Data-Over-Cable Service Interface Specifications

Cable Broadband and Wi-Fi Intercept Specification

CM-SP-CBI2.0-I10-160211

Issued

Notice

DISCLAIMER

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. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members 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.

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 entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any 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-I10-160211
Document Title:	Cable Broadband and Wi-Fi 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 I07 – Released 07/29/14 I08 – Released 06/25/15 I09 – Released 10/15/15 I10 – Released 02/11/16
Date:	February 11, 2016
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 generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks:

Contents

Figures

Tables

1 SCOPE

1.1 Introduction and Purpose [1]

This specification defines the interfaces between a cable Multiple System Operator's ("MSO's") DOCSIS® and public Wi-Fi network elements and the Law Enforcement Agency (LEA). These interfaces 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, revised per CBI2.0-N-14.1227-5 on 6/16/15 by PO.

2   REFERENCES

2.1   Normative References [2]

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.

[CBI2.0]   CBI2.0 XML Schema http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI/

[DHCPv4 Options]   IETF RFC 3396 Encoding Long Options in Dynamic Host Configuration Protocol (DHCPv4), November 2002.

[DHCPv4]   IETF RFC 2131 Dynamic Host Configuration Protocol for IPv4, March 1997.

[DHCPv6]   IETF RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.

[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/STD 05, Internet Protocol, Postel, J., Internet Protocol, 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, Location Object (PIDF-LO), February 2008.

[WIFI-1.0]   XML schema for Wi-Fi Lawful Intercept Records, http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI

---

[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. Updated by CBI2.0-N-14.1227-5 on 6/16/15 by PO.

2.2   Informative References

This specification uses the following informative references. [3]

[14FCC]	*In the Matter of Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794 (1999): http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1999/fcc99011.txt
[20FCC]	*In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, 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& =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
[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
[Wi-Fi GW]	WiFi Requirements for Cable Modem Gateways, WR-SP-WiFi-GW-I05-150515, May 15, 2015, Cable Television Laboratories, Inc.
[Wi-Fi ROAM]	WiFi Roaming Architecture and Interfaces Specification, WR-SP-WiFi-ROAM-I04-141201, December 1, 2014, Cable Television Laboratories, Inc.
[W3C-SCHEMA]	www.w3c.org/XML/Schema World Wide Web Consortium

---

[3] Updated by CBI2.0-N-14.1227-5 on 6/16/15 by PO.

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 [4]

This specification uses the following terms:

Term	Definition
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.
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 cable broadband communications of a Subject.
Broadband Intercept Function	The function that implements buffering of cable 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 sixtuple. 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.
Home Network	When used within the context of Wi-Fi Roaming, the Home Network holds the subscription of an MSO Wi-Fi subscriber and executes authentication for the sake of admission on the Home Wi-Fi network or a visited Wi-Fi 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.

---

[4] Updated by CBI2.0-N-07.0517-1, 10/23/07 by PO, CBI2.0-N-07.0517-1, 10/23/07 by PO, updated by CBI2.0-N-14.1227-5 on 6/16/15 by PO, updated by CBI2.0-N-15.1326-1 on 9/28/15 by PO.

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.
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 an 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.

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.
Subject Wi-Fi Device	The Wi-Fi device used by a Subject, as identified by a unique identifier (e.g., the MAC address of a public Wi-Fi subscriber device). A Subject Wi-Fi Device is only known and connected to the MSO network after it has attempted to be authorized.
Subject Wi-Fi Event	An Authentication, Authorization or Accounting action related to a Subject Wi-Fi Device when connecting or connected to the MSO public Wi-Fi network.
SummaryTimer	A variable that defines how frequently, in seconds, the Packet Data Summary Report is sent.
Visited Network	When used in the context of Wi-Fi Roaming, the visited network provides Wi-Fi access to roamed in subscribers from roaming partner networks.

These definitions are only used within this specification.

Exclusion	The act of removing a specific IP data flow from the data stream by filtering on the ordered set of IPv4 (five-tuple) or IPv6 (six-tuple) packet header parameters that uniquely identify a targeted stream.
Filter Criteria	Identifies the IP data flow(s) to be excluded.
On-Demand	The delivery of a movie, TV program or sports event to a TV set when the customer requests it.
Over the Top (OTT)	Delivery of audio, video and other media over the Internet independent of the MSOs involvement.

4 ABBREVIATIONS AND ACRONYMS [5]

This specification uses the following abbreviations:

AAA	Authentication, Authorization, and Accounting
ACK	Acknowledgement
ADMF	Administrative Function
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
CBI	Cable Broadband Intercept
CBIS	Cable Broadband Intercept Specification
CF	Collection Function
CFI	Collection Function Interface
CM	Cable Modem
CmCC	Communication Content
CmII	Communication Identifying Information
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
IPTV	Internet Protocol Television
LE	Law Enforcement
LEA	Law Enforcement Agency
LI	Lawful Intercept

---

[5] Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB, updated per CBI2.0-N-15.1326-1 on 9/28/15 by PO.

MAC	Media/Medium Access Control
MF	Mediation Function
MFI	Mediation Function Interface
MSO	Multiple System Operator
OOB	Out-of-Band
OOBI	Out-of-Band Interface
OTT	Over-the-Top
PCAP	Packet Capture
PDSR	Packet Data Summary Report
POC	Point of Contact
PPP	Point to Point Protocol
PSI	Packet Stream Interface
SLAAC	Stateless Address Autoconfiguration
SFTP	SSH-2 File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Universal Time Coordinated
VPN	Virtual Private Network

5 OVERVIEW [6]

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

5.1.1 Law Enforcement's Common 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.

5.1.1.1 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

5.1.1.2 Transparency

The Broadband Intercept must be conducted in a transparent manner, i.e., in a manner that prevents the Subject or the Subject Facility, or Subject Device 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.

5.1.1.3 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.

5.1.1.4 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.

---

[6] Updated by CBI2.0-N-14.1227-5 on 6/17/15 by PO.

5.1.1.4.1   Authentication

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

5.1.1.4.2   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.

5.1.1.4.3   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].

5.1.1.5   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 5.1.1.1 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 7.14.1 and Section 7.14.1.3 Broadband Surveillance Event Messages (For Broadband Intercept Order Only).

5.1.1.6   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.

5.1.1.7   Proportionality

Only the authorized communications categories may be intercepted. For more information, see Section 5.1.1.1 Intercept Categories and Section 7.12 Intercept Categories.

5.1.1.8   Completeness

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

5.1.1.9   Compression

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

5.1.1.10   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.

5.1.1.11 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.

5.1.1.12 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.

5.1.2   Intercept Requirements for Wi-Fi Roaming[7]

Cable operators may arrange for internetwork Wi-Fi roaming, where a subscriber from one operator is allowed access onto a roaming partner network. See [Wi-Fi ROAM]. Interception functions in the Home and Visited Wi-Fi networks operate independently and transparently from each other.

5.1.2.1   Additional Public Wi-Fi Requirements for Chronology

Wi-Fi Device MAC addresses and subscriber credential user names can be used as subject intercept identifiers in the Home Wi-Fi network. Visited networks may not have access to subscription credentials, and may only be able to detect and verify the Wi-Fi MAC address of roamed in subscriber devices.

5.1.2.2   Additional Public Wi-Fi Requirements for Correlation

Correlation of intercepted events and intercepted user traffic are required for services executed within a single Wi-Fi operator network. Correlation of reported events and traffic reported across the Visited and Home networks is not required.

5.1.2.3   Additional Public Wi-Fi Requirements for Isolation

When subject facilities segregate traffic into multiple domains (e.g., the private versus public sides of a Community Wi-Fi-capable CM), the MSO must be capable of isolating the traffic within one or more domains.

If a Subject Wi-Fi Device identifier ceases to be associated with the subject, the MSO must expeditiously cease interception based on that identifier. This may occur when a user device with a particular MAC address that had registered for hotspot access with the network using a subject user name/password, is re-registered with the network using a different user name and password. Note that this requirement does not apply to visited networks that do not have access to the subject subscriber user name credential.

5.1.2.4   Completeness

All communications of subject facilities identified by the Wi-Fi Intercept Order must be intercepted for the entire period authorized by the Wi-Fi Intercept Order.

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 5.1.1:

- 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

---

[7] Added by CBI2.0-N-14.1227-5 on 6/17/15 by PO.

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.
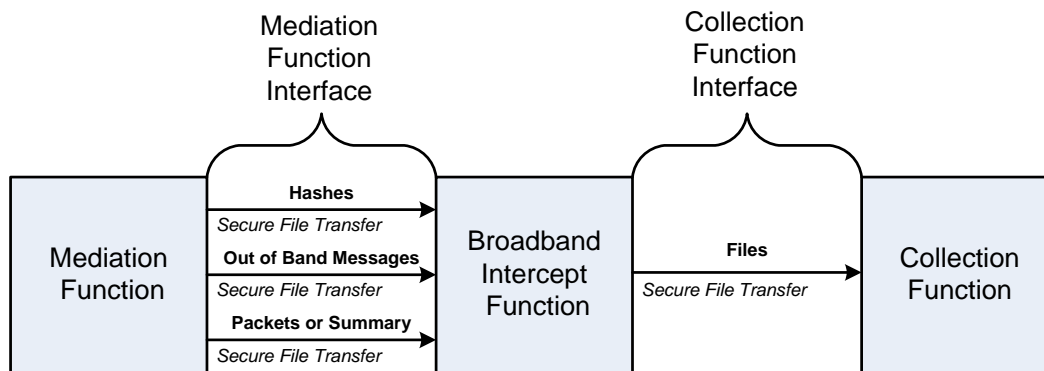
Figure 1 - Logical Network Diagram
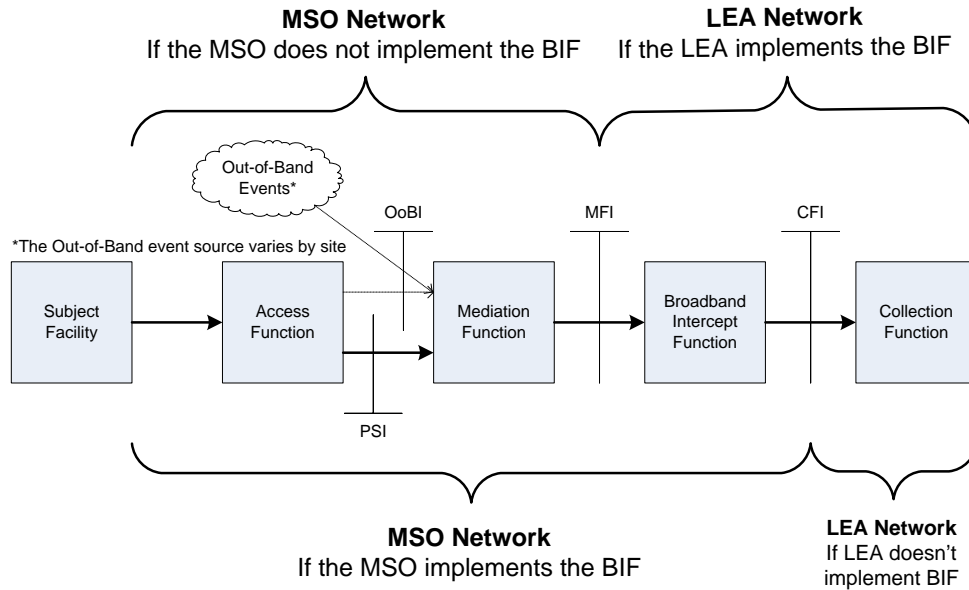
Figure 2 - Broadband Intercept Interfaces

5.3   Cable Operator Public Wi-Fi Intercept Architecture[8]

The interface between cable operator public Wi-Fi networks and the LEA will be at the CFI or MFI as shown in Figure 2.

