Data-Over-Cable Service Interface Specifications

Cable Broadband Intercept Specification

CM-SP-CBI2.0-I01-070611

ISSUED

Document Status Sheet

Document Control Number:	CM-SP-CBI2.0-I01-070611			
Document Title:	Cable Broadband Intercept Specification			
Revision History:	I01 – Released 06/11/07			
Date:	June 11, 2007			
Status:	~~Work in Progress~~	~~Draft~~	Issued	~~Closed~~
Distribution Restrictions:	~~Authors Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	Public

Key to Document Status Codes:

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

Trademarks:

Contents

Figures

Tables

This page left blank intentionally.

1 SCOPE

1.1 Introduction and Purpose

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

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

This first release is specifically directed toward network elements using IPv4 only. Future releases of this specification (e.g., I02 or later) may update this specification to address network traffic using IPv6 and IPv6 services such as mobility or a mixed system of both IPv4 and IPv6 network elements in furtherance of a LEA conducting lawful surveillance under CALEA. Similarly, 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.

2 REFERENCES

2.1 Normative References

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, Section3, 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.

[LIBPCAP] The libpcap format: http://www.tcpdump.org/

[PCAP-FF] PCAP File Format. http://www.tcpdump.org

[T1.IAS] ATIS T1.IAS Draft Standard. Available to ATIS members from http://www.atis.org.

[PC-ESP1.5] PacketCable™ 1.5 Specifications, Electronic Surveillance, PKT-SP-ESP1.5-I02-070412, April 12, 2007, Cable Television Laboratories, Inc.

[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.

2.2 Informative References

This specification uses the following informative references.

[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

[47CFR 64.2100] 47 C.F.R. § 64.2100. Purpose: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2100&YEAR=2000&TYPE=TEXT

[47CFR 64.2101] 47 C.F.R. § 64.2101. Scope: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2101&YEAR=2000&TYPE=TEXT

[47CFR 64.2102] 47 C.F.R. § 64.2102. Definitions: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2102&YEAR=2000&TYPE=TEXT

[47CFR 64.2103] 47 C.F.R. § 64.2103. Policies and procedures for employee supervision and control: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2103&YEAR=2000&TYPE=TEXT

[47CFR 64.2104] 47 C.F.R. § 64.2104. Maintaining secure and accurate records: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2104&YEAR=2000&TYPE=TEXT

[47CFR 64.2105] 47 C.F.R. § 64.2105. Submission of policies and procedures and commission review: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2105&YEAR=2000&TYPE=TEXT

[47CFR 64.2106] 47 C.F.R. § 64.2106. Penalties: http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=47&PART=64&SECTION=2106&YEAR=2000&TYPE=TEXT

[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

[PCAP] PCAP Man Page. http://www.tcpdump.org/pcap3_man.html

[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

[IPFIX] IETF IP Flow Information Export (IPFIX) information: http://www.ietf.org/html.charters/ipfix-charter.html

[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-I09-050812, August 12, 2005, Cable Television Laboratories, Inc.

[W3C-SCHEMA] www.w3c.org/XML/Schema World Wide Web Consortium

2.3 Reference Acquisition

- ATIS, 1200 G Street NW, Ste. 500, Washington DC 20005, USA
  Phone: +1-202-628-6380, Fax: +1-202-393-5453, Internet: http://www.atis.org.
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: http://www.cablelabs.com/.
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org.
- Institute of Electrical and Electronics Engineers (IEEE), IEEE Operations Center, 445 Hoes Lane, Piscataway, New Jersey 08854-1331, USA, Phone: +1-732 981 0060, Fax: +1-732 981 1721, Internet: http://standards.ieee.org.
- U.S. Code, http://www.access.gpo.gov/
  U.S. FCC, http://www.fcc.gov
- World Wide Web Consortium, www.w3c.org, c/o MIT, 32 Vassar Street, Room 32-G515
  Cambridge, MA 02139

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Appropriate Legal Authorization	A Broadband Intercept Order or other authorization, pursuant to [18 U.S.C. 2518], or any other relevant federal or state statute.
Authentication	A process by which a network provides assurances of a user's identity in conjunction with the use of a Subject Facility.
Authorization	The process by which a network grants a user access to network resources. Authorization usually follows Authentication.
Broadband Intercept	The interception of the broadband communications of a Subject.
Broadband Intercept Function	The function that implements buffering of broadband communications.
Broadband Intercept Order	A court order signed by a judge, magistrate, or other authority with jurisdiction that authorizes the interception of the broadband-based wire or electronic communications of a Subject.
Case Identity	Identifies the intercept Subject. This identity remains constant for the entire surveillance period.
Collection Function	The LEA function that receives the communications intercepted pursuant to the Broadband Intercept Order.
Five-tuple	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 packets sharing the same 5-tuple. Also referred to as a stream.
Full Content Broadband Intercept Order	A Broadband Intercept Order that authorizes the interception of any and all information concerning the timing, addressing, substance, purport, or meaning of the broadband communications of a Subject.
Hand-off	The process by which a network negotiates the transfer of a communication to another network.
Internet	The public Internet.
IP Network Access Provider	An entity that offers IP Network Access service to customers. This definition includes, but is not limited to, entities that provide broadband Internet access to customers/subscribers.
Law Enforcement (LE)	Any officer of the United States, or of a State or political subdivision thereof, who is empowered to conduct investigations, make arrests, or otherwise enforce and ensure obedience of the law.
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.
Session	The collective set of IP data packets containing the IP address assigned to the Subject's data communication and carried over the connection between the Subject equipment and access network (e.g., via PPP, L2TP). These are the IP data packets intercepted and delivered to the LEA. There is a one-to-one mapping between a session and an Access Session ID.
SFTP	SFTP is a ssh-2 utility that provides secure file transfer functionality.
Stream	A set of packets sharing the same 5-tuple. 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 equipment, 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), and listed in the Broadband Intercept Order.
Subject Traffic	All IP data traffic, both upstream and downstream, that is bridged by the cable modem(s) identified in the Broadband Intercept Order at the Subject Facility.
SummaryTimer	A variable that defines how frequently, in seconds, the Packet Data Summary Report is sent.
Validation	For the purposes of this document, the process used to provide assurance that an intercepted communication is associated with the correct Subject by confirming that it involves the use of a Subject Facility.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

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

5 OVERVIEW

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

5.1 Law Enforcement's High-Level Requirements

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

5.1.1 Intercept Categories

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

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

5.1.2 Transparency

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

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

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

5.1.3 Confidentiality / Access Control

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

5.1.4 Chronology of an Intercept

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

Subject Facility. Non-Repudiation confirms after the intercept is completed that the intercept was in fact associated with the Subject Facility

5.1.4.1 Authentication

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

5.1.4.2 Validation

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

5.1.4.3 Non-Repudiation

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

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

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

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

5.1.5 Correlation

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

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

5.1.6 Isolation

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

5.1.7 Proportionality

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

5.1.8 Completeness

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

5.1.9 Compression

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

5.1.10 Encryption

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

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

5.1.11 Performance

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

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

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

5.1.12 Availability and Reliability

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

5.2 Cable Broadband Intercept Architecture

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

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

- Collection Function (CF) – The LEA function that receives the communications intercepted pursuant to the Broadband Intercept Order.

