



**SLOVENSKI STANDARD**  
**SIST-TS ETSI/TS 102 232-3 V3.14.1:2024**  
**01-september-2024**

---

**Zakonito prestrežanje (LI) - Izročilni vmesnik in storitveno specifične podrobnosti (SSD) za IP-dostavo vsebin - 3. del: Storitveno specifične podrobnosti za storitve internetnega dostopa**

Lawful Interception (LI) - Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 3: Service-specific details for internet access services

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

**Ta slovenski standard je istoveten z: ETSI TS 102 232-3 V3.14.1 (2024-07)**

SIST-TS ETSI/TS 102 232-3 V3.14.1:2024

<https://standards.iteh.ai/catalog/standards/sist/f54b4134-962b-4888-9459-df89b7d5eded/sist-ts-etsi-ts-102-232-3-v3-14-1-2024>

**ICS:**

35.240.95 Spletne uporabniške rešitve Internet applications

**SIST-TS ETSI/TS 102 232-3 V3.14.1:2024 en**



# ETSI TS 102 232-3 V3.14.1 (2024-07)



**Lawful Interception (LI);  
Handover Interface and  
Service-Specific Details (SSD) for IP delivery;  
Part 3: Service-specific details for internet access services**

[SIST-TS ETSI/TS 102 232-3 V3.14.1:2024](https://standards.iteh.ai/catalog/standards/sist/f54b4134-962b-4888-9459-df89b7d5eded/sist-ts-etsi-ts-102-232-3-v3-14-1-2024)

<https://standards.iteh.ai/catalog/standards/sist/f54b4134-962b-4888-9459-df89b7d5eded/sist-ts-etsi-ts-102-232-3-v3-14-1-2024>



---

**Reference**

RTS/LI-00261-3

---

**Keywords**access, internet, IP, lawful interception, security,  
service**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 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#).

Users should be aware that the present document may be revised or have its status changed,  
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to  
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our  
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.  
All rights reserved.

# Contents

Intellectual Property Rights .....	6
Foreword.....	6
Modal verbs terminology.....	6
Introduction .....	6
1 Scope .....	7
2 References .....	7
2.1 Normative references .....	7
2.2 Informative references.....	8
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	9
3.3 Abbreviations .....	9
4 General .....	11
4.1 Internet Access Service (IAS) .....	11
4.2 Target identity and IP address .....	11
4.3 Lawful Interception requirements .....	12
4.3.0 Introduction.....	12
4.3.1 Target identity.....	12
4.3.2 Result of interception.....	12
4.3.3 Intercept related information messages.....	13
4.3.4 Time constraints.....	13
4.3.5 Preventing over and under collection of intercept data.....	13
5 System model .....	14
5.1 Reference network topologies .....	14
5.1.0 Introduction.....	14
5.1.1 Dial-up access .....	14
5.1.2 xDSL access.....	15
5.1.3 Cable modem access .....	16
5.1.4 IEEE 802.11 Access (with Wireless LAN profile) .....	17
5.2 Reference scenarios .....	17
5.2.1 Logon.....	17
5.2.2 Multi logon .....	17
5.2.3 Multilink logon .....	17
5.2.4 IP transport.....	18
5.2.5 Logoff .....	18
5.2.6 Connection loss.....	18
6 Intercept Related Information (IRI) .....	18
6.1 IRI events .....	18
6.2 HI2 attributes.....	20
6.2.0 List of HI2 attributes .....	20
6.2.1 Use of targetIPAddress, additionalIPAddress and otherTargetIdentifiers fields .....	21
6.2.2 Use of location field.....	22
6.2.3 Packet Data Header Reporting (PDHR).....	22
6.2.3.1 General .....	22
6.2.3.2 IPv4Information .....	23
6.2.3.3 IPv6Information .....	23
6.2.3.4 TCPInformation .....	23
6.2.3.5 UDPInformation.....	23
6.2.4 Packet Data Summary Reporting (PDSR) .....	24
6.2.4.1 General .....	24
6.2.4.2 Packet flow.....	24
6.2.4.3 Triggers .....	24

