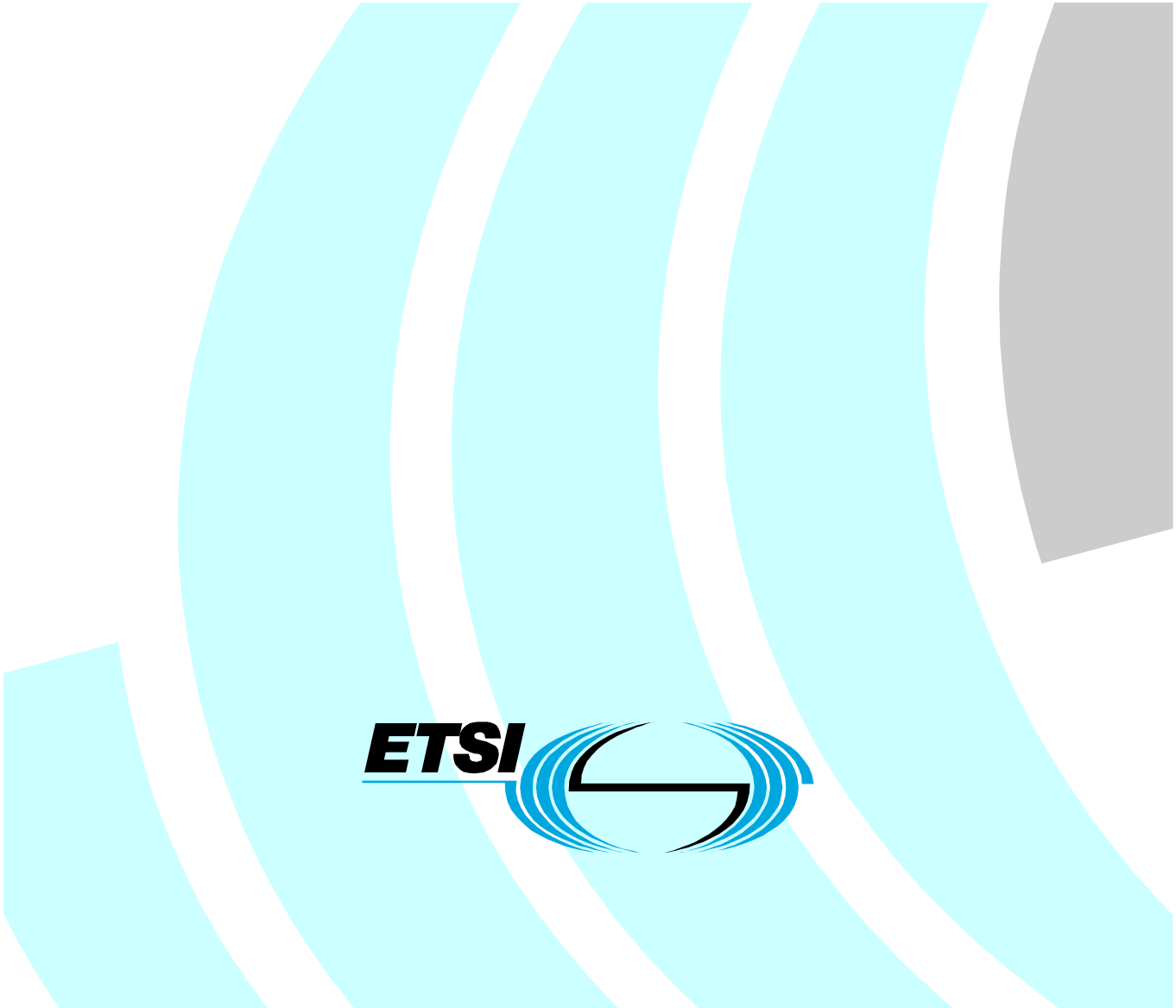
ETSI TS 102 815 V1.1.1 (2005-09)

Technical Specification

Lawful Interception (LI);
Service-specific details for Layer 2 Lawful Interception



Reference
DTS/LI-00017

Keywords
layer 2, Lawful Interception, IP, security

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2005.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

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 Lawful Interception (LI).

Introduction

The present document focuses on layer 2 interception of IP-encoded information. It is to be used in conjunction with TS 102 232 [2], in which the handling of the intercepted information is described.

1 Scope

The present document specifies lawful interception for an Access Provider that has access to layer 2 session information and that is not required to have layer 3 information. In this case, the focus of lawful interception for IP Network Access is on the portion of the network, commonly referred to as "layer 2 interception", that facilitates subscriber access to the Public IP network.

The present document describes the LI at the interception domain of the access network.

The specification contains:

- a stage 1 description of the lawful interception service;
- a stage 2 description of the information flows between the functional entities (including the information elements involved) and triggering events; and
- a stage 3 description of the protocol and procedures to be used in mapping from stage 2 information flows and elements to Intercept Related Information (IRI) and Content of Communication (CC).

The present document is consistent with the definition of the Handover Interface, as described in TS 102 232 [2].

NOTE 1: Layer 3 interception is described in TS 102 234 [11].

NOTE 2: Layer 2 interception is not applicable to the PS domain of the GSM/UMTS networks (3GPP TS 23.060 [14]).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

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

[2] ETSI TS 102 232: "Lawful Interception (LI); Handover Specification for IP Delivery".

[3] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[4] IETF RFC 1570: "PPP LCP Extensions".

[5] IETF RFC 3046: "DHCP Relay Agent Information Option".

[6] ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[7] IETF RFC 2341: "Cisco Layer Two Forwarding (Protocol) (L2F)".

[8] IETF RFC 2637: "Point-to-Point Tunneling Protocol (PPTP)".

[9] IETF RFC 2661: "Layer Two Tunneling Protocol (L2TP)".

[10] IETF RFC 1661: "The Point To Point Protocol (PPP)".

[11] ETSI TS 102 234: "Lawful Interception (LI); Service-specific details for internet access services".

[12] ETSI TS 102 233: "Lawful Interception (LI); Service-specific details for E-mail services".