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

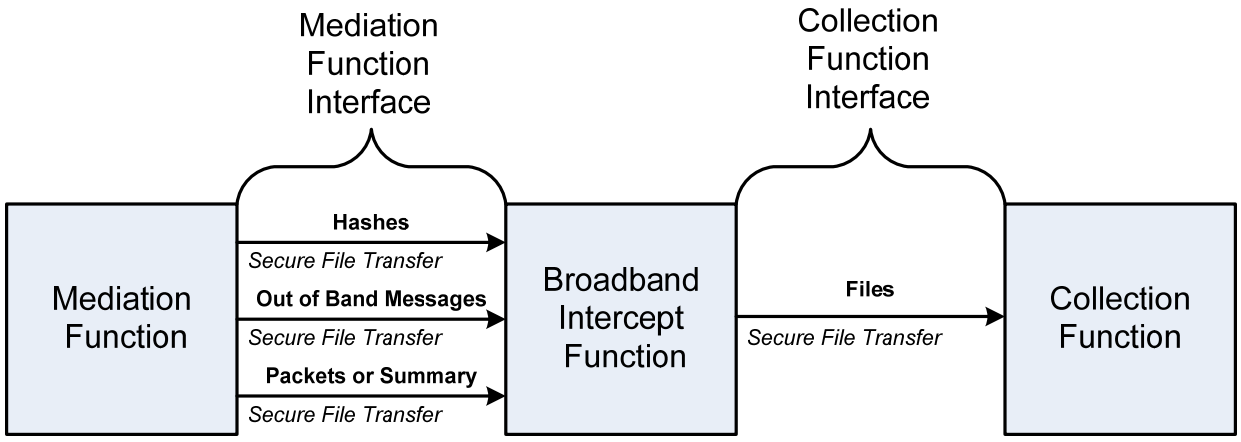

Figure 1 - Logical Network Diagram

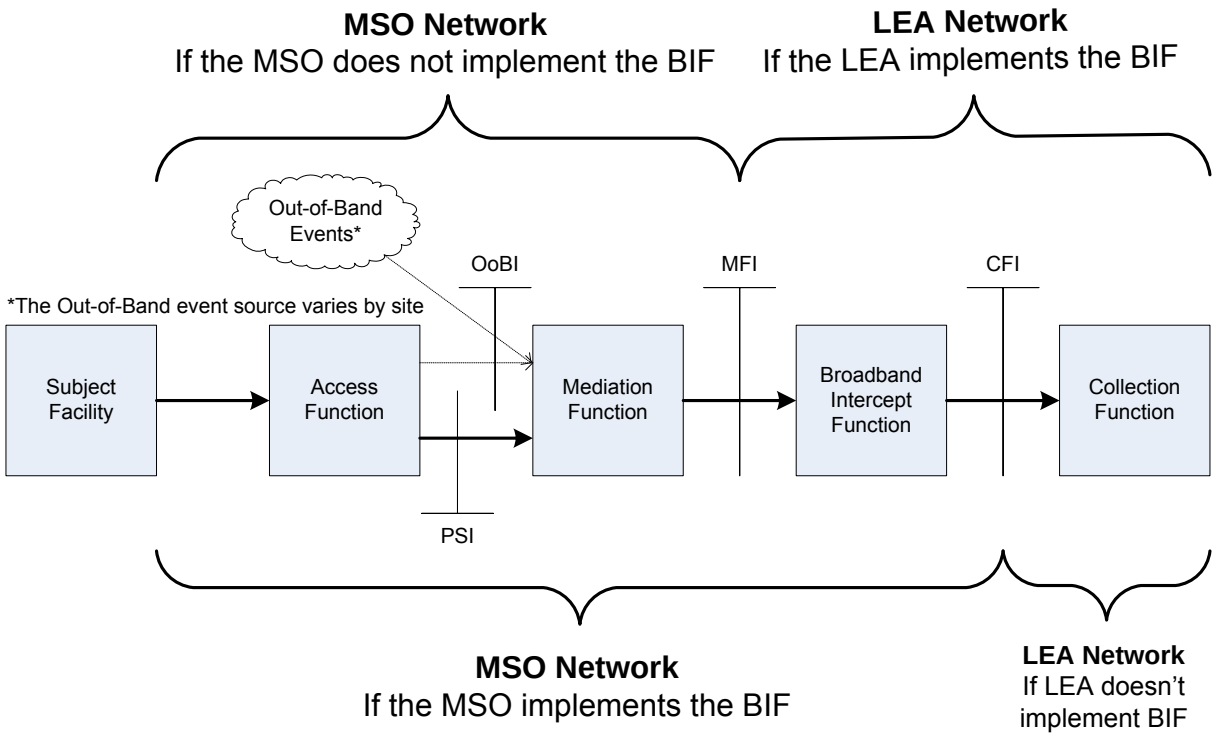

Figure 2 - Broadband Intercept Interfaces

6 ACCESS FUNCTION

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

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

6.1 Out of Band Interface

The Out of Band Interface (OoBI) MUST provide the highest tier of service used in 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 the incoming event traffic rate.

When the AF serves multiple intercepts via one or more IAPs, then the OoBI MUST be able to transport the full aggregation of OoB event data at a data rate faster that the full aggregation of incoming OoB data rate.

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

The Packet Stream Interface (PSI) MUST provide the highest tier of service used in forwarding packets comprising one or more streams from the AF to the MF. The PSI MUST be able to transport the full set of IP packets associated with the Subject Facility at a data rate faster than the incoming packet data rate.

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

7 MEDIATION FUNCTION REQUIREMENTS

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

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

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

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

7.1 Transparency

R-10 The MF MUST perform the intercept in a manner that is transparent (undetectable) by the Subject or the Subject Facility (e.g., non-privileged entities in a call center should not be aware of intercept, service parameters such as bandwidth, latency, or availability)

R-20 MFI The intercept MUST be transparent to multiple intercepting LEAs.

R-20 CFI The intercept MUST be transparent to multiple intercepting LEAs. For example, the intercept can be implemented by means of virtual file links and reference counting, such that once the file has been deleted by all intercepting LEAs it can be deleted from the BIF.

7.2 Data Integrity

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/xxxxx.dmp file and oob/xxxxx.dmp for full intercepts and
- limited/xxxxx.xml file and oob/xxxxx.dmp for limited intercepts.

R-50 MFI The BIF MUST store the hashes received from the MF.

R-50 CFI The BIF MUST store the hashes for
- full/xxxxx.dmp file and oob/xxxxx.dmp for full intercepts and
- limited/xxxxx.xml file and oob/xxxxx.dmp for limited intercepts.

R-60 PacketCaptureCount and PacketCaptureDuration MUST be negotiated by the LEA and MSO prior to intercept initiation.

R-70 Copies of the hashes MUST be delivered to the LEA along with the intercepted communications, and kept by the MSO as a business record.

7.3 Isolation

R-80 The MF MUST be provisioned and operated such that only communications associated with the Subject Facility are intercepted. Communications associated with the Subject Facility MUST be isolated, and communications not authorized to be intercepted (e.g., those not associated with the Subject Facility) MUST NOT be delivered to the LEA.

7.4 Proportionality

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

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

7.5 Completeness

R-100 All Subject traffic, both to and from the Subject Facility, MUST be intercepted for the entire period authorized by the Broadband Intercept Order.

7.6 Compression

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

7.7 Encryption

R-120 If the MSO provides encryption services to its customers or subscribers, the MSO MUST either:

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

7.8 Performance

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

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

The two variables, PacketCaptureDuration and PacketCaptureCount, are intended to assist the MSOs and LEAs in achieving the required performance outlined in R120 and R130.

