ETSI TS 102 232-3 V3.16.1 (2025-08)

TECHNICAL SPECIFICATION

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

Reference
RTS/LI-00288-3

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

Contents

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 in the ETSI docbox.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[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: "Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (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.

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

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

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
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
IT	Information Technology
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.

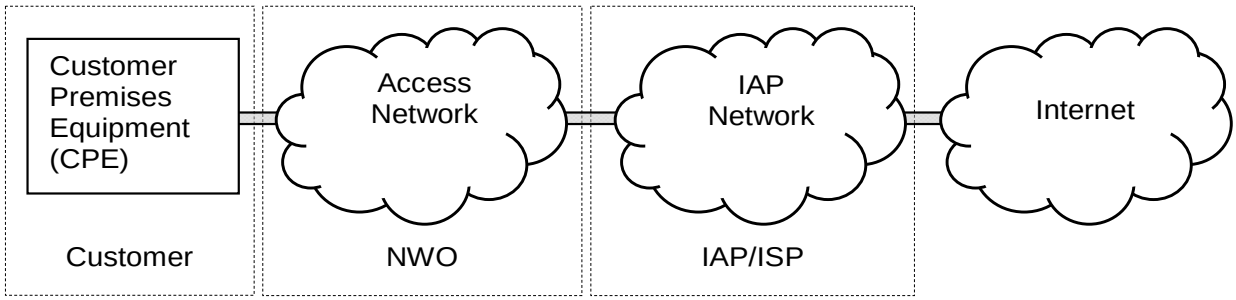


Figure 1: Internet access

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).

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 IP datagram sent through the IAP's network that:

a) Has the target's IP address as the IP source address.

b) Has the target's IP address as the IP destination address.

The CC shall contain:

a) A stream of octets for every captured datagram, containing a copy of the datagram from layer 3 upwards.

NOTE: Due to the possibility of IP source address spoofing, the fact that an intercepted packet has the target's IP address as the IP source address does not guarantee that the packet was transmitted by the target; i.e. an intercept in place at the interface connected to the target may not include packets originating from other users spoofing the target's IP address and will not include packets from the actual target that contain a spoofed IP address.

4.3.3 Intercept related information messages

Intercept Related Information (IRI) shall be conveyed to the LEMF in messages, or IRI data records, respectively. Four types of IRI 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 records refer to ETSI TS 102 232-1 [2].

4.3.4 Time constraints

The delays for generating the Intercept Related Information (IRI) will only be caused by the access protocol handling and the automated forwarding of this information to the delivery function.

The interception that takes places as a result of the identification of the target in the access service will experience no unnecessary delay. The delay will only be caused by the access protocol handling and the automated forwarding of this information to the interception function(s).

4.3.5 Preventing over and under collection of intercept data

Measures shall be taken to:

1) enable timely detection of system, network or software failures that may cause the interception system to over or under collect data;

2) take appropriate action to prevent further over or under collection; and

3) report on the anomaly to allow for corrective action by the LEA.

NOTE 1: The terms over and under collection refer to either wrongfully including data that is not part of the intercept or not capturing data that should have been part of the intercept.

If an interception is started based on an IP-address binding event that contains session-timeout information and at the time of the expected session-timeout no explicit session-termination event has been captured, the interception shall be stopped and the situation shall be reported upon.

If an IP-address binding event is captured that contains an IP address already in use in an active intercept, but for a different user, the intercept shall be stopped and the situation shall be reported upon.

NOTE 2: Due to various kinds of failures or delays in the LI infrastructure, the event indicating the logoff of a target could be missed by the Interception function. The actual logoff would release the IP address for reassignment to another user, which would lead to a serious kind of over collection.

5 System model

5.1 Reference network topologies

5.1.0 Introduction

This clause describes a number of reference network topologies, typically used for Internet access over various types of access networks.

5.1.1 Dial-up access

Internet access over a switched telephony network is typically referred to as dial-up access. Figure 2 shows the principal equipment involved in this kind of Internet access.

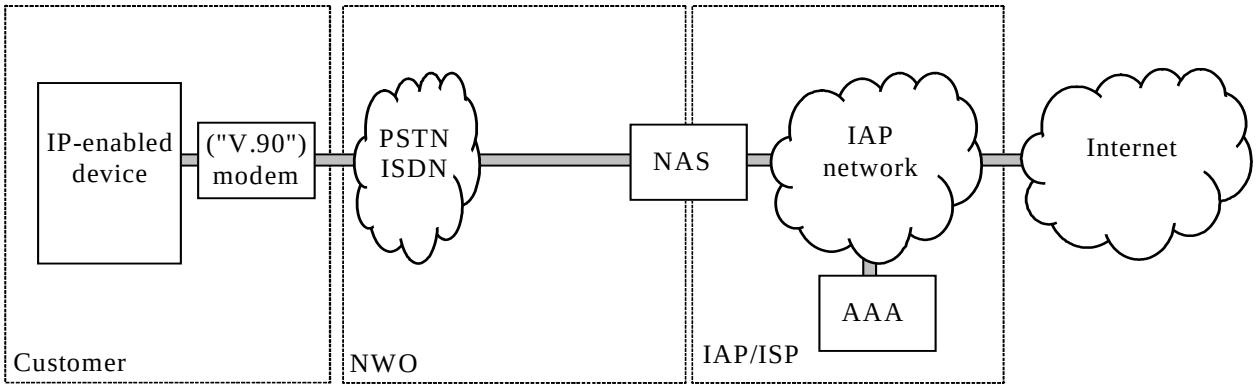


Figure 2: Dial-up access

The CPE for dial-up access typically consists of a computer, laptop or PDA that is equipped with a modem connected to the regular telephone network. Via this modem, the telephone number of the Network Access Server (NAS) of the IAP is dialled. The NAS answers the call and the NAS and the end-user typically establish a Point-to-Point Protocol (PPP) connection. Due to the distributed nature of dial-up access, a user may dial into any NAS in the network.

Once the PPP connection is established, the NAS will request the user to identify himself and to provide a password. The NAS will then request the AAA server in the IAP infrastructure (for dial-up access typically a RADIUS server) to perform the authentication based on the provided username and password. Additionally, the AAA server will check whether the user is authorized to use the Internet Access Service (IAS). If so, the AAA server may provide the NAS with an IP address that is to be used by the user. In other cases, the NAS allocates the IP address from a locally configured pool of addresses and the AAA server does not know the IP address at the time of authentication.