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

[14] ETSI TS 123 060: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS) Service description; Stage 2 (3GPP TS 23.060)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 232 [2], TS 102 234 [11] and the following apply:

access provider: Communication Service Provider (CSP), providing access to networks. APs generally provide dial-up access through a modem and PPP connection, though companies that offer Internet access with other devices, such as cable modems or wireless connections, could also be considered APs

NOTE: In the context of the present document, the network access is defined as IP-based network access to the Internet.

access service: set of access methods provided to a user to access a service and/or a supplementary service

NOTE: In the context of the present document, the service to be accessed is defined as the Internet.

application service provider: third-party entity that manages and distributes software-based services and solutions to customers across a wide area network from a central data center

NOTE: In the context of the present document, a company that offers services that are accessible to users who have connectivity via the Internet.

interconnect network: network connecting the AP and the IAP, across which the layer 2 tunnel is established

internet access provider: company that provides access to the Internet

NOTE: The IAP provides subscribers a username, password and an IP address that enables subscribers to log onto the Internet for virtual connectivity to Application Service Providers.

layer 2: link layer, as defined in RFC 1122 [3]

layer 2 interception: lawful interception using technology that can access layer 2 information

physical line termination point: point in the access provider's infrastructure where the physical line to the customer is terminated

EXAMPLE: E.g. xDSL-line termination point, Cable-line termination point, Ethernet-line termination point).

tunnel router: router that is an endpoint of a layer 2 tunnel; there are at least two tunnel routers for each layer 2 tunnel

3.2 Abbreviations

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

AAA	Authentication, Authorization and Accounting
AP	Access Provider
ASN.1	Abstract Syntax Notation 1
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode

CC	Content of Communication
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CSP	Communications Service Provider
DF	Delivery Function
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
IAP	Internet Access Provider
IAS	Internet Access Service
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAES	Lawful Authorized Electronic Surveillance
LCP	Link Control Protocol
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAC	Media Access Control
NAS	Network Access Server
PLTP	Physical Line Termination Point
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial In User Service
VoIP	Voice over Internet Protocol

4 General

4.1 Access Network

An access network provides layer 2 connectivity from the Physical Line Termination Point (PLTP) for end-users to an Application Service Provider (ASP) through an Internet Access Provider (IAP). The access provided may be via a telephone-, cable-, or wireless-network. The present document describes the LI at the access network.

The figures contained in the following clauses do not necessarily refer to physical configurations but identify the business roles associated with various scenarios to provide services. A provider can have one or more of following roles: Access Provider, Internet Access Provider and Application Provider.

Lawful interception of communications must accommodate a multitude of scenarios for public telecommunications. Four representative scenarios are described below.

4.1.1 Scenario 1

This scenario reflects the situation in which the three identified provider roles are provisioned by independent providers.

For example, an ASP provides Call Control for VoIP service, and is using the transport facilities of an IAP for connectivity to the AP.

In this scenario, the specifications of the present document are relevant to the AP, while the IAP and ASP may be involved with interception according to the specifications of TS 102 233 [12] and TS 102 234 [11].

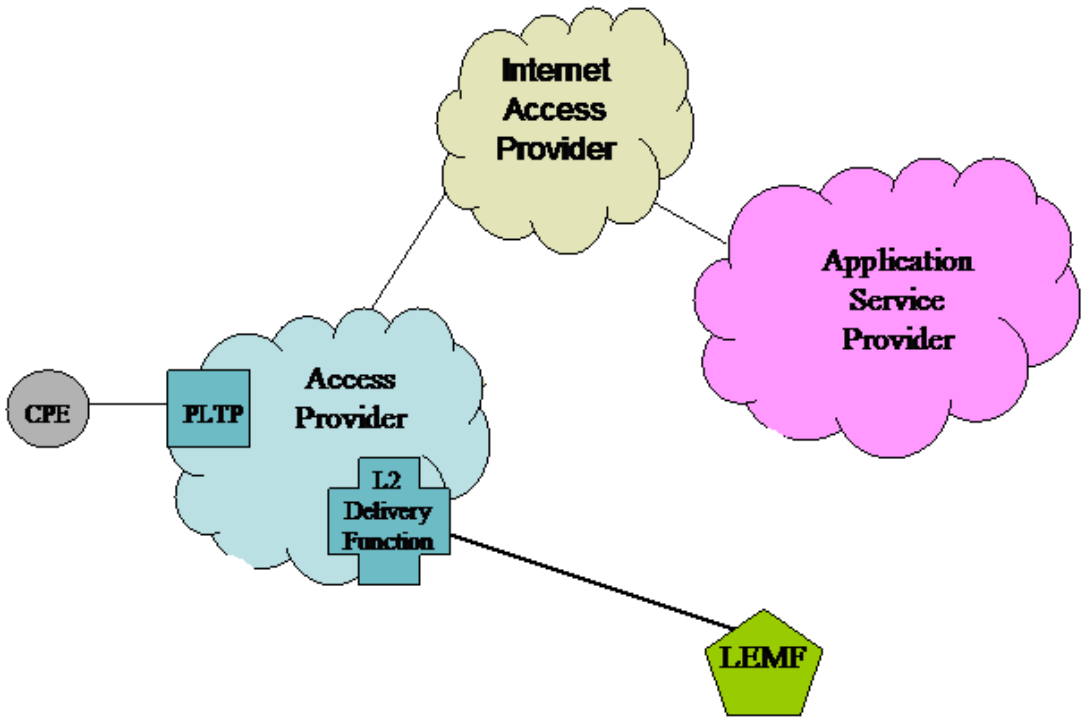


Figure 1: Scenario in which access, transport and application services are offered by three different providers

4.1.2 Scenario 2

This scenario reflects the situation in which a network operator is acting only as an AP, and not as an IAP or ASP.

In this scenario, the specifications of the present document are relevant to the AP, while the IAP / ASP may be involved with interception according to the specifications of TS 102 233 [12] and TS 102 234 [11].

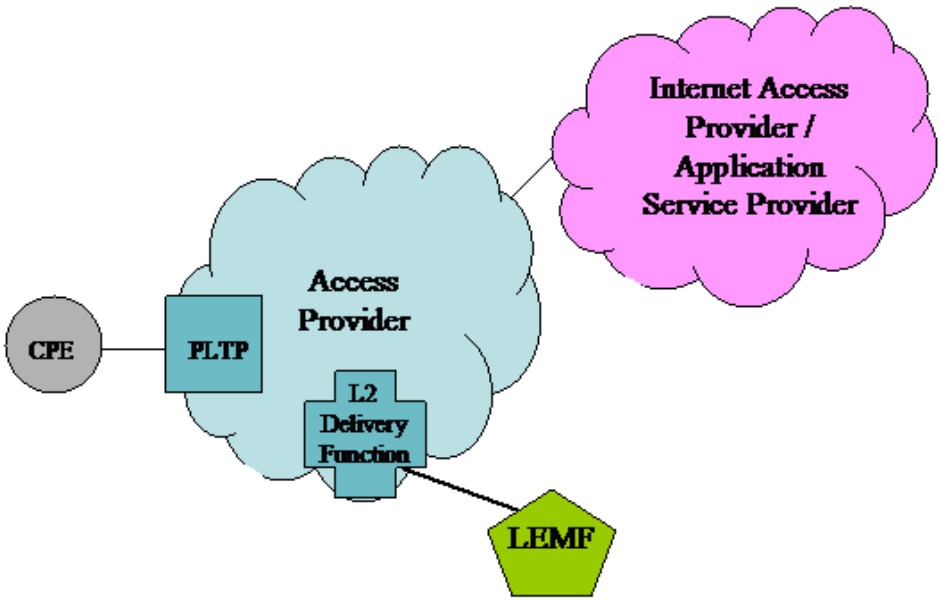


Figure 2: Scenario in which access is offered by a provider separate from the one that is offering Internet transport and application service

4.1.3 Scenario 3

This scenario reflects the situation in which the AP and IAP roles are offered by a single provider.

