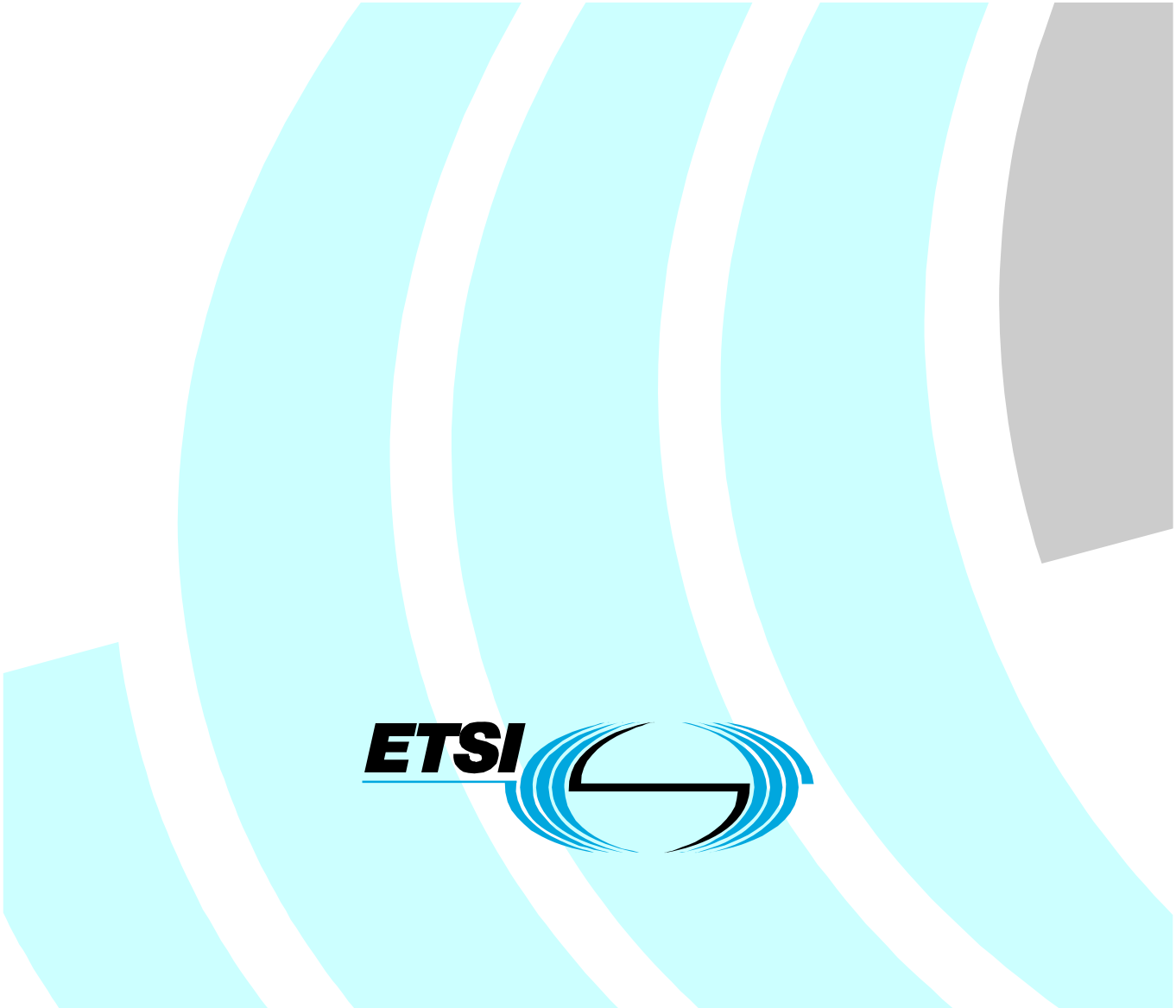
ETSI TS 102 836-2 V1.1.1 (2009-11)

Technical Specification

**Access, Terminals, Transmission and Multiplexing (ATTM);
Lawful Interception (LI);
Part 2: Interception of IP Data Service on Cable Operator's Broadband IP Network: Internal Network Interfaces**



Reference
DTS/ATTM-02007-2

Keywords
access, cable, lawful interception

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 4
Foreword 4
Introduction 4
1 Scope 5
1.1 Requirements notation 5
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Abbreviations 7
4 Requirements 8
5 Overview 9
6 Internal Cable Network Interfaces 10
6.1 Introduction 10
6.2 INI1 10
6.2.1 Dynamically assigned IP-addresses 11
6.2.2 DHCPv4 requirements on CMTS 11
6.2.3 DHCPv6 requirements on CMTS 12
6.2.4 Non-dynamically assigned IP-addresses 12
6.3 INI2b 12
6.4 INI3 - Call Content (CC) of Communication Interface 12
6.4.1 Call Content Connection Identifier 13
6.4.2 Original IP Header 13
6.4.3 Original other header 13
6.4.5 Original Payload 14
6.5 SBCF (SNMP based Configuration Function) 14
7 LI Cable Broadband IP Network Architecture 14
7.1 Dimensioning and Capacity 15
7.2 Elements of Cable Broadband IP Network 15
7.3 Functional Description 15
7.3.1 LI Process: Interception of provisioning messaging 16
7.3.2 LI Process: interception of IP data 18
7 Security 19
Annex A (informative): Requirements listed in Council Resolution of 17 January 1995 20
History 22

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

NOTE: An earlier specification to the current document referring to Lawful Interception within a Cable Network was produced by ETSI Access and Terminals, subgroup AT-D (Digital).

The present document is part 2 of a multi-part deliverable covering Data Over Cable Systems, as identified below:

Part 1: "Interception of IP Telephony Service on Cable Operator's Broadband IP Network: Intenral Network Interfaces";

Part 2: **"Interception of IP Data Service on Cable Operator's Broadband IP Network: Intenral Network Interfaces";**

Part 3: "Interception of email Service on Cable Operator's Broadband IP Network: Intenral Network Interfaces".

Introduction

The cable industry in Europe and across other global regions have already deployed broadband cable television Hybrid Fibre/Coaxial (HFC) IP data and telephony networks running the Cable Modem Protocol. The cable industry is in the rapid stages of implementing interfaces that provide the capabilities for lawful interception (LI) of these services in accordance with requirements of Law Enforcement Agencies.

The cable industry has recognized the urgent need to develop ETSI Technical Specifications aimed at developing interoperable interface specifications and mechanisms for LI of IP telephony communications services.

The present document specifies the Lawful Interception (LI) and implementation of IP Data services within a Cable Operators Broadband IP Network for the purpose of providing such intercepted information to Law Enforcement Agencies (LEAs).