Next, the NAS informs the user about the assigned IP addresses and other network configuration information, such as the address of the DNS server and/or the address of the gateway to the Internet. The CPE can now set-up its IP protocol stack and establish IP based communication with the Internet.

After the NAS has established a PPP session with the CPE, the NAS may provide the Accounting server with information indicating the start of the session and the parameters in use for the session (e.g. IP addresses, NAS address). The Accounting server may be a physically separate server from the Authentication/Authorization server. In the case in which the NAS assigns IP addresses from a local pool, this is the first time the IP addresses assigned to the target is known externally to the NAS.

At the end of the session, either when the user logs off or when the connection to the NAS is lost, the NAS will provide the Accounting server with details regarding usage of the Internet connection, e.g. duration, bytes sent and received, etc. This information can be used for accounting purposes.

From an LI perspective, the assignment of IP addresses, in relation to the usernames they are assigned to, as well as the moment of deassignment, i.e. the exchange of accounting information, are of interest.

NOTE: Many IAPs also support tunnelling the PPP session from the NAS to a home gateway either at another location within the IAP or residing on another network (e.g. another IAP or an enterprise). The standard protocol used to support this is Layer 2 Tunnelling Protocol which tunnels the PPP frames from the NAS to the home gateway. Proprietary tunnelling techniques might also be used based on the service provider. Many of the technologies described in the present document may be used to support the tunnelling service (e.g. RADIUS); however, since this service is not an Internet Access Service (IAS) as defined in the present document, it is outside the scope of the present document.

5.1.2 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 3 only shows the principal equipment involved in this kind of Internet access.

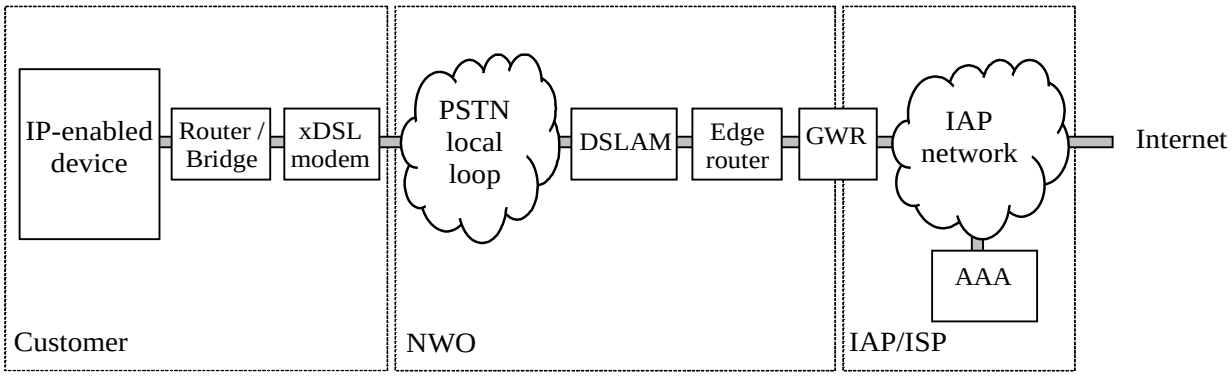


Figure 3: xDSL access

The CPE can consist of a single IP enabled device which is connected to an xDSL modem or, in order to support multiple IP enabled devices to share the xDSL connection, to a router or bridge that is connected to an xDSL modem.

The modem is connected to the copper wire of the telephone network, the local loop. In the telephone switch, this wire, and wires from other xDSL lines, are connected to the DSL Access Multiplexer (DSLAM). By utilizing frequencies above the telephone bandwidth, the xDSL modem and the DSLAM can encode more data to achieve a higher bandwidth than would otherwise be possible in the restricted frequency range of a PSTN network.

For large scale xDSL infrastructures, two main approaches are used for protocol layering; PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE). In the PPPoA architecture, a CPE router encapsulates IP packets into PPP frames and then segments them into ATM cells. The PPP link is commonly terminated at the GateWay Router (GWR) of the IAP, which concentrates PPP links from multiple Edge routers. The GWR routes the user's IP packets to their final destination. The GWR typically uses a RADIUS server to authenticate and authorize the user. A DHCP server may be used to assign the IP address. A PPPoA implementation involves configuring the CPE router with username and password.

In the PPPoE architecture, at the user premises an Ethernet-to-WAN bridge is used as opposed to a router and the PPP session is established between the end user's computer and the GWR. PPPoE requires PPP client software to be installed on the user's computer. The client software initiates a PPP session by encapsulating IP packets into PPP frames into a MAC frame and then bridges the frames (over ATM/DSL) via the edge router to the GWR. From this point, PPP sessions can be established, authenticated, etc. As well as in the PPPoA architecture, the GWR typically uses a RADIUS server to authenticate and authorize the user and again DHCP may use to assign the IP address.

In the PPPoA architecture, the CPE router may keep the connection established, even if the user's computer has been shut down. Therefore, in this architecture IP address assignment will happen very rarely; only once until either the router is shutdown or, if due to network or equipment failure, the connection is lost and re-established. In the PPPoE architecture, the IP address is assigned every time the user's computer logs on.

In some cases the IAP will resort to assigning static IP addresses to xDSL users. When in this case the user establishes an IP connection, the IP address will still be assigned by means of a RADIUS and or DHCP server, but it will always be the same IP address. If this is the case, especially in combination with a PPPoA architecture, for LI purposes it is a lot easier to obtain a user's IP address from the IAP administration, rather than to obtain it from the network by technical means, e.g. capturing and interpreting RADIUS or DHCP traffic.

If it is decided to resort to technical means for intercepting the IP address, for a timely start of the interception, it may be considered to bounce the user's connection in order to enforce assignment of a new IP address.

5.1.3 Cable modem access

Internet access over the cable network by means of using specialized equipment for achieving a high bandwidth over coaxial wire is commonly referred to as cable modem access. As for xDSL, there is great variety of possible architectures and technologies that can be applied for realizing a cable modem network. Therefore, Figure 4 only shows the principal equipment involved in this kind of Internet access.