In this scenario the Service Provider, having roles as an AP and an IAP, may be involved with interception according to TS 102 234 [11] and layer 2 interception is not preferred.

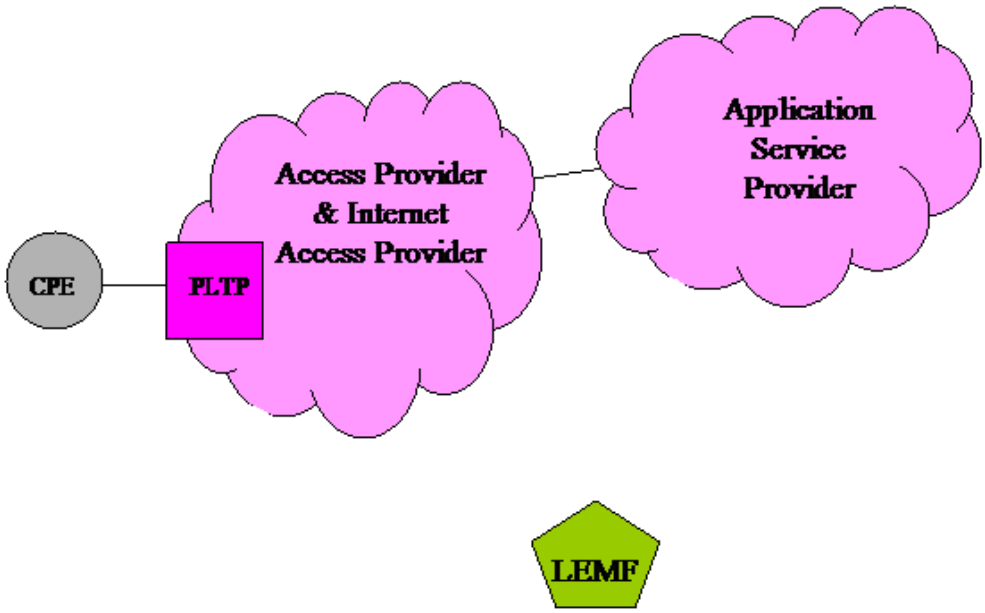


Figure 3: Scenario in which access and Internet transport are offered by a single provider that does not offer application service

4.1.4 Scenario 4

This scenario reflects the situation in which the AP, IAP and ASP roles are offered by a single provider.

In this scenario the Service Provider, having roles as an AP, an IAP and an ASP, may be involved with interception according to TS 102 233 [12] and TS 102 234 [11], and layer 2 interception is not preferred.

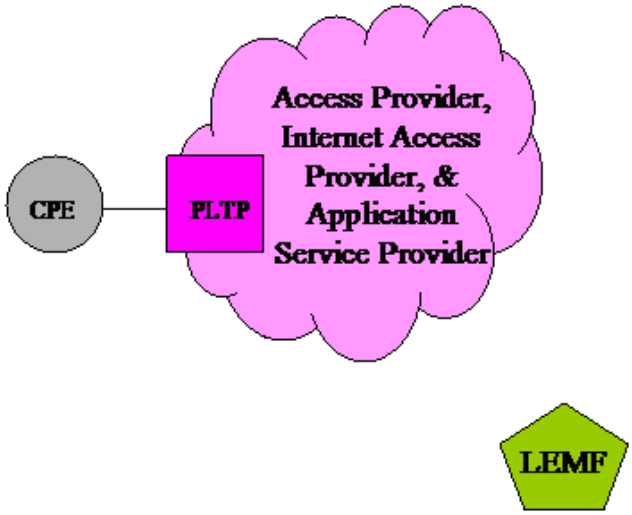


Figure 4: Scenario in which access, transport and application services are offered by the same provider

4.2 Lawful Interception requirements

This clause lists the requirements for Lawful Interception. These requirements are derived from higher-level requirements listed in TS 101 331 [13] and TS 102 232 [2] and are specific to Internet Access Services. These requirements focus on both the administrative part of Internet Access for delivery over HI2 as well as capturing traffic for delivery over HI3.

4.2.1 Target identity

Where the special properties of a given service, and the justified requirements of the LEAs, necessitate the use of various identifying characteristics for determination of the traffic to be intercepted, the provider (CSP) shall ensure that the traffic can be intercepted on the basis of these characteristics. The target identity known by the layer 2 mechanisms is not an application or network identity; therefore, layer 2 interception must be registered against a known layer 2 identity. The access network shall identify targeted activity by other means, e.g., the termination point of the xDSL-line or the Cable-line.

In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear determination of the traffic to be intercepted.

The target identity should uniquely identify the target in the provider's network. The target identity will be dependant on the access mechanism used and the parameters available with the AP. The target identity could be based on:

a) MAC address or vMAC. For example, the MAC address of the cable modem which is identified by the CMTS can be requested to identify the target identity;

b) xDSL-line termination point, including, e.g., the IP- address of the Network Access Server (NAS), and the NAS port; the NAS port is identified by the ATM virtual path, virtual channel and port number (slot, sub-slot and port) ;

c) Cable-line termination point (including e.g. IP address, interface information of the CMTS);

d) DHCP option 82, line Id and remote Id, as defined in IETF RFC 3046 [5];

e) Calling party number (E.164, Network-provided or User-provided, verified and passed);

f) Other unique identifier agreed between AP and LEA.

4.2.2 Result of interception

The network operator shall provide Intercept Related Information (IRI), in relation to each target service:

a) when an attempt is made by the target to utilize the network;

b) when an attempt is made to reach the target from the network;

c) when an access to the network is permitted;

d) when an access to the network is not permitted;

e) when an access to the network is terminated.

The IRI shall contain:

a) identities used by or associated with the target identity;

b) details of services used and their associated parameters;

c) information relating to status;

d) timestamps.

Content of Communication (CC) shall be provided for every layer 2 datagram sent through the access network that is addressed to, or sent from, the line termination point of the target.

The Content of communication (CC) shall be a bit-exact copy of every intercepted layer 2 datagram.

4.2.3 Intercept related information messages

Intercept Related Information shall be conveyed to the LEMF in IRI data records. Four types of IRI data records are defined:

1) IRI-BEGIN record at the first event of a communication attempt, opening the IRI transaction;

2) IRI-END record at the end of a communication attempt, closing the IRI transaction;

3) IRI-CONTINUE record at any time during a communication attempt within the IRI transaction;

4) IRI-REPORT record used in general for non-communication related events.

For a description of the use and purpose of the various IRI data records refer to TS 102 232[2]. Which IRI events are available for the different IRI data record types is described in clause 6.1 IRI events.