6.2.4.4	Use of the IPIROnly record .....	25
6.2.5	Internet Protocol Packet Reporting (IPPR) .....	25
6.2.5.1	General .....	25
6.2.5.2	Packet Report Trigger .....	26
6.2.5.3	Fragmentation .....	27
7	Content of Communication (CC) .....	27
7.1	CC events .....	27
7.2	HI3 attributes .....	27
7.2A	HI3 truncated attributes .....	27
7.3	CC without session context .....	27
8	ASN.1 for IRI and CC .....	28
<b>Annex A (informative): Stage 1 - RADIUS characteristics.....</b>		<b>29</b>
A.1	Network topology .....	29
A.1.0	RADIUS deployment options .....	29
A.1.1	RADIUS server .....	29
A.1.2	RADIUS proxy .....	30
A.2	RADIUS service .....	31
A.2.1	Authentication service .....	31
A.2.2	Accounting service .....	31
A.2.3	IPv6 .....	32
A.3	RADIUS protocol .....	32
A.3.1	Authentication protocol .....	32
A.3.2	Accounting protocol .....	33
A.4	RADIUS main attributes .....	33
A.5	RADIUS interception .....	34
A.5.0	Introduction .....	34
A.5.1	Collecting RADIUS packets .....	34
A.5.2	Processing RADIUS packets .....	34
A.5.2.1	Mapping events to RADIUS packets .....	34
A.5.2.2	Functional model .....	37
A.5.2.3	RADIUS spoofing .....	40
A.5.2.4	Mapping of Acct-Terminate-Cause to endReason .....	40
A.5.2.5	Use of Event-Time .....	40
A.5.2.6	Use of targetIPAddress, additionalIPAddress and otherTargetIdentifiers fields .....	41
A.5.3	Mapping RADIUS on the IRI structure .....	41
<b>Annex B (informative): Stage 1 - DHCP characteristics.....</b>		<b>45</b>
B.1	Network topology .....	45
B.2	DHCP service .....	45
B.3	BOOTP protocol .....	46
B.4	DHCP protocol .....	46
B.4.0	Overview .....	46
B.4.1	Address assignment .....	47
B.4.2	Message transmission and relay agents .....	48
B.4.3	Security and authentication .....	48
B.5	DHCP main attributes .....	48
B.6	DHCP interception .....	49
B.6.1	Introduction .....	49
B.6.2	DHCP packets .....	49
B.6.3	State machine .....	50
B.6.3.0	Overview .....	50
B.6.3.1	Mapping DHCP packets to events .....	50
B.6.3.2	Timers and administrative events .....	51

B.6.3.3	State information .....	51
B.6.3.4	State machine diagram.....	52
B.6.4	Mapping DHCP on the IRI structure.....	52
<b>Annex C (informative):</b>	<b>IP IRI interception.....</b>	<b>54</b>
C.1	Introduction .....	54
C.2	Requirements.....	54
C.3	Proposed implementation.....	54
<b>Annex D (informative):</b>	<b>TCP and UDP IRI interception .....</b>	<b>55</b>
D.1	Introduction .....	55
D.2	Requirements.....	55
D.3	HI2 requirements.....	55
D.4	HI3 requirements.....	56
D.5	General requirements .....	56
<b>Annex E (informative):</b>	<b>Considerations regarding publicly exposed IP addresses .....</b>	<b>57</b>
<b>Annex F (informative):</b>	<b>Bibliography.....</b>	<b>58</b>
<b>Annex G (informative):</b>	<b>Change Request history.....</b>	<b>59</b>
History .....		62

iTech Standards  
(<https://standards.iteh.ai>)  
Document Preview

[SIST-TS ETSI/TS 102 232-3 V3.14.1:2024](https://standards.iteh.ai/catalog/standards/sist/f54b4134-962b-4888-9459-df89b7d5eded/sist-ts-etsi-ts-102-232-3-v3-14-1-2024)

<https://standards.iteh.ai/catalog/standards/sist/f54b4134-962b-4888-9459-df89b7d5eded/sist-ts-etsi-ts-102-232-3-v3-14-1-2024>

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

## Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [2].