7.9 Connectivity Requirements

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 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.

R-210 The SFTP cryptographic algorithms/strength MUST be negotiated by the MSO and LE prior to initiating the intercept.

7.10 Availability, Performance and Reliability

R-220 MFI The intercept event messages, packet data, five-tuples and summary reports MUST be delivered to the Broadband Intercept Function across the MFI.

R-230 MFI Appropriate performance and reliability mechanisms and parameters to enable the MF to determine whether intercept event messages, packet data, five-tuples 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-240 An Out-of-Band Event MUST be timestamped at the time it is detected at the MF.

R-250 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-260 A Limited Broadband Intercept Order MUST include material conforming to the requirements in Sections 7.12.2 Limited IP Stream Intercept (For Limited Broadband Intercept Orders), and Section 7.13 xml Requirements.

R-270 A Full Content Order MUST include material conforming to the requirements in Section 7.12.1 Full IP Stream Intercept (For Full Content Broadband Intercept Orders) and Section 7.13 xml Requirements

R-280 The intercept categories (Limited broadband intercept or Full Content Intercept) MUST be provisionable on a per–intercept basis.

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

R-290 The full set of IP packets associated with the Subject Facility MUST be isolated and captured.

R-300 The MF MUST transfer the file containing the packets to the BIF upon reaching PacketCaptureCount or the PacketCaptureDuration timeout.

R-310 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)

R-320 The packet signature, as defined in ***R-330*** MUST be captured and delivered for each flow.

R-330 The Packet Signature is a sequence of a Five-tuple that defines a unique flow and the count of packets for that flow since the last report (numPktsSinceLastReport).

R-340 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-350 If no packets were detected for the duration of the Summary Timer, then the Packet Data Summary Report MUST NOT be sent.

7.13 xml Requirements

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

7.13.1 Out-of-Band (DHCP) Event Messages

This section describes the requirement for reporting surveillance events of interest to Law Enforcement (LE). The following table illuminates the relationship between DHCP messages and LE events of interest:

Table 1 - DHCP Events of Interest to LE

DHCP Event	Server to Client	Client to Server	Purpose of DHCP Event	CBIS OoB Message
DHCPDISCOVER		X	Client broadcast to find available servers	Access Attempt
DHCPOFFER	X		Server to client in response to DCHPDISCOVER with an offer of configuration parameters	Access Attempt
DHCPREQUEST		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	X		Committed configuration parameters	Access Accepted
DHCPNAK	X		The committed IP address is invalid (e.g., lease expired or wrong subnet).	Assess Failed
DHCPDECLINE		X	Upon testing (e.g., ARP or ping) the committed	Access Declined

			IP address is already in use.	
DHCPRELEASE		X	Cancel remaining lease and return IP address	Access Session End
DHCPINFORM		X	Request local parameters; client already has valid IP address.	Access Attempt

7.13.1.1 Access Attempt

R-360 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 DISCOVER or DHCP OFFER or DHCP REQUEST or DHCP INFORM).

R-370 If the MSO allows multiple IP addresses to be allocated to an account, separate Access Attempt events MUST be reported for each IP address allocated.

7.13.1.2 Access Accepted

R-380 The Access 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).

R-390 If the MSO allows multiple IP addresses to be allocated to an account, separate Access Accepted events MUST be reported for each IP address allocated.

7.13.1.3 Access Failed

R-400 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).

7.13.1.4 Access Session End

R-410 The Access Session End event MUST be reported when the Subject has initiated a DHCP RELEASE.

7.13.1.5 Access Declined

R-420 The Access Declined event MUST be reported when the intercept Subject sends a DHCP DECLINE message to the network.

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

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

R-430 The Packet Data Summary Report MUST be reported when the expiration of a configurable timer per intercept occurs. The timers are configurable in units of seconds.

The event message reports source and destination information (i.e., Five-tuple information) extracted from the packet headers, and provides summary information for the number of packets transmitted or received by the Subject for each unique flow defined by a Five-tuple.

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

7.13.3 Surveillance **Status Report**

This event is used to provide surveillance status reports.

R-440 The Surveillance Status Report MUST be reported

- when there is a change in status of a surveillance
  1. Up: Surveillance is activated.
  2. Down: Surveillance is deactivated.
  3. Error: An error occurred. The second text field adds explanatory text.
  4. Unknown: Indeterminate status
- 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.
  5. Heartbeat

The Surveillance Status Report is not hashed.

7.13.4 Event Parameters

7.13.4.1 Parameter Definitions

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

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

Information Element	DataType	Description
Access Method	**sequence**	When available, this element consists of two information elements: Method and EquipmentID. 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 Identity	**integer**	Uniquely identifies the intercept Subject's network access session (see session definition in Section 3) for a given surveillance. This parameter is generated in the Mediation Function.
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.
Device Address	**ipAddress**	Identifies the IP address bound to the Subject Facility for the duration of the Access session.
EquipmentID	**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 Method.
Failure Reason	**string**	The value is "DHCPNAK"
FiveTuple Set	**sequence**	Describes an ordered set of five tuples (i.e., IP Source, IP Dest, Source Port, Dest Port, Protocol).
Hash	**hexBinary**	An SHA-256 hash of the original intercepted packet headers or the network-generated event.
IAPSystemIdentity	**string**	Describes the Intercept Access Point (IAP) associated with the Intercept Subject

Information Element	DataType	Description
Lease Duration	**unsignedInt**	Defines the IP address lease time in units of seconds associated with the Intercept Subject's Access Method.
Location Information	**string**	Identifies the location of the Subject Facility. When reasonably available and covered by the Broadband Intercept Order, location type and actual content of the location field MUST be delivered to the LEA.
Method	**string**	Specifies the type of equipment used to gain access to the network resources. This is the first information element within the Access Method element. The valid values are: "cm", "eMTA", "dsg", "other"
MF System Identity	**string**	Identifies the system with the MF.
Network Access Node Identity	**string**	Identifies the network node providing access to the intercept Subject Facility for example FQDN.
Num Pkts Since Last Report	**unsignedLong**	Counter of the number of packets associated to a FiveTuple Set
Packet Signature	**sequence**	Describes a sequence of FiveTuple and the count of packets for that FiveTuple since the last report (numPktsSinceLastReport).
Signal Capture File Name	**string**	Pointer to actual file containing the DHCP messages captured
Status	**sequence**	Describes the status of a surveillance. The status has two components. The first component is one of the enumerated values indicating active, not active, unknown an error condition or heartbeat. The second component is a text string to provide further explanation. The presence of this string is optional.
Subscriber Identity	**string**	Uniquely identifies the subscriber to the service. This is the alias used by the MSO to identify the intercept Subject (e.g., user ID, Service Account ID). There can be more than one form of identity used.
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.