A subscriber device can attach to public Wi-Fi access points in either the user's Home network or an interconnected Visited network. The intercepted packet data and intercept related event information can be delivered for only activities on that given public Wi-Fi network. In general, the Home network will not have access to user traffic of subscribers roamed out onto Visited networks.

In a cable operator public Wi-Fi network, the subject of an intercept order is no longer identified in the network by a fixed CM attached to a CMTS. The subject of an intercept can be identified by either the MAC address of the subject Wi-Fi device or the subject's subscription credential User-name. In the visited network, the subscription credential User-name is often passed in an encrypted tunnel between the subject Wi-Fi device and the Home network AAA server, with the Visited network AAA proxy serving as the conduit for the encrypted tunnel. When the Home network has authenticated and authorized a subscriber based on User-name, the Visited network will be informed and traffic sessions will be setup based on the authenticated credentials and authorized MAC address. Thus, only the Visited network would be able to correlate the Wi-Fi device MAC address with one or more dynamically assigned IP addresses used for the session. Only the Home network may be able to correlate the User-name with an authorized MAC address.

---

[8] Added by CBI2.0-N-14.1227-5 on 6/17/15 by PO.

---

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 [9]

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 [10]

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 that 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

---

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

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.

3.   If the MSO implements the public Wi-Fi network service, it MUST follow the "R-XX W" requirements.

The requirements without an MFI, CFI or Wi-Fi 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 of the cases.

7.1   Transparency

R-10   The MF MUST perform the intercept in a manner that is transparent (undetectable) by the Subject, 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) a Subject Device, or the customer premise equipment.

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 Integrity [12]

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.

---

[11] Updated by CBI2.0-N-14.1227-5 on 6/17/15 by PO.
[12] Changed section per CBI2.0-N-08.0678-1, 12/02/08 by JS.

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 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 5.1.1.1 Intercept Categories and Section 7.12 Intercept Categories.

7.5   Completeness [13]

R-100   All Subject traffic, both to and from the Subject Facility with the exception of what has been requested to be specifically excluded by the LEA through an Exclusion of Flow(s) request, MUST be intercepted for the entire period authorized by the Broadband Intercept Order. For Wi-Fi, service begins after the subject is authenticated to the wireless system. 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.[14]

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.

---

[13] Updated by CBI2.0-N-14.1227-5 on 6/17/15 by PO, and CBI2.0-N-15.1326-1 on 9/28/15 by PO.
[14] CBI2.0-N-07.0517-2, 10/22/07, PO.

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.

The two variables, PacketCaptureDuration and PacketCaptureCount, are intended to assist the MSOs and LEAs in achieving the required performance outlined in R130 and R140.[15]

7.9   Connectivity Requirements [16]

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 R-389.

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.

By 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).

---

[15] CBI2.0-N-07.0517-2, 10/22/07 by PO.
[16] CBI2.0-N-13.1098-1, 5/2/13 by PO.

R-240   The SFTP cryptographic algorithms/strength MUST be negotiated by the MSO and LE prior to initiating the intercept.[17]

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.

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 7.14 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 7.14 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) [18]

R-320   The full set of IP packets associated with the Subject Facility MUST be isolated and captured.

R-322   When an Exclusion of Flow(s) has been authorized and implemented, the IP packets matching the filter criteria MUST be excluded.

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.[19]

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) [20]

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 sixtuple that defines a unique flow, the count of packets for that flow since the last report (numPktsSinceLastReport), and the number of

---

[17] New changes 210-230 and subsequent renumbering per CBI2.0-N-07.0517-2, 10/22/07, PO.
[18] CBI2.0-N-15.1326-1 on 9/28/15 by PO.
[19] CBI2.0-N-07.0517-2, 10/22/07, PO.
[20] Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.

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.

7.13 Interception within the Home and Visited Network [21]

R-382   The network in which the subject's device is attached for public Wi-Fi services MUST report Out-of-band events and Subject Traffic as authorized by intercept order.

R-384   The Home Network MUST reports related to authentication and accounting signaling that is used by the Home Network to authenticate, authorize and account for subscribers for services on a roaming partner Visited Network. The Home Network cannot report Subject Traffic for subscribers roamed out onto Visited Networks.

7.14 xml Requirements [22]

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.

The requirements are broken down into the following sections.

Table 1 - xml Requirement Categories

Section	Title	Common, Broadband, or Wi-Fi
7.14.1	Common Event Messages and Reports	Common
7.14.1.3	Broadband Surveillance Event Messages	Broadband
7.14.2	Wi-Fi Surveillance Event Messages	Wi-Fi
7.14.3	Event Parameters	
7.14.3.1	Parameter Definitions	Common
7.14.3.2	Common Message Parameters	Common
7.14.3.3	Broadband Message Parameters	Broadband
7.14.3.4	Public Wi-Fi Message Parameters	Wi-Fi

7.14.1 Common Event Messages and Reports

The Packet Data Summary Report and the Surveillance Status Report apply to all intercept order types.

7.14.1.1 *Packet Data Summary Report (For Limited Intercept Order Only)* [23]

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

---

[21] Added by CBI2.0-N-14.1227-5 on 6/17/15 by PO.
[22] Section changed and renumbered by JS per CBI2.0-N-07.0677-1 on 12/2/08 and CBI2.0-N-09.0767-1 on 1/15/09; updated by CBI2.0-N-14.1227-5 on 6/17/15 by PO.
[23] Modified per CBI2.0-N-15.1396-1 by KB on 1/29/15.

     R-388   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.

     R-386   Each Packet Data Summary Report within each unique flow MUST add a sequence number to the packet summary report which can be used to determine if a summary report is missing. The start and end time MUST correspond to the first and last packets of each flow within that report period.

     R-387   Packet Data Summary Reports MUST be reported per IAP.

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 (i.e., the Packet Count and Byte Count) 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 Byte Count is a directional count, and needs to be clearly identified.

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

7.14.1.2 Surveillance Status Report

This event is used to provide surveillance status reports.

     R-389   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.
  - 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.

7.14.1.3 Broadband Surveillance Event Messages (For Broadband Intercept Order Only) [24]

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

The following table illuminates the relationship between DHCP messages and LE events of interest. If a DHCP Event packet is received, the corresponding CBIS 0oB message, shown in Table 2, 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 an 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.[25]

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

---

[24] Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.
[25] Surveillance Event messages section modified by CBI2.0-N-07.0517-1, 10/23/07, PO.

Table 2 - DHCP Events of Interest to LE [26]

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
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[27]
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

7.14.1.3.1 Access Attempt [28]

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).

---

[26] Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB.
[27] CBI2.0-N-07.0517-1, 10/23/07, PO.
[28] Updated per CBI2.0-N-13.1111-2 on 9/26/13 by PO.

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.

7.14.1.3.2 Access Session Accepted [29]

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 activity to determine if an IP address under surveillance has been allocated to a different device. Such DHCP activity MUST be captured.[30]

7.14.1.3.3 Access Failed [31]

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.

7.14.1.3.4 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.[32]

---

[29] Updated per CBI2.0-N-13.1111-2 on 9/26/13 by PO.
[30] CBI2.0-N-07.0517-1, 10/23/07
[31] Revised per CBI2.0-13.1110-2 on 9/25/13 by PO.
[32] 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.

7.14.2 Wi-Fi Surveillance Event Messages (For public Wi-Fi Intercept Order Only) [33]

The following Subject Wi-Fi Events are applicable to the AAA Server in the Home network:

- Access Attempt

- Access Failed

- Access Session Accepted

- Access Session End (when available)

- Surveillance Status Report

The following subject Wi-Fi Events are applicable to the Public Access Control Gateway & AAA Proxy in the Visited network:

- Access Attempt

- Access Failed

- Access Session Accepted

- Access Session End (when available)

- Packet Data Summary Report

- Surveillance Status Report.

A formal Access Session End event may not be a common occurrence in the public Wi-Fi network. There are three ways the Visited network determines a session end: (1) a session time out value is exceeded based on a time out value set in the initial authorization; (2) an idle time out value is exceeded based on a time out value set in the initial authorization; and (3) an explicit request from the Home network. The first two cases do not result in any formal actions or reporting in the Visited network unless RADIUS accounting is enabled within the Visited network.

7.14.2.1 Subject Identity

The subject of an intercept can be identified by either a User-name or a Wi-Fi device MAC address. A subject connects to the network via one or more Wi-Fi devices. At the time of authorization and authentication, the Home network authenticates a Wi-Fi device based on the credentials, typically a User-name and password, supplied by the user device in the authentication messages securely tunneled between the Wi-Fi device and the AAA server in the Home network. Once the Home network authenticates the user, it authorizes the Visited network to provide service to a specific device MAC address. The Home network MAY authorize multiple device MAC addresses for the same User-name in one or more public Wi-Fi networks. Visited networks may only know a subject based on an authorized device MAC address.

7.14.2.2 Location Information Reporting

When location information is lawfully authorized and is reasonably available, the MSO must report the location type and the actual location of the subject facility at the start and end of a communication. The MSO must report all location information reasonably available, which may include multiple sets of location information, for example:

- Location Type = "civic address", Location = PIDF-LO;

- Location Type = "lat/long", Location = " 38.8951N, 77.0367W";

- Location Type = "access point ID", Location = "Hotspot-01.mso.com".

When authorized and reasonably available, location information must be reported at the time of Access Session Accepted and Access Session End events (see Sections 7.14.2.5 and 7.14.2.6) and Surveillance Status Report events when the Surveillance Status Report event is associated with the activation or deactivation of an intercept during an active session (see Section 7.14.1.2).

---

[33] Added by CBI2.0-N-14.1227-5 on 6/17/15 by PO.

7.14.2.3 Access Attempt

This event occurs when an MSO network detects that a subject facility has attempted to register or re-register with the MSO network.

If the MSO allows multi-login, where the same registration credentials are used multiple times to establish multiple concurrent and distinct access sessions, a separate Access Attempt event occurs for each session.