The ASN.1 module is available as an electronic attachment to the present document (see clause 8 for more details).

---

## Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

---

## Introduction

The intention of the present document has been to follow the advice given at ETSI meetings in all cases.

The present document focuses on intercepting IP data in relation to the use of Internet Access Services (IASs) and is to be used in conjunction with ETSI TS 102 232-1 [2]. In the latter document the handing over of the intercepted data is described.



---

# 1 Scope

The present document contains a stage 1 description of the interception information in relation to the process of binding a "target identity" to an IP address when providing Internet access and a stage 2 description of when Intercept Related Information (IRI) and Content of Communication (CC) need to be sent, and what information it needs to contain.

The present document includes but is not restricted to IRI based on application of Dynamic Host Configuration Protocol (DHCP) and Remote Authentication Dial-In User Service (RADIUS) technology for binding a "target identity" to an IP address and CC for the intercepted IP packets.

The definition of the Handover Interface 2 (HI2) and Handover Interface 3 (HI3) is outside the scope of the present document. For the handover interface is referred to ETSI TS 102 232-1 [2].

---

## 2 References

### 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://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.

The following referenced documents are necessary for the application of the present document.

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

NOTE: ETSI TS 101 671 is in status "historical" and is not maintained.

- [2] [ETSI TS 102 232-1](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: 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 1990](#): "The PPP Multilink Protocol (MP)".
- [6] [IETF RFC 2131](#): "Dynamic Host Configuration Protocol".
- [7] [IETF RFC 7542](#): "The Network Access Identifier".
- [8] [IETF RFC 2865](#): "Remote Authentication Dial In User Service (RADIUS)".
- [9] [IETF RFC 2866](#): "RADIUS Accounting".
- [10] [IETF RFC 3046](#): "DHCP Relay Agent Information Option".
- [11] [IETF RFC 3118](#): "Authentication for DHCP Messages".
- [12] [IETF RFC 3396](#): "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)".

- [13] [IEEE 802.11™](#) (ISO/IEC 8802-11): "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
- [14] [Recommendation ITU-T X.680](#): "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation".
- [15] [IETF RFC 2132](#): "DHCP Options and BOOTP Vendor Extensions".
- [16] [ISO 3166-1](#): "Codes for the representation of names of countries and their subdivisions -- Part 1: Country code".
- [17] [IETF RFC 2869](#): "RADIUS Extensions".
- [18] [IETF RFC 3162](#): "RADIUS and IPv6".
- [19] [IETF RFC 4818](#): "RADIUS Delegated-IPv6-Prefix Attribute".
- [20] [IETF RFC 6911](#): "RADIUS Attributes for IPv6 Access Networks".
- [21] [IETF RFC 791](#): "Internet Protocol".
- [22] [IETF RFC 8200](#): "Internet Protocol, Version 6 (IPv6) Specification".
- [23] [IETF RFC 793](#): "Transmission Control Protocol".
- [24] [IETF RFC 3168](#): "The Addition of Explicit Congestion Notification (ECN) to IP".
- [25] [IETF RFC 3540](#): "Robust Explicit Congestion Notification (ECN) Signaling with Nonces".
- [26] [IETF RFC 768](#): "User Datagram Protocol".
- [27] [ETSI TS 103 120](#): "Lawful Interception (LI); Interface for warrant information".

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI TR 102 205: "Methods for Testing and Specification (MTS); UML 2.0 action syntax feasibility study".
- [i.2] IEEE 802.1X™-2001: "IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control".
- [i.3] draft-ietf-dhc-agentopt-radius-04.txt: "RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option".
- [i.4] [IANA bootp parameters](#).
- [i.5] ETSI TS 102 232-3 (V3.4.1): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".
- [i.6] [IETF RFC 2663](#): "IP Network Address Translator (NAT) Terminology and Considerations".
- [i.7] [IETF RFC 6264](#): "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition".
- [i.8] [IETF RFC 6888](#): "Common Requirements for Carrier-Grade NATs (CGNs)".