1 Scope

The present document specifies the internal network interfaces to enable the lawful interception (LI) of IP Data services over cable operators broadband IP Networks. The current document describes the LI functional elements and interfaces for both the NCS based and SIP protocol signalling architectures within a PacketCable™ network architecture framework.

The present document provides the requirements for the internal cable network interfaces and there functions for those network elements within a Cable Operators network that are involved in the production of the interception of call content and call related information relating to the interception target of IP Data communication services.

The provision of a (LI) interface for a Cable Operators Broadband IP Network is a national option, however where it is provided it shall be provided as described in the present document.

The structure of (LI) in telecommunications is in two parts: The internal interface of a network that is built using a particular technology; and, the external interface (known as the Handover Interface) that links the LEA to the network. Between these two parts is described a LI mediation device (MD) whose functions cater for managing and provisioning the network elements for interception as well as national variances and delivery of the result of interception. The administration of LI is a function that is typically integrated within the manufactuers MD but may also be a separate device. For the purpose of the current document the administration frunction is assumed as integrated within the MD.

The subject of the present document is the internal network LI interfaces that lies between the elements of a Cable Operators IP Broadband infrastructure and the functions of the MD.

The Handover Interface is out of scope of the present document. The current document assumes the delivery requirements specified by ETSI Technical Committee Lawful Intercept (TC LI), ES 201 671 [2], TS 101 671 [3] and TS 102 232 [4]. In addition the Handover Interface may be the subject of national regulation and therefore the function of the mediation device for delivery of the intercepted information to the LEA may also be a matter of national regulation.

The document specifies the internal interfaces for IPv4 and IPv6 networks. For systems that are used in networks that only use IPv4, the requirements specific for IPv6 are not applicable.

Systems that use SIP based on Packet Cable™ 2.0 is out of scope of the present document.

Systems that use PPPoE over cable networks are out-of-scope.

1.1 Requirements notation

If the present document is implemented, the key words "MUST" and "SHALL" as well as "REQUIRED" are to be interpreted as indicating a mandatory aspect of the present document. The keywords indicating a certain level of significance of a particular requirement that are used throughout the present document are summarized below.

MUST This word or the adjective "REQUIRED" means that the item is an absolute requirement of the present document.

MUST NOT This phrase means that the item is an absolute prohibition of the present document.

SHOULD This word or the adjective "RECOMMENDED" 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 behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY This word or the adjective "OPTIONAL" 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

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] Council Resolution of 17 January 1995 on the lawful interception of telecommunications.

[2] ETSI ES 201 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[3] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[4] ETSI TS 102 232: "Lawful Interception (LI); Handover specification for IP delivery".

[5] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services;Part 4: Network Call Signalling Protocol [Partial Endorsement of ITU-T Recommendation J.162 (11/2005), modified]".

[6] IETF RFC 3261: "SIP: Session Initiation Protocol".

[7] CableLabs PKT-SP-ESP1.5-IO2-070412: "Electronic Surveillience", April 12 2007.

[8] IETF RFC 768/ST0006 (August 1980): "User Datagram Protocol".

[9] IETF RFC 1305 (March 1992): "Network Time Protocol (Version 3) Specification, Implementation and Analysis.

[10] IETF RFC 791/STD0005 (September 1981): "Internet Protocol".

[11] Void.

[12] Void.

[13] IETF RFC 3924: "Cisco Architecture for Lawful Intercept in IP Networks".

[14] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 102 661 (November 2008): "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

[i.2] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CC	Call Content
CCC	Communication Call Content
CMTS	Cable Modem Termination System
CRD	Call Related Details
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
eMTA	embedded Media Terminal Adapter
HFC	Hybrid Fiber Coax
HI	Handover Interface
IAP	Intercept Access Point
IETF	Internet Engineering Task Force
IIF	Internal Intercept Function
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Law Interception
LIAF	Lawful Interception Administration Function
LIMD	Lawful Intercept Mediation Device
MAC	Media Access Control
MD	Mediation Device
MF	Mediation Function
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MTA	Media Terminal Adapter
NCS	Network-based Call Signalling
NWO	Network Operator
SBCF	SNMP Based Configuration Function
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SvP	Service Provider
TAP	Tapping
TCP	Transmission Control Protocol
UDP	User Data Protocol
USM	User-based Security Module
VACM	View-based Access Control Module

4 Requirements

European cable operators are required to have the capability of intercepting messages passed over their networks system in any form. This capability should be covert, not affect the operation of the system in any discernible way or be detectable by the end user. Therefore, a European implementation for a Cable Broadband IP network should include the following functionality:

a) the network equipment needs to be capable of copying all Communication Call Content (CCC) being carried to and from specified target addresses to an additional delivery address specified by the network operator;

b) in the short term, for practical reasons, identification of voice related calls (including fax and modem calls) may use E.164 addresses;

c) where interception of both data and multi-media content is also required, the delivery address will be specified as an IP address in either the standard IPv4 or IPv6 formats; the target addresses may be either service addresses or IP addresses;

d) the mechanism for lawful interception, where provided, in an IPCablecom system will ideally be capable of correct operation in networks where a customer's IP address is allocated dynamically, e.g. by a DHCP server, by relating the current IP address to the customer's equipment MAC address, or otherwise;

e) it needs to be possible to provide both the Call Content and the Intercept Related Information (IRI) regarding the communication, including that added by the network operator to facilitate correct identification of the intercept to the law enforcement agencies;

f) the mechanism for LI should correctly relate the 'Call Content' and the 'CRD';

g) the capacity of the LI mechanism to provide multiple intercepts should be adequate; this requirement is subject of National Legislation.

h) the LI facility should be capable of providing numerous simultaneous intercepts and be capable of providing several independent intercepts of the same target address; this requirement is subject of National Legislation.

i) operation of the intercept should be invisible to any customer, even by the use of 'traceroute', 'ping' and similar utilities;

j) any malfunction or mis-operation of the interception facility should not affect the customer's service;

k) control of the facility needs to be segregated from normal operation of the system;

l) it needs to be possible to address and control the interception facility remotely by secure means.

The above should be related to fundamental principles of country specific regulations. Their application in the voice, data and multi-media environments will differ depending on the cable operator's overall network strategy, for example, with legacy circuit switched network solutions or other intermediate network solutions that migrate towards a European DOCSIS© and PacketCable™ network architecture.

NOTE: It is recognized that attempts at compliance with clause (d) may lead to specific difficulties; these should not be allowed to delay early implementation of systems, though it will be necessary to devise a solution in the longer term. This will need further detailed evaluation.

Additional information on LI Requirements as listed in council resolution of 17 January 1995 [1] may also be found in annex B.

