo.gov/>
U.S. FCC, <http://www.fcc.gov>.
- World Wide Web Consortium, www.w3c.org, c/o MIT, 32 Vassar Street, Room 32-G515
Cambridge, MA 02139.

3 TERMS AND DEFINITIONS

This specification uses the following terms:

| | |
|---|---|
| Access Session | The set of IP data packets each of which containing an IP address assigned to the devices at the Subject's facility and carried over the connection between the access device and access network via DOCSIS. These are the IP data packets intercepted and delivered to the LEA. An access session starts with an Access Session Accept message and ends with an Access Session End message. ³ |
| Appropriate Legal Authorization | A Broadband Intercept Order or other authorization, pursuant to [18 U.S.C. 2518], or any other relevant federal or state statute. |
| Authentication | A process by which a network provides assurances of a user's identity in conjunction with the use of a Subject Facility. |
| Authorization | The process by which a network grants a user access to network resources. Authorization usually follows Authentication. |
| Broadband Intercept | The interception of the broadband communications of a Subject. |
| Broadband Intercept Function | The function that implements buffering of broadband communications. |
| Broadband Intercept Order | A court order signed by a judge, magistrate, or other authority with jurisdiction that authorizes the interception of the broadband-based wire or electronic communications of a Subject. |
| Case Identity | Identifies the intercept Subject. This identity remains constant for the entire surveillance period. |
| Collection Function | The LEA function that receives the communications intercepted pursuant to the Broadband Intercept Order. |
| Fivetuple | The ordered set of packet header parameters that uniquely identify a stream. The parameters are the two IP addresses, protocol and the two port numbers. |
| Flow | A set of IPv4 packets sharing the same fivetuple or a set of IPv6 packets sharing the same sextuple. Also referred to as a stream. |
| Flowlabel | A 20-bit unsigned integer for future use that is always set to zero at this time |
| Full Content Broadband Intercept Order | A Broadband Intercept Order that authorizes the interception of any and all information concerning the timing, addressing, substance, purport, or meaning of the broadband communications of a Subject. |
| Hand-off | The process by which a network negotiates the transfer of a communication to another network. |
| Internet | The public Internet. |
| IP Network Access Provider | An entity that offers IP Network Access service to customers. This definition includes, but is not limited to, entities that provide broadband Internet access to customers/subscribers. |
| Law Enforcement (LE) | Any officer of the United States, or of a State or political subdivision thereof, who is empowered to conduct investigations, make arrests, or otherwise enforce and ensure obedience of the law. |

³ Session definition removed, Access Session definition added per CBI2.0-N-07.0517-1, 10/23/07, PO.

| | |
|--|---|
| Law Enforcement Agency (LEA) | Any agency of the United States, or of a State or political subdivision thereof, that enforces the law, including local or state police, and federal agencies such as the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA). |
| Limited Broadband Intercept | The interception of Out of Band data and partial packet data up to and including layer 4 port numbers. |
| Limited Broadband Intercept Order | A Broadband Intercept Order that authorizes the interception of limited information known as "Packet Signature" contained in the broadband communications of a Subject. |
| Multiple System Operator (MSO) | A cable company that operates more than one cable television system. |
| MSO Access Network | The MSO-owned and managed network that provides access to MSO provided services, including Internet access. |
| MSO Network Element | For purposes of this document, the MSO equipment that, for this purpose, will interface directly to the Broadband Intercept Function (e.g., a CMTS, a router, or other networking device). |
| Network Element | Equipment that is addressable and manageable, provides support or services to the user, and can be managed through an element manager. A group of interconnected network elements form a network. |
| Non-Repudiation | For the purposes of this document, the process used to minimize to the extent practicable in the circumstances, the ability of a user to effectively deny taking part in a particular communication or communication session using a Subject Facility. |
| PacketCaptureCount | A variable that defines the number of packets used to delimit a volume prior to hashing and file transfer. This is negotiated between the MSO and LE before initiating the intercept. |
| PacketCaptureDuration | A variable that defines the inactivity timeout (in seconds) used to delimit a volume prior to hashing and file transfer. For example, if no traffic is seen for PacketCaptureDuration, then the file is truncated, hashed, and transferred. This is negotiated between the MSO and LE before initiating the intercept. |
| Roaming | The process that enables a user to use networks other than his/her "home network" or those which he/she has a direct provisioning/billing relationship. |
| SFTP | SFTP is a ssh-2 utility that provides secure file transfer functionality. |
| Sixtuple | The ordered set of packet header parameters that uniquely identify an IPv6 stream. The parameters are the two IP addresses, protocol, the two port numbers and a flow label that is always set to zero at this time. |
| Stream | A set of packets sharing the same fivetuple. Also referred to as a flow. |
| Subject | An individual who is the object of a law Enforcement or LEA investigation and whose broadband communications and sessions are being intercepted pursuant to a Broadband Intercept Order. |
| Subject Facility | The devices, facilities, and/or services used by a Subject, as identified by a unique identifier (e.g., the MAC address of the cable modem associated with the Subject) or the IP address of a CPE behind the cm. A Subject Facility may be associated with zero, one or more Access Sessions at any time. ⁴ |

⁴ CBI2.0-N-07.0517-1, 10/23/07, PO.

| | |
|------------------------|---|
| Subject Traffic | All IP data traffic, both upstream and downstream, that is bridged by the cable modem(s) identified in the Broadband Intercept Order at the Subject Facility. |
| SummaryTimer | A variable that defines how frequently, in seconds, the Packet Data Summary Report is sent. |
| Validation | For the purposes of this document, the process used to provide assurance that an intercepted communication is associated with the correct Subject by confirming that it involves the use of a Subject Facility. |

4 ABBREVIATIONS AND ACRONYMS⁵

This specification uses the following abbreviations:

| | |
|---------------|--|
| AF | Access Function |
| ASCII | American Standard Code for Information Interchange |
| BIF | Broadband Intercept Function |
| BPF | Berkley Packet Filter |
| CALEA | Communication Assistance for Law Enforcement Act |
| CF | Collection Function |
| CFI | Collection Function Interface |
| CM | Cable Modem |
| CMTS | Cable Modem Termination System |
| CPE | Consumer Premises Equipment |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System/Service/Server |
| DOCSIS | Data-Over-Cable Service Interface Specification |
| FCC | Federal Communications Commission |
| GMT | Greenwich Mean Time |
| IAP | Intercept Access Point |
| ID | Identity/Identifier |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IPDR | IP Data Record |
| IPFIX | Internet Protocol Flow Information exchange |
| LE | Law Enforcement |
| LEA | Law Enforcement Agency |
| MAC | Media/Medium Access Control |
| MSO | Multiple System Operator |
| PCAP | Packet Capture |
| PDSR | Packet Data Summary Report |
| PPP | Point to Point Protocol |
| SFTP | SSH-2 File Transfer Protocol |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |

⁵ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

| | |
|------------|----------------------------|
| UTC | Universal Time Coordinated |
| VPN | Virtual Private Network |

5 OVERVIEW

This Cable Broadband Intercept Specification is intended to specify the means by which MSOs may facilitate the lawful interception of IP traffic destined to and sourced from a Subject Facility, along with the associated and relevant network events in a manner to ensure subscriber privacy and that Law Enforcement (LE) only intercepts the target facility IP traffic. This specification identifies the specific interface points between the MSO and the LEA that has served the Broadband Intercept Order. It also enumerates the specific requirements for these interface points.

5.1 Law Enforcement's High-Level Requirements

The following sections provide an informative high-level summary of Law Enforcement's (LE) objectives and requirements for Broadband Intercepts to guide the implementation of solutions that conform to those requirements. This summary should also be informative for MSOs with respect to provisioning a Broadband Intercept Order.

5.1.1 Intercept Categories

There are two intercept categories of interest to LE with respect to Broadband Intercepts. Information associated with the two categories is listed below:

- Full Intercept
- Full Packet Data
- Out of Band Events
- Limited Intercept
- Packet Header Summary
- Out-of-Band Events

5.1.2 Transparency

The Broadband Intercept must be conducted in a transparent manner, i.e., in a manner that prevents the Subject or the Subject Facility from detecting that an intercept is being conducted. Service parameters (e.g., bandwidth, latency, availability) must not be affected in any way by the intercept.

The fact that an interception is being conducted must be transparent (i.e., undetectable) to all non-authorized employees of the MSO, as well as to all other non-authorized persons.

The fact that there are or may be interceptions being conducted by multiple different LEAs on the same Subject must be transparent (i.e., undetectable) to each receiving LEA.

5.1.3 Confidentiality / Access Control

Access to, or knowledge of, an intercept, interception capabilities, intercept-related equipment, and intercepted communications and data must be protected and limited to only authorized persons.

5.1.4 Chronology of an Intercept

These three processes (Authentication, Validation, and Non-Repudiation) are part of the logical chronology of an intercept. Authentication is performed at the inception of an intercept to establish the connection between the communication and the Subject Facility. Validation then verifies that an intercepted stream is associated with the Subject Facility. Non-Repudiation confirms after the intercept is completed that the intercept was in fact associated with the Subject Facility.

5.1.4.1 Authentication

The intercepted communications must be authenticated in order to prove that they originated from, or were directed to, the Subject Facility.

5.1.4.2 Validation

While an intercept is active, that intercept must be validated (i.e., verified and audited) in order to prove that the intercepted communications are associated with the Subject Facility.

5.1.4.3 Non-Repudiation

Mechanisms must be in place to minimize the prospect of effective repudiation with respect to the intercepted communications.

Accurate records of service subscriptions must be securely kept in order to prove, after the intercept has taken place, that the intercepted communications were in fact associated with the Subject Facility.

Hashing algorithms (i.e., intercept hashes) must be used for data integrity in order to ensure that the intercepted communications have not been altered.

Accurate records of intercept parameters, implementation (e.g., requesting agency, time, and date implemented), and intercept hashes must be securely maintained. For more information, see [47CFR 64.2103].

5.1.5 Correlation

If more than one category of intercept is active at any time for a Subject, the interception information delivered to the LEA must be accurately correlated by intercept category. For more information, see Section 5.1.1 Intercept Categories and Section 7.12 Intercept Categories.

The Out-of-Band events must be accurately correlated in the intercepted information delivered to the LEA. For more information, see Section 7.13.1 Out-of-Band (DHCP) Event Messages.

5.1.6 Isolation

Only communications associated with the Subject Facility may be intercepted. Communications associated with the Subject Facility must be isolated, and communications not associated with the Subject Facility must not be captured, stored, or delivered to the LEA.

5.1.7 Proportionality

Only the authorized communications categories may be intercepted. For more information, see Section 5.1.1 Intercept Categories and Section 7.12 Intercept Categories.

5.1.8 Completeness

All communications to and from Subject Facility must be intercepted for the entire period authorized by the Broadband Intercept Order.

5.1.9 Compression

Compression must not be used in transmitting, buffering, storing, or delivering the intercepted communications to the LEA.

5.1.10 Encryption

If the MSO provides encryption services to its customers or subscribers, the MSO must either:

- deliver the intercepted communications to the LEA in unencrypted form, or
- provide information about the encryption algorithms used and the encryption keys to the LEA to enable the LEA to decrypt the intercepted communications.

5.1.11 Performance

The MSO must be able to provision multiple simultaneous intercepts on a single Subject.

The MSO must be able to provision multiple simultaneous intercepts on multiple Subjects.

If the MSO requests that the LEA provide the Broadband Intercept Function, the MSO must provide physical facilities at the MSO's premises (e.g., power, rack space) at which the LEA can co-locate the LEA-provided Broadband Intercept Function.

5.1.12 Availability and Reliability

The MSO must use appropriate performance and reliability mechanisms and parameters to enable the Broadband Intercept to be performed in a manner that substantially eliminates the likelihood that the intercept will be corrupted due to dropped packets.

5.2 Cable Broadband Intercept Architecture

The following specific interfaces and functions have been identified and defined as shown in Figure 1 in order to meet these high-level requirements outlined in Section 5.1:

- **Access Function (AF)** – The function in the MSO Network that provides access to the Subject Facility specified in the Broadband Intercept Order, and isolates, duplicates, and forwards the intercepted packet stream and Out of Band Events towards the Mediation Function.
- **Mediation Function (MF)** – The function in the MSO network that formats the events, CmC and CmII received from the AF for delivery across the Mediation Function Interface. The Mediation Function is provided by the MSO. Internal network events are sent to the Mediation Function for formatting. The Out-of-Band Event Source could be the Cable Modem Termination System (CMTS) itself, the IP Data Record (IPDR) Collector, the Dynamic Host Configuration Protocol (DHCP) Server, or another MSO Network Element depending on the particular MSO's network configuration.
- **Mediation Function Interface (MFI)** – The interface between the MF and the Broadband Intercept Function (BIF).
- **Broadband Intercept Function (BIF)** – The function that implements the buffering of the content and/or information that the MSO has intercepted pursuant to a Broadband Intercept Order. The interfaces of the Broadband Intercept Function are specified in this document. An MSO may choose to provide the Broadband Intercept Function or may request that it be provided by the LEA.
- **Collection Function Interface (CFI)** – The interface between the Broadband Intercept Function and the Collection Function.
- **Collection Function (CF)** – The LEA function that receives the communications intercepted pursuant to the Broadband Intercept Order.