[i.9] [IETF RFC 7422](#): "Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT Deployments".

## 3 Definition of terms, symbols and abbreviations

### 3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 232-1 [2] and the following apply:

**access provider:** Communications Service Provider (CSP), providing access to a network

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.

**accounting:** act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation

**authentication:** property by which the correct identity of an entity or party is established with a required assurance

**authorization:** property by which the access rights to resources are established and enforced

**NAT translated IP address:** address realm, which has been mapped from an IP address in another address realm as a result of the application of NAT techniques

NOTE: IETF RFC 2663 [i.6] provides general information about NAT terminology and considerations whereas the IETF RFC 6264 [i.7], IETF RFC 6888 [i.8] and IETF RFC 7422 [i.9] provide information regarding the use of CGN.

**publicly exposed IP address:** NAT translated IP address where the IP address is a public IP address

**public IP address:** address realm with unique network addresses assigned by IANA or an equivalent address registry

### 3.2 Symbols

Void.

### 3.3 Abbreviations

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

AAA	Authentication, Authorization and Accounting
ACK	Acknowledge
ADSL	Asymmetric Digital Subscriber Line
ANP	Access Network Provider
AP	Access Provider
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BOOTP	BOOTstrap Protocol
CC	Content of Communication
CGN	Carrier-Grade NAT
CHAP	Challenge Handshake Authentication Protocol
CIN	Communication Identity Number
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment

CSP	Communications Service Provider (covers all AP/NWO/SvP)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ECN	Explicit Congestion Notification
FQDN	Fully Qualified Domain Name
GWR	GateWay Router
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
IANA	Internet Assigned Numbers Authority
IAP	Internet Access Provider
IAS	Internet Access Service
IEEE	Institute of Electrical and Electronic Engineers
IETF	International Engineering Task Force
IF	Interception Function
IIF	Internal Interception Function
IT	Information Technology
IP	Internet Protocol
IPCC	Internet Protocol Call Content
IPFIX	Internet Protocol Flow Information eXport
IPPR	Internet Protocol Packet Reporting
IPSEC	Internet Protocol Security
IPv4	Internet Protocol (version 4)
IPv6	Internet Protocol (version 6)
iPV6	IP version 6
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
LCP	Link Control Protocol
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAC	Media Access Control
MF	Mediation Function
NA	Not Applicable
NAS	Network Access Server
NAT	Network Address Translation
NIC	Network Interface Controller
NWO	NetWork Operator
OID	Object IDentifier
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PC	Personal Computer
PDA	Personal Digital Assistant
PDHR	Packet Data Header Reporting
PDSR	Packet Data Summary Reporting
PDU	Packet Data Unit
POP	Point of Presence
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SLIP	Serial Line Interface Protocol
SvP	Service Provider
TCLI	Technical Committee for Lawful Interception
TCP	Transmission Control Protocol

TLV	Type-Length Value
UDP	User Datagram Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
xDSL	any Digital Subscriber Line technology

## 4 General

### 4.1 Internet Access Service (IAS)

An Internet Access Service (IAS) provides access to the Internet to end users via a modem connected to a telephone, cable or wireless access network owned by a Network Operator (NWO). The IAS is typically provided by an Internet Access Provider (IAP) or Internet Service Providers (ISP), where an ISP also provides supplementary services such as E-Mail, Chat, News, etc. For the remainder of the present document, the provider of the Internet Access Service (IAS) will be referred to as IAP and although NWO and IAP may be the same party, in all figures in the present document, they are depicted as separate entities.