The following general requirements apply:

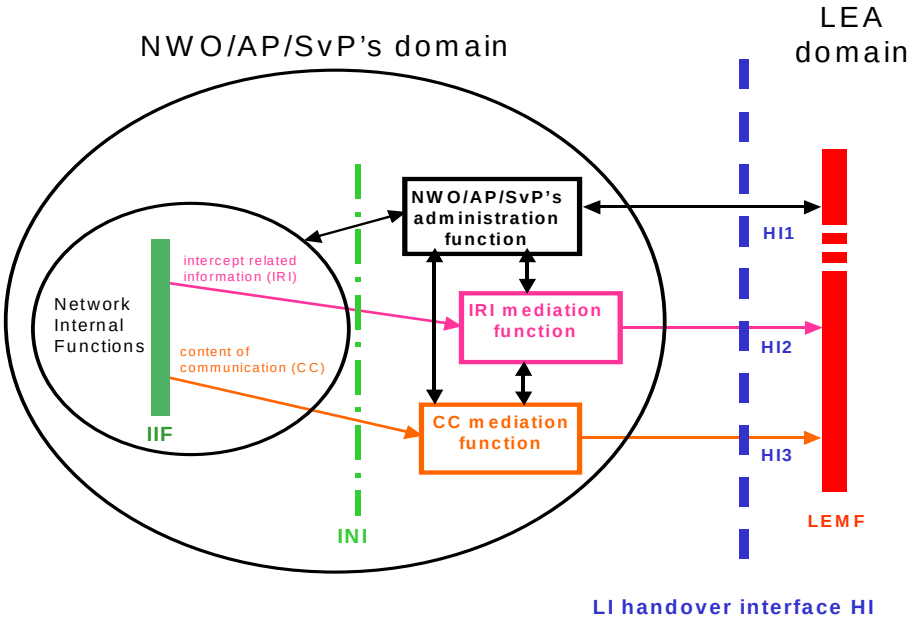
- The LI general requirements as given by TS 101 331 [i.2], including the requirements below apply:
  - Deliver content of communications for voice, fax.
  - Deliver intercept related information.
  - Interception of call features.
  - Real-time delivery.
  - Non-disclosure of information including interception methods and targets.
  - Protection of interception information and information transmission from unauthorized access.
- Solution must meet delivery requirements as given by the ETSI handover interface requirements as given by ETSI TC-LI standards [2], [3] and [4].

Optional requirements where applicable may be defined at a national level, for example:

- Multiple Subscriber Number, in the case of Basic Access services.
- Direct Dialling In number, in the case of Primary Access services.

5 Overview

The overall interception framework is extended from the model described in clause 5.2 of ES 201 158 [14] and from the architecture identified in clause 5 of TS 101 671 as given by [3].



IIF: internal interception function
INI: internal network interface
HI1: administrative information
HI2: intercept related information
HI3: content of communication

Figure 1: Functional block diagram showing Handover Interface HI (from ES 101 671 [2])

The scope of the present document is the NWO/AP/SvP's domain as shown in figure 1 describing the internal interfaces INI1, INI2 and INI3.

The current solution adopts elements of the reference model for LI systems in IP networks defined in RFC 3924 [13], see figure 2.

Automatic discovery of network topology is out-of-scope, i.e. it is assumed that the Mediation Device has it's own means of knowing the network topology.

A mediation device might need to translate signalling on the IP-part of the network to signalling on a different interface type towards the LEA. The translation of this information is out-of-scope for the present document.

The description of the functional elements and interfaces at a generic level as given by RFC 3924 [13], section 2.1 are applied to Cable Networks as described witin clause 5 of the present document.

6 Internal Cable Network Interfaces

6.1 Introduction

The Cable Network provides data services using the (Euro) DOCSIS™ [5] architecture.

The diagram given by figure 2 illustrates the reference model as specified for a Cable Network.

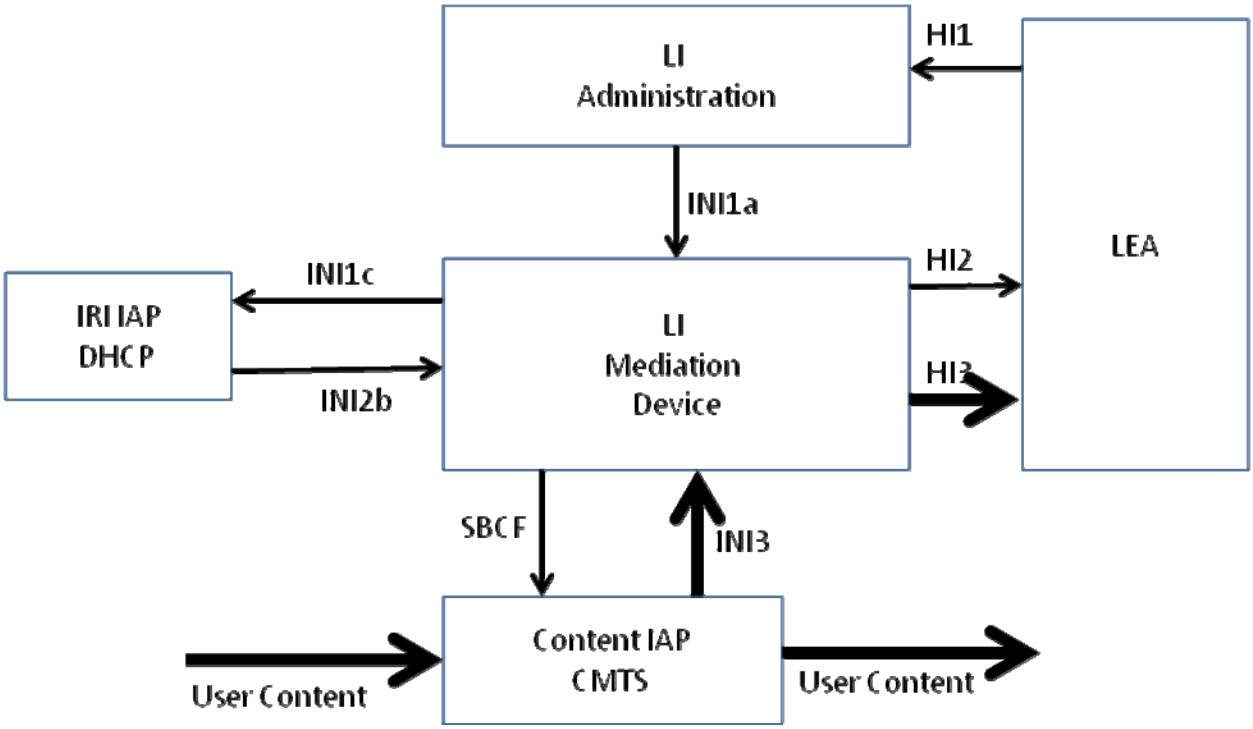


Figure 2: Cable Network Reference model for Lawful Interception

In this model, a Mediation System interacts with LEA and with the cable service provider's network: an LI Administration Function of the Mediation System serves staff at service provider or LEA to manage and provision intercepts; an LI Mediation Function gathers interception information from a diversity of Cable elements Intercept Access Points (IAPs) across the cable service provider's network, and delivers it to one or more LEAs through handover interfaces as defined by ETSI as given by [2], [3] and [4].