7.13.4.1.1 Type Definitions

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

Table 3 - xml Defined Types

Defined Type	Definition	Permitted Values
IpAddress	string	IPv4 dotted address notation
MacAddress	hexBinary	Mac Address

7.13.4.2 Message Parameters

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

7.13.4.2.1 Access Attempt Message

Table 4 - Information for Access Attempt Message

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

7.13.4.2.2 Access Accepted Message

Table 5 - Information for Access Accepted Message

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

7.13.4.2.3 Access Failed Message

Table 6 - Information for Access Failed Message

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

7.13.4.2.4 Access Session End Message

Table 7 - Information for Access Session End Message

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

7.13.4.2.5 Packet Data Summary Report Message

Table 8 - Information for Packet Data Summary Report Message

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

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

7.13.4.2.6 Surveillance Status Report Message

Table 9 - Information for Surveillance Status Report Message

Information Element	M/O/C	Condition
Case Identity	M	
MF System Identity	M	
Time Stamp	M	
Access Session Identity	M	
Status	M	

7.14 Correlation

R-450 The MSO MUST ensure that the intercepted Out of Band Events and Full Packet Streams (or headers in the case of a Limited broadband intercept) delivered to the LEA must be accurately correlated within an intercept category per Subject.

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

8 BROADBAND INTERCEPT FUNCTION, COLLECTION INTERFACE REQUIREMENTS AND FILE FORMAT

8.1 Broadband Intercept Function Requirements

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-460 The BIF MUST make available a temporary directory and a limited privilege account (create and directory read) to the MF.

R-470 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-480 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-490 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-500 The Broadband Intercept Function MUST be provisioned with a buffering capacity that will accommodate 24 hours of network usage by Subject per intercept.

R-510 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-520 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 (e.g., xxxxx.dmp and `xxxxx.hash`).

R-530 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-540 There MUST be one directory per intercept, named with the MSO generated Case Identity defined above in Table 2. This is referenced for the directory structure as *`caseIdentity.`*

R-550 This intercept directory MUST contain three sub-directories, named *`full, limited, and oob`*. Example paths are as follows:

*caseIdentity/**full**/xxxxx.**dmp***
*caseIdentity/**full**/xxxxx.**hash***

*caseIdentity/**limited**/xxxxx.**xml***

*caseIdentity/**limited**/ xxxxx.**hash***

*caseIdentity/**oob**/xxxxx.**dmp***
*caseIdentity/**oob**/message_Name-yyyyy.**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 9 points to the file as listed immediately above. The hash value in the hash parameter is the hash of that file.

The parameter "Message_Name" is the name of the event message name in Table 4 through Table 9. The numeric sequence is appended by the Mediation Function (e.g.

*caseIdentity/**oob**/message_Name-yyyyy.**xml*** becomes
Casedea001/oob/AccessAttempt-00013.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/13.dmp.`

R-560 The intercepted data captured pursuant to a Limited Broadband Intercept Order as described in Section 7.12.2 of this document MUST be captured in the *caseIdentity/limited* and *caseIdentity/oob* subdirectories using the XML schema defined in Annex C.

R-570 The intercepted packets captured pursuant to a Full Content Broadband Intercept Order as described in Section 7.12.1 of this document MUST be stored in the *caseIdentity/full* subdirectory using the PCAP format, and the out of band events MUST be stored in the *caseIdentity/oob* subdirectory using the XML schema defined in Annex C.

R-580 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.

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.

⚠ 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;
```

- 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

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 and
- the oob .dmp file.

Hash files have a .hash file extension.

B.3 xml Encoded Events

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

B.4 File Formats for Intercept Data

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

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

B.4.1 XML Instance Documents Format for Limited Intercept

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

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

The elements defined in the PacketDataSummaryReport sequence follows the above header

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

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

```
<?xml version="1.0"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:ipdr="http://www.ipdr.org/namespaces/ipdr">
   <import namespace="http://www.ipdr.org/namespaces/ipdr"
schemaLocation="http://www.ipdr.org/public/IPDRDoc3.5.1.xsd"/>
   <include schemaLocation="http://www.ipdr.org/public/IPDRTypes.xsd"/>

   <element name="AccessMethod">
      <complexType>
         <sequence>
            <element ref="CBI:Method"/>
            <element ref="CBI:EquipmentID"/>
         </sequence>
      </complexType>
   </element>
   <element name="AccessSessionCharacteristics">
      <simpleType>
         <restriction base="string"/>
      </simpleType>
   </element>
   <element name="AccessSessionId">
      <simpleType>
         <restriction base="integer"/>
      </simpleType>
   </element>
   <element name="CaseIdentity">
      <simpleType>
         <restriction base="string"/>
      </simpleType>
   </element>
   <element name="Hash">
      <simpleType>
         <restriction base="hexBinary">
            <minLength value="32"/>
         </restriction>
      </simpleType>
   </element>
   <element name="DeviceAddress">
      <simpleType>
         <restriction base="ipdr:macAddress"/>
      </simpleType>
   </element>
   <element name="LocationInformation">
      <simpleType>
         <restriction base="string">
            <enumeration value="home"/>
            <enumeration value="remoteAccess"/>
            <enumeration value="offNetwork"/>
            <enumeration value="other"/>
         </restriction>
```

```
    </simpleType>
  </element>
  <element name="MFSystemIdentity">
    <simpleType>
      <restriction base="string"/>
    </simpleType>
  </element>
  <element name="NetworkAccessNodeIdentity">
    <simpleType>
      <restriction base="string"/>
    </simpleType>
  </element>
  <element name="FailureReason">
    <simpleType>
      <restriction base="string">
        <enumeration value="DHCPv4NAK"/>
      </restriction>
    </simpleType>
  </element>
  <element name="SignalCaptureFileName">
    <simpleType>
      <restriction base="string"/>
    </simpleType>
  </element>
  <element name="Status">
    <complexType>
      <sequence>


        <element ref="CBI:StatU.S.C.ode"/>
        <element ref="CBI:StatusDetails" minOccurs="0"/>
      </sequence>
    </complexType>
  </element>
  <element name="SubscriberIdentity">
    <simpleType>
      <restriction base="string"/>
    </simpleType>
  </element>
  <element name="TimeStamp">
    <simpleType>
      <restriction base="ipdr:dateTimeUsec"/>
    </simpleType>
  </element>
  <element name="Method">
    <simpleType>
      <restriction base="string">
        <enumeration value="cm"/>
        <enumeration value="emta"/>
        <enumeration value="dsg"/>
        <enumeration value="other"/>
      </restriction>
    </simpleType>
  </element>
  <element name="LeaseDuration">
```

```
    <simpleType>
      <restriction base="nonNegativeInteger"/>
    </simpleType>
  </element>
  <element name="IAPSystemIdentity">
    <simpleType>
      <restriction base="string"/>
    </simpleType>
  </element>
  <element name="EquipmentID">
    <simpleType>
      <restriction base="ipdr:macAddress">
        <length value="6"/>
      </restriction>
    </simpleType>
  </element>
  <element name="sourceAddress" type="ipdr:ipAddr"/>
  <element name="destAddress" type="ipdr:ipAddr"/>
  <element name="sourcePort" type="unsignedInt"/>
  <element name="destPort" type="unsignedInt"/>
  <element name="protocol" type="unsignedByte"/>
  <element name="NumPktsSinceLastReport">
    <simpleType>
      <restriction base="unsignedInt"/>
    </simpleType>
  </element>
  <element name="StatU.S.C.ode">
    <simpleType>
      <restriction base="string">
        <enumeration value="Up"/>
        <enumeration value="Down"/>
        <enumeration value="Unknown"/>
      <enumeration value="Heartbeat"/></restriction>
    </simpleType>
  </element>
  <element name="StatusDetails" type="string"/>
  <element name="PacketSignature">
    <complexType>
      <sequence>
        <element ref="CBI:sourceAddress"/>
        <element ref="CBI:destAddress"/>
        <element ref="CBI:sourcePort"/>
        <element ref="CBI:destPort"/>
        <element ref="CBI:protocol"/>
        <element ref="CBI:NumPktsSinceLastReport"/>
      </sequence>
    </complexType>
  </element>
  <element name="AccessAttempt">
    <complexType>
      <sequence>
        <element ref="CBI:CaseIdentity"/>
        <element ref="CBI:MFSystemIdentity"/>
        <element ref="CBI:TimeStamp"/>
        <element ref="CBI:SubscriberIdentity"/>
```