4.2.4 Time constraints

Intercept Related Information shall be transmitted without undue delay. This delay should only be caused by the access protocol handling and the automated forwarding of this information to the delivery function.

5 System model

5.1 Reference configuration

Figure 5 contains the reference configuration for the lawful interception.

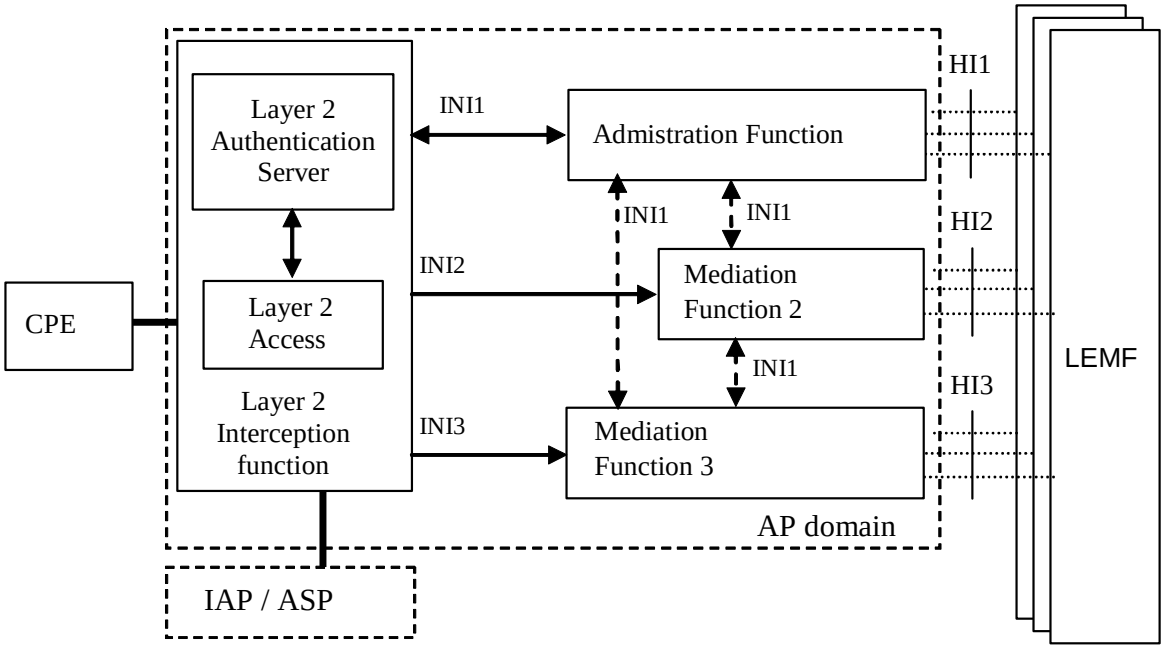


Figure 5: Reference configuration for lawful interception

The reference configuration is only a logical representation of the entities involved in lawful interception and does not mandate separate physical entities. This allows for higher levels of integration.

The messages sent in an implementation-specific manner between the Administrative Function and the other Access Provider domain entities may contain:

- target identities;
- correlation information;
- information whether the Content of Communication (CC) shall be provided;
- the address of Mediation Function 2 for IRI;
- the address of Mediation Function 3 for the intercepted CC;
- the address for delivery of IRI (= LEMF address);
- the address of delivery for CC (= LEMF address);
- Lawful Interception Identifier (LIID).

The messages sent in an implementation-specific manner between the Interception Function and Mediation Function 2 contains the IRI.

The messages sent in an implementation-specific manner between the Interception Function and Mediation Function 3 contains the CC.

5.2 Reference states

5.2.1 Logon

If the xDSL-line or cable line is not owned by the party that provides the authentication server, then user identification takes place in the network of the AP and the user identity and access request are forwarded to the authentication server of the IAP. To exchange data between the user and IAP, a layer 2 tunnel is established, e.g. a L2TP tunnel per RFC 2661 [9]. All data between the IAP and the user is transported via this tunnel. If access is granted, an IP address is provided by the IAP and communicated to the user via the layer 2 tunnel and then the user can communicate with the Internet via the layer 2 tunnel.

If a layer 2 tunnel to an IAP is established, other users may be using the same tunnel, as only one tunnel is established typically to each IAP.

5.2.2 Data transport

While having an active, virtual IP connection, the CPE can transmit IP datagrams towards any IP-enabled destination connected to the Internet. These datagrams may contain other, higher-level IP- based protocols. Similarly, the CPE can receive IP datagrams directed towards it from any IP-enabled source connected to the Internet.

It is possible that the CPE is connected to an Access Network that does not provide the Internet Access, e.g. if the AP and the IAP are different parties as demonstrated in clauses 4.1.1 and 4.1.2. The AP provides the xDSL-line and routes all datagrams that are destined to the IAP through a layer 2 tunnel via a gateway to the network of the IAP. Thus, all datagrams from the user CPE are encapsulated in a specific layer 2 protocol (e.g. L2TP RFC 2661 [9]) and transmitted by the AP to the IAP.

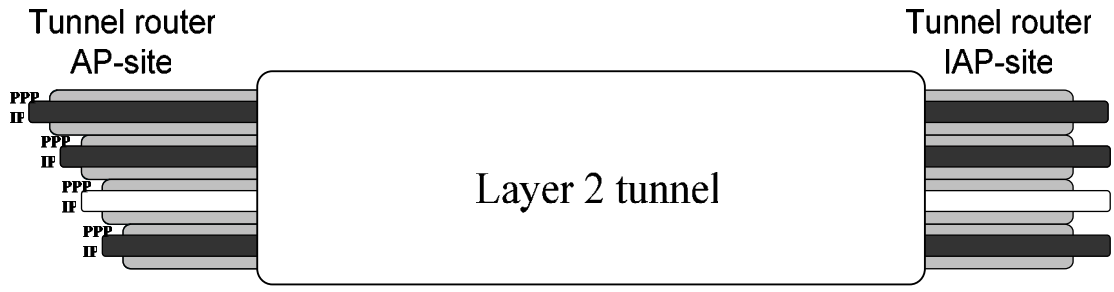


Figure 6: Layer 2 tunnel shared by multiple users

Figure 6 shows the usage of a layer 2 tunnel. It is possible that only the traffic associated with one PLTP connected to the CPE of one target is intercepted, as represented by the white IP-stream in figure 6. The other connections through the tunnel are not intercepted. If the target session is terminated and the other connections are not terminated, the layer 2 tunnel stays online.

It is also possible that the communication of more than one target may be intercepted via the same layer 2 tunnel. Furthermore, it is possible that a single IP-stream may be the subject of multiple, simultaneous lawful interceptions; therefore, that single, intercepted IP-stream may be delivered to multiple LEMFs, or multiple copies of the stream may have to be delivered to the same LEMF (once for each interception authorization).