R-w71   The Access Attempt event MUST be reported when an access request has been attempted (e.g. when a Subject attempts to connect a Wi-Fi device to the MSO public Wi-Fi network).

R-w72   If the MSO allows multiple devices to access the network using the same credentials (e.g. Username), then each access attempt MUST be considered a new access attempt.

7.14.2.4 Access Failed

This event occurs when the MSO is aware that network authentication on its network for a subject facility failed or was rejected and an access session is not established.

R-xxx   The Access Failed event MUST be reported by the Home and Visited networks independently when authorization has failed and access is rejected.

R-w72   If the MSO allows multiple devices to access the network using the same credentials (e.g. Username), then each access failure MUST be reported separately.

7.14.2.5 Access Session Accepted

This event occurs when an MSO public Wi-Fi network grants or re-grants access to its network to a subject facility and IP address(es) are assigned to the subject facility or user device.

If the MSO allows multi-login, where the same registration credentials are used multiple times to establish multiple concurrent and distinct access sessions, a separate Access Session Accepted event is considered to occur for each session.

R-440   The Access Session Accepted event MUST be reported in the Home and Visited networks independently when the authorization is successful and the access has been accepted.

R-445   If the MSO allows multiple devices to access the network using the same credentials (e.g. Username), then each access acceptance MUST be considered a new access accept.

7.14.2.6 Access Session End

This event occurs when the visited MSO network determines that either a session time out or an idle time out has occurred or the Home MSO network makes an explicit request to end the session to the Visited MSO network via a RADIUS message. In the case of a session or idle time out, the Visited MSO network Access Gateway will only report an access session end if RADIUS accounting has been activated. If RADIUS accounting has been activated in the Visited network, a formal RADIUS accounting stop message will be generated when a session or idle time out occurs.

R-xxx   The Access Session End event MUST be independently reported in the Home and Visited network if a RADIUS accounting stop message is generated in the Visited network and sent to the Home network.

R-xxx   The Access Session End event MUST be reported in the Home network when the Home network initiates an explicit request to end the session.

R-xxx   The Access Session End event MUST be reported in the Visited network when it receives a formal request to end a session and the session is active in the Visited network.

7.14.3 Event Parameters

7.14.3.1 Parameter Definitions

The following information elements appear in the Message Parameter tables in Section 7.14.3.2, 7.14.3.3, and 7.14.3.4.

Table 3 - Information Elements and sub elements in Message Parameter Tables [34]

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.
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.
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"
AccountSessionId	string	This attribute is a unique Wi-Fi Accounting ID to make it easy to match start and stop records in a log file
Called Station ID	string	This attribute is the Wi-Fi AP MAC address in ASCII format (upper case only), with octet values separated by a "-". Example: "00-10-A4-23-19-C0".
Calling Station ID	string	This attribute is the Wi-Fi device MAC address in ASCII format (upper case only), with octet values separated by a "-". Example: "00-10-A4-23-19-C0".
Calling station IP address	four octets	IPv4 address of the Wi-Fi device
Calling station ipv6 address	128 bits	IPv6 address of the Wi-Fi device
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.
Content ID	string	Identifies available metadata of the content that was IP filtered, if available.
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.

---

[34] 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, revised CBI2.0-N-13.1111-2 on 9/26/13 by PO, and revised by CBI2.0-N-14.1227-5 on 6/17/15 by PO, revised by CBI2.0-N-15.1326-1 on 9/28/15 by PO; per CBI2.0-N-15.1396-1 by KB on 1/29/15.

Information Element	DataType	Description
Excluded Packet Signature	sequence	Describes a sequence of Five-tuple (in the case of IPv4) and the count of packets and bytes for that Five-tuple or a sequence of Six-tuple (in the case of IPv6) and the count of packets and bytes for that Six-tuple.
Failure Code	string	Report reason why filter could not be implemented.
Failure Reason	string	The value is "DHCPNAK" or "DHCPDECLINE" for IPv4 or "REPLY" or "DECLINE" for IPv6.
Filter Action	string	"Start" or "Stop" exclusion.
Filter Criteria	sequence	Identifies the IP data flow(s) to be excluded.
First Packet Time	sequence	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. 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. See Annex A.2.
Fivetuple Set	sequence	Describes an ordered set of fivetuples (i.e., IP Source, IP Destination, Source Port, Destination Port, Protocol).
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.
Idle Timeout	unsigned integer	The maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.
Last Packet Time	sequence	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. 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. See Annex A.2.
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.

Information Element	DataType	Description
NAS IP Address	octets	Identifies the IPv4 address of the NAS originating the Wi-Fi Access Request
NAS IPv6 Address	binary	Identifies the IPv6 address of the NAS originating the Wi-Fi Access Request
NASId	string	Identifies the NAS originating the Wi-Fi Access-Request
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).
Remarks	string	Provides additional information.
ReplyMessage	text	This Attribute indicates text which MAY be displayed to the Wi-Fi user, although it is not typically reported to the user in current implementations.
Sequence Number	String	Identifies each Packet Data Summary Report within each unique flow. The Sequence Number can be used to determine if a summary report is missing.
Service Type	enumerated list	Indicates the type of service delivered to the Wi-Fi user.
Session Time Out	unsigned integer	This Attribute from the Wi-Fi home network requests the maximum number of seconds of service to be provided to the user before termination of the session or prompt.
Signal Capture File Name	string	Pointer to actual file containing the DHCP messages captured.
Sixtuple Set	sequence	Describes an ordered set of sixtuples (i.e., IPv6 Source, IP v6 Destination, Source Port, Destination port, protocol and flowlabel).
Start Exclusion Time	sequence	Identifies the date and time the exclusion was established.
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.
Stop Exclusion Time	sequence	Identifies the date and time the exclusion was stopped.
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	DataType	Description
Time Stamp	sequence	Identifies the date and time that the event triggering the message was detected. 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. See Annex A.2.

7.14.3.1.1 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 4 - xml Defined Types [35]

Defined Type	Definition	Permitted Values
IpAddr	hexBinary	IPv4 or IPv6 address in hex notation
MacAddress	hexBinary	Mac Address
unsignedLong	64 byte unsigned long integer	0 - to - (2^64 -1)

7.14.3.2 Common Message Parameters [36]

7.14.3.2.1 Packet Data Summary Report Message

Table 5 - Information for Packet Data Summary Report Message [37]

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.
Sequence Number	M	

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.

---

[35] Revised per CBI2.0-N-10.0976-1 on 2/10/11 by JB, revised per CBI2.0-N-14.1139-1 on 7/10/14 by PO.
[36] Added per CBI2.0-N-14.1227-5 by PO on 6/17/15.
[37] Modified per CBI2.0-N-15.1396-1 by KB on 1/29/15.

7.14.3.2.2 Surveillance Status Report Message

Table 6 - Information for Surveillance Status Report Message [38]

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	

7.14.3.2.3 Filter Implementation Message [39]

Table 7 - Information for Filter Implementation Message

Information Element	M/O/C	Condition
Access Session Identity	M	
Case Identity	M	
Device Address	M	
Failure Code	C	Report reason why filter could not be implemented
Filter Action	M	Start or Stop exclusion.
Filter Criteria	M	Identifies the IP data flow(s) to be excluded.
IAP System Identity	M	
MF System Identity	M	
Subscriber Identity	M	
Time Stamp	M	Identifies when the filter criteria has been applied.

---

[38] 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.
[39] Added per CBI2.0-N-15.1326-1 on 9/29/15 by PO.

7.14.3.2.4 Excluded Flow Start Message [40]

Table 8 - Information for Excluded Flow Start Message

Information Element	M/O/C	Condition
Access Session Identity	M	
Case Identity	M	
Device Address	M	
Filter Criteria	M	Identifies the IP data flow(s) to exclude.
IAP System Identity	M	
MF System Identity	M	
Start Exclusion Time	M	Identifies the date and time the exclusion was established.
Subscriber Identity	M	

7.14.3.2.5 Excluded Flow Stop Message [41]

Table 9 - Information for Excluded Flow Stop Message[42]

Information Element	M/O/C	Condition
Access Session Identity	M	
Case Identity	M	
Device Address	M	
Filter Criteria	M	Identifies the IP data flow(s) to exclude.
IAP System Identity	M	
MF System Identity	M	
Stop Exclusion Time	M	Identifies the date and time the exclusion was stopped.
Subscriber Identity	M	

7.14.3.2.6 Periodic Filter Summary Log Report Message

Table 10 - Information for Periodic Filter Summary Log Message

Information Element	M/O/C	Condition
Access Session Identity	M	
Case Identity	M	
Content ID	C	Identifies information about the content that was filtered, if available
Device Address	M	Identifies the set of IP address(es)/address block(s) bound to the Subject Facility for the duration of the Access session.

---

[40] Added per CBI2.0-N-15.1326-1 on 9/29/15 by PO.
[41] Added per CBI2.0-N-15.1326-1 on 9/29/15 by PO.
[42] Added per CBI2.0-N-15.1326-1 on 9/29/15 by PO.

Information Element	M/O/C	Condition
Excluded Packet Signature	M	Describes a sequence of Five-tuple (in the case of IPv4) and the count of packets and bytes for that Five-tuple or a sequence of Six-tuple (in the case of IPv6) and the count of packets and bytes for that Six-tuple. There may be one or more Packet Signature elements included.
Filter Criteria	M	Identifies the IP data flow(s) to exclude
IAP System Identity	M	
MF System Identity	M	
Remarks	O	Provides additional information.
Subscriber Identity	M	
Time Stamp	M	Date/time the Periodic Filter Summary Log Message was created.

7.14.3.3 Broadband 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.

7.14.3.3.1 Access Attempt Message

Table 11 - 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.

7.14.3.3.2 Access Accepted Message

Table 12 - Information for Access Accepted Message [43]

Information Element	M/O/C	Conditions
Case Identity	M	
MF System Identity	M	

---

[43] Table revised per CBI2.0-N-08.0677-1 on 12/02/08 by JS.

Information Element	M/O/C	Conditions
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 DCHP capture is not available, this field would contain relevant parameters from a DCHP server).
Location Information	C	Provide when reasonably available and when authorized by the Broadband Intercept Order.
Lease Duration	C	
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.

7.14.3.3.3 Access Failed Message

Table 13 - 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.

7.14.3.3.4 Access Session End Message

Table 14 - 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	

Information Element	M/O/C	Conditions
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.[44]

7.14.3.4 Public Wi-Fi Message Parameters [45]

7.14.3.4.1 Access Attempt Message

Table 15 - Information for Access Attempt Message

Information Element	M/O/C	Conditions
Case Identity	M	
MF System Identity	M	
Time Stamp	M	Time stamp is applied by MF
User Name	C	Provide when available
Called Station ID	M	
Calling Station ID	M	
Account Session ID	C	Provide when available
Serving System (NAS)	M	Indicated the NAS FQDN or NAS IP Address
Service Type	C	Provide when available
Calling Station IP address	C	Provide when available
Location Information	C	Provide when available and authorized by warrant

7.14.3.4.2 Access Session Accepted Message

Table 16 - Information for Access Session Accepted

Information Element	M/O/C	Conditions
Case Identity	M	
MF System Identity	M	
Time Stamp	M	Time stamp is applied by MF
User Name	C	Provide when available
Called Station ID	M	
Calling Station ID	M	
Serving System (NAS)	M	Indicated the NAS FQDN or NAS IP Address

---

[44] 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.
[45] Added per CBI2.0-N-13.1111-2 on 9/25/13 by PO.