```
            <element ref="CBI:AccessMethod"/>
            <element ref="CBI:NetworkAccessNodeIdentity"/>
            <element ref="CBI:SignalCaptureFileName" minOccurs="0"/>
            <element ref="CBI:Hash" minOccurs="0"/>
         </sequence>
      </complexType>
   </element>
   <element name="AccessAccepted">
      <complexType>
         <sequence>
            <element ref="CBI:CaseIdentity"/>
            <element ref="CBI:MFSystemIdentity"/>
            <element ref="CBI:TimeStamp"/>
            <element ref="CBI:SubscriberIdentity"/>
            <element ref="CBI:AccessMethod"/>
            <element ref="CBI:NetworkAccessNodeIdentity"/>
            <element ref="CBI:DeviceAddress"/>
            <element ref="CBI:AccessSessionId"/>
            <element ref="CBI:AccessSessionCharacteristics"/>
            <element ref="CBI:LocationInformation"/>
            <element ref="CBI:LeaseDuration"/>
            <element ref="CBI:SignalCaptureFileName" minOccurs="0"/>
            <element ref="CBI:Hash" minOccurs="0"/>
         </sequence>
      </complexType>
   </element>
   <element name="AccessFailed">
      <complexType>
         <sequence>
            <element ref="CBI:CaseIdentity"/>
            <element ref="CBI:MFSystemIdentity"/>
            <element ref="CBI:TimeStamp"/>
            <element ref="CBI:SubscriberIdentity"/>
            <element ref="CBI:DeviceAddress"/>
            <element ref="CBI:FailureReason"/>
            <element ref="CBI:SignalCaptureFileName" minOccurs="0"/>
            <element ref="CBI:Hash" minOccurs="0"/>
         </sequence>
      </complexType>
   </element>
   <element name="AccessSessionEnd">
      <complexType>
         <sequence>
            <element ref="CBI:CaseIdentity"/>
            <element ref="CBI:MFSystemIdentity"/>
            <element ref="CBI:TimeStamp"/>
            <element ref="CBI:SubscriberIdentity"/>
            <element ref="CBI:DeviceAddress"/>
            <element ref="CBI:AccessSessionId"/>
            <element ref="CBI:SignalCaptureFileName" minOccurs="0"/>
            <element ref="CBI:Hash" minOccurs="0"/>
         </sequence>
      </complexType>
   </element>
```

```
  <element name="PacketDataSummaryReport">
    <complexType>
      <sequence>
        <element ref="CBI:CaseIdentity"/>
        <element ref="CBI:IAPSystemIdentity"/>
        <element ref="CBI:TimeStamp"/>
        <element ref="CBI:AccessSessionId"/>
        <element ref="CBI:PacketSignature" maxOccurs="unbounded"/>

      </sequence>
    </complexType>
  </element>
  <element name="SurveillanceStatusReport">
    <complexType>
      <sequence>
        <element ref="CBI:CaseIdentity"/>
        <element ref="CBI:MFSystemIdentity"/>
        <element ref="CBI:TimeStamp"/>
        <element ref="CBI:AccessSessionId"/>
        <element ref="CBI:Status"/>
      </sequence>
    </complexType>
  </element>
  <element name="CBISMessage">
    <complexType>
      <choice>
        <element ref="CBI:AccessAttempt"/>
        <element ref="CBI:AccessAccepted"/>
        <element ref="CBI:AccessFailed"/>
        <element ref="CBI:AccessSessionEnd"/>
         <element ref="CBI:SurveillanceStatusReport"/>
      </choice>
    </complexType>
  </element>
  <element name="CBISMessages">
    <complexType>
      <sequence>
        <element ref="CBI:CBISMessage" maxOccurs="unbounded"/>
      </sequence>
    </complexType>
  </element>
</schema>
```

Appendix I Limited Intercept XML Instance Document File

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

   <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
   <CBI:IAPSystemIdentity>cmts-col1.mso.com</CBI:IAPSystemIdentity>
   <CBI:TimeStamp>2007-04-06T17:16:34.000000Z</CBI:TimeStamp>
   <CBI:AccessSessionId>5671986</CBI:AccessSessionId>
   <CBI:PacketSignature>
      <CBI:sourceAddress>23.45.32.12</CBI:sourceAddress>
      <CBI:destAddress>197.200.1.45</CBI:destAddress>
      <CBI:sourcePort>32456</CBI:sourcePort>
      <CBI:destPort>80</CBI:destPort>
      <CBI:protocol>6</CBI:protocol>
      <CBI:NumPktsSinceLastReport>4564</CBI:NumPktsSinceLastReport>
   </CBI:PacketSignature>
   <CBI:PacketSignature>
      <CBI:sourceAddress>197.200.1.45</CBI:sourceAddress>
      <CBI:destAddress>23.45.32.12</CBI:destAddress>
      <CBI:sourcePort>80</CBI:sourcePort>
      <CBI:destPort>32456</CBI:destPort>
      <CBI:protocol>6</CBI:protocol>
      <CBI:NumPktsSinceLastReport>2855612</CBI:NumPktsSinceLastReport>
   </CBI:PacketSignature>
</CBI:PacketDataSummaryReport>
```

Appendix II Out of Band Messages XML Instance Document File

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

```
<?xml version="1.0"?>
< CBI:AccessAttempt xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-12T18:11:05.250000Z</CBI:TimeStamp>
        <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
        <CBI:AccessMethod>
          <CBI:Method>other</CBI:Method>
          <CBI:EquipmentID>11-00-AA-FE-80-1A</CBI:EquipmentID>
        </CBI:AccessMethod>
        <CBI:NetworkAccessNodeIdentity>MF-01.mso.com</CBI:NetworkAccessNodeIdentity>
        <CBI:SignalCaptureFileName>Bill-Kostka/oob/0045.dmp</CBI:SignalCaptureFileName>
        <CBI:Hash>1EEEC054802A56B0F2C612A596CF367EE392A84C30FC6826A21B951A9302A6BA</CBI:
Hash>
</CBI:AccessAttempt>
```

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

```
<CBI:AccessAccepted xmlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-12T18:11:08.500000Z</CBI:TimeStamp>
        <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
        <CBI:AccessMethod>
          <CBI:Method>other</CBI:Method>
          <CBI:EquipmentID>11-00-AA-FE-80-1A</CBI:EquipmentID>
        </CBI:AccessMethod>
        <CBI:NetworkAccessNodeIdentity>MF-01.mso.com</CBI:NetworkAccessNodeIdentity>
        <CBI:DeviceAddress>178.46.10.131</CBI:DeviceAddress>
        <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
        <CBI:AccessSessionCharacteristics>string</CBI:AccessSessionCharacteristics>
        <CBI:LocationInformation>142 Broadway New York, NY, 10025</CBI:LocationInformation>
        <CBI:LeaseDuration>259200</CBI:LeaseDuration>
        <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