It is anticipated that the Broadband Intercept Function may be co-located or in close proximity to the MSO Network Elements involved. Physical cabling (either electrical or optical, see Section 7.9 Connectivity Requirements below) between the Broadband Intercept Function and the MSO Network Elements will be required.

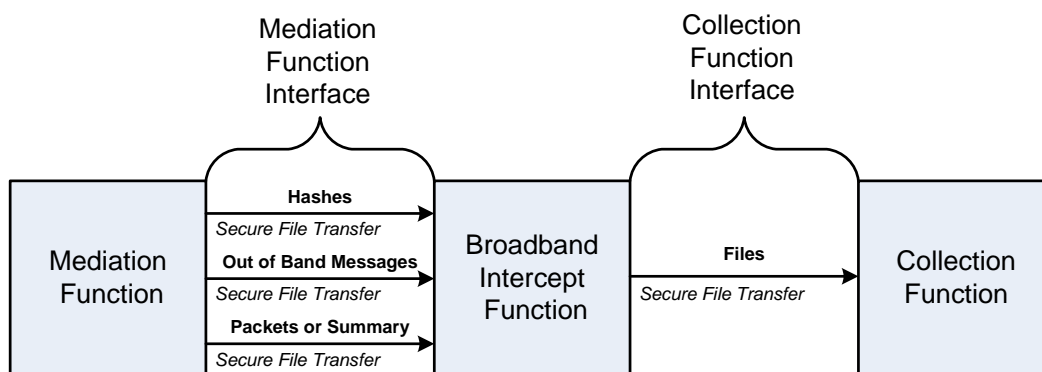


Figure 1 - Logical Network Diagram

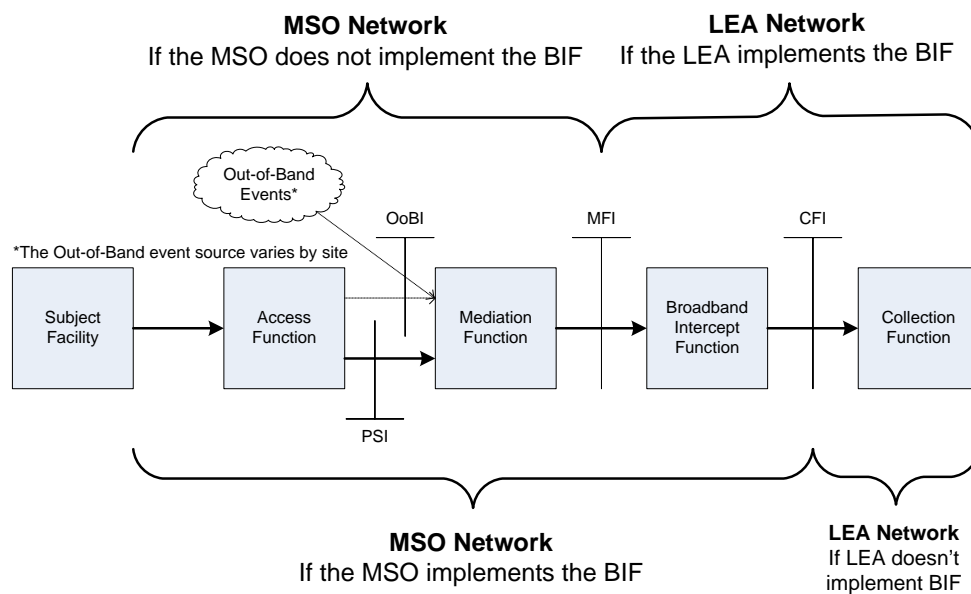


Figure 2 - Broadband Intercept Interfaces

6 ACCESS FUNCTION

The Access Function (AF) is the function in the MSO Network that provides connectivity to the subscriber's facility specified in the Broadband Intercept Order. The AF also isolates, duplicates, and forwards the intercepted packet stream and Out of Band Events towards the Mediation Function through their appropriate interface. Two interfaces provided for the two types of traffic: packet streams and out of band events.

The AF connects to the MSO Access network at an Intercept Access Point (IAP). The IAP can be a physical point (tap) or a logical point (policy-based port mirror).

6.1 Out of Band Interface ⁶

The Out of Band Interface (OoBI) MUST use the highest reliable transport rate available when forwarding Out of Band event traffic from the AF to the MF. The OoBI MUST be able to transport event traffic at a rate faster than all the incoming event traffic rate. The OoBI MAY provide a buffering function at the AF that provides assured delivery of packets over the OoBI.

The purpose of this section is to conceptually define the connection and source of the Out of Band events. The actual implementation of an OoBI will perform network termination and translation functions for the MSO's existing network infrastructure. For example, an existing network could be Ethernet, ATM, or Sonet SDH to name just a few. The IAP could be a tap, a port mirror, or even custom code running on the DHCP server or running on the provisioning server, in which case there may not even be a physical network connection. The exact implementation is highly site specific.

6.2 Packet Stream Interface ⁷

The Packet Stream Interface (PSI) MUST provide the highest reliable transport rate available when forwarding Packet Stream traffic from the AF to the MF. The PSI MUST be able to transport event traffic at a rate faster than all the incoming event traffic rate. The PSI MAY provide a buffering function at the AF that provides assured delivery of packets over the PSI.

When the AF serves multiple intercepts via one or more IAPs, then the PSI MUST be able to transport the full aggregation of packet stream data at a data rate faster than the full aggregation of incoming packet data rate.

As above, the purpose of this section is to conceptually define the connection and source of the packet stream(s); the definition of the Packet Stream Interface is out of scope for this document. The actual implementation of a PSI will perform network termination and translation functions for the MSO's existing network infrastructure. For example, an existing network could be Ethernet, ATM, or Sonet SDH, to name just a few. The IAP could be a tap, a port mirror, or a SPAN port driving the Access Function with a predefined UDP transport using predefined network interface parameters. The exact implementation is highly site specific.

6.3 Planning for future requirements

In a DOCSIS high-speed data system, the data termination point in the headend is the Cable Modem Termination System (CMTS). All traffic to any subscriber passes through the CMTS. This includes both Packet Stream Data and DHCP traffic. Even traffic that is locally looped back passes through the CMTS. The CMTS is the best source of real-time knowledge of IP address assignments to specific CPE MAC addresses, which are behind any specific Cable Modem. To provide a uniform IAP/AF, future CMTSs SHOULD include an intercept function that when provisioned with a cable modem MAC address, tags the appropriate CPE data structures to be used to identify packet streams that will be duplicated and forwarded to the PSI or OoBI as appropriate. While the intercept is active, if any Subject CPE IP address or CPE MAC address appears or changes, the CMTS would simply alter its intercept parameters to continue to duplicate and forward only data subject to the intercept. In such a case, the CMTS would also send a trap or alert or status message to log the event. The transport mechanisms and protocols used to forward

⁶ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

⁷ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

packets from a CMTS AF to a PSI or a OoBI should be simple and fast to maximize throughput and minimize CPU utilization.

7 MEDIATION FUNCTION REQUIREMENTS

This section presents normative requirements that apply to the two cases of MSO implementations:

1. If the MSO implements the Mediation Function Interface (MFI), it MUST follow the "R-XX MFI" requirements as described in Figure 1.
2. If the MSO implements the Collection Function Interface (CFI), it MUST follow the "R-XX CFI" requirements. In this case, the MFI is internal to the network and all of the requirements listed in Section 7 Mediation Function Requirements of the main body of the document still apply, except for the requirements in Section 7.9 Connectivity Requirements.

The requirements without an MFI or CFI indication "R-XX" MUST be applied to all implementations.

This section also provides guidance for changes in the Broadband Intercept Function (BIF) that result from implementing one or the other of the two cases.

7.1 Transparency

- R-10** The MF MUST perform the intercept in a manner that is transparent (undetectable) by the Subject or the Subject Facility (e.g., non-privileged entities in a call center should not be aware of intercept, service parameters, such as bandwidth, latency, or availability).
- R-20** MFI: The intercept MUST be transparent to multiple intercepting LEAs.
- R-20** CFI: The intercept MUST be transparent to multiple intercepting LEAs. For example, the intercept can be implemented by means of virtual file links and reference counting, such that once the file has been deleted by all intercepting LEAs it can be deleted from the BIF.

7.2 Data Integrity⁸

- R-30** The MF MUST employ the SHA256 hashing algorithm to ensure that the packets delivered to the LEA have not been modified.
- R-40** MFI: The MF MUST calculate the hash for the following files:
 - full/<filename>.dmp file and oob/<filename>.dmp for full intercepts and
 - limited/<filename>.xml file and oob/<filename>.dmp for limited intercepts
 where <filename> is of the format defined by R550.
- R-50** MFI: The BIF MUST store the hashes received from the MF.
- R-50** CFI: The BIF MUST store the hashes for
 - full/<filename>.dmp file and oob/<filename>.dmp for full intercepts and
 - limited/<filename>.xml file and oob/<filename>.dmp for limited intercepts
 where <filename> is of the format defined by R550.
- R-60** PacketCaptureCount and PacketCaptureDuration MUST be negotiated by the LEA and MSO prior to intercept initiation.
- R-70** Copies of the hashes MUST be delivered to the LEA along with the intercepted communications, and kept by the MSO as a business record.

7.3 Isolation

- R-80** The MF MUST be provisioned and operated such that only communications associated with the Subject Facility are intercepted. Communications associated with the Subject Facility MUST be

⁸ Changed section per CBI2.0-N-08.0678-1, 12/02/08 by JS.

isolated, and communications not authorized to be intercepted (e.g., those not associated with the Subject Facility) MUST NOT be delivered to the LEA.

7.4 Proportionality

R-90 The MF MUST ensure that only the authorized communications categories (Limited or Full) are intercepted.

For more information, see Section 5.1.1 Intercept Categories and Section 7.12 Intercept Categories.

7.5 Completeness

R-100 All Subject traffic, both to and from the Subject Facility, MUST be intercepted for the entire period authorized by the Broadband Intercept Order. Any intercepted traffic with a timestamp outside the period authorized by the Broadband Intercept Order MUST NOT be forwarded to the BIF and MUST be silently discarded. In the case where the Broadband Intercept Order is terminated early by court order, one of two actions will be taken:

1. The new termination date is in the future.
Continue normal intercept procedure.
2. The new termination date is now or in the past.
Immediately stop collecting traffic and complete processing of any intercepted data remaining in the MF that is within the newly authorized period of the intercept. Silently discard any intercepted data that has a timestamp outside the new period. If the data beyond the early termination date has not been sent to the CF, it is silently discarded.⁹

R-105 Communications being intercepted prior to the application of any routing optimization capability (e.g., local routing at the CMTS) MUST continue to be intercepted after the application of the optimization capability. If the application of the optimization capability would potentially cause some part of the communications covered by the Broadband Intercept Order not to be intercepted, the optimization capability MUST NOT be applied to that communication.

The event message reports source and destination information (i.e., fivetuple or sixtuple information) extracted from the packet headers, and provides summary information for the number of packets and bytes transmitted or received by the Subject for each unique flow defined by a fivetuple (in the case IPv4) or sixtuple (in the case IPv6), and the times that the first and last packets were detected for each unique flow.

7.6 Compression

R-110 Compression MUST NOT be used in delivering the intercepted communications to the LEA.

7.7 Encryption

R-120 If the MSO provides encryption services to its customers or subscribers, the MSO MUST either deliver the intercepted data to LE in unencrypted form, or provide information about the encryption algorithms used and the encryption keys to enable LE to decrypt the communications.

7.8 Performance

R-130 The MSO's CBI facilities MUST be capable of supporting and conducting multiple simultaneous intercepts on a single Subject.

R-140 The MSO's CBI facilities MUST be capable of supporting and conducting multiple simultaneous intercepts on multiple Subjects.

⁹ CBI2.0-N-0517-2, 10/22/07, PO.

The two variables, PacketCaptureDuration and PacketCaptureCount, are intended to assist the MSOs and LEAs in achieving the required performance outlined in R130 and R140.¹⁰

7.9 Connectivity Requirements¹¹

- R-150** If the LEA is providing the BIF, then the MF and the BIF MUST be collocated and implement one or more of the following Ethernet interfaces: twisted-pair or optical 100Base-X [100Base-X], twisted-pair, optical 1000Base-X [1000Base-X] or optical 10GBase-X [10GBase-X].
- R-160** The MFI data rate MUST be greater than the sum of the data rates required to transfer the out-of-band event, and packet summary captures hashes and retransmission overhead from the MF.
- R-170** MFI: If any form of WAN L2 is used, the MFI data rate MUST be greater than the sum of the data rates required to transfer the out-of-band event and packet/summary captures, hashes and retransmission overhead from the MF.
- R-180** MFI: The MF MAY support multiple simultaneous intercepts for different Subject Facilities served by the same MSO Network Element. Different Subject Facility intercepts MAY be delivered to LE through multiple MFs.
- R-190** The MFI link MUST be secured by a direct connection or an equivalently private and secure network.
- R-200** The MF MUST use SFTP to transport files across the MFI.
- R-210** The MF MUST move files to the temporary directory set up by the BIF for that purpose. See R500.
- R-220** The MF MUST verify transmission to the BIF by SFTP error returns and by comparing the sent and received file sizes. In the case of an error return or a mismatched file size, the file transfer MAY be retried one time with a ".retry" file extension. The retry file is uniquely named by appending ".retry" to the previous full file name. The MF MAY implement a queuing scheme to enable retransmission at a later time when the error condition has been repaired.
- R-230** To prevent multiple access synchronization problems, the MF and BIF MUST implement a mechanism using files that cause the BIF to wait until all files transferred from the MF have been successfully verified. Once the files have been verified, the BIF can be released to move the files from the temporary directory to the specific directory for that caseIdentity. The mechanism to accomplish this is described below.