5.2.3 Logoff

When a user logs off, the client running on the CPE will negotiate the closure of the session with the NAS of the AP. For example, a PPP session may be closed through an exchange of LCP Terminate packets (see RFC 1570 [4] for LCP and RFC 1661 [10] for PPP). Next, the NAS informs the authentication server in the IAP of the session closure and may provide statistics on the session as well.

5.2.4 Unexpected connection loss

During an active data session, the virtual connection may terminate unexpectedly for reasons such as loss of carrier, link quality failure, or the expiration of an idle-period timer. In such cases there can be no user-provided logoff indication, and it is up to the NAS to detect the connection loss and to propagate the session closure towards the accounting server of the IAP.

6 Intercept Related Information

6.1 IRI events

The following IRI-Events are applicable, if the traffic to and from the target is through the network of the AP.

Table 1: IRI events (Layer 2)

IRI Event	Description	IRI Record
Access_attempt	A target requests access to the Internet Access Service (IAS).	REPORT
Access_accept	The network elements are triggered to erect a layer 2 tunnel between the user and the foreign IAP network.	REPORT
Access_reject	The access is refused.	REPORT
Session_start	The target can use the connection to the IAP network, as a layer 2 tunnel and a corresponding session within this tunnel are available.	BEGIN
Session_end	The communication between the user and the IAP network terminated. This may be for numerous reasons that are not visible to the AP (e.g. the user logs off or shortage of network capacity between the AP and the IAP) (see note).	END
Start of Interception Session Active	As sessions can be active over longer periods, it is not unlikely for an intercept to start after a user session has started already. Available information about the status of this session is sent to the LEA.	BEGIN
End of Interception Session_Active	As sessions can be active over longer periods, it is not unlikely for an intercept to end before a user session ends. Available information about the status of this session is sent to the LEA.	END
NOTE: If there are other connections still using the same tunnel, the tunnel remains available.		

6.2 HI2 attributes

The attributes of IRI information for layer 2 interception is dependent upon the type of access technology utilized. Annex A defines for each technology that is relevant to the present document in which of the IRI messages a parameter value must be provided.

7 Content of Communication

Communication Content (CC) is provided for every layer 2 datagram sent through the AP's network that is addressed to, or sent from, the line termination point of the target.

The CC payload contains a copy of the intercepted layer 2 datagram.

NOTE: The ASN.1 definition for CC is presented as the L2CC PDU in clause 8.

8 ASN.1 for IRI and CC

8.1 ASN.1 syntax tree for HI2 and HI3 headers

Figure 7 shows the object identifier tree from the point of view of packet-switched lawful interception.