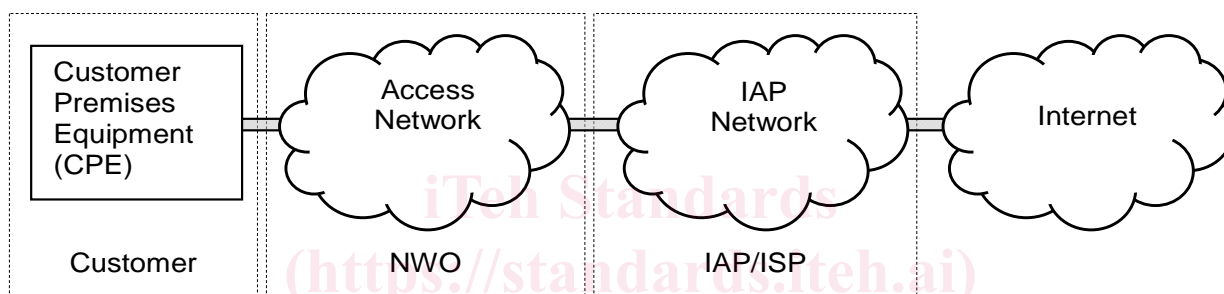


Figure 1: Internet access

The customer typically connects to the IAP via a Telco or cable company owned access network, such as the PSTN/ISDN telephony network for dial-up and xDSL access, the cable-TV network for cable modem access or alternatively a IEEE 802.11 [13] Wireless LAN.

The service provided by the IAP is no more and no less than to provide a user with a valid IP address for transporting and receiving data over an IP based network and to provide transit access to the Internet for this data.

### 4.2 Target identity and IP address

Before the IAP can provide a user with a valid IP address, there is a need for *Authentication*, *Authorization* and during or at the end of the communication session there is a need for *Accounting*.

In order to perform these functions, the IAP may deploy equipment in its network that implements an Authentication, Authorization and Accounting (AAA) protocol such as RADIUS. The other protocol mentioned in the scope declaration, DHCP, is not really an AAA protocol, since it does very limited authentication and no authorization or accounting. DHCP can assign IP addresses and provide network configuration information to the user and is therefore often used in combination with RADIUS or other (proprietary) equipment.

When a user is authenticated and authorized, the IAP will assign an IP address to the user. The assignment of the IP address can be performed by using RADIUS, DHCP or a combination of the two. In the latter case, often the RADIUS server will act as a client to the DHCP server, where the DHCP server assigns the IP address and the RADIUS server forwards the information towards the user. The user will use the assigned IP address to communicate over the Internet and therefore, for the duration of the session, traffic from and to this user can be identified by means of this IP address.

In some cases (e.g. dial-up access), the Network Access Server (NAS) may assign the IP address to the user; either from a local IP address pool or by using DHCP and does not use RADIUS authentication for IP address assignment.

From an LI perspective, the moments of assignment and deassignment of the IP address and the protocol used for it are of interest. It is at the moment of assignment, and only at that particular moment, that the target identity can be tied to a dynamically assigned IP address, which can then further be used to intercept IP traffic from the particular user. At the moment of deassignment, interception of IP data based on that particular IP address shall stop immediately, since the IP address may be handed out to another user shortly after.

## 4.3 Lawful Interception requirements

### 4.3.0 Introduction

This clause lists the requirements for Lawful Interception. These requirements are derived from higher-level requirements listed in ETSI TS 101 671 [1] and ETSI TS 102 232-1 [2] and are specific to Internet Access Services (IASs). These requirements focus on both the administrative part of Internet access for delivery over HI2 as well as capturing traffic for delivery over HI3.

#### 4.3.1 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.

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 will be dependent on the access mechanism used and the parameters available with the AP. The target identity could be based on:

- a) Username or Network Access Identifier (as defined in IETF RFC 7542 [7]).
- b) IP address (IPv4 or IPv6).
- c) Ethernet address.
- d) Dial-in number calling line identity.
- e) Cable modem identifier.
- f) Other unique identifier agreed between AP and LEA.

The target identity shall uniquely identify the target in the provider's network. Investigations prior to the interception might involve other identifiers such as a DNS name (Fully Qualified Domain Name (FQDN)).

#### 4.3.2 Result of interception

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

- a) When an attempt is made to access the access network.
- b) When an access to the access network is permitted.
- c) When an access to the access network is not permitted.
- d) On change of status (e.g. in the access network).
- e) On change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on).

The IRI shall contain:

- a) Identities used by or associated with the target identity (e.g. dial-in calling line number and called line number, access server identity, Ethernet addresses, access device identifier).