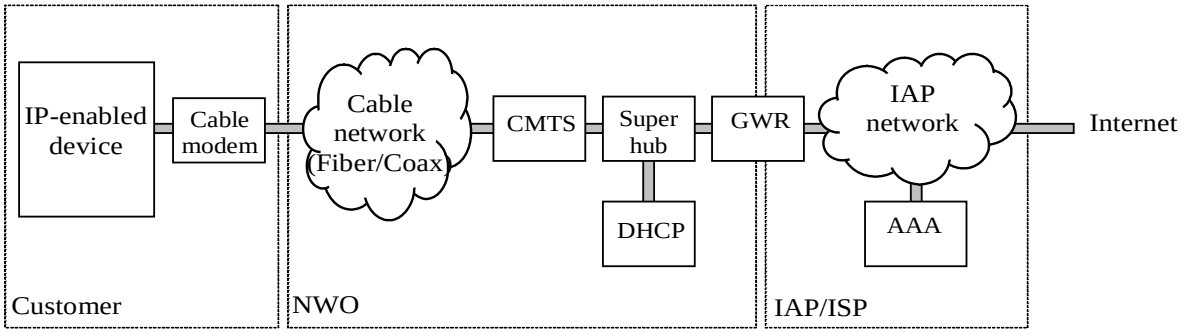


Figure 4: Cable modem access

The CPE typically consists of an IP enabled device connected to a cable modem via an Ethernet port. The cable modem connects to the Cable network using a coaxial cable.

At the NWO end, the data channels are terminated at a Cable Modem Termination System (CMTS). This CMTS aggregates multiple cable modem channels and routes the user's IP packets, either over Ethernet or over ATM, into an IP network. Depending on the applied standards, network architecture and geographical factors, multiple CMTSs may be aggregated by a distribution hub, multiple distribution hubs by a super hub and multiple super hubs by a GateWay Router (GWR).

Typically, IP addresses are assigned by means of DHCP based on the MAC address of either the cable modem or the users' computer, depending on applied standards and equipment, where either the computer or the cable modem will broadcast a DHCP request. The DHCP servers are typically distributed at the Super hub level and provisioned from a central location with the MAC addresses of authorized users. Typically IP addresses are assigned dynamically to most users but may be fixed for particular users. The latter may be assigned by means of DHCP as well.

The IAP may authenticate and authorize users for the access service based on a username and password as well. Such additional authentication can also be used for the provision process, for example when a user replaces his computer and therefore changes his MAC address. The AAA protocol used for this may be RADIUS or proprietary.

From an LI perspective, the AAA process is less relevant than the DHCP based IP address assignment. An interception solution in a cable modem environment will typically capture DHCP traffic in an attempt to identify a user based on his MAC address. The potential geographical spread of DHCP servers may become an issue, since this implies that the interception solution shall therefore by distributed over a potentially large number of locations as well.

In some cases, the IAP may use PPPoE for access. This operation is similar to that described for xDSL.

5.1.4 IEEE 802.11 Access (with Wireless LAN profile)

Wi-Fi® (also known as "Wireless LAN") is a registered trademark of the Wi-Fi Alliance, and is used to indicate equipment which conforms to an interworking profile for IEEE 802.11 [13].

Figure 5 depicts a much used reference scenario of Wireless LAN access.

Most Wireless LAN networks use a standards based AAA protocol like RADIUS for authentication. Therefore, Wireless LAN could be intercepted like any other internet access scenario. However, because access points are often connected via a consumer grade broadband connection using one IP address, the internet traffic is masqueraded. To identify a unique target, interception thus should take place before the IP addresses are translated (in or near the access point), or traffic should be tunnelled to a central location.

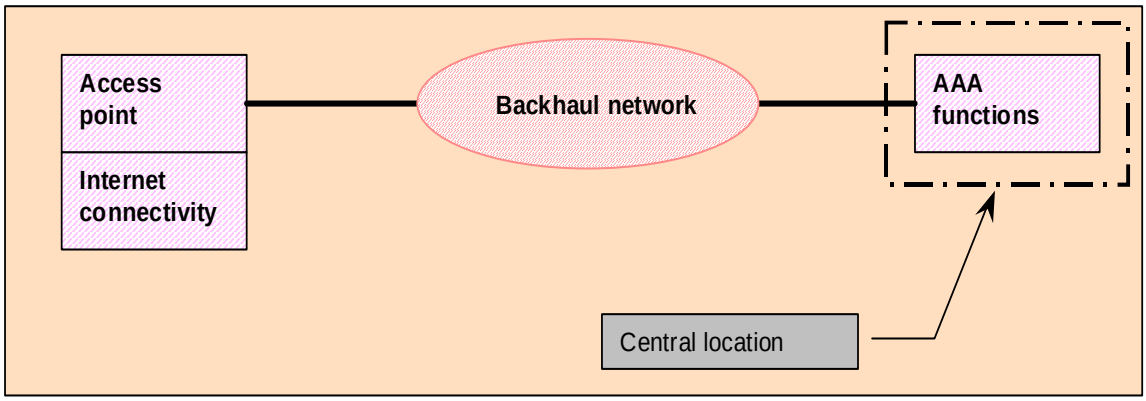


Figure 5: Reference scenario for Wireless LAN access

5.2 Reference scenarios

5.2.1 Logon

In order for a user to be able to use an Internet Access Service (IAS), the user shall first establish a network level connection to the Access Network. Next, either on the initiative of the user or the access network, authentication information is exchanged based on which an AAA server performs authentication and authorization. Depending on the outcome of the authentication and authorization, access is either granted or denied. In the case access is granted, an IP address is provided, the user sets up an IP stack and layer 3 communications can commence.

5.2.2 Multi logon

If the IAP allows for multi logon, the same UserID can be used multiple times (concurrently) to establish an IP connection along the lines of clause 5.2.1. The UserID and password provided by the user will be identical for all sessions; the provided IP address will differ for each of the sessions and the traffic transported for each of the IP addresses will belong to separate IP sessions.

5.2.3 Multilink logon

Multilink logon may be required for users connecting using a multilink protocol, such as the PPP multilink protocol for ISDN described in IETF RFC 1990 [5], where a separate authentication is performed, along the lines of clause 5.2.1, for each of the ISDN 64 kbit channels and the NAS combines multiple 64 kbit channels into a single logical channel. In this scenario, the same UserID and password may be used for authentication for each of the channels; the IP addresses provided by the NAS may differ. Depending on NAS implementation, typically the first IP address that is provided, the one for the base channel, is the IP address used for the combined channels. Subsequent IP addresses, provided for the additional channels, may be valid IP addresses or may be invalid IP addresses such as 0.0.0.0. In either case, IP addresses provided for additional channels are not used for transporting data, since all data is transported using the IP address of the base channel.

NOTE: When using multilink PPP to dial into a pool of NASes, each 64 kbit/s connection can terminate on a separate NAS. Many IAPs use multichassis multilink to support this scenario. In this case, the aggregation point of the multilink bundle will be on one of the NASes or on a separate piece of equipment. The IP address assigned to the multilink bundle will be allocated from the address pool of the equipment terminating the multilink bundle.