Information Element	M/O/C	Conditions
Service Type	C	Provide when available
Calling Station IP address	C	Provide when available
Session Timeout	C	Provide when applicable
Idle Timeout	C	Provide when applicable

Several elements in the Access Session Accepted message sent to law enforcement do not appear in the RADIUS Access-Accept message, although they may be present in the Access-Request message. Therefore, the MF will need to retrieve fields from the Access-Request and Access-Accept messages in order to populate the fields in the Access Session Accepted Message

7.14.3.4.3 Access Failed Message

Table 17 - Information for Access Failed Message

Information Element	M/O/C	Conditions
Case Identity	M	
MF System Identity	M	
Time Stamp	M	Time stamp is applied by MF.
User Name	C	Provide when available
Called Station ID	M	
Calling Station ID	M	
Account Session ID	C	Provide when available
Reply Message	C	Provide when available

7.14.3.4.4 Access Session End Message

Table 18 - Information for Access Session End Message

Information Element	M/O/C	Conditions
Case Identity	M	
MF System Identity	M	
Time Stamp	M	Time stamp is applied by MF
User Name	C	Provide when available
Called Station ID	M	
Calling Station ID	M	
Account Session ID	C	Provide when available
Location Information	C	Provide when available

7.14.4 *Exclusion of Flow(s) Messages* [46]

When authorized, the LI Exclusion of Flow(s) messages MUST be delivered to Law Enforcement over the CF interface, in addition to the messages defined in Section 7.14.1.3 Broadband Surveillance Event Messages. See Annex E for a complete description of capabilities and administrative aspects of the Exclusion of IP Data Flow(s) for Lawful Intercept.

7.14.4.1 *Filter Implementation*

R-502   When an Exclusion of Flow(s) has been authorized, the Filter Implementation event MUST be reported when the MSO Mediation Function begins or stops implementing the filter criteria in response to an LEA exclusion of flow(s) Request /MSO Acknowledgement.

7.14.4.2 *Excluded Flow Start*

R-504   When an Exclusion of Flow(s) has been authorized and implemented, the Excluded Flow Start event MUST be reported when the MSO Mediation Function matches the filter criteria with the first packet of an intercept subject's IP data flow.

The filter criteria consists of one or more of the following information elements:

For OTT services: IP header (see [RFC IPv4] and [RFC IPv6]) tuple fields (e.g., Five-tuple, Six-tuple).

For MSO/MSO business partner managed/provided services:

- IP header tuple fields (e.g., Five-tuple, Six-tuple)

- DOCSIS service flow – If the MSO Mediation Function has the ability to isolate downstream video between the Cable Modem Termination System and the Cable Modem to a discrete service flow then they MAY use this as a means to exclude the subject's video content.

7.14.4.3 *Excluded Flow Stop*

R-506   When an Exclusion of Flow(s) has been authorized and implemented, the Excluded Flow Stop event MUST be reported when the MSO Mediation Function stops excluding a IP data flow(s) (by auditable direction from LEA) or optionally at the end of surveillance authorization.

7.14.4.4 *Periodic Filter Summary Log Report*

This event is used to provide summary information about the intercept subject's excluded communications.

R-508   When an Exclusion of Flow(s) has been authorized and a Periodic Filter Summary Log Report has been requested by the LEA, the Periodic Filter Summary Log Report MUST be reported when the expiration of a configurable timer occurs. The timer duration is negotiated between the LEA and the MSO. The timer is configurable in hours and SHOULD not exceed 12 hours.

This event provides a periodic summary of content matching the filter criteria during a particular time frame and is triggered by the expiration of a configurable timer. When this trigger occurs, Packet Signatures will be captured along with the Content IDs (if available) for each IP data flow(s) matching the intercept subject's filter criteria. The configurable timer is reset at the conclusion of each timer period until final termination of the surveillance or the implementation of a new filter criteria. The configurable timer starts when the first packet from the first excluded packet is filtered based on the filter criteria. The timer duration is negotiated between the LEA and the MSO. The timer is configurable in hours and should not exceed 12 hours.

7.15 Correlation [47]

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.

---

[46] Added per CBI2.0-N-15.1326-1 on 9/28/15 by PO.
[47] Added per CBI2.1-N-13.1111-2 on 9/25/13 by PO.

R-510a   Correlation of intercepted events and intercepted user traffic is required for the intercept actions taken within a single Wi-Fi operator network. Correlation of reported events and traffic reported across the Visited and Home network is not required.

For more information, see Section 5.1.1.1 Intercept Categories and Section 7.12 Intercept Categories.

8   BROADBAND INTERCEPT FUNCTION, COLLECTION INTERFACE REQUIREMENTS AND FILE FORMAT

8.1   Broadband Intercept Function Requirements [48]

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 form 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 3. 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
```

---

[48] 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 14 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 13. The numeric sequence is appended by the Mediation Function for example:

```
Casedea001/oob/AccessAttemp-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.[49]

    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 [CBI2.0].

    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 [CBI2.0].

    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.

---

[49] 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 sixtuple used for packet identification.[50]