The BIF and the MF MUST be designed so that BIF will not move files from the temporary directory unless a zero-length file named using the same case Identity, intercept type, and sequence number with a flag extension is in the temporary directory. The temporary directory is not a filename component. When verification is done, the MF creates the .flag file in the temporary directory. The BIF is always triggered by the appearance of a flag file. When it sees a flag file, it moves the file or files in the same subdirectory with the same sequence number (as the flag file) to the provisioned directory and deletes the flag file in that order.
- R-235** The MF MUST be capable of connecting to multiple BIF and of sending the same intercept data for an intercept subject to all connected BIF (e.g. to facilitate multiple LEA intercept requests on a single Subject).
- R-240** The SFTP cryptographic algorithms/strength MUST be negotiated by the MSO and LE prior to initiating the intercept.¹²

7.10 Availability, Performance and Reliability

- R-250** MFI: The intercept event messages, packet data, fivetuples, and summary reports MUST be delivered to the Broadband Intercept Function across the MFI.

¹⁰ CBI2.0-N-0517-2, 10/22/07 by PO.

¹¹ CBI3.0-13.1098-1, 5/2/13 by PO.

¹² New changes 210-230 and subsequent renumbering per CBI2.0-N-0517-2, 10/22/07, PO.

- R-260** MFI: Appropriate performance and reliability mechanisms and parameters to enable the MF to determine whether intercept event messages, packet data, fivetuples, and summary reports have been properly and accurately delivered to the BIF MUST be implemented. In the case of a file transfer failure, the error MUST be logged on the MF and the file deleted.

7.11 Timing

- R-270** An Out-of-Band Event MUST be timestamped at the time it is detected at the MF.
- R-280** The timestamp MUST have an accuracy of at least 200 ms relative to time an event is detected at the MF and precision of 1 ms.

7.12 Intercept Categories

- R-290** A Limited Broadband Intercept Order MUST include material conforming to the requirements in Sections 7.12.2 Limited IP Stream Intercept (For Limited Broadband Intercept Orders) and Section 7.13 xml Requirements.
- R-300** A Full Content Order MUST include material conforming to the requirements in Section 7.12.1 Full IP Stream Intercept (For Full Content Broadband Intercept Orders) and Section 7.13 xml Requirements.
- R-310** The intercept categories (Limited broadband intercept or Full Content Intercept) MUST be provisionable on a per-intercept basis.

7.12.1 Full IP Stream Intercept (For Full Content Broadband Intercept Orders)

- R-320** The full set of IP packets associated with the Subject Facility MUST be isolated and captured.
- R-330** The MF MUST transfer the file containing the packets to the BIF upon reaching PacketCaptureCount or the PacketCaptureDuration timeout or when the Broadband Intercept Order terminates.¹³
- R-340** In the event of no packets being captured upon packetCaptureDuration timeout, the MF MUST NOT transmit a null pcap file.

7.12.2 Limited IP Stream Intercept (For Limited Broadband Intercept Orders)¹⁴

- R-350** The packet signature, as defined in **R-360**, MUST be captured and delivered for each flow.
- R-360** The Packet Signature is a sequence of a fivetuple that defines a unique flow and the count of packets for that flow since the last report (numPktsSinceLastReport), and the number of bytes for that flow since the last report (numBytesSinceLastReport). If the packets are IPv4, the number of bytes is the sum of the values contained in the Total Length field [RFC IPv4] of each packet.
- If the packet is IPv6, the Packet Signature is a sequence of a sextuple that defines a unique flow, the count of packets for that flow since the last report (numPktsSinceLastReport), and the number of bytes for that flow since the last report (numBytesSinceLastReport). The number of bytes is the sum of the values contained in the Payload Length field [RFC IPv6] for each packet.
- The PacketSignature, whether IPv4 or IPv6, also includes the times when the first and last packets for the flow included in the report were detected. (FirstPacketTime and LastPacketTime).
- R-370** For each unique flow the Packet Signature MUST be recorded in the summary report at the start of the flow. The counter, numPktsSinceLastReport, MUST be incremented with each packet in that flow. The Packet Signature MUST be included in the summary report if any packets were detected.
- R-380** If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report MUST NOT be sent.

¹³ CBI2.0-N-0517-2, 10/22/07, PO.

¹⁴ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

7.13 xml Requirements¹⁵

The event messages formatted as XML instance document files are sent from the MF to the BIF using the same SFTP mechanism used for transferring file captures.

7.13.1 Surveillance Event Messages¹⁶

This section describes the requirement for reporting surveillance events of interest to Law Enforcement (LE).

There are three types of messages:

1. CBIS OoBI Messages
2. Packet Data Summary Report
3. Surveillance Status Message.

The following table illuminates the relationship between DHCP messages and LE events of interest. If a DHCP Event packet is received, the corresponding CBIS OoB message, shown in Table 1, **MUST** be generated. A CBIS OoB message **MUST NOT** be generated except as a result of receiving a DHCP Event packet. The DHCP Event packet **MUST** be captured in a OoB .dmp file the name of which is saved in the SignalCaptureFileName information element.

NOTE: Operators are cautioned not to attempt to trigger DHCP Events manually. This is likely to violate the transparency requirement in Section 7.1.¹⁷

The DHCP events generations are based on DHCPv4 and DHCPv6 message exchange between the client and the server as shown:

Table 1 - DHCP Events of Interest to LE¹⁸

| DHCP Event | | Server to Client | Client to Server | Purpose of DHCP Event | CBIS OoB Message |
|--------------|---|------------------|------------------|---|------------------|
| DHCP v4c | DHCP V6 | | | | |
| DHCPDISCOVER | SOLICIT | | X | Client broadcast to find available servers | Access Attempt |
| DHCPOFFER | ADVERTISE | X | | Server to client in response to DCHPDISCOVER with an offer of configuration parameters | Access Attempt |
| DHCPREQUEST | REQUEST (a) CONFIRM (b) RENEW (c) REBIND (d) | | X | Either a) or b) or c): a) Requesting offered parameters from one server and implicitly declining offers from all other servers. b) Confirming network address after a system reboots. c) Extending a lease on an IP address. | Access Attempt |
| DHCPACK | REPLY/ RELAY-REPL | X | | Committed configuration parameters | Access Accepted |

¹⁵ Section changed and renumbered by JS per ECNs CBI2.0-N-07.0677-1 on 12/2/08 and CBI2.0-N-09.0767-1 on 1/15/09.

¹⁶ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

¹⁷ Surveillance Event messages section modified by CBI2.0-N-07.0517-1, 10/23/07, PO.

¹⁸ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

| DHCP Event | | Server to Client | Client to Server | Purpose of DHCP Event | CBIS OoB Message |
|-------------|---------------------|------------------|------------------|---|-----------------------------|
| DHCP v4c | DHCP V6 | | | | |
| DHCPNAK | REPLY | X | | The committed IP address is invalid (e.g., lease expired or wrong subnet). | Assess Failed |
| DHCPDECLINE | DECLINE | | X | Upon testing (e.g., ARP or ping) the committed IP address is already in use. | Access Failed ¹⁹ |
| DHCPRELEASE | RELEASE | | X | Cancel remaining lease and return IP address. | Access Session End |
| DHCPINFORM | INFORMATION-REQUEST | | X | Request local parameters; client already has valid IP address. | Access Attempt |
| | RECONFIGURE | X | | Server tells client that there is new data for the client and the client is to initiate a renew/reply or an information-request/reply | Access Attempt |

7.13.1.1 Access Attempt²⁰

R-390 The Access Attempt event MUST be reported when a network registration has been attempted (e.g., when a Subject Facility attempts to access the cable network through a DHCP v4 DISCOVER or DHCP v4 OFFER or DHCP v4 REQUEST or DHCP v4 INFORM). Additionally, the Access Attempt event MUST be reported when a network registration has been attempted using IPv6 (e.g., when a Subject Facility attempts to access the cable network through a DHCPv6 SOLICIT, DHCP v6 ADVERTISE, DHCPv6REQUEST, DHCPv6CONFIRM, DHCPv6RENEW, or a DHCPv6REBIND).

R-400 If the MSO allows multiple IP addresses to be allocated to an account, all addresses MUST be reported, either as individual addresses or as address blocks (i.e., prefixes). Multiple addresses and/or prefixes MAY be reported in the same Access Attempt event message, otherwise, separate Access Attempt events MUST be reported for each IP address or prefix allocated.

7.13.1.2 Access Session Accepted²¹

R-410 The Access Session Accepted event MUST be reported when the intercept Subject Facility or associated CPE network device has successfully authenticated by the DHCP server (e.g., when the DHCP server sends the DHCP ACK message). Additionally, the Access Session Accepted event MUST be reported when a network registration has been attempted using IPv6 (e.g., when a Subject Facility attempts to access the cable network through a DHCPv6 SOLICIT, DHCP v6 ADVERTISE, DHCPv6REQUEST, DHCPv6CONFIRM, DHCPv6RENEW or a DHCPv6REBIND).

R-420 If the MSO allows multiple IP addresses to be allocated to an account, all addresses MUST be reported, either as individual addresses or as address blocks (i.e., prefixes). Multiple addresses and/or prefixes MAY be reported in the same Access Attempt event message, otherwise, separate Access Accepted events MUST be reported for each IP address or prefix allocated.

R-430 If CPE IP addresses are added or changed as a result of DHCP Events at the Subject Facility, then the new IP addresses MUST be used to intercept data. The AF or MF SHOULD monitor all DHCP

¹⁹ CBI2.0-N-07.0517-1, 10/23/07, PO.

²⁰ Updated per CBI2.0-N-13.1111-2 on 9/26/13 by PO.

²¹ Updated per CBI2.0-N-13.1111-2 on 9/26/13 by PO.

activity to determine if an IP address under surveillance has been allocated to a different device. Such DHCP activity **MUST** be captured.²²

7.13.1.3 Access Failed²³

- R-440** The Access Failed event **MUST** be reported when network authentication has failed and the network is aware of the failed attempt. Consequently, an access session has not been successfully established (e.g., access to the cable network resources has been denied and the Subject's CPE has been explicitly denied a public IP network address through a DHCP NACK Response or when a DHCPv6 server sends a DHCPv6REPLY).
- R-445** The Access Failed event **MUST** be reported when the intercept Subject sends a DHCPv4 DHCPDECLINE or a DHCPv6 DECLINE message to the network.

7.13.1.4 Access Session End

- R-450** If a DHCPRELEASE packet or a DHCPv6RELEASE has been intercepted, the PCAP file **MUST** contain the packet
- R-460** The following parameters **MUST** be as follows.
1. Release reason is set to "DHCP".
 2. The Signal Capture File Name is present.
 3. The Hash is present.
- R-470** If it is determined by some other means that the IP address is no longer assigned to the Subject, then the following parameters **MUST** be as follows.
1. Release reason is set to "other".
 2. The Signal Capture File Name is not present.
 3. The Hash is not present.

The access session end event does not indicate the end of the surveillance; it signals the subject's release of the IP address.²⁴

7.13.2 Packet Data Summary Report (For Limited Broadband Intercept Order Only)

This event is used to provide packet data summary reports for Subject communications.

- R-490** The Packet Data Summary Report **MUST** be reported when the expiration of a configurable timer per intercept occurs. The timers are configurable in units of seconds.

The event message reports source and destination information (i.e., fivetuple information in the case of IPv4 or sixtuple in the case of IPv6) extracted from the packet headers, provides summary information for the number of packets and bytes transmitted or received by the Subject for each unique flow defined by a fivetuple in the case of IPv4 or sixtuple in the case of IPv6, and the times that the first and last packets were detected for each unique flow.

The hash for this message is contained in a separate file. File naming conventions of Section 8.1 apply.

7.13.3 Surveillance Status Report

This event is used to provide surveillance status reports.

- R-500** The Surveillance Status Report **MUST** be reported:
- when there is a change in status of a surveillance
 - Up: Surveillance is activated.
 - Down: Surveillance is deactivated.

²² CBI2.0-N-07.0517-1, 10/23/07

²³ Revised per CBI2.0-13.1110-2 on 9/25/13 by PO.

²⁴ CBI2.0-N-07.0517-1, 10/23/07; Section 7.3.1.5 deleted per CBI2.0-13.1110-2 on 9/25/13 by PO.

- Error: An error occurred. The second text field adds explanatory text.
- Unknown: Indeterminate status
- or to notify the LEA, on a periodic basis that surveillance is continuing/still active (i.e., a "heartbeat"). The heartbeat timer is configurable in seconds and SHOULD NOT exceed fifteen minutes.
- Heartbeat

The Surveillance Status Report is not hashed.

7.13.4 Event Parameters

7.13.4.1 Parameter Definitions

The following information elements appear in the Message Parameter tables in Section 7.13.4.2.