```
<CBI:AccessFailed mlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-14T18:23:12.750000Z</CBI:TimeStamp>
        <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
        <CBI:DeviceAddress>178.46.11.48</CBI:DeviceAddress>
        <CBI:FailureReason>DHCPv4NAK</CBI:FailureReason>
        <CBI:SignalCaptureFileName>Bill-Kostka/oob/0052.dmp</CBI:SignalCaptureFileName>
        <CBI:Hash>F84957A8AEE3F5B5563C48149F997FFE2978BB97B21EC49FCFC1E5229459DB65</CBI:
Hash>
</CBI:AccessFailed>
```

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

```
<CBI:AccessSessionEnd mlns:CBI="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.cablelabs.com/namespaces/CBI/2.0/xsd/CBI
file:///c:/DOCSIS3.0/DOCSIS3.0/CBI/schemaDetailsV5-with-IPDRTypes.xsd">
        <CBI:CaseIdentity>Bill-Kostka</CBI:CaseIdentity>
        <CBI:MFSystemIdentity>MF-01.mso.com</CBI:MFSystemIdentity>
        <CBI:TimeStamp>2007-05-12T21:03:34.250000Z</CBI:TimeStamp>
        <CBI:SubscriberIdentity>AC-DE-48-6E-4A-21</CBI:SubscriberIdentity>
        <CBI:DeviceAddress>178.46.10.131</CBI:DeviceAddress>
        <CBI:AccessSessionId>-9223372036854775808</CBI:AccessSessionId>
        <CBI:SignalCaptureFileName>Bill-Kostka/oob/0047.dmp</CBI:SignalCaptureFileName>
        <CBI:Hash>57CB73A6A68D706819D666889F085EF715181AF42B85E58A364BEA3F4C787A88</CBI:
Hash>
</CBI:AccessSessionEnd>
```

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

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

Appendix III Physical Consideration

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

Powering: 117 VAC or -48 VDC

Structural: 19" Racks or 23" racks

HVAC: Power consumption for all components

Physical space: Rack Space in RU's

Physical security: Rack doors, room access, etc.

Data Communication: Connectors and Wiring.

Appendix IV Example Flow Chart Implementation

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

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