⚠ 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;
```

---

[50] 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 UN*X 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 (Normative)

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.[51]

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 [CBI2.0].

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"

---

[51] CBI2.0-N-07.0517-1, 10/23/7, PO.

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"
                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 Schema (Normative) [52]

The XML schema [CBI2.0] for CBI2.0 XML Schema can be found at the following location
http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI/

---

[52] CBI2.0-N-15.1337-1 on 10/1/15 by PO.

Annex D   WIFI1.0 XML Schema [53]

The XML schema [WIFI-1.0] for the lawful interception of Wi-Fi services can be found at the following location:
http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI.

---

[53] Annex created by CBI2.0-N-14.1227-5 on 6/17/15 by PO.

Annex E Informative Service Description and Administrative Aspects of Exclusion of Internet Protocol (IP) Data Flow(s) for Lawful Intercept

E.1 Exclusion of Flow(s) Overview

Law Enforcement and industry have been challenged by growing data rates associated with high-volume broadband service which increase difficulties for industry in capturing and delivering all required Communication Content (CmCC) for Law Enforcement Agencies (LEA) collection functions (CF) to process. Much of the increased volume of data is associated with Over the Top (OTT) broadcast video (e.g., Netflix or Hulu streaming) or other commercial video content provided by the Multiple Service Operator (MSO). Exclusion of Flow(s) is mutually beneficial to the MSO by reducing the provisioned bandwidth required by the MSO to transfer a subject's CmCC to the CF.

E.2 Capability Description

The Exclusion of Internet Protocol (IP) Data Flow(s) for Lawful Intercept is an OPTIONAL capability where, based on a request from the LEA, the MSO excludes specific IP data flow(s) from the CmCC prior to delivery to LEA.

The Exclusion of flow(s) will be explicitly identified to the MSO by the LEA and only applies to full content lawful intercepts.

E.3 Scenarios

The Exclusion of flow(s) is focused on two scenarios:

(1) Over-the-Top (OTT) services that traverse the MSO's content stream, and
(2) Services provided by the MSO (or a partner on behalf of the MSO) that are delivered via the MSO.

E.3.1 Scenario 1: Exclusion of Specific Third-Party OTT Services

When the LEA determines that specific OTT content is not needed, the LEA identifies streams associated with that content to the MSO to exclude from the CmCC prior to delivery. The exclusion of OTT services is based on the identification of the IP data flow (i.e., Five-tuple or Six-tuple). The LEA is responsible for specifically identifying the flow(s) to be excluded.

E.3.2 Scenario 2: Exclusion of Services Provided by the MSO or on Behalf of the MSO

The intercepted broadband content stream may include services either provided or managed by the MSO or a business partner on behalf of the MSO. For example, the MSO may manage its own "on demand" Internet Protocol Television (IPTV) distribution system. The MSO may have a greater level of control with this content because it is aware of and manages this service as part of the MSO's service offering. As in the previous scenario, the exclusion of services provided by the MSO is based on the identification of the IP data flow (i.e., Five-tuple or Six-tuple). The LEA is responsible for specifically identifying the IP data flow(s) to be excluded. The MSO MAY have other capabilities in addition to the LEA provided IP identification to identify the IP data flow(s) to meet LEA needs.

E.4 Identification of IP Data Flow(s)

If an Exclusion of Flow(s) has been requested by the LEA, the following requirements must be met:

- The LEA shall provide the MSO with sufficient identification of the IP data flow(s), applicable to the type of service, to develop filter criteria that ensures proper exclusion.

- The filter criteria consists of one or more of the following information elements:

  1. For OTT services: IP header (see [RFC 791] and [RFC 2460]) tuple fields (e.g., Five-tuple, Six-tuple)

  2. For MSO/MSO business partner managed/provided services:

     - IP header tuple fields (e.g., Five-tuple, Six-tuple)

- DOCSIS service flow – If the MSO Mediation Function has the ability to isolate downstream video between the Cable Modem Termination System and the Cable Modem to a discrete service flow then they MAY use this as a means to exclude the subject's video content.

- The MSO may employ one or more filter criteria parameters to exclude IP traffic flow(s).

- The MSO shall ensure that all of the subject's data flow(s), both to and from the subject's equipment, facilities, or service, shall be delivered for the entire period authorized by the lawful authorization with the exception of what has been requested to be specifically excluded by the LEA.

E.5   Administrative Process

This section describes the administrative procedures and recommends optional communication requirements for the exclusion of flow(s) from the delivery of an intercept subject's IP data stream. The administrative communication sent between the LEA and MSO to request an exclusion of flow(s) will be communicated using an existing MSO-LEA communications capability (e.g., web portal or secure email). The communication capability is negotiated between the MSO and LEA and is out of scope of this document.

E.5.1   Administrative Communications

This section describes potential administrative communications between the LEA-MSO.

The following administrative communications provide an example of a request and acknowledgement to setup the exclusion of flow(s):

1. The LEA communicates to the MSO an exclusion of flow(s) request.

2. The MSO responds to the LEA an acknowledgement of the exclusion of flow(s) request.

E.5.1.1   *Exclusion of Flow(s) Communication Request*

The LEA communicates to the MSO an exclusion of flow(s) request providing the specific identity of the IP data flow(s) to be excluded. The filter criteria MAY contain a single IP flow, multiple IP flows, or block(s) of IP flows. The MSO shall apply the exclusion of flow(s) within the timeframe negotiated between the LEA and MSO. Initially this timeframe will be set to not exceed twelve (12) hours, once the MSO receives the exclusion of flow(s) communication request from the LEA. Ideally the request would be facilitated by the MSO as soon as reasonably possible

If a previous exclusion of flow(s) request needs to be modified with a new filter criteria, the LEA SHALL communicate a new exclusion of flow(s) request to the MSO. This communication overwrites (or "stops") the original exclusion of flow(s) request and begins a new exclusion of flow(s) request based on the new filter criteria defined in the latest communication. In other words, there is only one exclusion of flow(s) request implemented at a time.

If an exclusion of flow(s) request needs to be deleted (or stopped), the LEA SHALL communicate a new exclusion of flow(s) request to the MSO indicating the filter action to "stop". This communication indicates to discontinue the exclusion of flow(s) and resume the delivery of CmCC and Communication Identifying Information (CmII) according to the original lawful authorization. Requests to stop an active exclusion of flow(s) shall be complied with as soon as reasonably possible, but not to exceed 30 minutes from receipt of the stop request.

The LEA should communicate (as an example) the following information to the MSO by administrative communication when requesting an exclusion of flow(s):

- Lawful Authorization ID - Identifies the lawful authorization.

- Filter Criteria - Identifies the IP data flow(s) to be excluded.

- Filter Action - Start or Stop of excluded flow(s).

- Time Stamp- Date and time of the request.

- Point of Contact (POC) - Provides the LEA POC information for acknowledgement, when different from communication request source (e.g., secure email account).

- Delivery Information - Provides updated delivery instructions, if different from the original authorization.

- Message ID - Unique number to reference the LEA exclusion of flow(s) request. Used to correlate Acknowledgement of MSO response. Starts numbering at 4000 and is incremented by 1.

- Periodic Filter Summary Log Report Action - This indicates if the MSO SHOULD report the Periodic Filter Summary Log Report message.

- Periodic Filter Timer - A configurable timer negotiated between the LEA and the MSO for the periodic filter summary log report message. This timer is configurable in hours and SHOULD not exceed 24 hours. When this timer expires the Periodic Filter Summary Log Report message is sent.

- Additional Remarks - Provides additional information if necessary.

E.5.1.2   *MSO Exclusion of Flow(s) Communication Acknowledgement*

The MSO communicates to the LEA a positive acknowledgement of an exclusion of flow(s) request. This communication indicates that an action to implement the exclusion of flow(s) is forthcoming.

The MSO should communicate (as an example) the following information to the LEA by administrative communication when acknowledging an exclusion of flow(s) request:

- Lawful Authorization ID - Identifies the lawful authorization.

- Filter Criteria - Identifies the IP data flow(s) to be excluded.

- Filter Action - Start or Stop of excluded flow(s).

- Time Stamp - Date and time of the request.

- Message ID - Unique number to reference the LEA exclusion of flow(s) request. Used to correlate Acknowledgement of MSO response. Starts numbering at 4000 and is incremented by 1.

- Implementation timeframe - Provides the LEA with an estimated timeframe for filter implementation; otherwise the filter shall be implemented within 12 hours of receipt of the LEA's exclusion of flow(s) request.

- Periodic Filter Summary Log Report Acknowledgement - This confirms the MSO acknowledgement to the LEA to report the Periodic Filter Summary Log Report message.

- Periodic Filter Timer Acknowledgement - This confirms the configurable timer negotiations between the LEA and the MSO for the periodic filter summary log report message.

- Additional Remarks - Provides additional information if necessary.

E.6   Lawful Intercept Exclusion of Flow(s) Events and Messages

The Lawful Intercept (LI) Exclusion of Flow(s) surveillance event messages are delivered by the Mediation Function Interface (MFI) to the Broadband Intercept Function (BIF) to send over the LEA Collection Function (CF).

When authorized, these messages shall be delivered to LE over the Collection Function Interface (CFI),

It is law enforcement's preference that the Exclusion of Flow(s) surveillance event messages are sent towards the CF within eight (8) seconds of the trigger event at the MF at least 95% of the time.

The four LI Exclusion of Flow(s) surveillance event messages below are described in Section 7.14.4.1 thru Section 7.14.4.4.

1,   Filter Implementation Message

2.   Excluded Flow Start Message

3.   Excluded Flow Stop Message

4.   Periodic Filter Summary Log Report Message

Figure 3 is an example of the high-level invocation process for an exclusion of flow(s). It describes both the administrative procedures and LI Exclusion of Flow(s) surveillance event messages for an intercept subject's IP data stream.
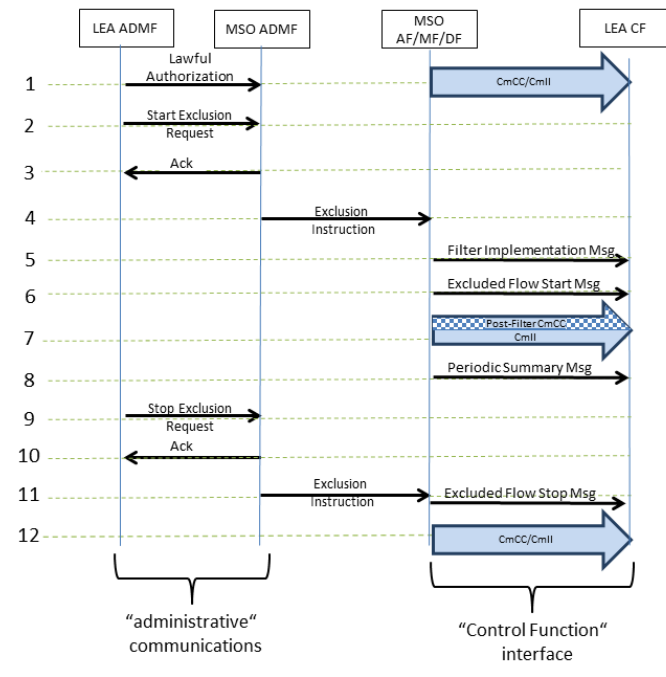
Figure 3 - Exclusion of Flow(s)

Steps for Exclusion of Flow(s)

1. The LEA provides the MSO with a lawful authorization. The MSO delivers CmCC and CmII to the LEA according to the lawful authorization.

2. MSO receives an auditable request from the LEA with the specific identity of the IP data flow(s) to be excluded and indicates if *Periodic Summary Log Report Message* is to be reported.

3. MSO acknowledges the exclusion of flow(s) request.

4. MSO implements the exclusion of flow(s) on CmCC for the identified IP data flow(s); reporting of CmCC and CmII according to the original lawful authorization will continue unchanged.

5. MSO delivers the *Filter Implementation Message* (Section 7.14.4.1) to LEA.

6. MSO delivers the Excluded Flow Start Message (Section 7.14.4.2) when the first IP data flow matching the filter criteria is excluded.

7. MSO delivers the modified CmCC which consists of the full content minus what was excluded.

8. MSO delivers the Periodic Filter Summary Log Report Message (as described in Section 7.14.4.4) at the expiration of a configurable timer (the timer is negotiated between the LEA and the MSO).

9. The MSO receives an auditable request from the LEA to stop excluding a specific IP data flow(s).

10. MSO acknowledges the request.

11. MSO implements the stop exclusion of flow(s) and delivers the Excluded Flow Stop Message as described in Section 7.14.4.3 to the LEA when the last flow matching the filter criteria is excluded.

12. The LEA once again receives the CmCC and CmII according to the original lawful authorization.

Appendix I   Limited Intercept XML Instance Document File (Informative) [54]

```
<?xml version="1.0"?>
<CBI:PacketDataSummaryReport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-
1.0.xsd"
    xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
    xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
    <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
    <CBI:IAPSystemIdentity>cmts-col1.mso.com</CBI:IAPSystemIdentity>
    <CBI:TimeStamp>2007-04-06T17:16:34.000000Z</CBI:TimeStamp>
    <CBI:AccessSessionId>5671986</CBI:AccessSessionId>
    <CBI:PacketSignature>
        <CBI:sourceAddress>
            <ipv4Address>23.45.32.12</ipv4Address>
        </CBI:sourceAddress>
        <CBI:destAddress>
            <ipv4Address>197.200.1.45</ipv4Address>
        </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>
            <ipv4Address>197.200.1.45</ipv4Address>
        </CBI:sourceAddress>
        <CBI:destAddress>
            <ipv4Address>23.45.32.12</ipv4Address>
        </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:

```
<?xml version="1.0"?>
<CBI:PacketDataSummaryReport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-
1.0.xsd"
    xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
    xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
    <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
    <CBI:IAPSystemIdentity>cmts-col1.mso.com</CBI:IAPSystemIdentity>
```

---

[54] 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, updated by CBI2.0-N-15.1337-1 on 10/1/15 by PO.

```
    <CBI:TimeStamp>2007-04-06T17:16:34.000000Z</CBI:TimeStamp>
    <CBI:AccessSessionId>5671986</CBI:AccessSessionId>
    <CBI:PacketSignature>
        <CBI:sourceAddress>
            <ipv4Address>23.45.32.12</ipv4Address>
        </CBI:sourceAddress>
        <CBI:destAddress>
            <ipv4Address>197.200.1.45</ipv4Address>
        </CBI:destAddress>
        <CBI:protocol>6</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>
</CBI:PacketDataSummaryReport>


<?xml version="1.0"?>
<CBI:PacketDataSummaryReport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-
1.0.xsd"
    xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
    xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
    <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
    <CBI:IAPSystemIdentity>cmts-col1.mso.com</CBI:IAPSystemIdentity>
    <CBI:TimeStamp>2007-04-06T17:16:34.000000Z</CBI:TimeStamp>
    <CBI:AccessSessionId>5671986</CBI:AccessSessionId>
    <CBI:PacketSignature>
        <CBI:sourceAddress>
            <ipv6Address>FE80:0000:0000:0000:0202:B3FF:FE1E:8329</ipv6Address>
        </CBI:sourceAddress>
        <CBI:destAddress>
            <ipv6Address>CAFF:CA01:0000:0056:0000:ABCD:EF12:1234</ipv6Address>
        </CBI:destAddress>
        <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:ipv6FlowLabel>190</CBI:ipv6FlowLabel>
    </CBI:PacketSignature>
</CBI:PacketDataSummaryReport>
```

Appendix II   Out-of-Band Messages - XML Instance Document File (Informative) [55]

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

```
<?xml version="1.0"?>
<CBI:AccessAttempt xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-1.0.xsd"
xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
          <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:AccessDeviceType>
              <CBI:AccessDeviceID>00-09-36-A7-70-89</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>
```