Table 2 - Information Elements and sub elements in Message Parameter Tables²⁵

| Information Element | DataType | Description |
|---------------------------------------|-----------------------|--|
| Access Device | sequence | When available, this element consists of two information elements: AccessDeviceType and AccessDeviceID. The semantics of these elements are defined below. |
| Access Session Characteristics | string | Identifies characteristics of the intercept Subject's access session (e.g., bandwidth limits, noteworthy network-level filtering). This parameter is MSO/product specific. |
| AccessDeviceID | hexBinary | This information element contains the MAC address of the device used by the Subject for accessing the network resources. This is the second information element within the Access Device. |
| AccessDeviceType | string | Specifies the type of Device used to gain access to the network resources. This is the first information element within the Access Device element. The valid values are: "cm", "eMTA", "dsg", "other" |
| Access Session ID | string | Uniquely identifies the intercept Subject's network access session (see access session definition in Section 3) for a given surveillance. This parameter is generated in the Mediation Function. In the case where the access session has already been established because the surveillance started after the IP addresses have already been allocated by an earlier DHCPACK, then the MF must assign an Access Session ID prior to sending the surveillance status message. In case the IP addresses are statically assigned, there is only one Access Session ID assigned. |
| Case Identity | string | A unique value that identifies the intercept. This identity remains constant for the entire surveillance period. For example, this can be a phone number or an MSO's ticketing system identifier. |
| CMTSID | string | Identifies the network node providing access termination services to the intercept Subject Facility Access Device. FQDN or dotted decimal IP address assigned by MSO network ops to the CMTS. |
| Device Address | deviceAddress Element | Identifies the set of IP addresses and/or IP address prefixes and prefix lengths bound to the Subject Facility for the duration of the Access session. |

²⁵ Table revised per CBI2.0-N-07.0517-1, 10/23/07 by PO, revised per CBI2.0-N-08.0677-1 on 12/02/08 by JS, revised per CBI2.0-N-10.0976-1 on 2/2/11 by JB, and revised CBI2.0-N-13.1111-2 on 9/26/13 by PO.

| Information Element | DataType | Description |
|------------------------------------|--------------|--|
| Failure Reason | string | The value is "DHCPNAK" or "DHCPDECLINE" for IPv4 or "REPLY" or "DECLINE" for IPv6. |
| Fivetuple Set | sequence | Describes an ordered set of fivetuples (i.e., IP Source, IP Destination, Source Port, Destination Port, Protocol). |
| Sixtuple Set | sequence | Describes an ordered set of sixtuples (i.e., IPv6 Source, IP v6 Destination, Source Port, Destination port, protocol and flowlabel). |
| Hash | hexBinary | An SHA-256 hash of the original intercepted packet headers or the network-generated event. The hash covers the packet and the PCAP headers. |
| IAPSystemIdentity | string | Describes the Intercept Access Point (IAP) associated with the Intercept Subject. |
| Lease Duration | unsignedInt | Defines the IP address lease time in units of seconds associated with the Intercept Subject's Access Device. |
| Location Information | civicAddress | Identifies the location of the Subject Facility in Presence Information Data Format (PIDF) [RFC 5139]. When reasonably available and covered by the Broadband Intercept Order, location information must be delivered to the LEA. |
| MF System Identity | string | A unique identifier enabling multiple active MF's simultaneously. For example, a FQDN or dotted decimal IP address assigned by MSO network ops to MF system. |
| Num Bytes Since Last Report | unsignedLong | Counter of the number of bytes associated with a fivetuple set (in the case of IPv4) or sixtuple set (in the case of IPv6). |
| Num Pkts Since Last Report | unsignedLong | Counter of the number of packets associated to a fivetuple set (in the case of IPv4) or sixtuple set (in the case of IPv6). |
| Packet Signature | sequence | Describes a sequence of fivetuple (in the case of IPv4) and the count of packets and bytes for that fivetuple or a sequence of sixtuple (in the case of IPv6) and the count of packets and bytes for that sixtuple, and the time of the first and last packet sent since the last report (numPktsSinceLastReport, numBytesSinceLastReport, FirstPacketTime, LastPacketTime). |
| Signal Capture File Name | string | Pointer to actual file containing the DHCP messages captured. |
| Status | sequence | Describes the status of a surveillance. The status has two components. The first component is one of the enumerated values indicating active, not active, unknown, an error condition, or heartbeat. The second component is a text string to provide further explanation. The presence of this string is optional. |
| Subscriber Identity | string | Uniquely identifies the subscriber to the service. This is the alias used by the MSO to identify the intercept Subject (e.g., user ID, Service Account ID). |

| Information Element | Data Type | Description |
|--------------------------|-----------|---|
| Time Stamp | Sequence | <p>Identifies the date and time that the event triggering the message was detected.</p> <ol style="list-style-type: none"> 1. timeStampSeconds: This value is in seconds since 00:00:00 UTC on January 1, 1970. 2. timeStampMicroseconds: The microsecond count when the packet was captured. This is a synchronized offset to data element 1. This value SHOULD be less than one million or timeStampSeconds MUST be incremented by 1. <p>See Annex A.2.</p> |
| First Packet Time | Sequence | <p>Identifies the date and time that the first packet in a fivetuple set (in the case of IPv4) or sixtuple set (in the case of IPv6) was detected.</p> <ol style="list-style-type: none"> 1. timeStampSeconds: This value is in seconds since 00:00:00 UTC on January 1, 1970. 2. timeStampMicroseconds: The microsecond count when the packet was captured. This is a synchronized offset to data element 1. This value SHOULD be less than one million or timeStampSeconds MUST be incremented by 1. <p>See Annex A.2.</p> |
| Last Packet Time | Sequence | <p>Identifies the date and time that the last packet in a fivetuple set (in the case of IPv4) or sixtuple set (in the case of IPv6) was detected.</p> <ol style="list-style-type: none"> 1. timeStampSeconds: This value is in seconds since 00:00:00 UTC on January 1, 1970. 2. timeStampMicroseconds: The microsecond count when the packet was captured. This is a synchronized offset to data element 1. This value SHOULD be less than one million or timeStampSeconds MUST be incremented by 1. <p>See Annex A.2.</p> |

7.13.4.1.1 Type Definitions

The data types referenced in the message parameter tables are defined using the basic xml types in the following table. Included where applicable are the permitted values for these defined types.

Table 3 - xml Defined Types²⁶

| Defined Type | Definition | Permitted Values |
|--------------|------------|--------------------------------------|
| IpAddr | hexBinary | IPv4 or IPv6 address in hex notation |
| MacAddress | hexBinary | Mac Address |

7.13.4.2 Message Parameters

The parameters of the messages defined in this section are specified using XML schema data types [W3C-SCHEMA]. The data types used in the message parameter tables are specified in terms of the basic xml types in the following tables.

²⁶ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

7.13.4.2.1 Access Attempt Message

Table 4 - Information for Access Attempt Message

| Information Element | M/O/C | Conditions |
|------------------------------|-------|---|
| Case Identity | M | |
| MF System Identity | M | |
| Time Stamp | M | |
| Subscriber Identity | M | |
| Access Device | C | Provide when known. |
| Network Access Node Identity | C | Provide when known. |
| Signal Capture File Name | M | Provide when DHCP message capture is used. |
| Hash | M | Must be present if Signal Capture File Name is populated. Hash covers DHCP packet and PCAP headers. |

7.13.4.2.2 Access Accepted Message

Table 5 - Information for Access Accepted Message

| Information Element | M/O/C | Conditions |
|--------------------------------|-----------------|--|
| Case Identity | M | |
| MF System Identity | M | |
| Time Stamp | M | |
| Subscriber Identity | M | |
| Access Device | C | Provide when known. |
| Network Access Node Identity | C | Provide when known. |
| Device Address | C | Provide when known. |
| Access Session Identity | M | |
| Access Session Characteristics | C | Provide when known. (e.g., if the DHCP capture is not available, this field would contain relevant parameters from a DHCP server.) |
| Location Information | C | Provide when reasonably available and when authorized by the Broadband Intercept Order. |
| Lease Duration | C ²⁷ | |
| Signal Capture File Name | M | Provide when DHCP message capture is used. |
| Hash | M | Must be present if Signal Capture File Name is populated. Hash covers DHCP packet and PCAP headers. |

²⁷ Changed per CBI2.0-N-08.0677-1 on 12/02/08 by JS.

7.13.4.2.3 Access Failed Message

Table 6 - Information for Access Failed Message

| Information Element | M/O/C | Conditions |
|--------------------------|-------|---|
| Case Identity | M | |
| MF System Identity | M | |
| Time Stamp | M | |
| Subscriber Identity | M | |
| Device Address | C | Provide when known. |
| Failure Reason | C | Provide when known. |
| Signal Capture File Name | M | Provide when DHCP message capture is used. |
| Hash | M | Must be present if Signal Capture File Name is populated. Hash covers DHCP packet and PCAP headers. |

7.13.4.2.4 Access Session End Message

Table 7 - Information for Access Session End Message

| Information Element | M/O/C | Conditions |
|--------------------------|-------|---|
| Case Identity | M | |
| MF System Identity | M | |
| Time Stamp | M | |
| Subscriber Identity | M | |
| Device Address | M | |
| Access Session Identity | M | |
| Signal Capture File Name | M | Provide when DHCP message capture is used |
| Hash | M | Must be present if Signal Capture File Name is populated. Hash covers DHCP packet and PCAP headers. ²⁸ |

7.13.4.2.5 Packet Data Summary Report Message

Table 8 - Information for Packet Data Summary Report Message

| Information Element | M/O/C | Condition |
|-------------------------|-------|---|
| Case Identity | M | |
| IAP System Identity | M | |
| Time Stamp | M | |
| Access Session Identity | M | |
| PacketSignature | M | There may be one or more PacketSignature elements included. |

²⁸ M/O/C column in last 2 rows in Tables 4-7 changed from C to M per CMI2.0-N-07.0517-1, 10/23/07, PO.

A hash **MUST** be calculated over the xml file containing the Packet Data Summary Report. That hash is written in the caseIdentity/limited/xxxxx.hash file. The timestamp is written to the Packet Data Summary Report Message when the Summary Timer times out.

7.13.4.2.6 Surveillance Status Report Message

Table 9 - Information for Surveillance Status Report Message²⁹

| Information Element | M/O/C | Condition |
|-------------------------|-------|---|
| Case Identity | M | |
| MF System Identity | M | |
| Time Stamp | M | |
| Device Address | C | Identifies the IP address(es)/address block(s) bound to the Subject Facility for the duration of the Access session. Provide when the message is used to report intercept activation and a session has already been established. |
| Access Session Identity | M | |
| Location Information | C | Provide when reasonably available, when authorized by the Broadband Intercept Order, and when the Surveillance Status message is reporting the activation or deactivation of an intercept during an active session, using Presence Information Data Format (PIDF) [RFC 5139]. |
| Status | M | |

7.14 Correlation

R-510 The MSO **MUST** ensure that the intercepted Out of Band Events and Full Packet Streams (or headers in the case of a Limited broadband intercept) delivered to the LEA must be accurately correlated within an intercept category per Subject.

For more information, see Section 5.1.1 Intercept Categories and Section 7.12 Intercept Categories.

²⁹ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB, revised per CBI2.0-N-13.1097-1 on 5/2/13 by PO, revised per CBI2.1-N-13.1111-2 on 9/25/13 by PO.

8 BROADBAND INTERCEPT FUNCTION, COLLECTION INTERFACE REQUIREMENTS AND FILE FORMAT

8.1 Broadband Intercept Function Requirements³⁰

If an MSO implements the CFI, all of the requirements listed in Section 7 Mediation Function Requirements of the main body of the document still apply, except for the requirements in Section 7.9 Connectivity Requirements.

The following requirements apply to Broadband Intercept Function and the CFI:

- R-520** The BIF MUST make available a temporary directory and a limited privilege account (create and directory read) to the MF.
- R-530** The BIF MAY verify each hash and if the hash is correct, the BIF MUST move the file from the temporary directory to the 24-hour storage area. If the hash is incorrect, the BIF MAY move the file to a quarantine area and report it to the MSO by a means beyond the scope of this specification. For example, syslog might be used.
- R-540** The Broadband Intercept Function MUST only buffer and deliver the specific intercept categories (Full or Limited Intercept) that are authorized by the Broadband Intercept Order.
- R-550** The Broadband Intercept Function MUST implement SFTP over SSH-2 and MAY implement a VPN standard or some other secure means and serve it to the CF client.
- R-560** The Broadband Intercept Function MUST be provisioned with a buffering capacity that will accommodate 24 hours of network usage by Subject per intercept.
- R-570** Once the intercept files have been downloaded to the CF, the LEA MUST delete the files from the BIF. Otherwise, if the amount of intercepted packets contained in the provisioned buffering space becomes so great that it causes an overflow, the packets contained in the buffer MAY be automatically deleted in a cyclical "first-in, first-out" manner by the BIF.
- R-580** The BIF MUST store the hashes received from the MF with a naming convention that allows the hash file to be easily paired with the hashed file (see R-610 for filename format).
- R-590** The hashes MUST be stored in the same subdirectory as the corresponding hashed file.

8.2 Broadband Intercept Function Directory Structure

A mechanism to allow current tools to correctly parse intercepts is needed. This MUST be accomplished by employing the following file directory structure:

- R-600** There MUST be one directory per intercept, named with the MSO-generated Case Identity defined above in Table 2. This is referenced for the directory structure as *caseIdentity*.
- R-610** This intercept directory MUST contain three sub-directories, named *full*, *limited*, and *oob*. The filenames must use the following format:

[A-Za-z0-9_-]*[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9].(dmp|hash|xml)

The format contains an optional variable-length string followed an 8-digit integer with the extension dmp, hash, or xml. The string prefix MUST be unique per mediation function. It is recommended that the string prefix be the MFSystemIdentity.