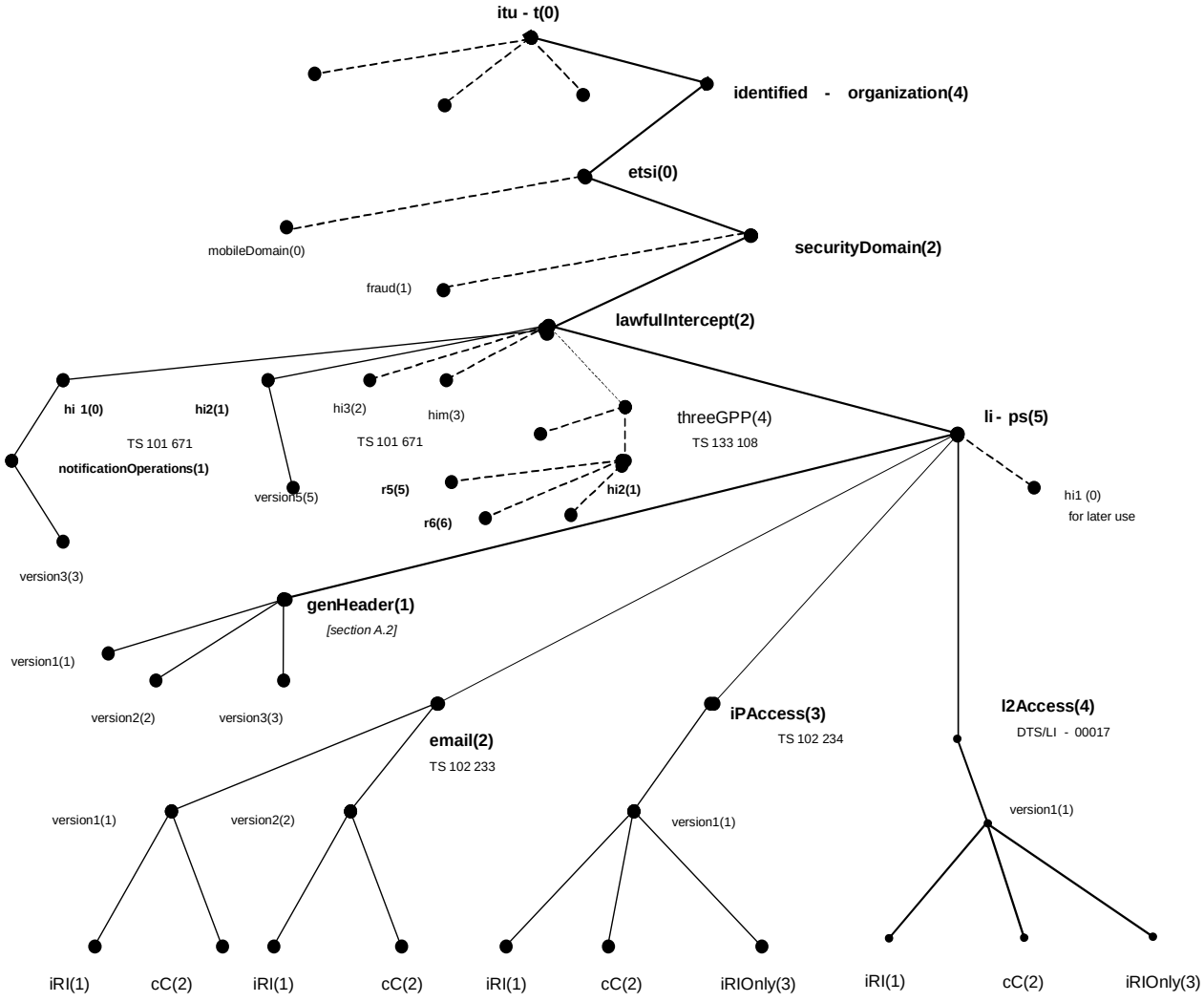


Figure 7: Object identifier tree

8.2 ASN.1 specification

The ASN.1 (ITU-T Recommendation X.680 [6]) module that represents the information in the present document and meets all stated requirements is shown below:

```
L2AccessPDU {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
li-ps(5) l2Access(4) version1(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
   IPAddress
      FROM HI2Operations
      {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version7(7)};
      -- from ETSI HI2Operations TS 101 671 [1]

--============================
-- Object Identifier Definition
--============================

l2IRIObjId RELATIVE-OID            ::= {li-ps(5) l2Access(4)v1(1) iRI(1)}
l2CCObjId RELATIVE-OID             ::= {li-ps(5) l2Access(4)v1(1) cC(2)}
l2IRIOnlyObjId RELATIVE-OID        ::= {li-ps(5) l2Access(4)v1(1) iRIOnly(3)}
   -- all three definitions relative to {itu-t(0) identified-organization(4)
   -- etsi(0) securityDomain(2) lawfulintercept(2)}

--============================
-- L2 Communications Contents
--============================

L2CC     ::= SEQUENCE
{
   l2CCObjId            [0] RELATIVE-OID,
   l2CCContents         [1] CHOICE
      {
      l2TP         [1] OCTET STRING,
      l2F          [2] OCTET STRING,
      pPTP         [3] OCTET STRING,
      pPP          [4] OCTET STRING,
      ethernet     [5] OCTET STRING,
      ...
      }
}

--====================================================
-- Intercept-related information for general L2-Access
--====================================================

L2IRI       ::= SEQUENCE
{
   l2IRIObjId        [0] RELATIVE-OID,
   l2IRIContents     [1] L2IRIContents,
   ...
}
```

```
L2IRIContents        ::= SEQUENCE
{
   accessEventType         [0] AccessEventType,
   internetAccessType      [2] InternetAccessType OPTIONAL,
   targetNetworkID         [5] UTF8String (SIZE (1..20)) OPTIONAL,
      -- Target network ID (e.g. MAC address, PSTN number)
   targetCPEID             [6] UTF8String (SIZE (1..128)) OPTIONAL,
      -- CPEID (e.g. Relay Agent info, computer name)
   targetLocation          [7] UTF8String (SIZE (1..64))OPTIONAL,
      -- <for further study>
   nASPortNumber           [8] INTEGER (0..4294967295) OPTIONAL,
      -- The NAS port number used by the target
   callBackNumber          [9] UTF8String (SIZE (1..20)) OPTIONAL,
      -- The number used to call-back the target
   startTime               [10] GeneralizedTime OPTIONAL,
      -- The start date-time of the session or lease
   endTime                 [11] GeneralizedTime OPTIONAL,
         -- The end date-time of the session or lease
   endReason               [12] EndReason OPTIONAL,
      -- The reason for the session to end
   octetsReceived          [13]  INTEGER (0..18446744073709551615) OPTIONAL,
      -- The number of octets the target received
   octetsTransmitted       [14]  INTEGER (0..18446744073709551615) OPTIONAL,
      -- The number of octets the target transmitted
   rawAAAData              [15]  OCTET STRING OPTIONAL
      -- Content of the raw AAA record
}
```

```
AccessEventType         ::= ENUMERATED
{
   accessAttempt(0),
      -- A target requests access to the IAS
   accessAccept(1),
       -- IAS access is granted to the target
   accessReject(2),
      -- IAS access is refused to the target
   accessFailed(3),
      -- The Access_attempt timed-out or failed otherwise
   sessionStart(4),
      -- A target starts using the IAS
   sessionEnd(5),
      -- A target stops using the IAS
   interimUpdate(6),
      -- Intermediate status report on service status or usage
   unknown(7),
   ...
}
```

```
InternetAccessType      ::= ENUMERATED
{
   undefined(0),
   dialUp(1),
      -- IAS via DialUp access
   xDSL(2),
      -- IAS via DSL access
   cableModem(3),
      -- IAS via Cable access
   lAN(4),
      -- IAS via LAN access
   ...
}
```

```
EndReason         ::= ENUMERATED
{
   undefined(0),
   regularLogoff(1),
      -- The target logged off
   connectionLoss(2),
      -- The connection was lost
   connectionTimeout(3),
      -- The connection timed-out
   leaseExpired(4),
      -- The DHCP lease expired
   ...
}
```

```
--=====================================================
-- Intercept-related information for IRI-Only intercepts
--=====================================================

L2IRIOnly      ::= SEQUENCE
{
   l2IRIOnlyObjId            [0] RELATIVE-OID,
   l2protocolInformation     [2] L2ProtocolInformation,
   l2AggregatedNbrOfPackets  [3] INTEGER OPTIONAL,
   l2AggregatedNbrOfBytes    [4] INTEGER OPTIONAL,
   ...
}

L2ProtocolInformation      ::= ENUMERATED
{
   l2ProtocolL2tp(1),
      -- The L2TP protocol is used
   l2ProtocolL2f(2),
      -- The L2F protocol is used
   l2ProtocolPptp(3),
      -- The PPTP protcol is used
   l2ProtocolPpp(4),
      -- The PPP protocol is used
   ethernetProtocol(5),
      -- The ethernet protocol is used
   undefined(6),
   ...
}

END -- end of L2 Access
```

Annex A (normative): Reference network topologies

There are different possible network topologies, dependent upon the means of network access:

a) xDSL access

b) Cable modem access

c) WLAN access

A.1 xDSL access

Internet Access over the local loop by means of using specialized equipment for achieving a high bandwidth over copper wire is commonly referred to as xDSL Access. There is great variety of possible architectures and technologies that can be applied for realizing an xDSL network. Therefore, figure A.1 only shows the principal equipment involved in this kind of Internet Access.

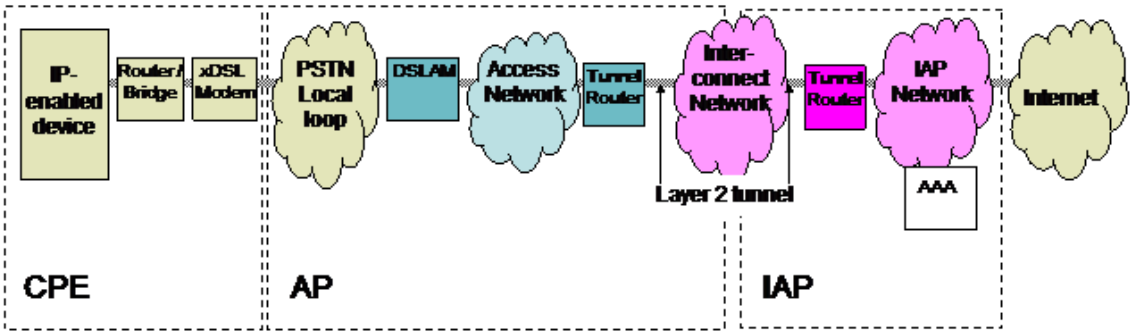


Figure A.1: Example of xDSL access

In some cases, the services of an AP and IAP are offered by a single company and the PPP session of a user is terminated in a gateway to the Internet. In this case, the intercepted data may be provided from layer 3, as specified in TS 102 234 [11].