5.2.4 IP transport

While having an active IP connection, the CPE can transmit IP datagrams, embedding any higher-level IP based protocol, towards any IP enabled destination connected to the Internet or receive IP datagrams directed towards it from any IP enabled source connected to the Internet.

5.2.5 Logoff

When a user logs off, the client running on the CPE will negotiate the closure of the session with the NAS, e.g. for a PPP session LCP (see IETF RFC 1570 [4]) is used to close the link through an exchange of Terminate packets. Next, the NAS informs the AAA server of the session closure and may provide statistics on the session as well.

5.2.6 Connection loss

During an active IP session, for reasons such as loss of carrier, link quality failure, the expiration of an idle-period timer, the connection may terminate (unexpectedly). In this case there will be no user provided logoff indication and it is up to the NAS to detect the connection loss and propagate the session closure towards the Accounting server.

5.2.7 Interception without network session events

Apart from the reference scenarios previously described in clause 5.2, interception may occur in parts of a network where a network session context is not available. An example could be a point of interception where IP packets are passively copied into an MF. That MF is then only aware of the IP packets it has to intercept and not of the session context pertaining to those packets.

Subject to national agreement, this scenario may be implemented as one of the following options:

1) CC only without IRI. In this option, and subject to national agreement, the CC CIN value may be omitted.

2) An interception session with IRI generated by the MF, using appropriate IRI event types (see clause 6.1) based on other events such as LI activation and deactivation. These IRI sessions may be started either on LI activation or upon first IP packet received after LI activation, subject to national agreement.

5.2.8 Mediation session expiry

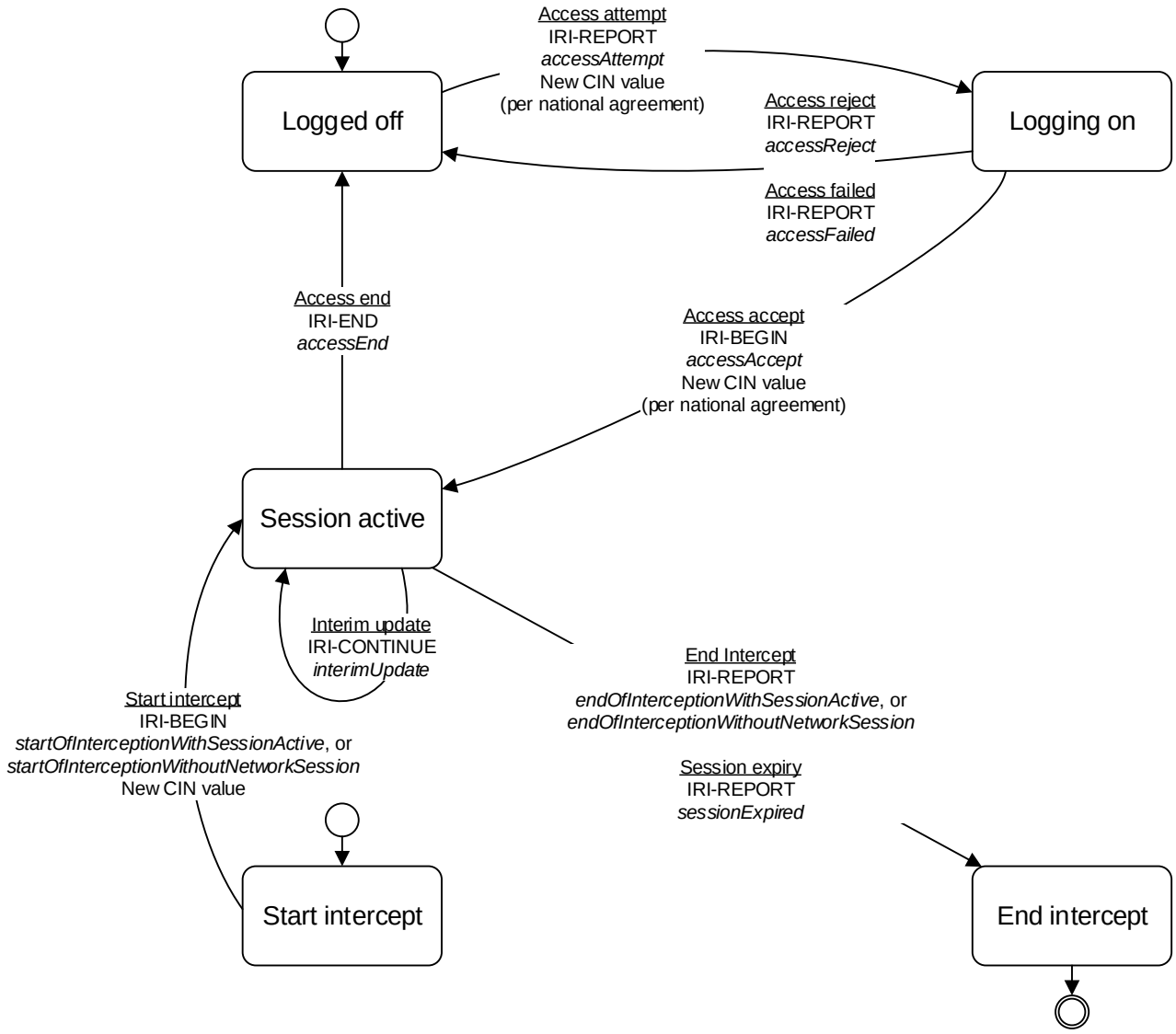
Certain fault conditions in the interception process may require the MF to terminate an interception session without an explicit network session event (e.g. DHCP or RADIUS) from the NAS, in order to prevent the interception sessions consuming MF resources indefinitely. These fault conditions may include the non-receipt of a specific multiple of expected regular network session events from the NAS.

NOTE: This is separate to an endReason (see clause 6.2.0, Table 2) of *connectionTimeout*, which may have a direct mapping to a specific network event's (e.g. DHCP or RADIUS) service-specific parameter.

6 Intercept Related Information (IRI)

6.1 IRI events

Figure 6 shows the life cycle of a generic internet access session.



NOTE 1: Depending on the signalling implementation, there may be duplicate events due to resends. Resends of events shall be ignored as far as state-changes are concerned; this is not depicted in the diagram.
NOTE 2: Session expiry may occur from any state for an existing interception session.