Example paths are provided:

```
caseIdentity/full/00000001.dmp
caseIdentity/full/00000001.hash
caseIdentity/full/mf100000001.dmp
caseIdentity/full/mf100000001.hash
```

³⁰ Requirements renumbered and modified by JS per CBI2.0-N-08.0678-1 on 1/07/09 and CBI2.0-N-09.0767-1 on 1/07/09.

```

caseIdentity/limited/00000001.xml
caseIdentity/limited/00000001.hash
caseIdentity/limited/mf2.mso.com00000001.xml
caseIdentity/limited/mf2.mso.com00000001.hash

caseIdentity/oob/00000001.dmp
caseIdentity/oob/00000001.xml
caseIdentity/oob/mf2.mso.com00000001.dmp
caseIdentity/oob/mf2.mso.com00000001.xml
caseIdentity/oob/AccessAttempt-00000001.xml

```

NOTE: The hash for the oob.dmp file is contained within elements of the oob.xml file. The filename in the SignalCapture FileName Parameter in Table 4 through Table 7 points to the file as listed immediately above. The hash value in the hash parameter is the hash of that file.

The parameter "Message_Name" is the name of the event message name in Table 4 through Table 9. The numeric sequence is appended by the Mediation Function for example:

Casedea001/oob/AccessAttempt-00000013.xml)

The sequence number in the full intercept is generated by the Mediation Function file manager and is inserted in the filename for example *casefbi321/full/00000013.dmp* . The sequence number starts at one and increases by one in a strictly monotonic manner as each file is numbered. Leading zeros are suppressed. Sequence numbers are reusable between full, limited, and oob directories.³¹

- R-620** The intercepted data captured pursuant to a Limited Broadband Intercept Order as described in Section 7.12.2 of this document **MUST** be captured in the *caseIdentity/limited* and *caseIdentity/oob* subdirectories using the XML schema defined in Annex C.
- R-630** The intercepted packets captured pursuant to a Full Content Broadband Intercept Order as described in Section 7.12.1 of this document **MUST** be stored in the *caseIdentity/full* subdirectory using the PCAP format, and the out of band events **MUST** be stored in the *caseIdentity/oob* subdirectory using the XML schema defined in Annex C.
- R-640** Under a Limited Broadband Intercept Order, as described in Section 7.12.2 of this document, the *caseIdentity/full* directory **MUST** either remain empty, or not exist at all.

³¹ Text in this section modified per CBI2.0-N-07.0517-1, 10/23/07, PO.

Annex A libpcap Format [PCAP-FF] (Normative)


A.1 Global Header

This header starts the libpcap file and will be followed by the first packet header:

```
typedef struct pcap_hdr_s {
    guint32 magic_number; /* magic number */
    guint16 version_major; /* major version number */
    guint16 version_minor; /* minor version number */
    gint32 thiszone; /* GMT to local correction */
    guint32 sigfigs; /* accuracy of timestamps */
    guint32 snaplen; /* max length of captured packets, in octets */
    guint32 network; /* data link type */
} pcap_hdr_t;
```

- **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. The reading application will read either 0xa1b2c3d4 (identical) or 0xd4c3b2a1 (swapped). If the reading application reads the swapped 0xd4c3b2a1 value, it knows that all the following fields will have to be swapped too.
- **version_major, version_minor:** the version number of this file format (current version is 2.4)
- **thiszone:** the correction time in seconds between GMT (UTC) and the local timezone of the following packet header timestamps. Examples: If the timestamps are in GMT (UTC), thiszone is simply 0. If the timestamps are in central European time (Amsterdam, Berlin, ...), which is GMT + 1:00, thiszone must be -3600. In practice, time stamps are always in GMT, so thiszone is always 0.
- **sigfigs:** in theory, the accuracy of time stamps in the capture; in practice, all tools set it to 0.
- **snaplen:** the maximum size of each packet (typically 65535 or even more, but might be limited by the user), see: `incl_len` vs. `orig_len` below
- **network:** data link layer type (e.g., 1 for Ethernet, see [WWW]wiretap/libpcap.c or libpcap's pcap-bpf.h for details), this can be various types like Token Ring, FDDI, etc. The data link layer type must be set accurately to ensure complete and accurate packet capture.

In the case of an Ethernet (1) capture. The data link layer MAC addresses may be overwritten when capturing packets on a network segment physically separated from the Subject Facility. This can happen when the IAP is not on the CMTS, but is a hop or more distant. In that case, the Ethernet addresses may be ignored and the fivetuple or sextuple used for packet identification.³²


 **Note:** If you need a new encapsulation type for libpcap files (the value for the network field), do NOT use ANY of the existing values! In other words, do NOT add a new encapsulation type by changing an existing entry; leave the existing entries alone. Instead, send mail to [MAILTO]tcpdump-workers@tcpdump.org, asking for a new DLT_ value, and specifying the purpose of the new value.

A.2 Record (Packet) Header

Each captured packet starts with (any byte alignment possible):

```
typedef struct pcaprec_hdr_s {
    guint32 ts_sec; /* timestamp seconds */
    guint32 ts_usec; /* timestamp microseconds */
    guint32 incl_len; /* number of octets of packet saved in file */
    guint32 orig_len; /* actual length of packet */
} pcaprec_hdr_t;
```

³² CBI2.0-N-07.0517-1, 10/23/7, PO. Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

- `ts_sec`: the date and time when this packet was captured. This value is in seconds since 00:00:00 UTC on January 1, 1970; this is also known as a UNIX `time_t`. You can use the ANSI C `time()` function from `time.h` to get this value, but you might use a more optimized way to get this timestamp value. If this timestamp isn't based on GMT (UTC), use `thiszone` from the global header for adjustments.
- `ts_usec`: the microseconds when this packet was captured, as an offset to `ts_sec`.  Beware: this value SHOULD NOT reach 1 second (1 000 000). In this case `ts_sec` MUST be increased instead!
- `incl_len`: the number of bytes actually saved in the file. This value SHOULD NOT become larger than `orig_len` or the `snaplen` value of the global header.
- `orig_len`: the length of the packet "on the wire" when it was captured. If `incl_len` and `orig_len` differ, the actually saved packet size was limited by `snaplen`.

A.3 Packet Data

The actual packet data will immediately follow the packet header as a data blob of `incl_len` bytes without a specific byte alignment.

Annex B MFI File Transfer Formats

All data is transferred from the Mediation Function across the Mediation Function Interface to the Broadband Intercept Function as a file structure by SFTP. Three file formats are used.

B.1 Data Packets and DHCP Packets

These file types are pcap encoded. The pcap files have a .dmp file extension. Full intercept .dmp files MAY have more than one record (packet) per file. OoB .dmp files MUST contain exactly one record (DHCP packet) per file.

B.2 Hashes

This file type contains a single hash per file, in sequence with actual file transfers, correlated by file name (e.g., *caseIdentity/full/interceptfile-xxxxx.hash*). A hash file exists for:

- the full intercept .dmp file,
- the limited intercept .xml file.³³

Hash files have a “.hash file” extension.

B.3 xml Encoded Events

These files have an “.xml” file extension. For xml encoded DHCP events, elements in the xml file point to the .dmp file that contains the DHCP message in pcap encapsulation.

B.4 File Formats for Intercept Data

For Full Content Intercept data captures, see Annex A for file format.

The MF MUST generate XML instance document files for Limited intercept data captures and OOB messages according to the XML schema specified in Annex C.

B.4.1 XML Instance Documents Format for Limited Intercept

The MF MUST generate the Limited Intercept instance Document Files as follows:

1. The XML Instance documents are compatible with the XML 1.0 version. The document starts with: `<?xml version="1.0" ?>`.
2. The PacketDataSummaryReport element is the outermost element that describes the Summary Report. It defines the xml namespace and the identity of the XML schema document. This document contains a single record.
3. The attributes of the PacketDataSummaryReport element are:
 - `xmlns:="xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"`
 - `xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
 - `xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI-1.0.xsd"`

The elements defined in the PacketDataSummaryReport sequence follows the above header.

The start of the XML instance document and the content of the PacketDataSummaryReport element is as follows:

```
<?xml version="1.0"?>
<CBI:PacketDataSummaryReport xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

³³ CBI2.0-N-07.0517-1, 10/23/7, PO.

```
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI-1.0.xsd">
```

An example of a complete Limited Intercept Instance Document file is shown in Appendix I.

B.4.2 XML Instance Documents Format for OOB Messages

The MF MUST generate the Limited Intercept instance Document Files as follows:

1. The XML Instance documents are compatible with the XML 1.0 version. The document starts with: `<?xml version="1.0" ?>`
2. A CBISMessage 'choice' element (one of CBI:AccessAttempt, CBI:AccessAccepted, CBI:AccessFailed, CBI:AccessSessionEnd, CBI:SurveillanceStatusReport) is the outermost element that describes the OOB message file document. It defines the XML namespace and the identity of the XML schema document. An OOB message file document contains only one of these elements.
3. The attributes of this element are:
 - `xmlns:="xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"`
 - `xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
 - `xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI-1.0.xsd"`

One of the elements of the "choice" elements in the CBISMessage follows the above header.

An example of the start of the XML instance document for an Access Accepted message is as follows:

```
<?xml version="1.0" ?>
< CBI:AccessAccepted xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI-1.0.xsd">
```

An example of a complete OOB Message Instance Document file is shown in Appendix II.

Annex C CBI2.0 XML Schema³⁴

```
<?xml version="1.0"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:ipdr="http://www.ipdr.org/namespaces/ipdr">
  xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
    <import namespace="http://www.ipdr.org/namespaces/ipdr"
schemaLocation="http://www.ipdr.org/public/IPDRDoc3.5.1.xsd"/>
    <import namespace="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
schemaLocation="http://www.iana.org/assignments/xmlregistry/schema/pidf/geopriv10/civi
cAddr.xsd"/>
    <include schemaLocation="http://www.ipdr.org/public/IPDRTypes.xsd"/>
    <element name="AccessDevice">
      <complexType>
        <sequence>
          <element ref="CBI:AccessDeviceType"/>
          <element ref="CBI:AccessDeviceID"/>
        </sequence>
      </complexType>
    </element>
    <element name="AccessSessionCharacteristics">
      <simpleType>
        <restriction base="string"/>
      </simpleType>
    </element>
    <element name="AccessSessionId">
      <simpleType>
        <restriction base="integer"/>
      </simpleType>
    </element>
    <element name="CaseIdentity">
      <simpleType>
        <restriction base="string"/>
      </simpleType>
    </element>
    <element name="Hash">
      <simpleType>
        <restriction base="hexBinary">
          <minLength value="32"/>
        </restriction>
      </simpleType>
    </element>
    <element name="DeviceAddress">
      <simpleType>
        <restriction base="ipdr:macAddress"/>
      </simpleType>
    </element>
    <element name="LocationInformation" type="ca:civicAddress" minOccurs="0"
maxOccurs="1"/>
    <element name="MFSsystemIdentity">
      <simpleType>
        <restriction base="string"/>
      </simpleType>
    </element>
  </schema>
```

³⁴ CBI2.0-N-07.0517-1, 10/26/07 by PO, changed per CBI2.0-N-08.0677-1, 12/02/08 by JS, revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB, revised per CBI2.0-N-13.1097-1 on 5/3/13 by PO, revised per CBI2.0-N-13.1110-2 and CBI2.0-N-13.1111-2 9/25/13 by PO.