6.2 INI1

The protocol used for INI1a is not specified and dependant on the MD equipment. The INI1a between the LI Adminstration and LI MD is assumed to be integrated within the Mediation Device.

The administrative information relating to the target to be intercepted is exchanged between the internal elements of the LI Administration function and LI MD.

In the case that the customer uses dynamic IP-addresses assigned by the operator, the IRI information consist of the DHCP-messages that indicate when the customer connected and disconnected to the network. In the case that the IP-addresses are not dynamically assigned by the operator, there is no IRI information available. Note that the cable operator must ensure that spoofing of IP-addresses is prevented, both for dynamically assigned and non-dynamicaly assigned IP-addresses. This has to be done according to good industry practice.

The IRI information for IP data intercept consists of DHCP messages. The MD provisions a network monitor or the DHCP-server with information on the target for which IRI has to be delivered to the MD over INI2b.

The interface finction and protocol used for INI1c is not specified and dependant on the MD and DHCP server or DHCP server wiretap.

NOTE: Standardisation of interface INI1c to DHCP-server or DHCP server wiretap is for further study.

A target for data intercept will be identified at the cable operator by the MAC-address of the cable modem. The authorized cable operator personel will check if that customer is using dynamic or non-dynamic IP-addresses.

6.2.1 Dynamically assigned IP-addresses

The auhorized cable operator personel must ensure that information related to MAC-addresses behind the cable modem that do not have to be tapped (i.e. MAC-addresses of eMTAs, etc.) is available to the MD. Dynamic IP-addresses assigned to these MAC-addresses must be excluded from the TAP.

In the case that the target is assigned dynamic IP-addresses, the CMTS will be required to insert information in the relayed DHCP-messages towards the DHCP-server to identify the cable modem from which behind the DHCP-messages originate. (specifics for DHCPv4 and DHCPv6 are explained further).

The DHCP-server or DHCP server wiretap is in that case informed about the cable modem MAC-addresses of the target, and also needs to be informed about which MAC-addresses behind this cable modem are excluded from the TAP. (i.e. MAC-address of MTA-device). The DHCP-server or DHCP-server wiretap sent to the MD over the INI2 interface the DHCP-messages to and from the target. Based on the DHCP-messages the MD can identify the IP-addresses that need to be placed under TAP and installs the TAPs over the SBCF interface.

The system must support that a single MAC-address acquires both and IPv4 and IPv6 addresses.

Dynamic IP-addresses are handed out for a limited time (lease-time). The MD in cooperation with the DHCP-server or DHCP-server wiretap must ensure that at the moment the lease of the IP-address for the target is timed-out, that the TAP is removed. Failure to do this could result in tapping customers for which no warrant is present. To be able to detect leases that are timed-out the DHCP-renew messages have to be taken into account.

It could be that at the moment that the TAP is installed the customer was already on-line. To make sure that the system can identify the DHCP messages originating from behind a cable modem in all cases, the CMTS must also insert the MAC-address of the cable modem in the applicable field (see section on DHCPv4 and DHCPv6 requirements on CMTS) for DHCP renew messages. The system must observe DHCP-messages to ensure the TAP is removed or changed at the proper time. (lease expired, change of IP-address).

For systems that only support IPv4, only the requirements relating to DHCPv4 need to be supported. For systems that support both IPv4 and IPv6 the requirements for both DHCPv4 and DHCPv6 must be supported.

In DHCPv6, the IPv6 prefix delegation can be used. The DHCP-server or wiretap must support the feature in cooperation with the MD to install TAPs on subnets based on IPv6 prefrix delegation.

6.2.2 DHCPv4 requirements on CMTS

To identify in the DHCPv4 messages that are intercepted by the relay agent from the CMTS from behind which cable modem the DHCP message originates DHCP option 82 sub-option remote-id needs to be used. This field is added to intercepted DHCP messages by the CMTS and contains the MAC-address of the cable modem from behind which the DHCP message originated. Note that certain MAC-addresses (e.g. from MTA-part in eMTA) need to be excluded from the TAP. Note that all DHCP messages need to be intercepted by the CMTS, including renew-messages.

6.2.3 DHCPv6 requirements on CMTS

To identify in the DHCPv6 messages that are intercepted by the relay agent from the CMTS from behind which cable modem the DHCP message originates the CM MAC ADDRESS option defined in [CANN-DHCP-Req] needs to be used. This field is added to intercepted DHCP messages by the CMTS and contains the MAC-address of the cable modem from behind which the DHCP message originated. Note that certain MAC-addresses (e.g. from MTA-part in eMTA) need to be excluded from the TAP. Note that all DHCP messages need to be intercepted by the CMTS, including renew messages.

6.2.4 Non-dynamically assigned IP-addresses

For cable operators that use IP-addresses that are not dynamically assigned by a DHCP-server from the operator (this can be a single IP-address or an IP-subnet behind a cable modem), the MD needs to get to know the IP-addresses that need to be tapped through other means. (out-of-scope). Those IP-addresses are provisioned to the MD over the INI1a interface. The MD must support a mechanism to support tapping of IP-addresses and IP-subnets. At the moment the MD receives the information over INI1a which IP-addresses need to be tapped the TAP is installed using the SBCF interface.

The MD must support the tapping of a single IP-address, multiple IP-addresses and IP-subnets behind a cable modem.

6.3 INI2b

The Provisioing Function sends all events related to an IP data session that is under intercept to the MD.

Internal interface INI2b carries Intercept Related Information (IRI) from the Provisioning Function relating to the communication session that is under intercept to the MD.

If dynamically assigned IP-addresses are used, the IRI the MD will invoke the SBCF to trigger delivery of the CC.

The IRI information is forwarded over HI2.

The INI2 delivers all IRI information to the MD over INI2b.

The format of INI2 is not specified and could be an internal interface of the MD. The Provisioning Function functionality can be implemented as a wiretap for all traffic to the DHCP-server.

TS 102 232 [4] part 3 provides information on how to map DHCP messages to the required information to be delivered over HI2.

6.4 INI3 - Call Content (CC) of Communication Interface

Internal interface INI3 carries Call Content (CC) of Communication information related to the intercept from the CMTS to the mediation function, consistent with PacketCable™ PC ESP [7], section 5.

This clause describes the mechanism for delivery of call content, via (CC) Connections from the cable operators network LI mediation device (MD) to the Law Enforcement's Mediation Function (LEMF).