II.2   Out-of-Band Access Accepted Message - XML Instance Document File [56]

```
<?xml version="1.0"?>
<CBI:AccessAccepted xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-1.0.xsd"
  xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
  xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
          <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:AccessDeviceType>
             <CBI:AccessDeviceID>00-09-36-A7-70-89</CBI:AccessDeviceID>
          </CBI:AccessDevice>
          <CBI:CMTSID>MF-01.mso.com</CBI:CMTSID>
          <CBI:DeviceAddress>
             <PrefixLength>24</PrefixLength>
             <IpAddress>
                <ipv4Address>192.168.10.20</ipv4Address>
             </IpAddress>
          </CBI:DeviceAddress>
          <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
           <CBI:LocationInformation>
                <ca:country>US</ca:country>
                <ca:A1>New York</ca:A1>
                <ca:A3>New York</ca:A3>
                <ca:A6>Broadway</ca:A6>
                <ca:HNO>123</ca:HNO>
```

---

[55] 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, updated by CBI2.0-N-15.1337-1 on 10/1/15 by PO.
[56] 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, updated by CBI2.0-N-15.1337-1 on 10/1/15 by PO.

```
                <ca:LOC>Suite 75</ca:LOC>
                <ca:PC>10027-0401</ca:PC>
        </CBI:LocationInformation>
        <CBI:SignalCaptureFileName>Bill-
Kostka/oob/0046.dmp</CBI:SignalCaptureFileName>

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

II.3   Out-of-Band Access Failed Message - XML Instance Document File [57]

```
<?xml version="1.0"?>
<CBI:AccessFailed xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-1.0.xsd"
 xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
 xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-14T18:23:12.750000Z</CBI:TimeStamp>
        <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
        <CBI:DeviceAddress>
                <PrefixLength>24</PrefixLength>
                <IpAddress>
                        <ipv4Address>192.168.10.20</ipv4Address>
                </IpAddress>
        </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 File [57]

```
<?xml version="1.0"?>
<CBI:AccessSessionEnd xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
CBI-1.0.xsd"
        xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
        xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-12T21:03:34.250000Z</CBI:TimeStamp>
        <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
        <CBI:DeviceAddress>
                <PrefixLength>24</PrefixLength>
                <IpAddress>
                        <ipv4Address>192.168.10.20</ipv4Address>
                </IpAddress>
        </CBI:DeviceAddress>
        <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
        <CBI:SignalCaptureFileName>Bill-
Kostka/oob/0047.dmp</CBI:SignalCaptureFileName>

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

---

[57] Changed per CBI2.0-N-08.0677-1, 12/02/08 by JS, updated by CBI2.0-N-15.1337-1 on 10/1/15 by PO.

II.5 Out-of-Band Surveillance Status Report Message - XML Instance Document File [57]

```xml
<?xml version="1.0"?>
<CBI:SurveillanceStatusReport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI CBI-
1.0.xsd"
    xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
    xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
            <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
            <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
            <CBI:TimeStamp>2007-05-12T19:38:15.000000Z</CBI:TimeStamp>
            <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
            <CBI:DeviceAddress>
              <PrefixLength>24</PrefixLength>
                <IpAddress>
                    <ipv4Address>192.168.10.20</ipv4Address>
                </IpAddress>
            </CBI:DeviceAddress>
            <CBI:Status>
                <CBI:StatusCode>Heartbeat</CBI:StatusCode>
            </CBI:Status>
</CBI:SurveillanceStatusReport>
```

Appendix III Out-of-Band Wi-Fi Messages - XML Instance Document File (Informative) [58]

III.1 Out-of-Band WiFi Access Accepted Message – XML Instance Document File

```
<?xml version="1.0"?>
<WIFI:AccessSessionAccepted
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI WIFI-1.0.xsd"
  xmlns:WIFI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI"
  xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
  xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
        <WIFI:UserName>bkostka</WIFI:UserName>
        <WIFI:CalledStationId>00-09-36-A7-70-89</WIFI:CalledStationId>
        <WIFI:CallingStationId>00-09-36-A8-78-90</WIFI:CallingStationId>
        <WIFI:NASId>
          <NASIpAddress>
            <ipv4Address>192.168.120.220</ipv4Address>
          </NASIpAddress>
        </WIFI:NASId>
        <WIFI:ServiceType>Authenticate Only</WIFI:ServiceType>
        <WIFI:CallingStationIpAddress>
          <ipv4Address>192.168.10.20</ipv4Address>
        </WIFI:CallingStationIpAddress>
        <WIFI:SessionTimeout>250000</WIFI:SessionTimeout>
        <WIFI:IdleTimeout>250</WIFI:IdleTimeout>

</WIFI:AccessSessionAccepted>
```

III.2 Out-of-Band WiFi Access Attempt – XML Instance Document File

```
<?xml version="1.0"?>
<WIFI:AccessAttempt
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI WIFI-1.0.xsd"
  xmlns:WIFI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI"
  xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
  xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
        <WIFI:UserName>bkostka</WIFI:UserName>
        <WIFI:CalledStationId>00-09-36-A7-70-89</WIFI:CalledStationId>
        <WIFI:CallingStationId>00-09-36-A8-78-90</WIFI:CallingStationId>
        <WIFI:AccountSessionId>34659</WIFI:AccountSessionId>
        <WIFI:NASId>
          <NASFQDN>MF-02.mso.com</NASFQDN>
        </WIFI:NASId>
        <WIFI:ServiceType>Callback Login</WIFI:ServiceType>
        <WIFI:CallingStationIpAddress>
          <ipv4Address>192.168.10.20</ipv4Address>
        </WIFI:CallingStationIpAddress>
        <CBI:LocationInformation>
```

---

[58] CBI2.0-N-14.1227-5 on 6/17/15 by PO.

```
            <ca:country>US</ca:country>
            <ca:A1>New York</ca:A1>
            <ca:A3>New York</ca:A3>
            <ca:A6>Broadway</ca:A6>
            <ca:HNO>123</ca:HNO>
            <ca:LOC>Suite 75</ca:LOC>
            <ca:PC>10027-0401</ca:PC>
         </CBI:LocationInformation>

</WIFI:AccessAttempt>
```

III.3   Out-of-Band WiFi Access Failed – XML Instance Document File

```
<?xml version="1.0"?>
<WIFI:AccessSessionEnd
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI WIFI-1.0.xsd"
   xmlns:WIFI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI"
   xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
   xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
         <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
         <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
         <WIFI:UserName>bkostka</WIFI:UserName>
         <WIFI:CalledStationId>00-09-36-A7-70-89</WIFI:CalledStationId>
         <WIFI:CallingStationId>00-09-36-A8-78-90</WIFI:CallingStationId>
         <WIFI:AccountSessionId>34659</WIFI:AccountSessionId>
         <CBI:LocationInformation>
           <ca:country>US</ca:country>
           <ca:A1>New York</ca:A1>
           <ca:A3>New York</ca:A3>
           <ca:A6>Broadway</ca:A6>
           <ca:HNO>123</ca:HNO>
           <ca:LOC>Suite 75</ca:LOC>
           <ca:PC>10027-0401</ca:PC>
         </CBI:LocationInformation>

</WIFI:AccessSessionEnd>
```

III.4   Out-of-Band WiFi Access Session End- XML Instance Document File

```
<?xml version="1.0"?>
<WIFI:AccessSessionEnd
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI WIFI-1.0.xsd"
   xmlns:WIFI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI"
   xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
   xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
         <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
         <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
         <WIFI:UserName>bkostka</WIFI:UserName>
         <WIFI:CalledStationId>00-09-36-A7-70-89</WIFI:CalledStationId>
         <WIFI:CallingStationId>00-09-36-A8-78-90</WIFI:CallingStationId>
         <WIFI:AccountSessionId>34659</WIFI:AccountSessionId>
         <CBI:LocationInformation>
          <ca:country>US</ca:country>
          <ca:A1>New York</ca:A1>
          <ca:A3>New York</ca:A3>
          <ca:A6>Broadway</ca:A6>
          <ca:HNO>123</ca:HNO>
```

```
              <ca:LOC>Suite 75</ca:LOC>
              <ca:PC>10027-0401</ca:PC>
            </CBI:LocationInformation>

</WIFI:AccessSessionEnd>
```

III.5   Out-of-Band WiFi IPv6 Access Accepted – XML Instance Document File

```
<?xml version="1.0"?>
<WIFI:AccessSessionAccepted
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI WIFI-1.0.xsd"
   xmlns:WIFI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/WIFI"
   xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
   xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
            <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
            <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
            <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
            <WIFI:UserName>bkostka</WIFI:UserName>
            <WIFI:CalledStationId>00-09-36-A7-70-89</WIFI:CalledStationId>
            <WIFI:CallingStationId>00-09-36-A8-78-90</WIFI:CallingStationId>
            <WIFI:NASId>
              <NASIpAddress>
                <ipv6Address>CAFF:CA01:0000:0056:0000:A123:EE34:5735</ipv6Address>
              </NASIpAddress>
            </WIFI:NASId>
            <WIFI:ServiceType>Authenticate Only</WIFI:ServiceType>
            <WIFI:CallingStationIpAddress>
              <ipv6Address>CAFF:CA01:0000:0056:0000:ABCD:BA10:5678</ipv6Address>
            </WIFI:CallingStationIpAddress>
            <WIFI:SessionTimeout>10034</WIFI:SessionTimeout>
            <WIFI:IdleTimeout>25</WIFI:IdleTimeout>