In other cases, the services of an AP and IAP are split between different companies. The datagrams of the tunnel routers are collected by a NAS that belongs to the AP. These datagrams are tunnelled through the network using a specific tunnelling protocol (e.g. RFC 2341 L2F [7], RFC 2661 L2TP [9], RFC 2637 PPTP [8]) to another tunnel router that is operated by the IAP. This second router represents the termination point of the user's PPP session and initiates authentication and authorization, e.g. through the AAA on the IAP's RADIUS-Server. Thus, on the AP side, only layer 2 information is available.

A.1.1 Events and information

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawfully Authorized Electronic Surveillance (LAES). The information is described as records and the parameters carried by a record. This focus is on describing the information being transferred to the LEMF.

The value in the Mandatory / Optional / Conditional (MOC) column in the following tables indicates whether inclusion of the indicated parameter in the indicated record is Mandatory (M), Optional (O), or Conditional (C).

Each record described in this clause consists of a set of parameters. Each parameter is either:

- A *Mandatory (M)* value means that the sender of the message shall always include this parameter in the message.
- An *Optional (O)* value means that the sender of the message may include this parameter in the message at the discretion of the implementation.
- A *Conditional (C)* value means that the sender of the message shall include this parameter in the message when the conditions specified in the Description/Conditions column are met.

Table A.1: Access_attempt REPORT Record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access); to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider	callBackNumber
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

Table A.2: Access_accept REPORT Record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access); to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider	callBackNumber
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

Table A.3: Access_reject REPORT Record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access) ; to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider	callBackNumber
endReason	M	The reason for the session to end (e.g. logoff, connection loss, time out, lease expiration); to be included if accessible by the provider	endReason
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

Table A.4: Session_start BEGIN record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access); to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider	callBackNumber
startTime	M	The date & time of the start of the session (or lease)	startTime
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

Table A.5: Session_end END record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access); to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider; to be included if accessible by the provider	callBackNumber
endTime	M	The date & time of the end of the session (or lease)	endTime
endReason	C	The reason for the session to end (e.g. logoff, connection loss, time out, lease expiration); to be included if accessible by the provider	endReason
octetsReceived	C	The number of octets the target received during the session; to be included if accessible by the provider	octetsReceived
octetsTransmitted	C	The number of octets the target sent during the session; to be included if accessible by the provider	octetsTransmitted
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

Table A.6: Start of Interception Session Active BEGIN record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access); to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider	callBackNumber
startTime	C	The date & time of the start of the session (or lease); to be included if accessible by the provider	startTime
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

Table A.7: End of Interception Session_Active END record

Attribute	MOC	Description/Conditions	HI2 ASN.1 parameter
EventType	M	Type of IRI event (e.g. Access_attempt, Access_failed, Session_start, etc.)	accessEventType
AccessType	C	The type of internet access (e.g. Ethernet, ADSL, Cable Modem, LAN Access); to be included if accessible by the provider	internetAccessType
targetNetworkID	C	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up; to be included if accessible by the provider	targetNetworkID
targetCPEID	C	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.); to be included if accessible by the provider	targetCPEID
targetLocation	C	Location information (to be defined); to be included if accessible by the provider	targetLocation
nASPortNumber	C	The 32-bit NAS port number the target uses for dial-up access. The content and the structure are defined by the network access provider; to be included if accessible by the provider.	nASPortNumber
callBackNumber	C	The target PSTN/ISDN number used for call-back by the NAS; to be included if accessible by the provider	callBackNumber
octetsReceived	C	The number of octets the target received during the session; to be included if accessible by the provider	octetsReceived
octetsTransmitted	C	The number of octets the target sent during the session; to be included if accessible by the provider	octetsTransmitted
rawAAAData	C	An unformatted OCTET string that may contain the raw AAA records as they were intercepted; to be included if accessible by the provider	rawAAAData

A.2 Cable modem access

The same scenarios for tunnelled sessions between the AP and the IAP, as described for xDSL access in clause A.1, could also apply for access to the internet via Cable Networks. When the AP and the IAP are two different companies, then a layer 2 tunnel could be used between them. When the target's traffic is intercepted by the AP, typically only layer 2 datagrams can be provided to the LEMF. Detailed information about interception of digital broadband cable access is provided in TS 101 909-20-1 and TS 101 909-20-2 (see bibliography).

A.3 WLAN access

Layer 2 interception in the WLAN network is for further study.

Annex B (informative): Stage 1 - RADIUS characteristics

This annex provides information on RADIUS, specific to layer 2 interception. For more general information on RADIUS interception the reader is referred to annex A of TS 102 234 [11].

B.1 Network topology

RADIUS can be deployed as one or more RADIUS servers acting on their own or in combination with a RADIUS proxy. This clause provides and overview of the use of a RADIUS proxy in a layer 2 environment.

B.1.1 RADIUS proxy

In case the Access Network provider is not the same party as the IAP, the Access Network provider will typically deploy a RADIUS proxy. This RADIUS proxy will receive the authentication and authorization request from the RADIUS client and forwards this to the actual RADIUS server. In case the AP provides its services to multiple IAP's, based on some attribute provided by the NAS, the appropriate RADIUS server of the appropriate IAP is selected. In the case of Dial-up access, for example, the PSTN number of the NAS the user has dialled can be used for this purpose.