```

<element name="CMTSID">
  <simpleType>
    <restriction base="string"/>
  </simpleType>
</element>
<element name="FailureReason">
  <simpleType>
    <restriction base="string">
      <enumeration value="DHCPv4NAK"/>
      <enumeration value="DHCPv4DECLINE"/>
      <enumeration value="DHCPv6REPLY"/>
      <enumeration value="DHCPv6DECLINE"/>
    </restriction>
  </simpleType>
</element>
<element name="SignalCaptureFileName">
  <simpleType>
    <restriction base="string"/>
  </simpleType>
</element>
<element name="Status">
  <complexType>
    <sequence>
      <element ref="CBI:StatusCode"/>
      <element ref="CBI:StatusDetails" minOccurs="0"/>
    </sequence>
  </complexType>
</element>
<element name="SubscriberIdentity">
  <simpleType>
    <restriction base="string"/>
  </simpleType>
</element>
<element name="TimeStamp">
  <simpleType>
    <restriction base="ipdr:dateTimeUseC"/>
  </simpleType>
</element>
<element name="AccessDeviceType">
  <simpleType>
    <restriction base="string">
      <enumeration value="cm"/>
      <enumeration value="emta"/>
      <enumeration value="dsg"/>
      <enumeration value="other"/>
    </restriction>
  </simpleType>
</element>
<element name="LeaseDuration">
  <simpleType>
    <restriction base="nonNegativeInteger"/>
  </simpleType>
</element>
<element name="IAPSystemIdentity">
  <simpleType>
    <restriction base="string"/>
  </simpleType>
</element>
<element name="AccessDeviceID">
  <simpleType>
    <restriction base="ipdr:macAddress">
      <length value="6"/>
    </restriction>
  </simpleType>
</element>

```

```

        </simpleType>
    </element>
<element name="IpAddr">
    <complexType>
        <choice>
            <element ref="ipdr:ipV4Addr"/>
            <element ref="ipdr:ipV6Addr"/>
        </choice>
    </complexType>
</element>
<element name="PrefixLength">
    <simpleType>
        <restriction base="integer"/>
    </simpleType>
</element>
<element name=" DeviceAddressElement">
    <complexType>
        <sequence>
            <element ref="CBI:PrefixLength" minOccurs="0" maxOccurs="1"/>
            <element ref="CBI:IpAddr"/>
        </sequence>
    </complexType>
</element>
<element name="DeviceAddress" type="CBI:DeviceAddressElement" maxOccurs="unbounded"/>
<element name="sourceAddress" type="CBI:IpAddr"/>
<element name="destAddress" type="CBI:IpAddr"/>
<element name="sourcePort" type="unsignedInt"/>
    <element name="destPort" type="unsignedInt"/>
    <element name="protocol" type="unsignedByte"/>
    <element name="ipv6FlowLabel" type="unsignedInt"/>
    <element name="NumPktsSinceLastReport">
        <simpleType>
            <restriction base="unsignedLong"/>
        </simpleType>
    </element>
    <element name="NumBytesSinceLastReport">
        <simpleType>
            <restriction base="unsignedLong"/>
        </simpleType>
    </element>
    <element name="FirstPacketTime">
        <simpleType>
            <restriction base="ipdr:dateTimeUseC"/>
        </simpleType>
    </element>
    <element name="LastPacketTime">
        <simpleType>
            <restriction base="ipdr:dateTimeUseC"/>
        </simpleType>
    </element>
    <element name="StatusCode">
        <simpleType>
            <restriction base="string">
                <enumeration value="Up"/>
                <enumeration value="Down"/>
                <enumeration value="Unknown"/>
                <enumeration value="Heartbeat"/>
            </restriction>
        </simpleType>
    </element>
    <element name="StatusDetails" type="string"/>
    <element name="PacketSignature">
        <complexType>

```

```

    <sequence>
      <element ref="CBI:sourceAddress"/>
      <element ref="CBI:destAddress"/>
      <element ref="CBI:sourcePort"/>
      <element ref="CBI:destPort"/>
      <element ref="CBI:protocol"/>
      <element ref="CBI:NumPktsSinceLastReport"/>
      <element ref="CBI:NumBytesSinceLastReport"/>
      <element ref="CBI:FirstPacketTime"/>
      <element ref="CBI:LastPacketTime"/>
    </sequence>
  </complexType>
</element>
<element name="AccessAttempt">
  <complexType>
    <sequence>
      <element ref="CBI:CaseIdentity"/>
      <element ref="CBI:MFSYSTEMIdentity"/>
      <element ref="CBI:TimeStamp"/>
      <element ref="CBI:SubscriberIdentity"/>
      <element ref="CBI:AccessDevice"/>
      <element ref="CBI:CMTSID"/>
      <element ref="CBI:SignalCaptureFileName" minOccurs="1"/>
      <element ref="CBI:Hash" minOccurs="1"/>
    </sequence>
  </complexType>
</element>
<element name="AccessAccepted">
  <complexType>
    <sequence>
      <element ref="CBI:CaseIdentity"/>
      <element ref="CBI:MFSYSTEMIdentity"/>
      <element ref="CBI:TimeStamp"/>
      <element ref="CBI:SubscriberIdentity"/>
      <element ref="CBI:AccessDevice"/>
      <element ref="CBI:CMTSID"/>
      <element ref="CBI:DeviceAddress"/>
      <element ref="CBI:AccessSessionId"/>
      <element ref="CBI:AccessSessionCharacteristics"/>
      <element ref="CBI:LocationInformation"/>
      <element ref="CBI:LeaseDuration" minOccurs="0"/>
      <element ref="CBI:SignalCaptureFileName" minOccurs="1"/>
      <element ref="CBI:Hash" minOccurs="1" maxOccurs="1"/>
    </sequence>
  </complexType>
</element>
<element name="AccessFailed">
  <complexType>
    <sequence>
      <element ref="CBI:CaseIdentity"/>
      <element ref="CBI:MFSYSTEMIdentity"/>
      <element ref="CBI:TimeStamp"/>
      <element ref="CBI:SubscriberIdentity"/>
      <element ref="CBI:DeviceAddress"/>
      <element ref="CBI:FailureReason"/>
      <element ref="CBI:SignalCaptureFileName" minOccurs="1"/>
      <element ref="CBI:Hash" minOccurs="0"/>
    </sequence>
  </complexType>
</element>
<element name="AccessSessionEnd">
  <complexType>
    <sequence>

```

```

        <element ref="CBI:CaseIdentity"/>
        <element ref="CBI:MFSsystemIdentity"/>
        <element ref="CBI:TimeStamp"/>
        <element ref="CBI:SubscriberIdentity"/>
        <element ref="CBI:DeviceAddress"/>
        <element ref="CBI:AccessSessionId"/>
        <element ref="CBI:SignalCaptureFileName" minOccurs="1"/>
        <element ref="CBI:Hash" minOccurs="1"/>
    </sequence>
</complexType>
</element>
<element name="PacketDataSummaryReport">
    <complexType>
        <sequence>
            <element ref="CBI:CaseIdentity"/>
            <element ref="CBI:IAPSystemIdentity"/>
            <element ref="CBI:TimeStamp"/>
            <element ref="CBI:AccessSessionId"/>
            <element ref="CBI:PacketSignature" maxOccurs="unbounded"/>
        </sequence>
    </complexType>
</element>
<element name="SurveillanceStatusReport">
    <complexType>
        <sequence>
            <element ref="CBI:CaseIdentity"/>
            <element ref="CBI:MFSsystemIdentity"/>
            <element ref="CBI:TimeStamp"/>
            <element ref="CBI:AccessSessionId"/>
            <element ref="CBI:DeviceAddress"/>
            <element ref="CBI:LocationInformation"/>
            <element ref="CBI:Status"/>
        </sequence>
    </complexType>
</element>
<element name="CBISMessage">
    <complexType>
        <choice>
            <element ref="CBI:AccessAttempt"/>
            <element ref="CBI:AccessAccepted"/>
            <element ref="CBI:AccessFailed"/>
            <element ref="CBI:AccessSessionEnd"/>
            <element ref="CBI:SurveillanceStatusReport"/>
        </choice>
    </complexType>
</element>
<element name="CBISMessages">
    <complexType>
        <sequence>
            <element ref="CBI:CBISMessage" maxOccurs="unbounded"/>
        </sequence>
    </complexType>
</element>
</schema >

```

Appendix I Limited Intercept XML Instance Document File³⁵

```
<?xml version="1.0"?>
<CBI:PacketDataSummaryReport
xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI-1.0.xsd">
  <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
  <CBI:IAPSystemIdentity>cmts-coll.mso.com</CBI:IAPSystemIdentity>
  <CBI:TimeStamp>2007-04-06T17:16:34.000000Z</CBI:TimeStamp>
  <CBI:AccessSessionId>5671986</CBI:AccessSessionId>
  <CBI:PacketSignature>
    <CBI:sourceAddress>23.45.32.12</CBI:sourceAddress>
    <CBI:destAddress>197.200.1.45</CBI:destAddress>
    <CBI:sourcePort>32456</CBI:sourcePort>
    <CBI:destPort>80</CBI:destPort>
    <CBI:protocol>6</CBI:protocol>
    <CBI:NumPktsSinceLastReport>4564</CBI:NumPktsSinceLastReport>
    <CBI:NumBytesSinceLastReport>456422</CBI:NumBytesSinceLastReport>
    <CBI:FirstPacketTime>2007-04-06T17:16:31.000000Z</CBI:FirstPacketTime>
    <CBI:LastPacketTime>2007-04-06T17:16:33.000000Z</CBI:LastPacketTime>
  </CBI:PacketSignature>
  <CBI:PacketSignature>
    <CBI:sourceAddress>197.200.1.45</CBI:sourceAddress>
    <CBI:destAddress>23.45.32.12</CBI:destAddress>
    <CBI:sourcePort>80</CBI:sourcePort>
    <CBI:destPort>32456</CBI:destPort>
    <CBI:protocol>6</CBI:protocol>
    <CBI:NumPktsSinceLastReport>2855612</CBI:NumPktsSinceLastReport>
    <CBI:NumBytesSinceLastReport>285561223</CBI:NumBytesSinceLastReport>
    <CBI:FirstPacketTime>2007-04-06T17:16:21.000000Z</CBI:FirstPacketTime>
    <CBI:LastPacketTime>2007-04-06T17:16:33.000000Z</CBI:LastPacketTime>
  </CBI:PacketSignature>
</CBI:PacketDataSummaryReport>
```

In the case where there are no UDP ports, such as ICMP, the fivetuple structure is maintained by using a null UDP port field in the PacketSignature element. A PacketSignature element with null transport ports is shown as follows:

```
<CBI:PacketSignature>
  <CBI:sourceAddress>23.45.32.12</CBI:sourceAddress>
  <CBI:destAddress>197.200.1.45</CBI:destAddress>
  <CBI:sourcePort></CBI:sourcePort>
  <CBI:destPort></CBI:destPort>
  <CBI:protocol>1</CBI:protocol>
  <CBI:NumPktsSinceLastReport>4564</CBI:NumPktsSinceLastReport>
  <CBI:NumBytesSinceLastReport>285561223</CBI:NumBytesSinceLastReport>
  <CBI:FirstPacketTime>2007-04-06T17:16:21.000000Z</CBI:FirstPacketTime>
  <CBI:LastPacketTime>2007-04-06T17:16:33.000000Z</CBI:LastPacketTime>
</CBI:PacketSignature>
```

IPv6 example:

```
<CBI:PacketSignature>
  <CBI:sourceAddress>FE80:0:0:0:202:B3FF:FE1E:8329</CBI:sourceAddress>
  <CBI:destAddress>CAFF:CA01:0:56:0:ABCD:EF12:1234</CBI:destAddress>
  <CBI:sourcePort></CBI:sourcePort>
```

³⁵ CBI2.0-N-07.0517-1, 10/23/7, PO, revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB, revised per CBI2.0-13.1111-2 on 9/25/13 by PO.

```
<CBI:destPort></CBI:destPort>
<CBI:ipv6FlowLabel></CBI:ipv6FlowLabel>
<CBI:protocol>1</CBI:protocol>
<CBI:NumPktsSinceLastReport>4564</CBI:NumPktsSinceLastReport>
<CBI:NumBytesSinceLastReport>456422</CBI:NumBytesSinceLastReport>
<CBI:FirstPacketTime>2007-04-06T17:16:31.000000Z</CBI:FirstPacketTime>
<CBI:LastPacketTime>2007-04-06T17:16:33.000000Z</CBI:LastPacketTime>
</CBI:PacketSignature>
```

Appendix II Out of Band Messages - XML Instance Document File ³⁶

II.1 Out of Band Access Attempt Message - XML Instance Document File

```
<?xml version="1.0"?>
< CBI:AccessAttempt xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
  <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
  <CBI:MFSYSTEMIdentity>MF-01.mso.com</CBI:MFSYSTEMIdentity>
  <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
  <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
    <CBI:AccessDevice>
      <CBI:AccessDeviceType>other</CBI:AccessDevice Type>
      <CBI:AccessDeviceID>11-00-AA-FE-80-1A</CBI:AccessDeviceID>
    </CBI:AccessDevice>
  <CBI:CMTSID>MF-01.mso.com</CBI:CMTSID>
  <CBI:SignalCaptureFileName>Bill-
Kostka/oob/0045.dmp</CBI:SignalCaptureFileName>

  <CBI:Hash>1EEEC054802A56B0F2C612A596CF367EE392A84C30FC6826A21B951A9302A6BA</CBI:Hash>
</CBI:AccessAttempt>
```

II.2 Out of Band Access Accepted Message - XML Instance Document File ³⁷

```
<?xml version="1.0"?>
<CBI:AccessAccepted xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
  <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
  <CBI:MFSYSTEMIdentity>MF-01.mso.com</CBI:MFSYSTEMIdentity>
  <CBI:TimeStamp>2007-05-12T18:11:08.500000Z</CBI:TimeStamp>
  <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
    <CBI:AccessDevice>
      <CBI:AccessDeviceType>other</CBI:AccessDevice Type>
      <CBI:AccessDeviceID>11-00-AA-FE-80-1A</CBI:AccessDeviceID>
    </CBI:AccessDevice>
  <CBI:CMTSID>MF-01.mso.com</CBI:CMTSID>
  <CBI:DeviceAddress>178.46.11.48</CBI:DeviceAddress>
  <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
  <CBI:LocationInformation>
    <civicAddress>
      <country>US</cl:country>
      <A1>New York</cl:A1>
      <A3>New York</cl:A3>
      <A6>Broadway</cl:A6>
      <HNO>123</cl:HNO>
      <LOC>Suite 75</cl:LOC>
      <PC>10027-0401</cl:PC>
    </civicAddress>
  </CBI:LocationInformation>
  <CBI:SignalCaptureFileName>Bill-
Kostka/oob/0046.dmp</CBI:SignalCaptureFileName>