Call Content MUST be delivered as a stream of UDP/IP datagrams, as defined in [8] and [i.1], sent to the port number at the LEMF as provided during provisioning of the interception. The UDP/IP payload MUST adhere to the following format.

The CCC datagrams MAY contain a timestamp that allows the MD to identify the time at which the corresponding information was detected by the IAP. This timestamp MUST have an accuracy of at least 200 milliseconds. The Timestamp MUST adhere to the NTP time format as defined in [9]: a 64-bit unsigned fixed-point number, in seconds relative to 0000 on 1 January 1900. The integer (whole seconds) part is in the first 32 bits and the fractional part (fractional seconds) is in the last 32 bits. The timestamp MUST be accurate to within 200 milliseconds.

The timestamp is optional on the CCC interface, a CMTS has the option to include or not include this timestamp. A MD must be configurable to receive packets over INI3 with or without the timestamp. If the timestamp is provided on INI3 the MD must forward the timestamp as received over INI3 to the LEA over HI3. If the timestamp is not provided and the LEA requires a timestamp in the packet on HI3, the MD must insert a timestamp in the packet delivered over HI3 to the LEA.

Table 1: Payload of Call Content Connection Datagrams

CCC Identifier (4 bytes)
Timestamp (8 bytes) (optional)
Intercepted Information (arbitrary length)

Intercepted IP information will be of the following format:

Table 2: Intercepted Information

Original IP Header (20 bytes for IPV4, typically 40 bytes for IPv6)
Original other Header (variable length)
Original Payload (arbitrary length)

6.4.1 Call Content Connection Identifier

The CCC-Identifier is a 32-bit quantity, and is used to identify the intercept order to the Law Enforcement Agency.

A data session typically consists of two separate packet streams, each corresponding to a direction of the communication. Both are delivered to the demarcation point with the same CCC-Identifier. The partyreceiving the packets is identified by the combination of Destination Address (from Original IP Header).

The MD MUST generate a CCC-Identifier that is different from all other CCC-Identifiers in use between that MD and a particular LEA. That is, two streams of content delivered to a single LEA must have different CCC-Identifiers, but a single stream of content delivered to multiple LEAs may use a single CCC-Identifier, so long as no other stream being delivered to one of the LEAs is using the same CCC-Identifier.

6.4.2 Original IP Header

This is the IP header [10] as sent by the endpoint. Contained in this IP header is the IP Source Address (SA) and IP Destination Address (DA), that identify the internet addresses of the source and destination of the packet.

6.4.3 Original other header

The packets can be of any IP-protocol (TCP, UDP, etc.) The original headers are maintained in the CCC sent to the MD.

6.4.5 Original Payload

The payload field is the bit-sequence as sent by the endpoint identified in the Source Address and Source Port.

6.5 SBCF (SNMP based Configuration Function)

Based on SNMPv3, with the use of the IP intercept and IP TAP MIB.

An intercept and tap mib specifies mibs for tapping content at IP Layer and configuraing the delivery of the content to the MD.

7 LI Cable Broadband IP Network Architecture

The cable broadband IP network architecture given by PacketCable™ maps to the LI reference model as given in figure 3.

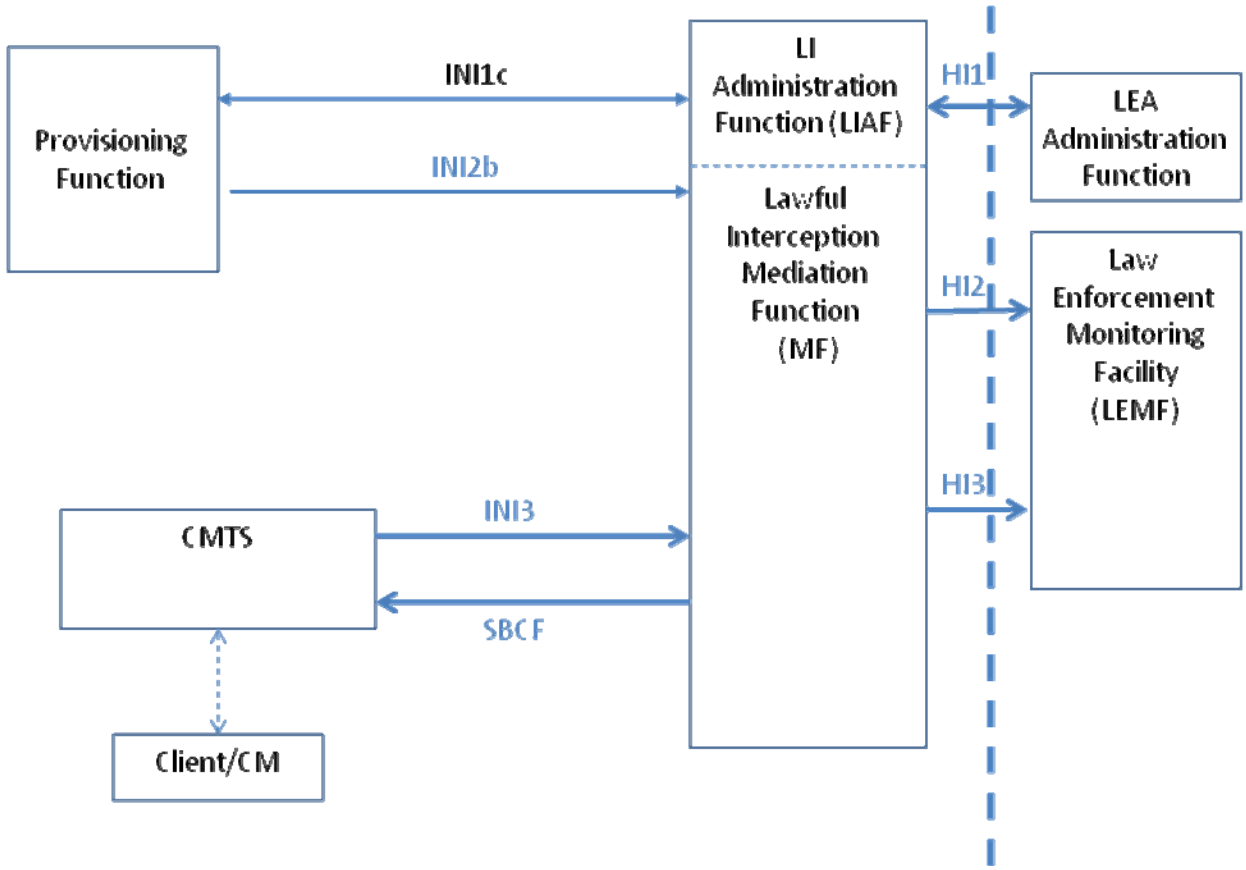


Figure 3: Cable Network Architecture for LI

The Provisioning Function provides the IRI. In an actual implementation of there may be more than one element of Provisioning Functions and MDs within a Cable Network Architecture.