</WIFI:AccessSessionAccepted>
```

Appendix IV   Physical Consideration (Informative)

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 V   Example Flow Chart Implementation (Informative)

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
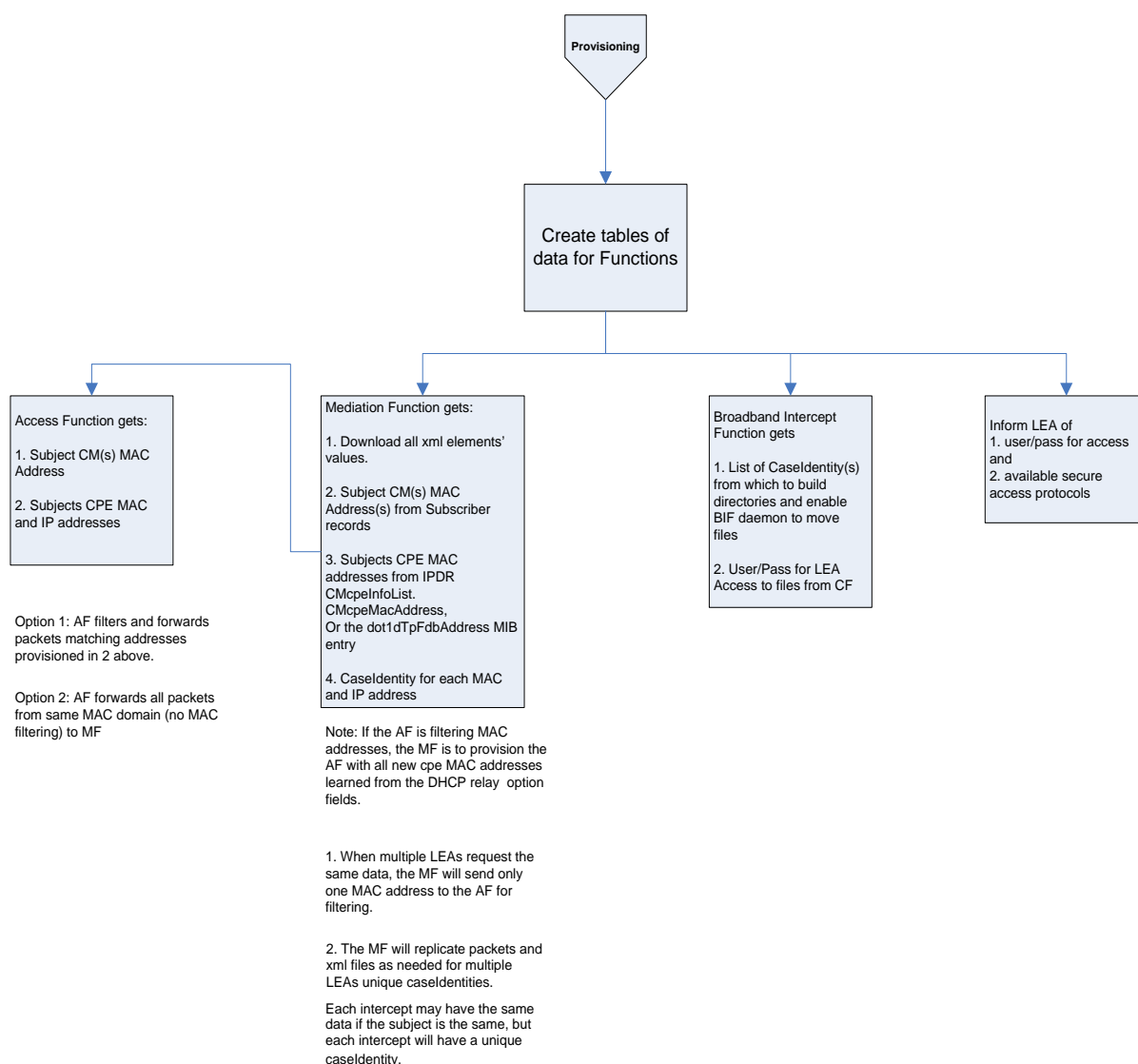
5. The Broadband Intercept Function

Provisioning

Create tables of data for Functions

Access Function gets:

1. Subject CM(s) MAC Address

2. Subjects CPE MAC and IP addresses

Option 1: AF filters and forwards packets matching addresses provisioned in 2 above.

Option 2: AF forwards all packets from same MAC domain (no MAC filtering) to MF

Mediation Function gets:

1. Download all xml elements' values.

2. Subject CM(s) MAC Address(es) from Subscriber records

3. Subjects CPE MAC addresses from IPDR CMcpeInfoList. CMcpeMacAddress, Or the dot1dTpFdbAddress MIB entry

4. CaseIdentity for each MAC and IP address

Note: If the AF is filtering MAC addresses, the MF is to provision the AF with all new cpe MAC addresses learned from the DHCP relay option fields.

1. When multiple LEAs request the same data, the MF will send only one MAC address to the AF for filtering.

2. The MF will replicate packets and xml files as needed for multiple LEAs unique caseIdentities.

Each intercept may have the same data if the subject is the same, but each intercept will have a unique caseIdentity.

Broadband Intercept Function gets

1. List of CaseIdentity(s) from which to build directories and enable BIF daemon to move files

2. User/Pass for LEA Access to files from CF

Inform LEA of
1. user/pass for access and
2. available secure access protocols

Figure 4 - Provisioning the functions with data from the CMTS[59]

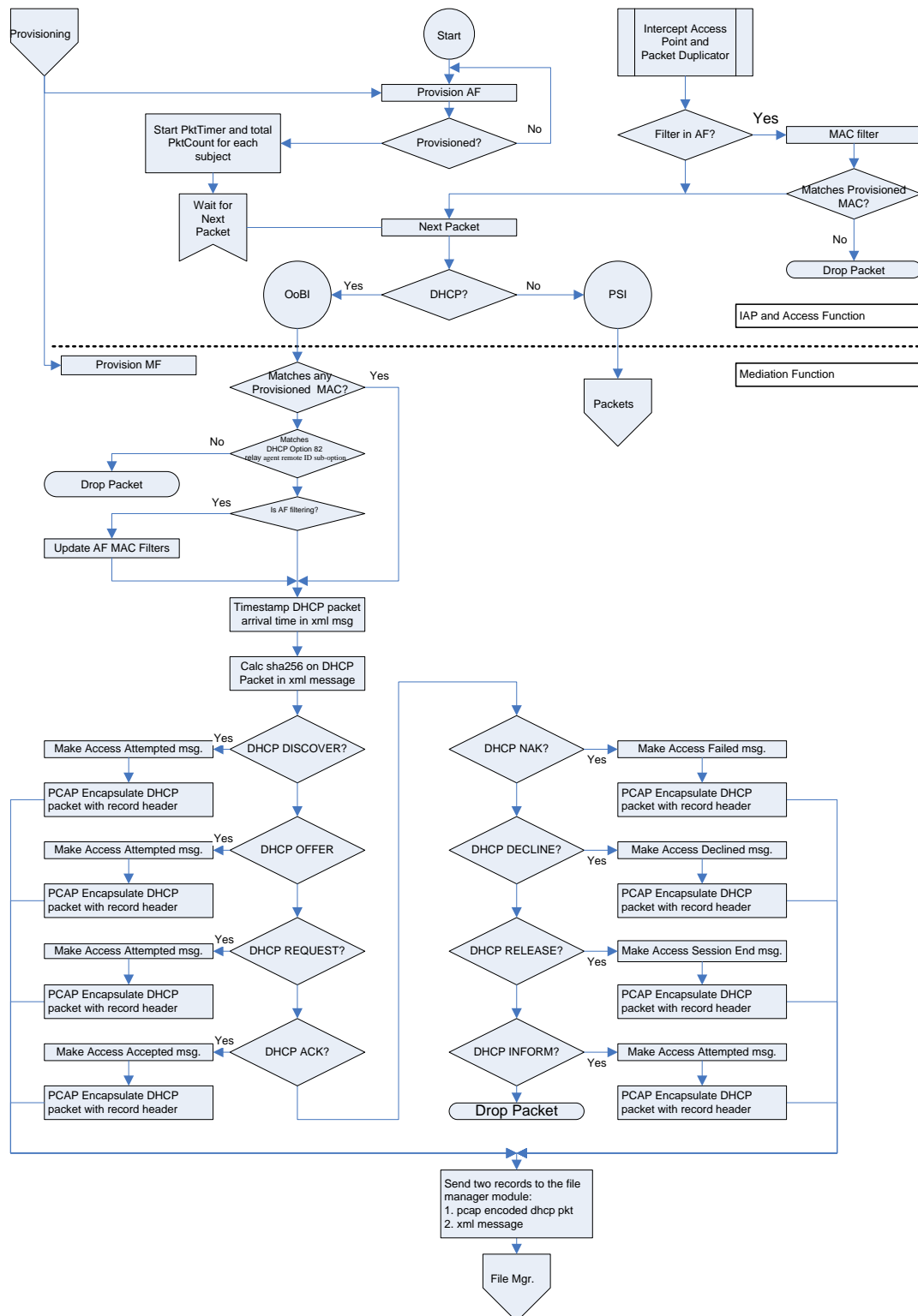[59] Figure 3 updated by CBI2.0-N-0517-2, 10/22/07, PO.

Figure 5 - The Access Function, Intercept Access Points, and Out-of-Band Processing[60]

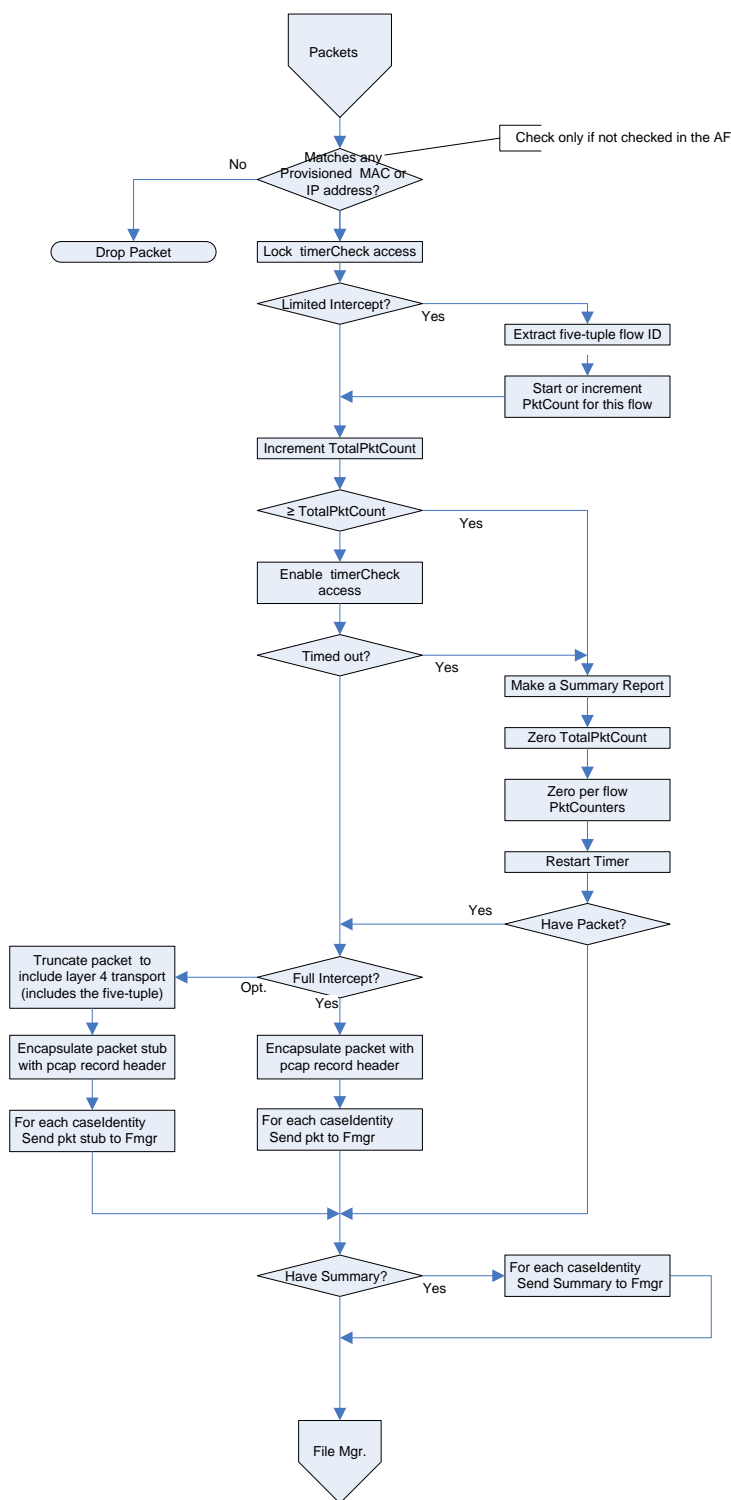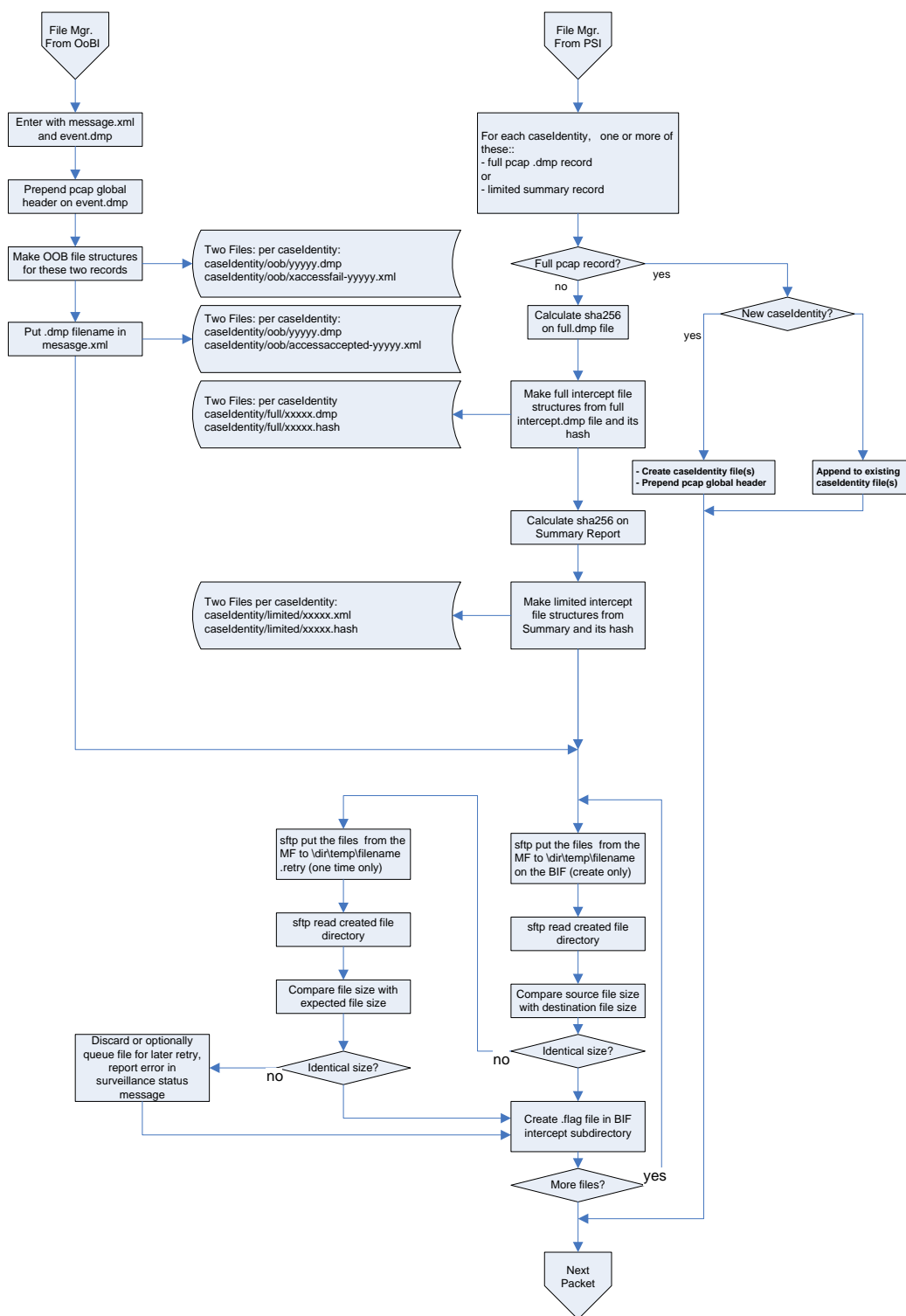---

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

Figure 6 - Packet Processing: full intercepts and limited intercepts [61]

---

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

Figure 7 - The file manager [62]

---

[62] Figure 6 updated by CBI2.0-N-0517-2, 10/22/07, PO.

BIF
Input

BIF daemon
wakes

Probably cron scheduled.
Independent of MF state

For example:
/dir/tmp/caseIdentity/oob/7878.dmp
/dir/tmp/caseIdentity/oob/AccessSessionEnd-7878.xml

Check for files in
\dir\temp

Any files?

BIF Sleeps

Yes

.flag
Present?

BIF Sleeps

Yes

Sort files on this
BIF:
key 1 create date
key 2 file size

Enough file
space?

Yes

Any files >24
hours old?

BIF Sleeps

Yes

In sort order delete
while space is
needed and files
are > 24 hours old

Check provisioned data for which LEA
gets these intercept files:
(LEA:caseIdentity)

Trim \dir\tmp and
prepend \LEA_ID
(LEA_ID be a link,
a directory or a
null field)

For example:
/LEA_1/caseIdentity/full/3259812.dmp
/LEA_1/caseIdentity/full/3259812.hash
/LEA_1/caseIdentity/oob/AccessAttempt-45789.xml
/LEA_1/caseIdentity/oob/45789.hash
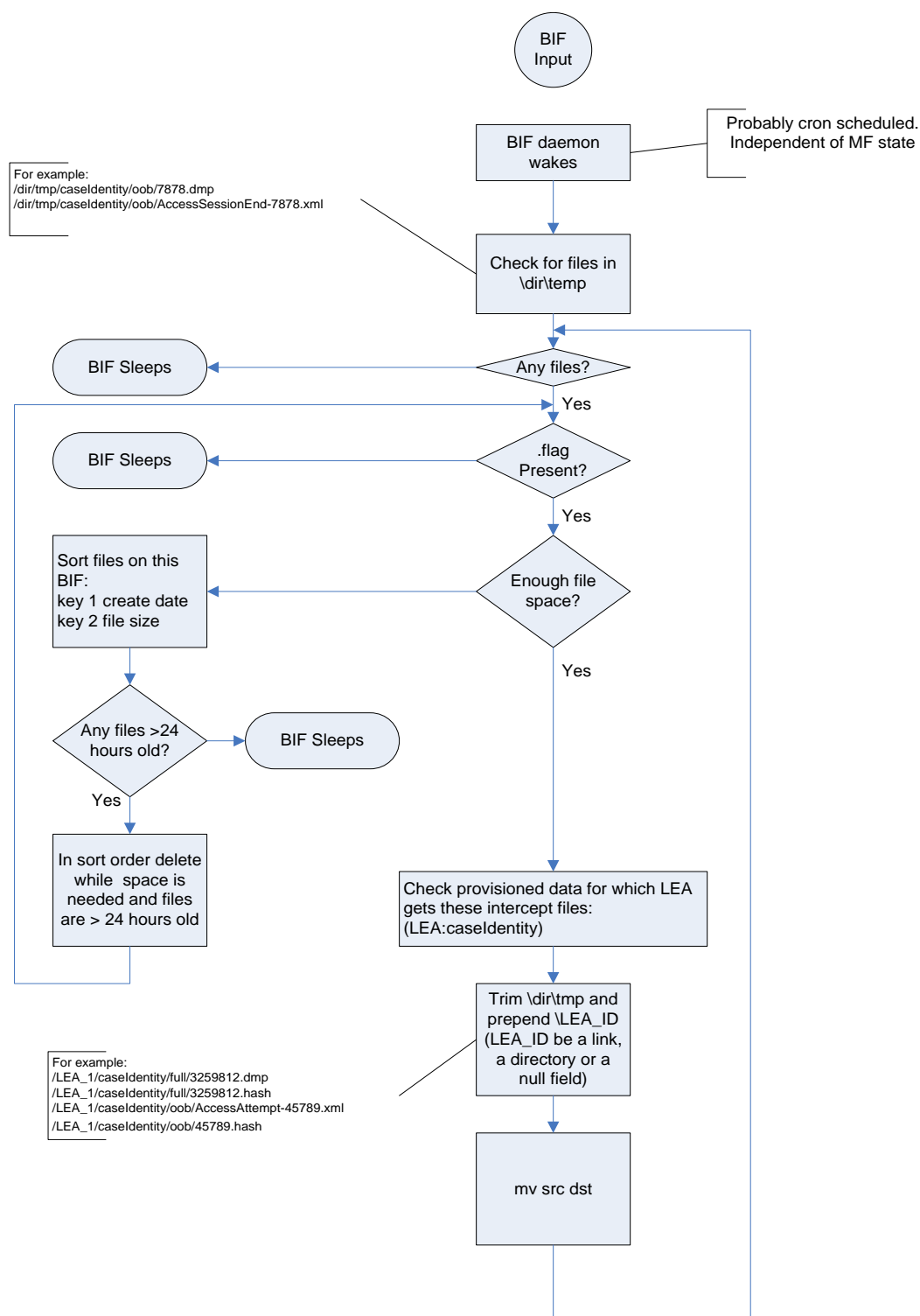
mv src dst

Figure 8 - The Broadband Intercept Function [63]

---

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

Appendix VI   Acknowledgements (Informative)

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

Appendix VII Revision History (Informative)

VII.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.

VII.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

VII.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

VII.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

VII.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

VII.6   Engineering Change for CM-SP-CBI2.0-I07-140729

The following Engineering Change is incorporated into CM-SP-CBI2.0-I07-140729.

ECN	Date Accepted	Summary	Author
CBI2.0-N-14.1139-1	4/2/2014	Use 64 bit field for Byte Count and Packet Count parameters	Sundaresan

VII.7   Engineering Change for CM-SP-CBI2.0-I08-150625

The following Engineering Change is incorporated into CM-SP-CBI2.0-I08-150625.

ECN	Date Accepted	Summary	Author
CBI2.0-N-14.1227-5	6/3/2015	MSO Public Wi-Fi additions to CBIS	McKibben

VII.8   Engineering Changes for CM-SP-CBI2.0-I09-151015

The following Engineering Changes are incorporated into CM-SP-CBI2.0-I09-151015.

ECN	Date Accepted	Summary	Author
CBI2.0-N-15.1326-1	8/5/2015	Exclusion of Flows	Stover
CBI2.0-N-15.1337-1	8/5/2015	CBIS Schema EC	Kim

VII.9   Engineering Change for CM-SP-CBI2.0-I10-160211

The following Engineering Change is incorporated into CM-SP-CBI2.0-I10-160211.

ECN	Date Accepted	Summary	Author
CBI2.0-N-15.1396-1	11/18/2015	Addition of Expanded PDSR Requirements	Gray