  <CBI:Hash>27BCB529476953D419FC029B7A558CEA50F72DD872E6D75229842FB9630B2844</CBI:Hash>
```

³⁶ Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB, updated by CBI2.0-N-13.1110-2 on 9/25/13 by PO.

³⁷ Updated per CBI2.0-N-08.0677-1, 12/02/08 by JS, updated by CBI2.0-N-13.1110-2 on 9/25/13 by PO.

</CBI:AccessAccepted>

II.3 Out of Band Access Failed Message - XML Instance Document File³⁸

```
<?xml version="1.0"?>
<CBI:AccessFailed xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
  <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
  <CBI:MFSsystemIdentity>MF-01.mso.com</CBI:MFSsystemIdentity>
  <CBI:TimeStamp>2007-05-14T18:23:12.750000Z</CBI:TimeStamp>
  <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
  <CBI:DeviceAddress>178.46.11.48</CBI:DeviceAddress>
  <CBI:FailureReason>DHCPv4NAK</CBI:FailureReason>
  <CBI:SignalCaptureFileName>Bill-
Kostka/oob/0052.dmp</CBI:SignalCaptureFileName>

  <CBI:Hash>F84957A8AEE3F5B5563C48149F997FFE2978BB97B21EC49FCFC1E5229459DB65</CBI:Hash>
</CBI:AccessFailed>
```

II.4 Out of Band Access Session End Message - XML Instance Document File³⁸

```
<?xml version="1.0"?>
<CBI:AccessSessionEnd xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
  <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
  <CBI:MFSsystemIdentity>MF-01.mso.com</CBI:MFSsystemIdentity>
  <CBI:TimeStamp>2007-05-12T21:03:34.250000Z</CBI:TimeStamp>
  <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
  <CBI:DeviceAddress>178.46.10.131</CBI:DeviceAddress>
  <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
  <CBI:SignalCaptureFileName>Bill-
Kostka/oob/0047.dmp</CBI:SignalCaptureFileName>

  <CBI:Hash>57CB73A6A68D706819D666889F085EF715181AF42B85E58A364BEA3F4C787A88</CBI:Hash>
</CBI:AccessSessionEnd>
```

II.5 Out of Band Surveillance Status Report Message - XML Instance Document File³⁸