The Provisioning Function provides IRI information to the MD.

IRI information is delivered to the LIMD by the Provisioning Function over INI2 and includes:

- All DHCP messages sent from and to target, note that the DHCP message itself will in many cases be a forwarded message by a DHCP relay agent (function of the CMTS).

The CMTS provides the CC over INI3.

The interception function within the CMTS provides the CC information to the MD as follows:

- Duplication of complete traffic belonging to a specific flow of IP packets based on IP-filter criteria (IP-addresses, port numbers, etc.)

7.1 Dimensioning and Capacity

The LI solution shall be scaled to accommodate the level of interception service that's proportionate with the subscriber base with minimum requirements defined by national legislation, e.g number of LEA's supported by the network provider with delivery to a number of LEMF's and a number of simultaneous interception orders for a single target.

7.2 Elements of Cable Broadband IP Network

LI Monitoring / LEMD Function: The LI Monitoring / Law Enforcement Monitoring function is the system used by the LEA for the receiving of the HI-2 and/or HI-3 information streams. This system requirements are out of sciope of the current document and assumed to be already available.

LI Administration: The LI administration function may be provided by the mediation device and may be located, operated and maintained at the Cable Operators premises by for example Cable Operator's personnel as authorised by the LEA or as decribed by national legislation.

LI Mediation: The LI Mediation function is to be provided by one or more Mediation Devices (and associated devices, for purposes of the present document "Mediation Device" may refer to one or more of these devices at the same time). This device is typically located and maintained at the Cable Operators premises, and managed by the Cable Operator through the LI Administration function.

CMS/MGC: These elements refer to the Cable Network softswitch devices. These devices are typlically located, maintained and operated at the Cable Operators premises. These devices provide signalling and control information, as well as all LI provisioning functions.

CONTENT-IAP: These elements refer to the Cable Network intercept access point. The IAP would reside on devices that carry the content of the traffic i.e. call content (CC). Such deviced as for example but not limited to, CMTS, Router, MG, etc.

7.3 Functional Description

The reference model RFC 3924 [13] is assumed as given in clause 5 with the elements of an LI Mediation Device (MD) and an LI Administrative Function located at the Cable Operators premises.

The DHCP server or DHCP wiretap must support the LI INI1b and INI2 as described by the current document.

The DHCP server or DHCP server wiretap receives over INI1b information relating to the target to be intercepted.

INI2 provides DHCP information, which in turn will enable the Mediation Device to activate the interception of the Communications Content at the appropriate network elements.

The following are functionalities of a MD:

- LI Administration function: LI administration typically might be performed by authorized Cable Operator staff, typically based on applicable warrants received from the LEA(s) or as prescribed by National Legislation.

- LI provisioning (Provisioning Function): IRI provisioning over INI1b must be implemented by the MD through the secure interface to each Provisioning Function.

- LI provisioning (network): CCC provisioning will be done by the MD. The MD acts on information received over INI2 i.e. IRI. If specified by LEA the MD shall invoke its SBCF to configure the IAP at the CMTS to copy the CC.

- IRI IAP (Provisioning Function): The DHCP server or DHCP server wiretap intercepts DHCP messages, this data will be provided to the MD according to INI2, then mediated into the appropriate HI-2 messages by the MD and delivered to LEMF.
- Content IAP (CMTS): All IP data will be intercepted by the IAP at the CMTS. The Content IAP will duplicate the required data to MD without disturbing the normal traffic flow from target to destination and vice versa.
- Timestamp: Where the LEA requires identify the time at which the corresponding information was detected by the MD, a timestamp of call content datagrams delivered between the MD and LEMF shall be supported by the MD.

7.3.1 LI Process: Interception of provisioning messaging

The functional model for interception of provisioning messaging is given by figure 4.

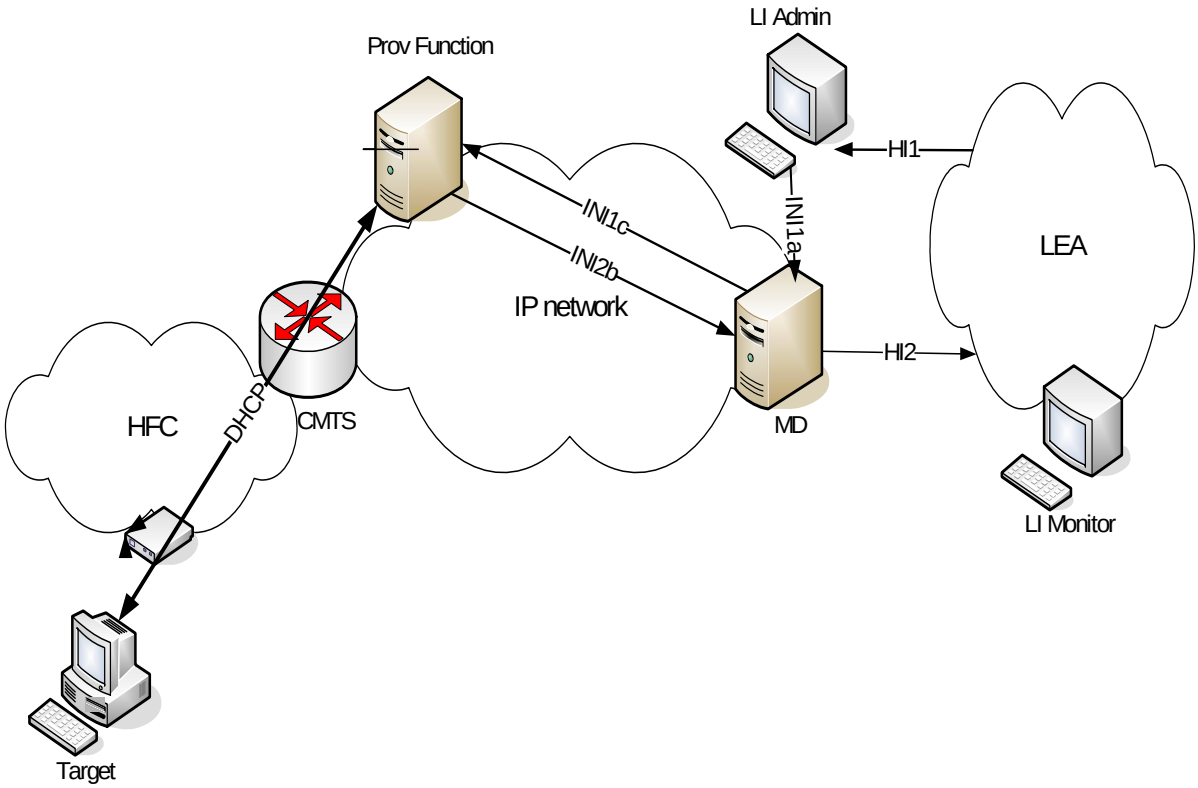


Figure 4: Interception of Provisioning messaging

All signalling will be intercepted at the DHCP server or DHCP server wiretap, concentrated and delivered by MD as given by figure 4.