Figure 6: State diagram for an Internet session

Subject to agreement on a national level, it is acceptable to perform the CIN allocation on the *accessAccept* rather than the *accessAttempt*. If this option is chosen, the CSPs shall allocate a new CIN only on the IRI-BEGIN messages; and, send *accessAttempt*, *accessReject* and *accessFailed* as standalone messages not associated with any other CC or IRI.

Figure 6 allows for a model where detailed information is available regarding the identification and authentication process as well as for a simple model where just a session start notification is available.

The IRI events depicted in Figure 6 are described in Table 1.

Table 1: IRI events

IRI Event	Description	IRI Message
accessAttempt	A target requests access to the Internet Access Service (IAS).	REPORT
accessAccept	The AAA server grants access to the target.	BEGIN
accessReject	The AAA server refuses access to the target.	REPORT
accessFailed	The *accessAttempt* timed-out or failed otherwise.	REPORT
startOfInterceptionWithSessionActive	As sessions can be active over longer periods, it is not unlikely for an intercept to start after a user session has started already.	BEGIN

IRI Event	Description	IRI Message
interimUpdate	Intermediate status report on service status or usage.	CONTINUE
accessEnd	A target stops using the IAS, either due to logoff or connection loss.	END
endOfInterceptionWithSessionActive	As sessions can be active over longer periods, it is not unlikely for an intercept to end whilst a user session remains active.	REPORT
startOfInterceptionWithoutNetworkSession	The interception session is started by the MF without a network session event.	BEGIN
endOfInterceptionWithoutNetworkSession	The interception session is ended by the MF without a network session event.	REPORT
sessionExpired	The interception session is expired by the MF.	REPORT

When LI is activated during an already active internet session, which the IAP is aware of, it is recommended that an IRI-BEGIN message is generated to mark the start of interception and the specific event type of *startOfInterceptionWithSessionActive* shall be used.

When LI is deactivated during an already active internet session, which the IAP is aware of, as a national option the MF may choose to either generate an IRI-REPORT message to mark the end of interception and shall use the specific event type of *endOfInterceptionWithSessionActive*, or not to generate an IRI-REPORT message and only communicate the end of interception by other means (e.g. HI1 *liDeactivated* message).

When LI is activated without a network session context (see clause 5.2.7), as a national option the MF may generate an IRI-BEGIN message to mark the start of interception and the specific event type of *startOfInterceptionWithoutNetworkSession* shall be used (see clause 5.2.7 option 2), or may generate CC without IRI (see clause 5.2.7 option 1).

When LI is deactivated without a network session context (see clause 5.2.7), as a national option the MF may generate an IRI-REPORT message to mark the end of interception and the specific event type of *endOfInterceptionWithoutNetworkSession* shall be used (see clause 5.2.7 option 2), or may not generate any IRI (see clause 5.2.7 option 1) and communicate end of interception by other means (e.g. HI1 *liDeactivated* message).

When the MF terminates an interception session due to an interception expiry condition (see clause 5.2.8), the MF shall generate an IRI-REPORT message to mark the end of interception of that interception session and shall use the specific event type of *sessionExpired*.

6.2 HI2 attributes

6.2.0 List of HI2 attributes

Table 2 lists the attributes for IRI for Internet access and defines in which of the IRI messages a value shall be provided for them, provided the attribute is relevant for the type of service.

Table 2: HI2 attributes

Attribute	Description	Report	Begin	Cont.	End
accessEventType	Type of IRI event (e.g. *accessAttempt*, *accessFailed*, *accessEnd*, etc.).	Y	Y	Y	Y
targetUsername	The Username (or other token used for identification) of the target.	Y	Y	Y	Y
internetAccessType	The type of Internet access (e.g. dial-up, ADSL, cable modem, LAN access).	Y	Y	Y	Y
iPVersion	IPv4 or IPv6 or iPV4andV6.	Y	Y	Y	Y
targetIPAddress	The IPv4 or IPv6 address that was assigned to the target. Refer to clause 6.2.1 for full description and usage.	Y	Y	Y	Y
targetNetworkID	The MAC address of the target CPE for layer 2 access or the target PSTN/ISDN number for dial-up.	Y*	Y*	-	-
targetCPEID	Secondary identification of the target CPE (e.g. DHCP Relay Agent Information, computer name, etc.).	Y*	Y*	-	-

Attribute	Description	Report	Begin	Cont.	End
targetLocation	Location information. New implementations are encouraged to use the imported "location" field (see below) where possible.	Y*	Y*	Y	-
pOPPhoneNumber	The POP telephone number used for dial-up access.	Y*	Y*	-	-
pOPIdentifier	The POP identifier or name.	Y*	Y*	-	-
pOPIPAddress	The POP IP address.	Y*	Y*	-	-
pOPPortNumber	The POP or 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.	Y*	Y*	-	-
callBackNumber	The target PSTN/ISDN number used for call-back by the NAS.	Y*	Y*	-	-
startTime	The date and time of the start of the session (or lease).	Y*	Y*	-	-
expectedEndTime	The date and time of a predicted session ending (e.g. lease expiration).	Y*	Y*	-	-
endTime	The date and time of the end of the session (or lease).	-	-	-	Y
endReason	The reason for the session to end (e.g. logoff, connection loss, time out, lease expiration).	-	-	-	Y
octetsTransmitted	The number of octets the target sent during the session.	-	-	-	Y
octetsReceived	The number of octets the target received during the session.	-	-	-	Y
rawAAAData	An unformatted OCTET string that may contain the raw AAA records as they were intercepted.	-	-	-	-
nationalIPIRIParameters	National IP IRI parameters.	Y	Y	Y	Y
additionalIPAddress	The IPv6 address that was assigned to the target. Refer to clause 6.2.1 for full description and usage.	Y	Y	Y	Y
authenticationType	Field used to identify the authentication type to assist with LEMF data validation.	Y	Y	-	-
otherTargetIdentifiers	This parameter is used when multiple subnet/prefix ranges are assigned to a target service. There can be multiple instances of OtherTargetIdentifiers. Refer to clause 6.2.1 for full description and usage.	Y	Y	Y	Y
location	The location associated with the target, if available.	Y	Y	Y	Y
pOPPortIdentifier	NAS-Port Identifier providing information about the physical connection on the NAS.	Y*	Y*	-	-
framedRoute	This parameter lists all assigned Framed Route and Framed IPv6 Route information.	Y	Y	Y	Y
Attributes marked with Y shall be provided, if a value is available for it. Attributes marked with * shall be reported in either the IRI-REPORT or the IRI-BEGIN record or both. Attributes marked with - may be reported in all IRI records if a correct value is available.					
NOTE 1: Void. NOTE 2: National legislation may prohibit the IAP to provide the users password. If so, the password shall be removed from the raw AAA data before handover.					