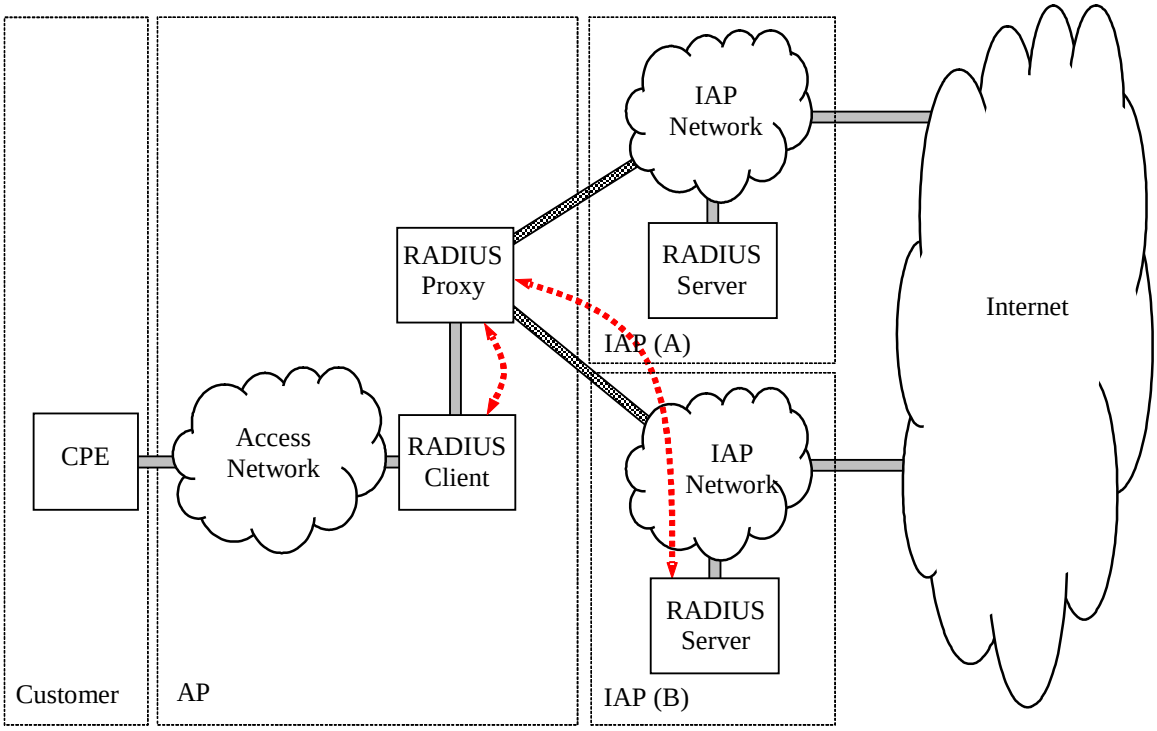


Figure B.1: RADIUS proxy

The RADIUS server will verify the password and authorization for the service against a customer database. The assignment of the IP address can be performed by either the RADIUS server or the RADIUS proxy, depending on network architecture decisions. In the latter case, the RADIUS proxy will typically assign IP addresses from ranges each belonging to a particular IAP. Alternatively, as mentioned previously, the IP address may also be assigned from the NAS operated by the AP.

Network based interception of both assignment and deassignment of IP addresses is most likely performed between the RADIUS proxy and the RADIUS server, since traffic between the RADIUS Client and the RADIUS proxy lays outside the infrastructure of the IAP. Alternatively, the RADIUS server can be extended with a function that will forward IP address assignment information to the interception function.

NOTE: Another common element used to identify the final RADIUS server or IAP is a Network Access Identifier. If the Network Access Identifier "foo@bar.com" indicates user "foo" at IAP "bar.com", the RADIUS Proxy could forward the RADIUS requests to the RADIUS server for IAP "bar.com".

If IP address assignment is done by the NAS operated by the AP, the interception of the IP address assignment and deassignment will most likely be performed between the RADIUS client and the IAP's RADIUS Accounting server.

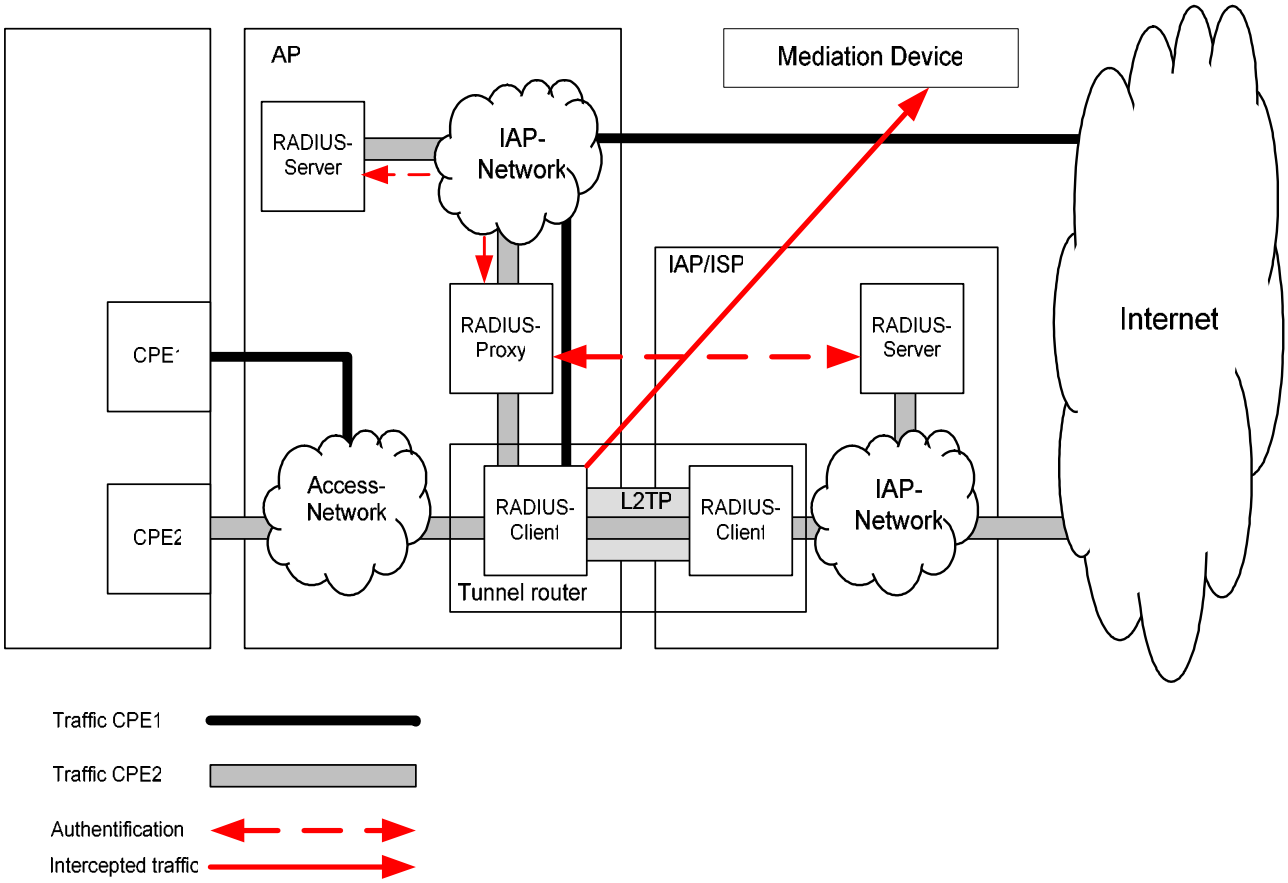


Figure B.2: RADIUS proxy, authentication for tunnelled session

Figure B.2 shows the authentication and authorization in cases where the user's session is tunnelled through the access network to the IAP network. The RADIUS proxy of the AP authenticates the user and triggers the RADIUS client (normally a NAS) to send all communication for this xDSL-line or the Cable-line through a layer 2 tunnel to the foreign IAP. All further information between the CPE and the IAP is exchanged via the layer 2 tunnel. Depending on the implementation of the RADIUS-Client, information about the beginning and end of the single user sessions may be signalled to the RADIUS-Proxy. The RADIUS-client on the AP-site, e.g. the NAS, may be used for copying the intercepted data to the MD. The layer 3 target information is unknown at the AP-site.

Annex C (informative): Bibliography

ETSI TS 101 909-20-1: "Digital Broadband Cable access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based VoicedTelephony Services".

ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".

History

Document history		
V1.1.1	September 2005	Publication