Interception would take place according to the following sequence.

1) LI warrant is provided by LEA to Cable Operator.
2) The Cable Operator provisions interception on the Mediation Device.
3) Mediation Device provisions DHCP server or DHCP server wiretap intercept all events in relation to the target of interception.
4) No interception is done until target registers activity.
5) Signaling activity takes place via the IP nework.
6) All signaling is captured by the DHCP server or DHCP server wiretap.
7) DHCP server or DHCP server wiretap delivers event records to Mediation Device.
8) Mediation Device delivers HI-2 records to LEMF.

Sequence diagram

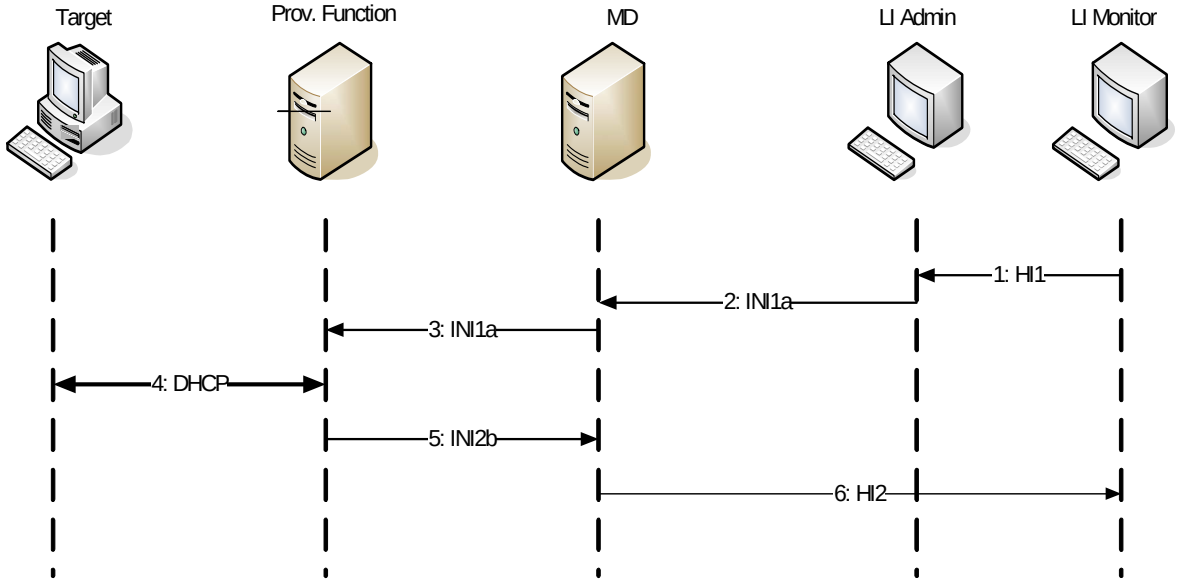


Figure 5: Sequence diagram for IRI for data intercept

Figure 5 shows the process for the interception of IRI for data. The following steps are done:

1) Cable operatore staff receives a warrant over HI1.
2) LI admin provisions Mediation Devices over INI1a (internal interface).
3) MD provisions DHCP-server or DHCP-server wiretap with information on which MAC-address (cable modem) that needs to be tapped. Additionally information is provided on excluded MAC-address for that cable modem.
4) Computer behind cable modem performs DHCP to acquire an IP-address.
5) DHCP-server or DHCP-server wiretap inform MD about activity of device behind computer.
6) DHCP-information on target is forwarded over HI2 to LI facilities of LEA.

7.3.2 LI Process: interception of IP data

The functional model for interception of IP data is given by figure 6.

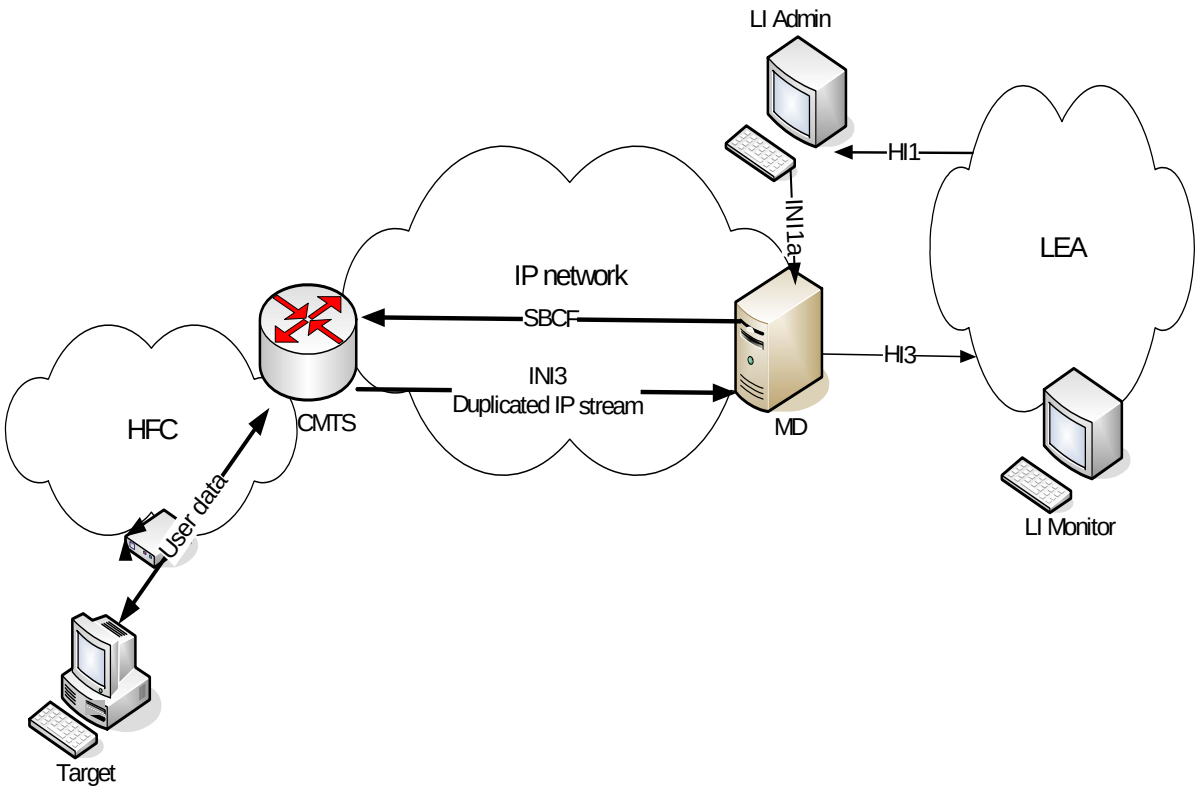


Figure 6: Interception of IP data

Interception shall be at the the IAP of the CMTS as given by figure 6. Call content traffic to and from the interception target will duplicated at the IAP of CMTS and sent to the Mediation Device, where it will be delivered to LEMF.