```
<?xml version="1.0"?>
<CBI:SurveillanceStatusReport
xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
  <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
  <CBI:MFSsystemIdentity>MF-01.mso.com</CBI:MFSsystemIdentity>
  <CBI:TimeStamp>2007-05-12T19:38:15.000000Z</CBI:TimeStamp>
  <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
  <CBI:Status>
    <CBI:StatU.S.C.ode>Heartbeat</CBI:StatU.S.C.ode>
    <CBI:StatusDetails/>
  </CBI:Status>
</CBI:SurveillanceStatusReport>
```

³⁸ Changed per CBI2.0-N-08.0677-1, 12/02/08 by JS.

Appendix III Physical Consideration

Under circumstances where the LEA is providing the BIF, the following list identifies some of the items the MSO and LEA should discuss and resolve prior to the intercept start date.

Powering: 117 VAC or -48 VDC

Structural: 19" Racks or 23" racks

HVAC: Power consumption for all components

Physical space: Rack Space in RU's

Physical security: Rack doors, room access, etc.

Data Communication: Connectors and Wiring

Appendix IV Example Flow Chart Implementation

These flowcharts are not intended to depict complete or reference implementations. They are intended to facilitate a better understanding of the Cable Broadband Intercept Specification. There are five sections that follow:

1. Provisioning the functions with data from the CMTS
2. The Access Function, Intercept Access Points, and Out-of-Band Processing
3. Packet Processing: full intercepts and limited intercepts
4. The file manager
5. The Broadband Intercept Function

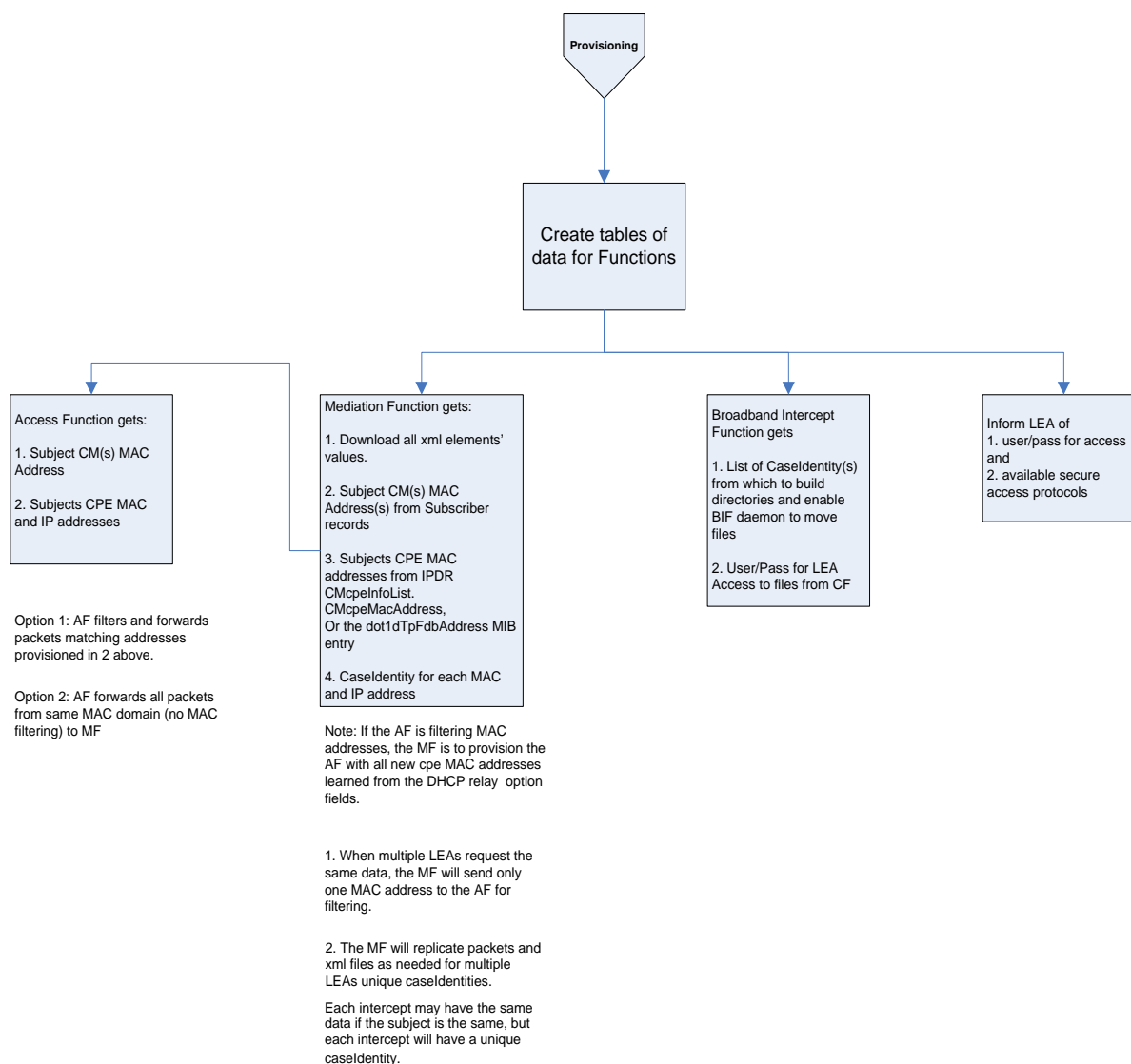


Figure 3 - Provisioning the functions with data from the CMTS³⁹

³⁹ Figure 3 updated by CBI2.0-N-0517-2, 10/22/07, PO.

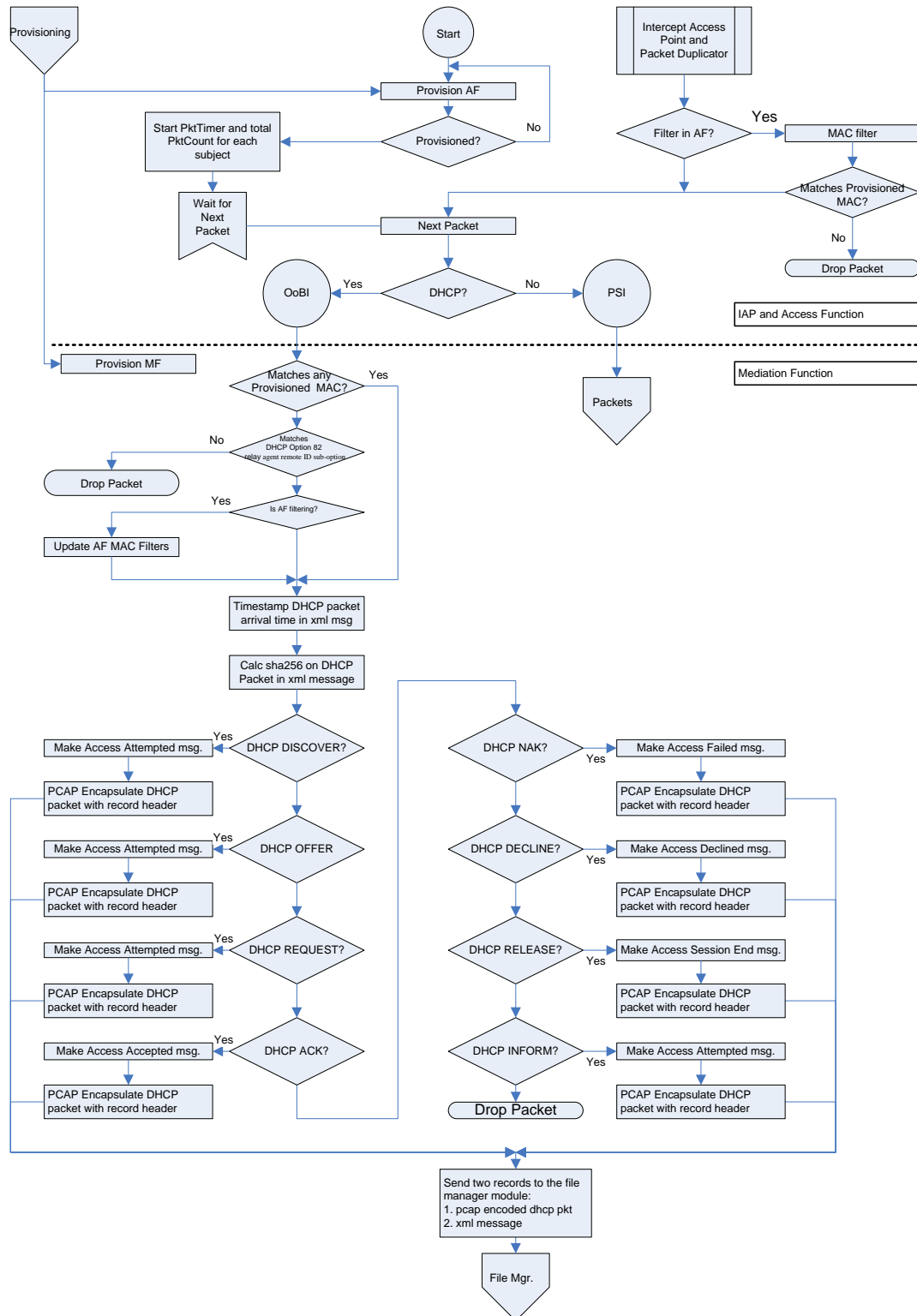


Figure 4 - The Access Function, Intercept Access Points, and Out-of-Band Processing⁴⁰

⁴⁰ Figure 4 updated by CBI2.0-N-0517-2, 10/22/07, PO.

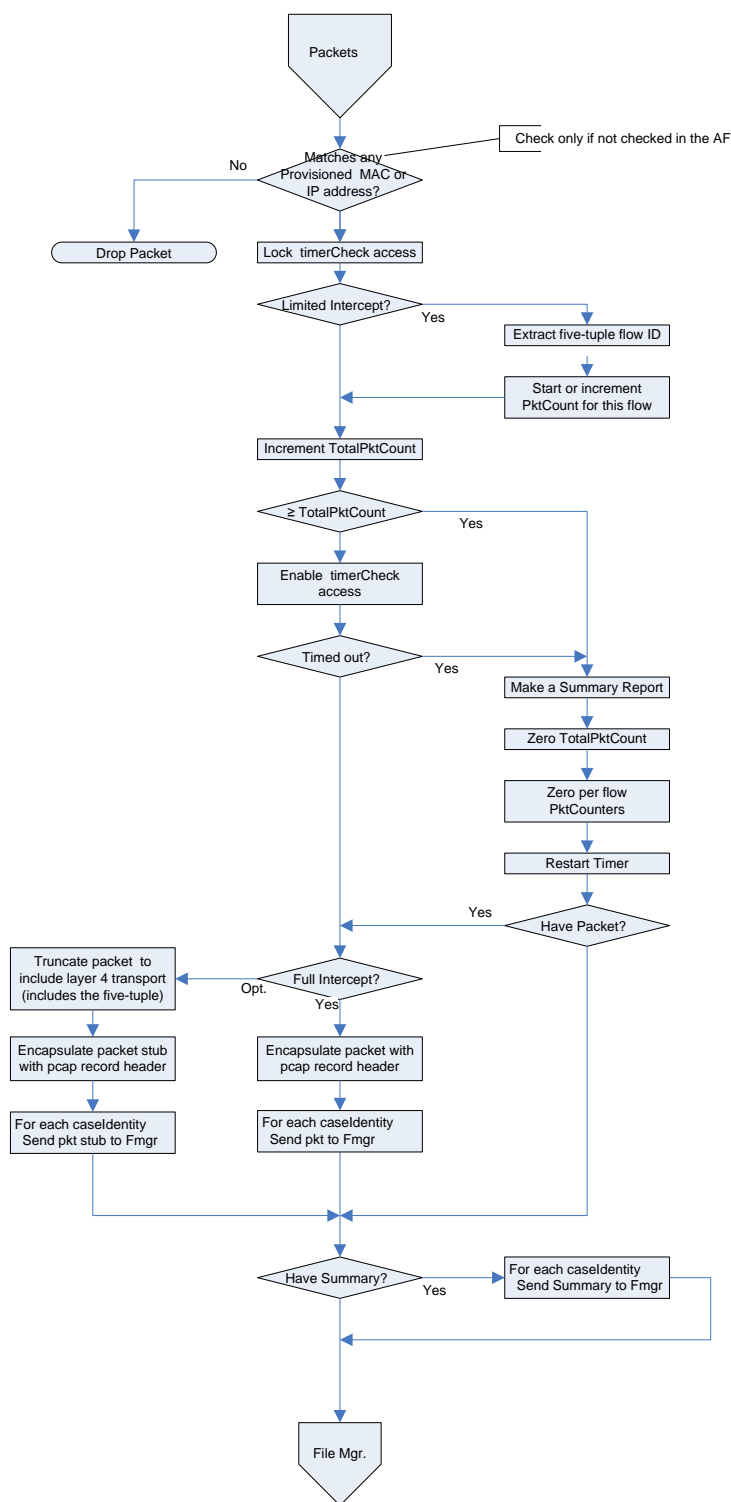
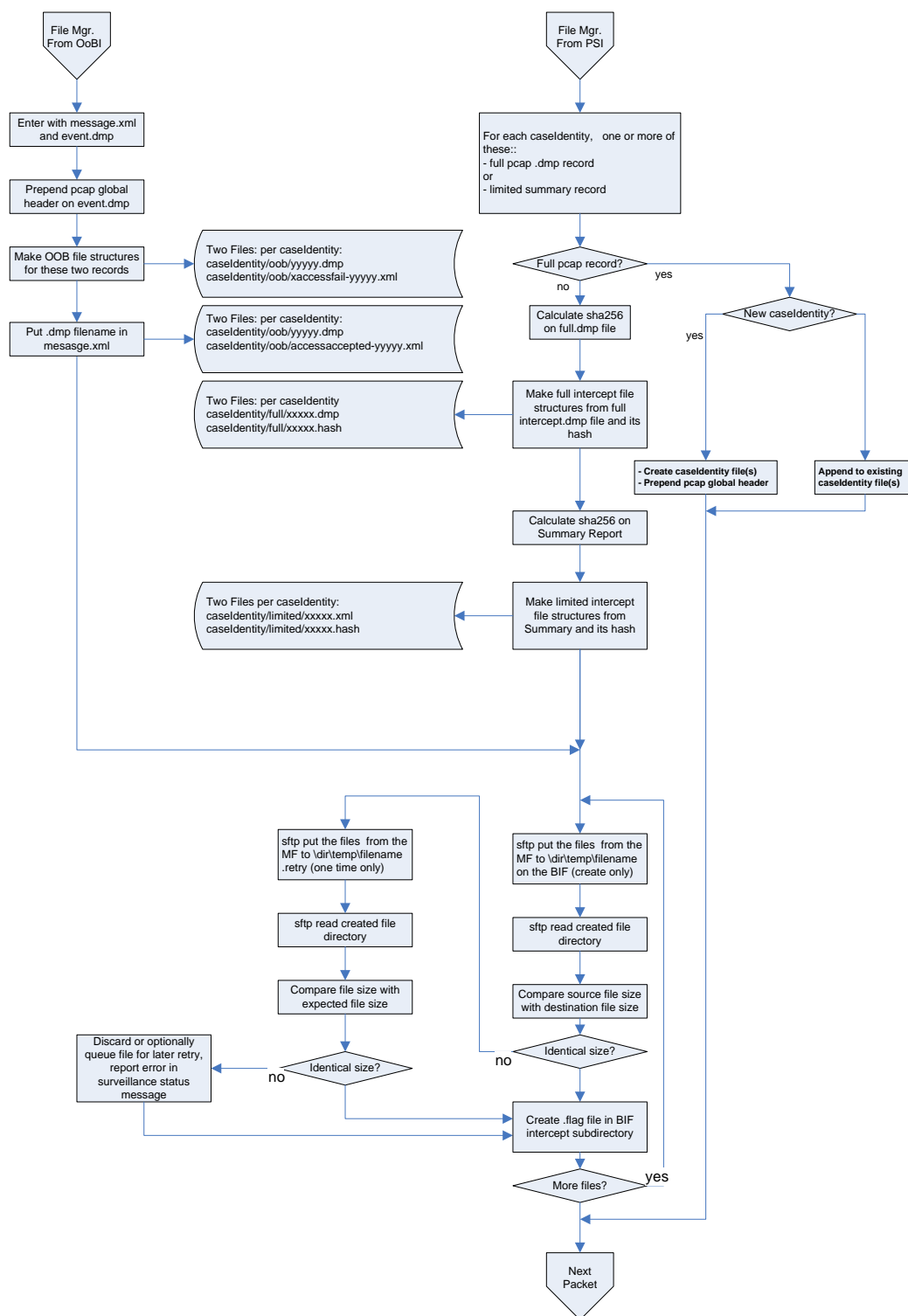


Figure 5 - Packet Processing: full intercepts and limited intercepts⁴¹

⁴¹ Figure 5 updated by CBI2.0-N-0517-2, 10/22/07, PO.

Figure 6 - The file manager⁴²⁴² Figure 6 updated by CBI2.0-N-0517-2, 10/22/07, PO.

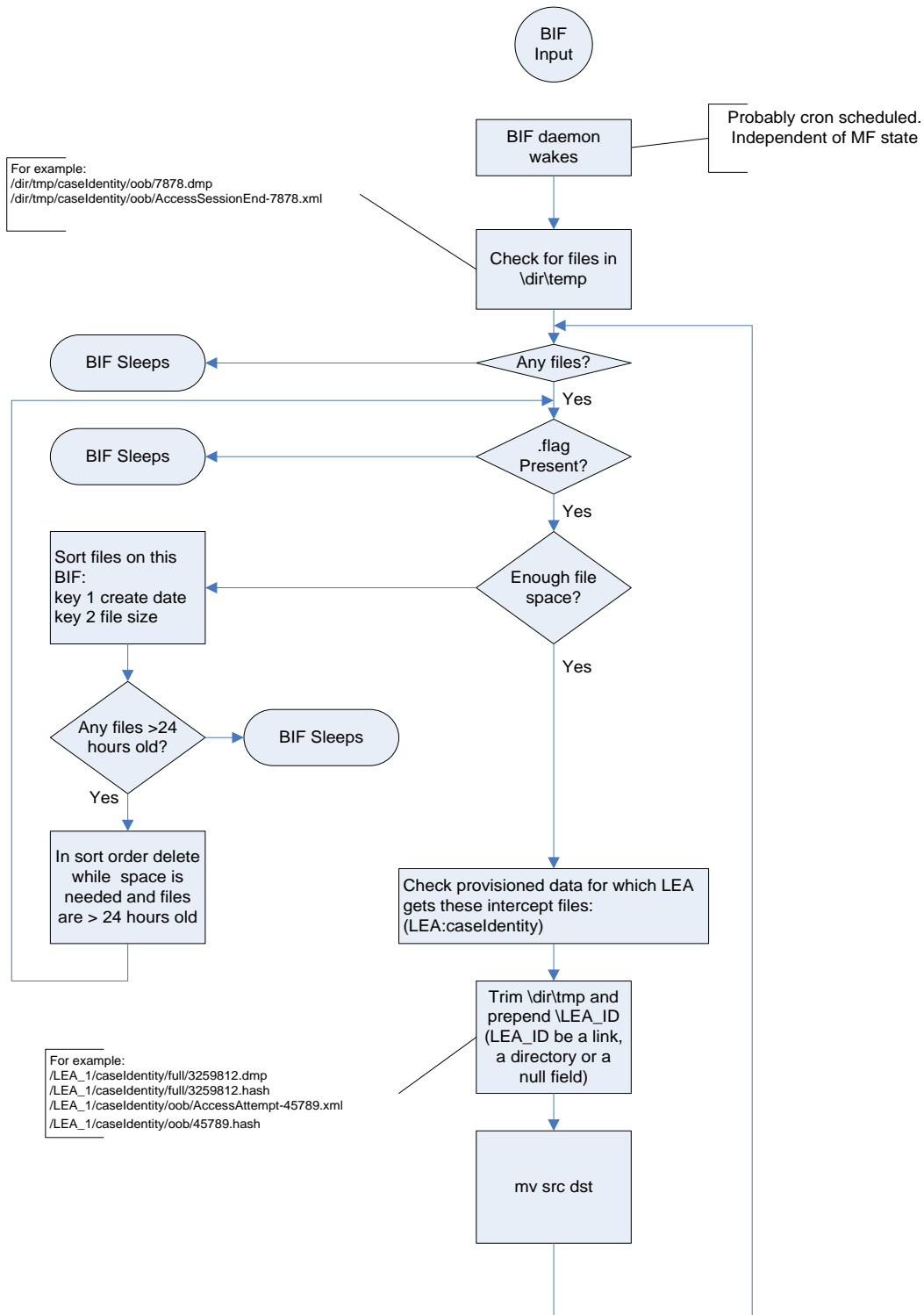


Figure 7 - The Broadband Intercept Function⁴³

⁴³ Figure 7 updated by CBI2.0-N-0517-2, 10/22/07, PO.

Appendix V Acknowledgements

We wish to thank the participants contributing directly to this document:

| | |
|------------------|---|
| Alex Hoff | Sandvine Incorporated |
| Dusty Hoffpauir | NeuStar, Inc. |
| Jeff Hartley | Intensify Security |
| Michael Bilca | FBI CALEA Implementation Unit (Trideaworks) |
| Robert Forsythe | Trideaworks |
| David Bushta | Comcast |
| Craig Mulholland | Cisco Systems |
| Ralph Brown | Cable Television Laboratories, Inc. |
| Eduardo Cardona | Cable Television Laboratories, Inc. |
| Chris Donley | Cable Television Laboratories, Inc. |
| Chris Grundemann | Cable Television Laboratories, Inc. |
| Bill Kostka | Cable Television Laboratories, Inc. |
| Simon Krauss | Cable Television Laboratories, Inc. |
| Lakshmi Raman | Cable Television Laboratories, Inc. |

Karthik Sundaesan, Cable Television Laboratories, Inc.

Appendix VI Revision History

VI.1 Engineering Change for CM-SP-CBI2.0-I02-071206.

The following Engineering Change is incorporated into CM-SP-CBI2.0-I02-071206:

| ECN | Date Accepted | Summary |
|--------------------|---------------|--|
| CBI2.0-N-07.0517-1 | 9/12/2007 | Compendium of minor fixes and clarifications to CBI2.0, editorially renumbered requirements. |

VI.2 Engineering Changes for CM-SP-CBI2.0-I03-090121.

The following Engineering Changes are incorporated into CM-SP-CBI2.0-I03-090121:

| ECN | Date Accepted | Summary |
|--------------------|---------------|---|
| CBI2.0-N-08.0677-1 | 7/2/2008 | CBIS I02 Omnibus |
| CBI2.0-N-08.0678-1 | 7/2/2008 | BIF Directory structure update |
| CBI2.0-N-09.0767-1 | 1/7/2009 | Correct Req Numbering error in CBI2.0-N-08.0677-1 |

VI.3 Engineering Change for CM-SP-CBI2.0-I04-110224.

The following Engineering Change is incorporated into CM-SP-CBI2.0-I04-110224:

| ECN | Date Accepted | Summary |
|--------------------|---------------|-------------------------------------|
| CBI2.0-N-10.0976-1 | 01/05/11 | I04 Update - update to include IPv6 |

VI.4 Engineering Change for CM-SP-CBI2.0-I05-130507.

The following Engineering Changes are incorporated into CM-SP-CBI2.0-I05-130507:

| ECN | Date Accepted | Summary | Author |
|--------------------|---------------|---|------------|
| CBI2.0-N-13.1097-1 | 4/3/2013 | Corrections to address issues raised by FBI CALEA Implementation Unit (CIU) at 12/5/11 meeting. | Brown |
| CBI2.0-N-13.1098-1 | 4/3/2013 | Multiple BIF | Grundemann |

VI.5 Engineering Change for CM-SP-CBI2.0-I06-131003.

The following Engineering Changes are incorporated into CM-SP-CBI2.0-I06-131003:

| ECN | Date Accepted | Summary | Author |
|--------------------|---------------|---|----------|
| CBI2.0-N-13.1111-2 | 7/3/2013 | Corrections to XML Schema and other definitions | Brown |
| CBI2.0-N-13.1110-2 | 7/3/2013 | Removal of vestiges of Access Decline event | Forsythe |