6.2.1 Use of targetIPAddress, additionalIPAddress and otherTargetIdentifiers fields

6.2.1.1 General

The IP address fields in any given IRI message shall reflect the current state of all IP addresses, i.e. any IRI-CONTINUE message generated by the MF shall not be interpreted as increment to any previous message.

If the iPVersion parameter is set to value IPv4:

- The targetIPAddress field shall contain the first (or only) target IPv4 address or subnet range.
- The additionalIPAddress field shall not be populated with any value.
- The otherTargetIdentifiers field shall contain the second and subsequent IPv4 target addresses (with or without subnet ranges) if any additional address ranges are assigned to the target service.

NOTE 1: The otherTargetIdentifiers field is intended to be extensible to accommodate other target identifiers and types which may be required in future.

If the iPVersion parameter is set to value IPv6:

- The targetIPAddress field shall contain the first (or only) target IPv6 address or prefix range.
- The additionalIPAddress field shall not be populated with any value.
- The otherTargetIdentifiers field shall contain the second and subsequent IPv6 target addresses (with or without prefix ranges) if any additional address ranges are assigned to the target service.

NOTE 2: The otherTargetIdentifiers field is intended to be extensible to accommodate other target identifiers and types which may be required in future.

If the iPVersion parameter is set to value iPV4andV6 (i.e. where the user service is dual-stacked):

- The targetIPAddress field shall contain the first (or only) target IPv4 address or subnet range.
- The additionalIPAddress field shall contain the first (or only) target IPv6 address or prefix range.
- The otherTargetIdentifiers field shall contain the second and subsequent IPv4 or IPv6 target addresses (with or without subnet or prefix ranges) if any additional address ranges are assigned to the target service.

NOTE 3: The otherTargetIdentifiers field is intended to be extensible to accommodate other target identifiers and types which may be required in future.

6.2.1.2 Handover of NAT translated IP addresses

There are scenarios where neither the targetIPaddress nor the additionalIPAddress field contains a public IP address. In such scenarios, any publicly exposed IP address that is known to be associated with the target via NAT translation should be provided using the otherTargetIdentifiers field, given that the respective IP address is available at the MF and the respective mapping between the exposed IP address and the IP address being not exposed is valid.

NOTE 1: There are situations where more than one publicly exposed IP address is assigned, e.g. in dual stack, dual stack light, multi- or dual-homing scenarios, respectively. The same holds true for NAT translated IP addresses in general.

If any of the following fields contain an IP address that is a NAT translated IP address, the iP-NAT-translated field of the IPAddress parameter (see ETSI TS 102 232-1 [2]) that is stored in the respective field should be set to the value TRUE, regardless of the value of the iPVersion parameter. The value shall be set to TRUE for any publicly exposed IP address that is contained in the otherTargetIdentifiers field:

- targetIPAddress
- additionalIPAddress
- otherTargetIdentifiers

Otherwise, i.e. the aforementioned IP address is not a NAT translated IP address, the respective field should be set to the value FALSE.

NOTE 2: According to ETSI TS 102 232-1 [2] any IP address can contain optional information given by the iP-NAT-translated field to indicate whether this IP address is NAT translated. Furthermore, the absence of the iP-NAT-translated field indicates that it is unknown whether the IP address has been translated via NAT-techniques.

If the otherTargetIdentifiers field contains a NAT translated IP address and the respective IP address is not valid anymore in the sense that this IP address loses its association with the target, the respective IP address parameter shall be removed from the otherTargetIdentifiers field and the MF shall generate an IRI-CONTINUE message and shall use the specific event type of interimUpdate (see clause 6.1), which shall contain in particular the otherTargetIdentifiers field with respectively updated value.

NOTE 3: An IP address may lose its association with the target, e.g. because it is no longer part of the respective NAT translation.

For further information regarding publicly exposed IP addresses, see Annex E.

6.2.2 Use of location field

The IRI Internal Interception Function (IIF) may report location information to satisfy the requirement in clause 4.3.2. The availability and format of location information in the IRI IIF may depend on the network access technology. Since version 3.4.1 of the present document [i.5] uses the common "location" parameter from ETSI TS 102 232-1 [2] to signal this information.

If a CPE provides location information, it shall be handed over in the cPEProvidedLocationAttributes parameter as defined in ETSI TS 102 232-1 [2].

6.2.3 Packet Data Header Reporting (PDHR)

6.2.3.1 General

The PDHR mechanism in this clause has been superseded by the IPPR mechanism in clause 6.2.5, which should be used in new implementations.

An IPIRIOnly structure may be used to deliver an IRI report for a packet in the target's access session if required by the warrant (either for IRI-only interception, as described in Annex C and Annex D, or for bandwidth-reduction purposes). The rules for determining whether a packet should be reported as CC or as a Packet Data Header Report are outside the scope of the present document. The IPIRIOnly report shall be assigned the same CIN as the other IRI records associated with the access session.

When reporting a packet data header, the fields in the IPIRIOnly structure are populated as described in Table 3.

Table 3: IPIRIOnly for Packet Data Header Reporting

Attribute	Contents
iPInformation	Information from the IPv4 or IPv6 header of the target packet, as appropriate. See clauses 6.2.3.2 and 6.2.3.3.
protocolInformation	Provides information from the layer 4 header if available. TCP header information is provided using the TCPInformation structure. UDP header information is provided using the UDPInformation structure. If no protocol information is provided, "none" is chosen. See clauses 6.2.3.4 and 6.2.3.5.
iPAggregatedNbrOfPackets	If provided, shall give the total number of packets that have been observed as part of the packet flow.
iPAggregatedNbrOfBytes	If provided, shall give the total number of bytes summed across all packets that have been observed for this packet flow. For IPv4 it is the sum of the "Total Length" fields across all packets in the summary as defined in Internet Protocol IETF RFC 791 [21], while for IPv6 it is the sum of the "Payload Length" fields across all packets in the summary as defined in Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 8200 [22].
pDSRInformation	Shall not be populated.

6.2.3.2 IPv4Information

Each field of the IPv4Information structure corresponds to a field in the IPv4 header of the target packet, as defined in IETF RFC 791 [21]. The value of each populated field shall be given as a copy of the relevant octet(s) with the byte ordering unchanged. Where values are smaller than an octet (e.g. the typeOfService field), bits that are not part of the relevant field shall be set to zero.