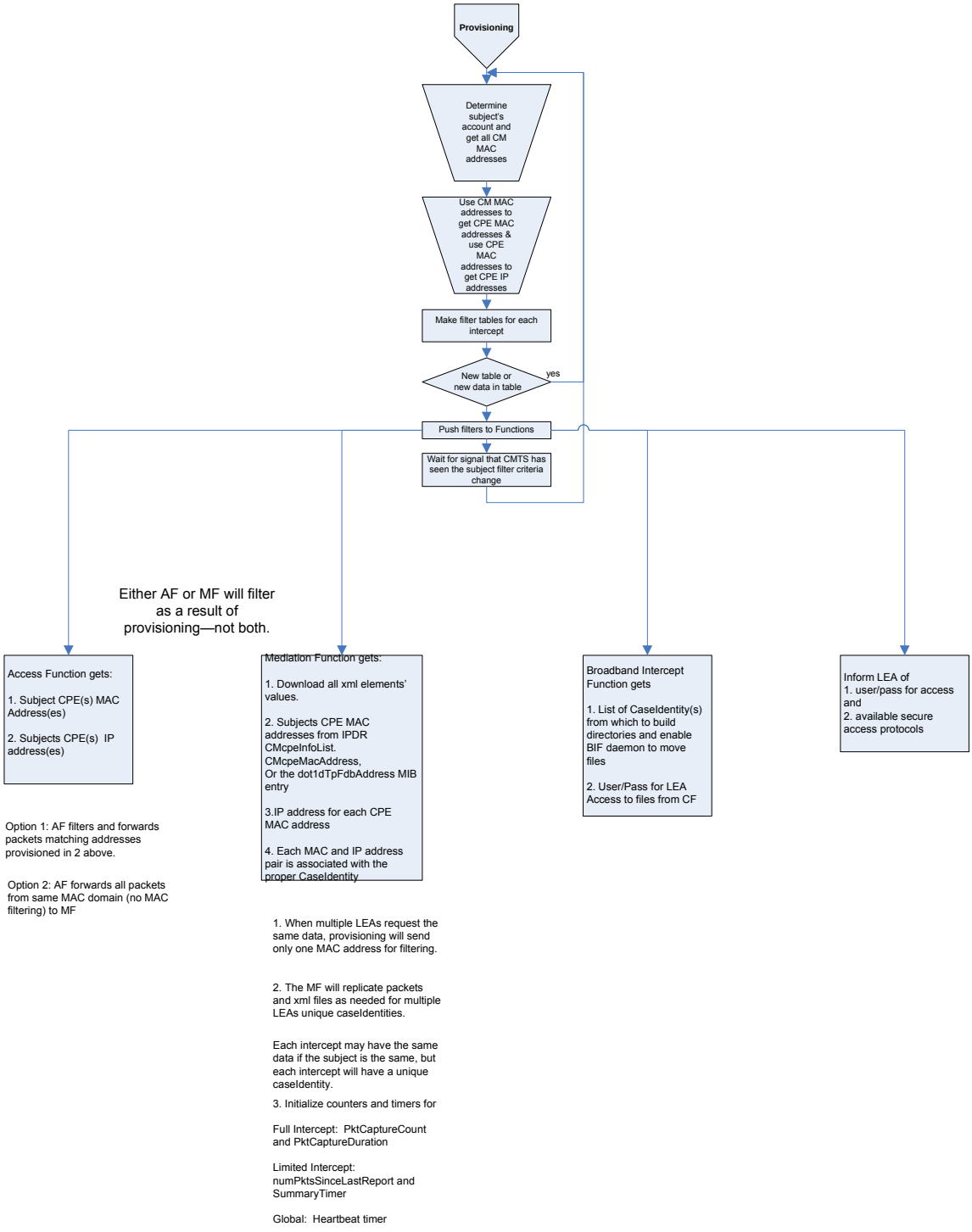

Figure 3 - Provisioning the functions with data from the CMTS

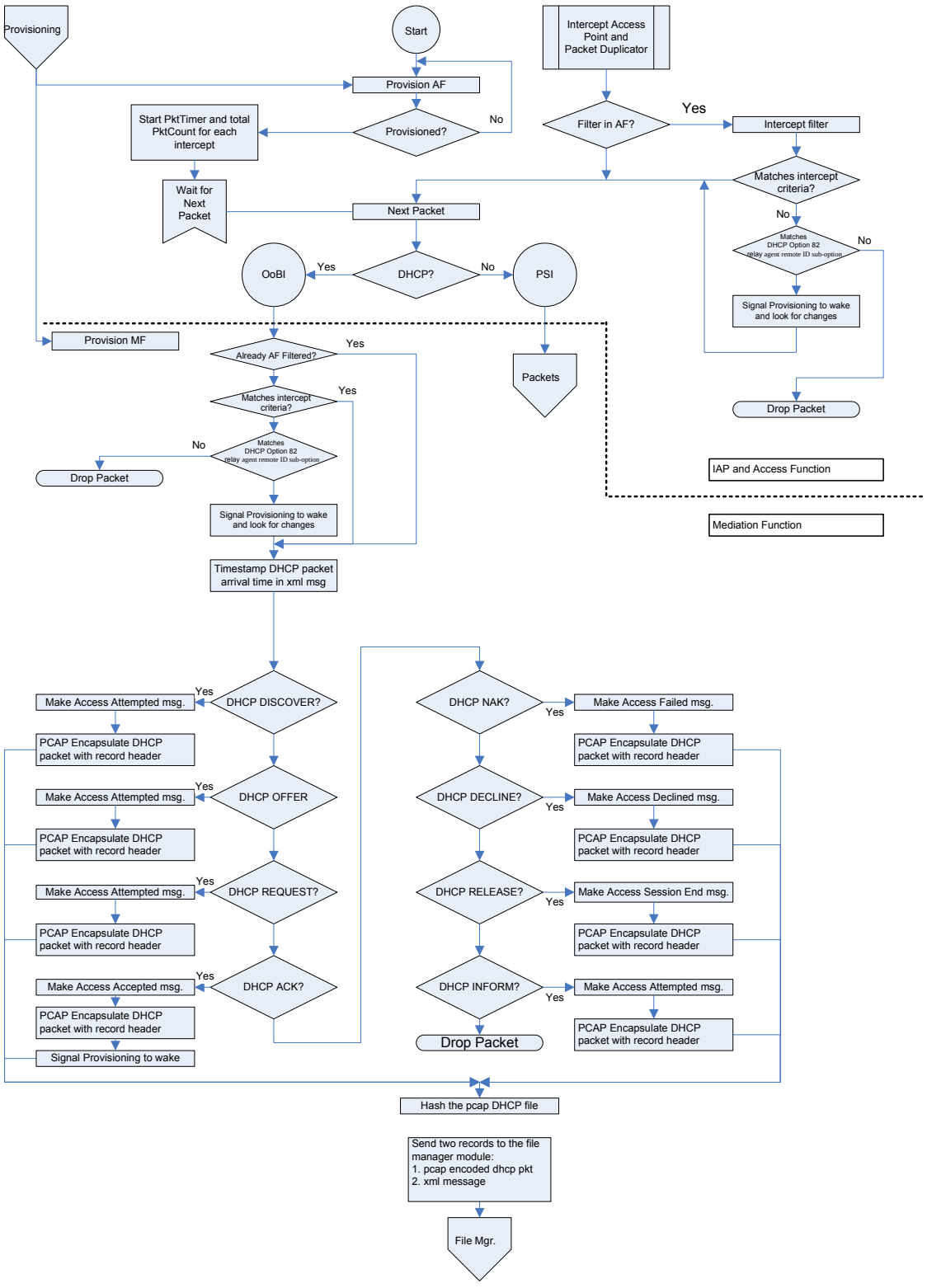

Figure 4 - The Access Function, Intercept Access Points, and Out-of-Band Processing

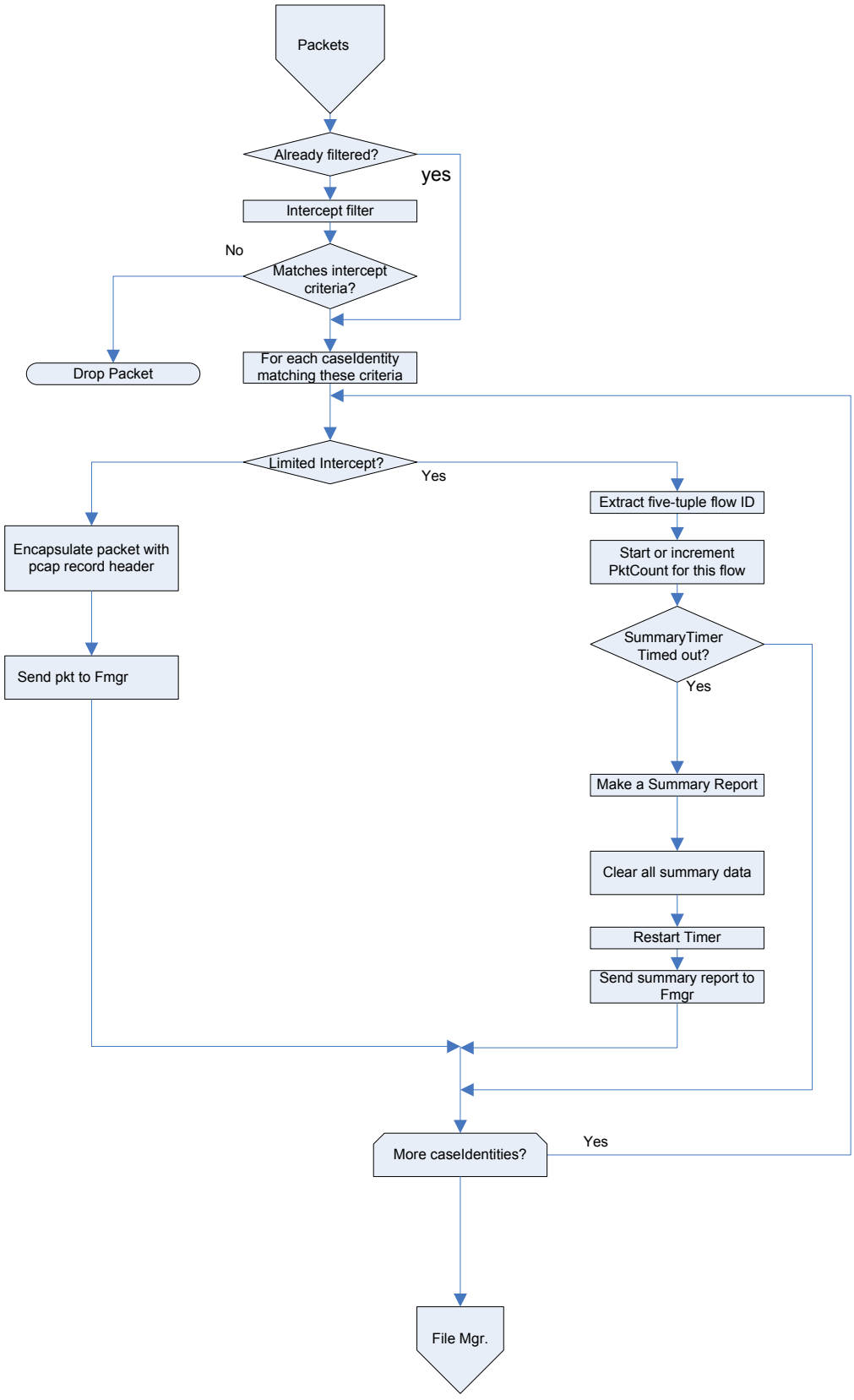

Figure 5 - Packet Processing: full intercepts and limited intercepts

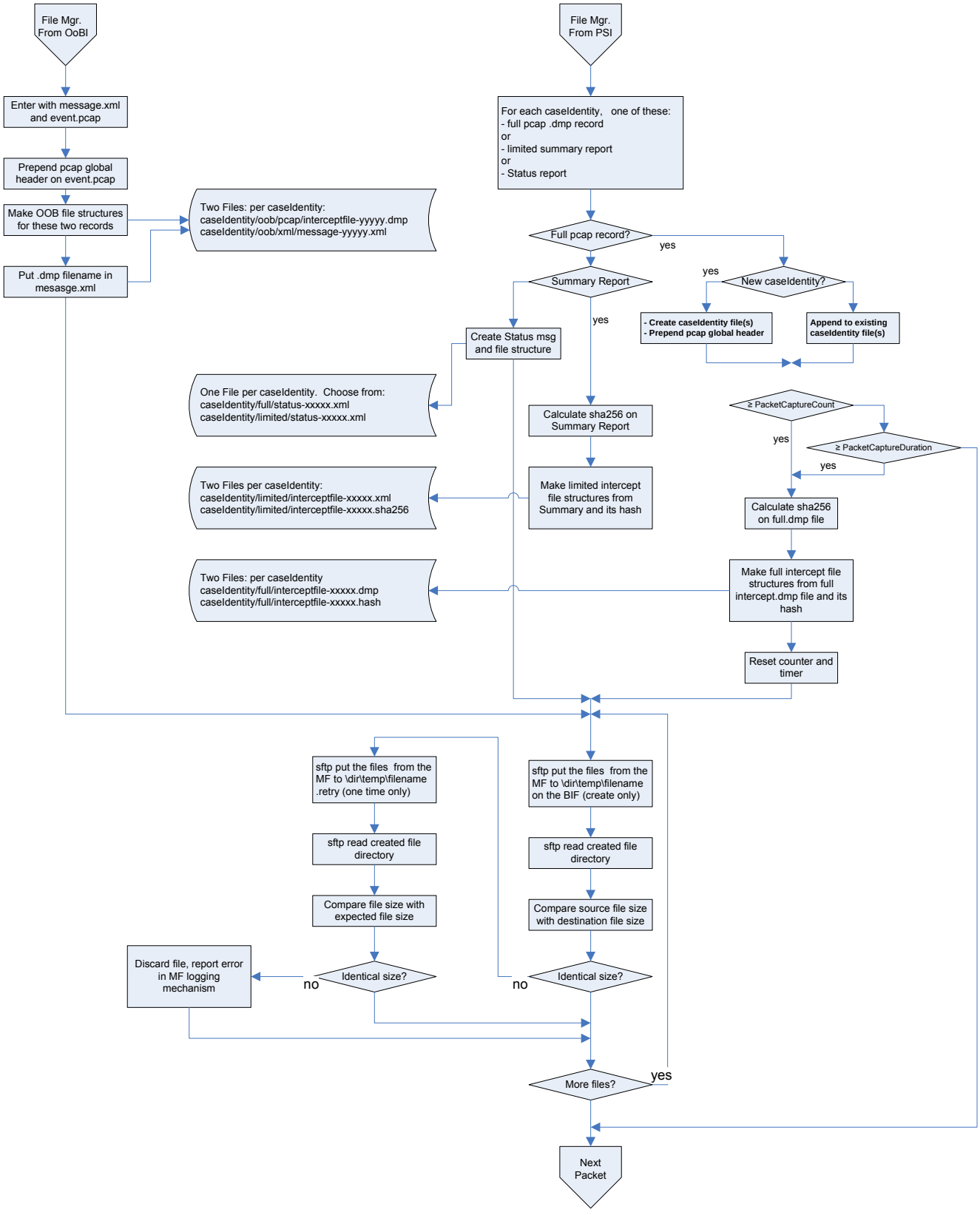

Figure 6 - The file manager

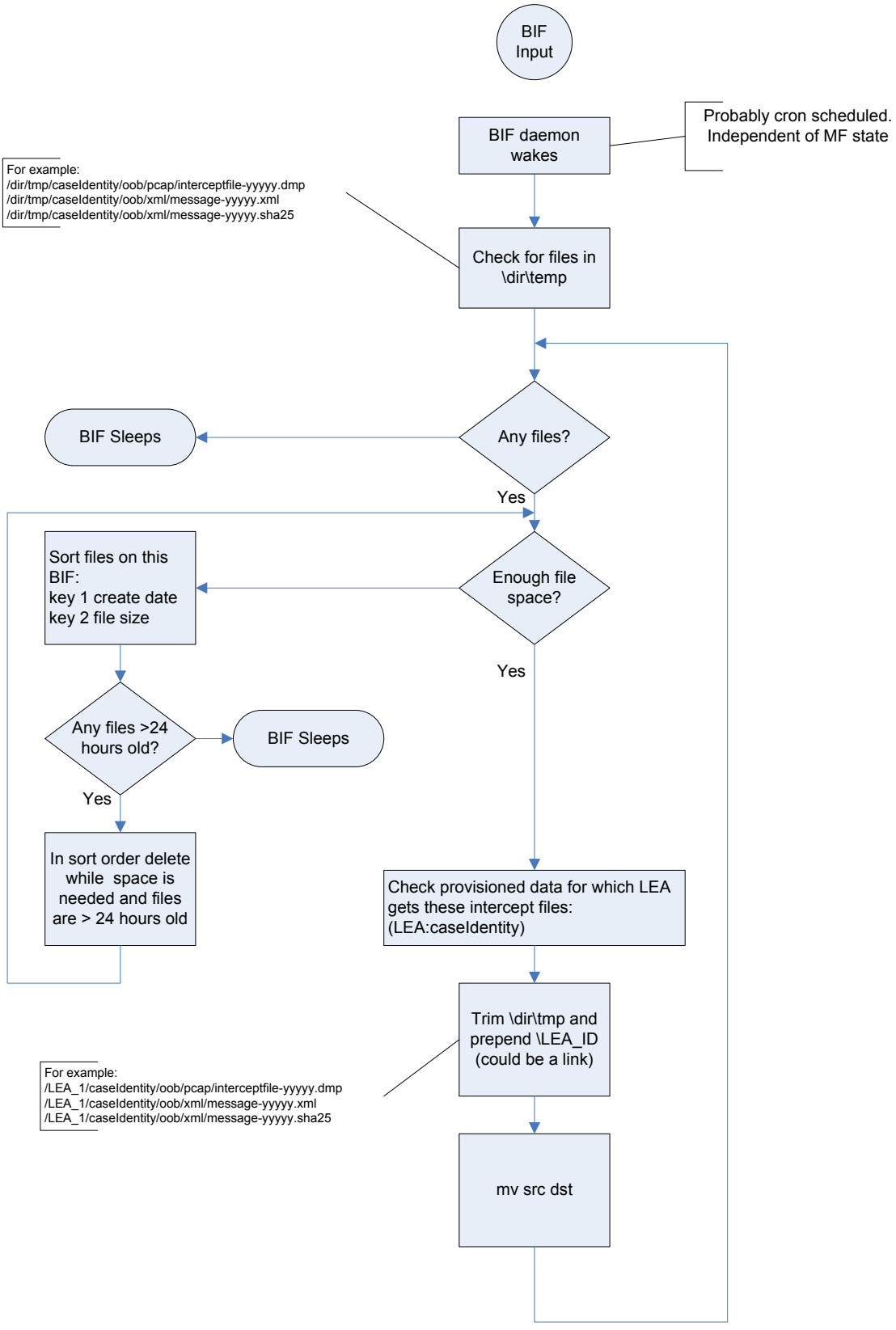

Figure 7 - The Broadband Intercept Function

Appendix V Acknowledgements

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

Alex Hoff	Sandvine Incorporated
Dusty Hoffpauir	NeoStar
Jeff Hartley	Intensify Security
Michael Bilca	FBI CALEA Implementation Unit (Tridea Works)
David Bushta	Comcast
Craig Mulholland	Cisco Systems
Eduardo Cardona	Cable Television Laboratories, Inc.
Simon Krauss	Cable Television Laboratories, Inc.
Lakshmi Raman	Cable Television Laboratories, Inc.

Bill Kostka, Cable Television Laboratories, Inc.