The interception shall be according to the sequence described below:

1) LI warrant is provided by LEA to Cable Operator.
2) The Cable operator provisions interception on the Mediation Device.
3) Mediation Device provisions DHCP server or DHCP server wiretap to intercept DHCP events in relation to the target of interception.
4) No interception is done until target registers activity.
5) Interception target has DHCP activity initiated via IP.
6) DHCP server or DHCP server wiretap delivers INI-2b to MD, triggering the content tap.
7) MD sets up interception of content via its SBCF on the IAP of CMTS.
8) IAP of CMTS duplicates IP data content and sends duplicated Content to Mediation Device.
9) Mediation Device delivers HI-2 and HI-3 to the LEMF.
10) DHCP server or DHCP server wiretap detects target disconnects (DHCP release).
11) MD removes TAP on CMTS for target.

Sequence diagram

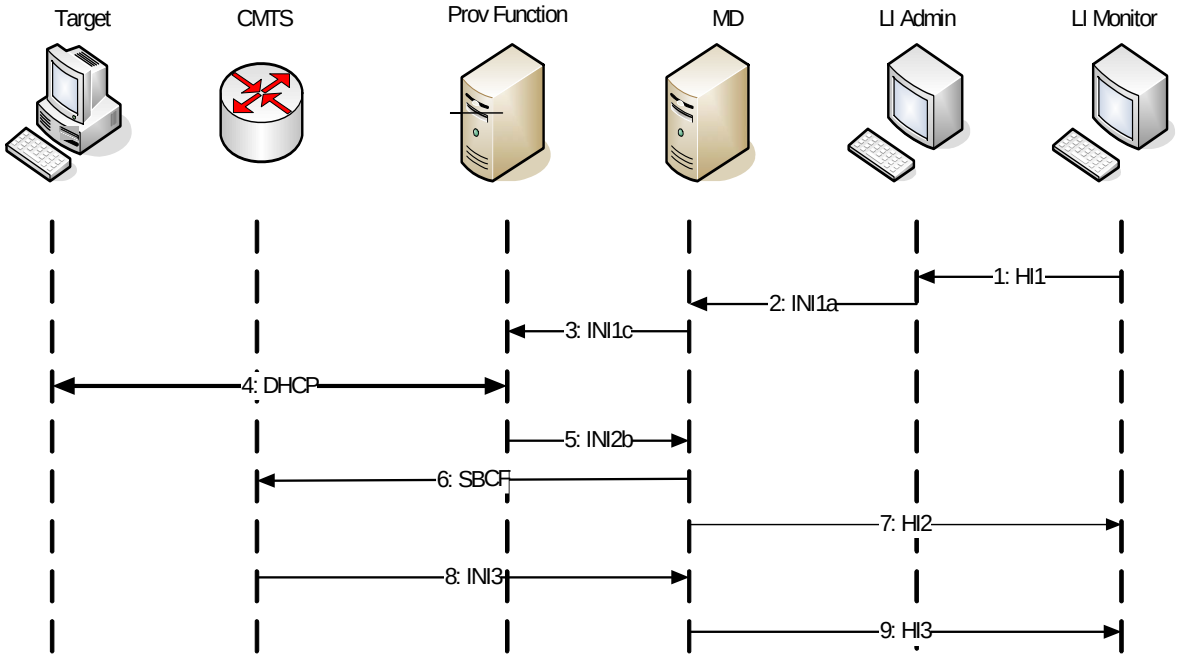


Figure 7: Sequence diagram for tapping of content for data

Figure 7 show the process for the interception of CCC for data. The following steps are done:

1) Cable operatore staff receives a warrant over HI1.

2) LI admin provisions Mediation Devices over INI1a (internal interface).

3) MD provisions DHCP-server or DHCP-server wiretap with information on which MAC-address (cable modem) that needs to be tapped. Additionally information is provided on excluded MAC-address for that cable modem.

4) Computer behind cable modem performs DHCP to acquire an IP-address.

5) DHCP-server or DHCP-server wiretap inform MD about activity of device behind computer.

6) MD provisions over SBCF taps on CMTS of target.

NOTE: Order of 6 and 7 can be interchanged.

7) DHCP-information on target is forwarded over HI2 to LI facilities of LEA.

8) CMTS forwards all IP-packets based on installed criteria in step 6 to MD over INI3.

9) MD forwards received IP-packets to LEA over HI3.

7 Security

The SNMP3 (VACM and USM MIBs) configuration must be such that only authorised personal can modify and view the MIBs used for LI.

Security requirements for LI are given by TR 102 661 [i.1].

Annex A (informative): Requirements listed in Council Resolution of 17 January 1995

The following requirements for Telecommunications Network operators to provide assistance to Law Enforcement agencies in the Member States are listed in the European Council Resolution of 17 January 1995 [1] and are included here for information.

Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that are generated to process the call.

Law enforcement agencies require access to all interception subjects operating temporarily or permanently within a telecommunications system.

Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications services or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

Law enforcement agencies require access to call associated data such as:

- signalling of access ready status;
- called party number for outgoing connections even if there is no successful connection established;
- calling party number for incoming connections even if there is no successful connection established;
- all signals emitted by the target, including post-connection dialled signals emitted to activate features such as conference calling and call transfer;
- beginning, end and duration of the connection;
- actual destination and intermediate directory numbers if call has been diverted.

Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

Law enforcement agencies require data on the specific services used by the interception subject and the technical parameters for those types of communication.

Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

Law enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries.

Law enforcement agencies require network operators/service providers to provide call associated data and Call Content from the target service in a way that allows for the accurate correlation of call associated data with Call Content.

Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format. This format will be agreed upon on an individual country basis.

If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications *en clair*.

Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable security requirements.

Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfil the interception order. In particular, the operation of the target service should appear unchanged to the interception subject.

Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

According to national regulations, network operators and service providers could be obliged to maintain an adequately protected record of the activation of interceptions.

Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require:

1) the interception subject's identity, service number or other distinctive identifier;

2) information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers; and

3) information on the technical parameters of the transmission to the law enforcement monitoring facility.

During the interception, law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service. The type of information and/or assistance required will vary according to the accepted practices in individual countries.

Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations. The maximum number of simultaneous interceptions for a given subscriber population will be in accordance with national requirements.

Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by country and by the type of target service to be intercepted.

For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

History

Document history		
V1.1.1	November 2009	Publication