6.2.3.3 IPv6Information

Each field of the IPv6Information structure corresponds to a field in the IPv6 header of the target packet, as defined in IETF RFC 8200 [22]. The value of each populated field shall be given as a copy of the relevant octet(s) with the byte ordering unchanged.

6.2.3.4 TCPInformation

Each field of the TCPInformation structure corresponds to a field in the TCP header of the target packet, as defined in IETF RFC 793 [23]. The value of each populated field shall be given as a copy of the relevant octet(s) with the byte ordering unchanged.

The controlBits field shall contain the right-most 6 control bits i.e. the ECN control bits defined in IETF RFC 3168 [24] and IETF RFC 3540 [25] are excluded.

6.2.3.5 UDPInformation

Each field of the UDPInformation structure corresponds to a field in the UDP header of the target packet, as defined in IETF RFC 768 [26]. The value of each populated field shall be given as a copy of the relevant octet(s) with the byte ordering unchanged.

6.2.4 Packet Data Summary Reporting (PDSR)

6.2.4.1 General

The PDSR mechanism in this clause has been superseded by the IPPR mechanism in clause 6.2.5, which should be used in new implementations.

An IPIRIOnly structure may be used to deliver an IRI report summarizing a packet flow within the target's internet access session, if required by the warrant. The rules for determining whether a summary should be reported for a given packet flow (see clause 6.2.4.3) are outside the scope of the present document.

The IPIRIOnly report shall be assigned the same CIN as the other IRI records associated with the access session.

When reporting a packet data summary, the fields in the IPIRIOnly structure are populated as described in Table 4.

Table 4: IPIRIOnly for Packet Data Summary Reporting

Attribute	Contents
iPInformation	Information from the IPv4 or IPv6 header that identifies the packet flow (see clause 6.2.4.2). Populated fields are given as per clauses 6.2.4.2 and 6.2.4.3. All other fields are omitted.
protocolInformation	Information from the layer 4 header that identifies the packet flow, if available. Populated fields are given as per clause 6.2.4.4. All other fields are omitted. TCP header information is provided using the TCPInformation structure. UDP header information is provided using the UDPInformation structure. If no protocol information is provided, "none" is chosen.
iPAggregatedNbrOfPackets	Total number of packets that have been observed as part of the packet flow.
iPAggregatedNbrOfBytes	Total number of bytes summed across all packets that have been observed for this packet flow. For IPv4 it is the sum of the "Total Length" fields across all packets in the summary as defined in Internet Protocol IETF RFC 791 [21], while for IPv6 it is the sum of the "Payload Length" fields across all packets in the summary as defined in Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 8200 [22].
pDSRInformation	Shall be populated according to clause 6.2.4.4.

6.2.4.2 Packet flow

A packet flow is defined as a set of packets within the target's internet access session that have the same:

a) source and destination IP-addresses;

b) IP next-layer protocol;

c) layer-4 ports; and

d) flow label, if the packet is IPv6.

6.2.4.3 Triggers

A packet data summary report for a given packet flow is reported in each of the following circumstances:

- Start of the packet flow within an access session.
- An interim report for a packet flow.
- End of a packet flow, either due to the end of the flow itself (if this can be determined), end of the internet access session, or termination of the interception.

An interim report can be triggered by:

- The expiration of a configurable timer.
- A configurable count threshold (e.g. packet count, byte count) is reached.

6.2.4.4 Use of the IPIRIOnly record

The PDSRInformation structure shall be given as follows.

Table 5: PDSRInformation

Attribute	Contents
summaryTrigger	Specifies the reason for the generation of the packet data summary record.
firstPacketTimestamp	Gives the timestamp of the first packet seen in the packet flow since the last summary record for this packet flow. The timestamp shall be qualified with a timezone.
lastPacketTimestamp	Gives the timestamp of the last packet seen in the packet flow before the creation of this summary record. The timestamp shall be qualified with a timezone.
packetCount	Gives the number of packets seen in the packet flow since the last summary record for this packet flow.
byteCount	Gives the total number of bytes summed across all packets that have been observed for this packet flow since the last summary record for this packet flow. For IPv4 it is the sum of the "Total Length" fields across all packets in the summary as defined in Internet Protocol IETF RFC 791 [21], while for IPv6 it is the sum of the "Payload Length" fields across all packets in the summary as defined in Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 8200 [22].

6.2.5 Internet Protocol Packet Reporting (IPPR)

6.2.5.1 General

The IPIRIPacketReport structure may be used to deliver an IRI report that either:

a) transmits the header of a packet;

b) transmits summary events of a packet flow.

When a report is generated is determined by the triggers that have been defined in clause 6.2.5.2 and national agreement on the configuration of these triggers.

As other IRI messages may be generated along with IPPR reports, the same CIN shall be assigned to all messages if they pertain to the same access session. The CIN assignment requirement also applies to IPPR that is enabled on specific flows while using the ETSI TS 103 120 [27] Traffic Policy [27] mechanism.

To generate an IPPR report, populate it as described in Table 6.

Table 6: IP Packet Report

Attribute	Contents	M/C/O
iPIRIPacketReportObjId	The RELATIVE-OID indicating the report is an IP Packet Report.	M
report	Shall contain one of the PacketReport types. See Table 7.	M

Table 7: PacketReport types

Choice	Contents
header	Shall be chosen if the IP Packet Report contains a PacketReportHeader. See Table 8.
summary	Shall be chosen if the IP Packet Report contains a PacketReportSummary. See Table 9.

Table 8: PacketReportHeader

Choice	Contents	M/C/O
header	A copy of the packet header (including TCP and UDP headers).	M

Table 9: PacketReportSummary

Choice	Contents	M/C/O
header	Shall contain a copy of the header which describes the packet flow on which the report has been generated.	M
indications	Specific fields in the IPv4, IPv6, TCP and UDP headers may have to be replaced in the header attribute. In that case, the specific header attributes shall be set to zero (relevant to the encoding and length of the field) and an indication bit for the specific field that was zeroed shall be set. If IPv6 Extension Headers are present, the headers shall be removed and an indication that they have been removed shall be set.	M
trigger	Specifies the reason for the generation of the IP packet report. See clause 6.2.5.2 for more information.	M
packetCount	Total number of packets that have been observed as part of the reported packet flow during the time period covered by this PacketReportSummary. If the count is not known, it may be omitted.	C
byteCount	Total number of bytes summed across all packets that have been observed for the reported packet flow during the time period covered by this PacketReportSummary. For IPv4 it is the sum of the "Total Length" fields across all packets in the summary as defined in Internet Protocol IETF RFC 791 [21], while for IPv6 it is the sum of the "Payload Length" fields across all packets in the summary as defined in Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 8200 [22]. If the count is not known, it may be omitted.	C
firstTimestamp	The time the first packet in the reported flow was observed during the time period covered by this PacketReportSummary. If the time is not known, it may be omitted.	C
lastTimestamp	The time of the last packet in the reported flow was observed during the time period covered by this PacketReportSummary. If the time is not known, it may be omitted.	C

6.2.5.2 Packet Report Trigger

The following packet report triggers exist:

- flowStart: used at the start of a new packet flow and when intermediate updates are being provided.
- flowEnd: used at the end of a packet flow (if determined by the mediation system).
- flowTimeout: used when a configurable amount of time has passed and no new packets for the packet flow have been observed.
- flowTimerExpiration: used for intermediate packet flow reports at a certain interval (in combination with startOfFlow and endOfFlow).

- flowPacketCount: used for intermediate packet flow reports at a certain number of observed packets within a packet flow.
- flowByteCount: used for intermediate packet flow reports at a certain number of observed transmitted bytes within a packet flow.
- sessionTimerExpiration: used for intermediate reports of all packet flows in an access session at a certain interval (in combination with startOfFlow and endOfFlow).
- sessionPacketCount: used for intermediate reports of all packet flows at a certain number of observed packets within the access session.
- sessionByteCount: used for intermediate reports of all packet flows at a certain number of observed transmitted bytes within the access session.
- reportEnd: used when the MF stops tracking a packet flow, i.e. the access session has ended, the MF stops/restarts or the interception was terminated.

6.2.5.3 Fragmentation

It is important to recognize that MFs typically do not perform TCP reassembly (as this has a significant performance overhead) and as such are not always able to match fragmented IP packets to a specific packet flow: a fragment may not contain the TCP/UDP port information. When generating summaries, this means that such fragments cannot be included in packet and/or byte counters.

7 Content of Communication (CC)

7.1 CC events

CC is provided for every IP datagram sent through the IAP's network that:

a) has the target's IP address as the IP source address;

b) has the target's IP address as the IP destination address.

7.2 HI3 attributes

CC is provided for every intercepted IP datagram. The CC payload contains a stream of octets, containing an exact copy of the intercepted datagram from the IP layer and upwards, i.e. Link layer data is removed from the payload.

7.2A HI3 truncated attributes

Subject to national agreement the CC may be provided as truncated IP datagram for every IP datagram pertaining to the target when the LEA explicitly request delivery of only a specified number of the first octets of all the intercepted IP datagrams. In this case only truncated IP datagrams are delivered via HI3 using the IPTruncatedPacket structure.

Table 10: IPTruncatedPacket attributes

Attribute	Contents
truncatedPacket	Copy of the truncated datagram from the IP layer. Shall be chosen only when the LEA explicitly requires the truncation mechanism to be applied for the particular interception.
originalLength	Original length in octets of the IP datagram. If the truncation is applied on an IP datagram before it reaches the mediation function and the original length is not available via other means, it may be omitted.

7.3 CC without session context

See clause 5.2.7, option 1.

8 ASN.1 for IRI and CC

The ASN.1 [14] definitions are given in file *IPAccessPDU,ver20.asn* contained in archive ts_10223203v031601p0.zip which accompanies the present document.

The *IPAccessPDU,ver20.asn* file also refers to:

- IETF RFC 2132 [15];
- ISO 3166-1 [16].

ETSI TR 102 205 [i.1] gives an overview of the relevant Object IDentifiers (OIDs) used in ASN.1 modules of the Lawful Intercept specifications and points to the specification where the modules can be found.

Annex A (informative): Stage 1 - RADIUS characteristics

A.1 Network topology

A.1.0 RADIUS deployment options

RADIUS can be deployed as one or more RADIUS servers acting on their own or in combination with a RADIUS proxy. Clause A.1 provides an overview of the differences between the two approaches.

A.1.1 RADIUS server

The RADIUS server approach is commonly seen in cases where the Internet access is provided by the same party that provides the Access Network. This situation is depicted in Figure A.1.

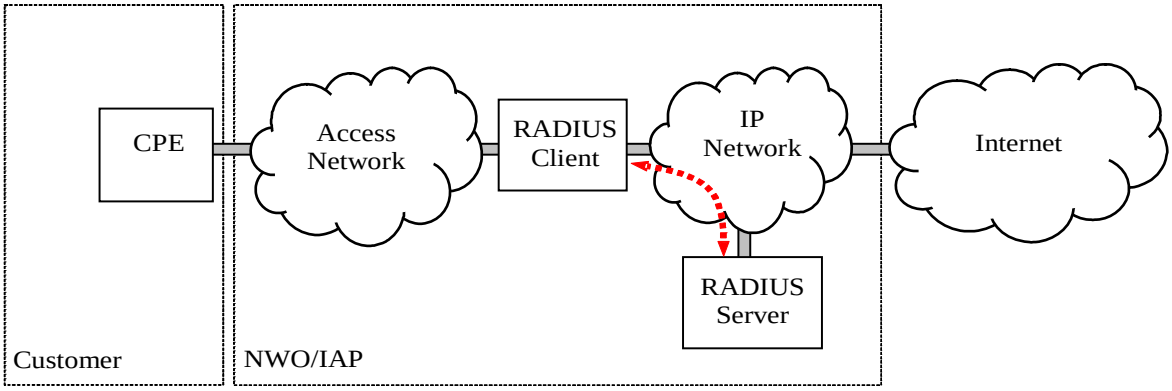


Figure A.1: RADIUS server

In this approach, the device that handles connection establishment is the RADIUS client and communicates with the RADIUS server directly. Depending on the type of access network and the network architecture, the RADIUS client can be a NAS, Edge router, GWR or CMTS.

The RADIUS client requests authentication and authorization for a given user by handing the user-provided username and password to the RADIUS server. The RADIUS server will verify the password and authorization against a customer database and, in the case of a successful result, will return an Access-Accept result to the client that may include an IP address to be assigned to the user.

Network based interception of both assignment and deassignment of IP addresses is performed between the RADIUS client and the RADIUS server. Alternatively, the RADIUS server can be extended with a function that will forward IP address assignment information to the interception function.

If the IP address is assigned by the NAS or by a DHCP server, the IP address will be reported in an accounting packet. In this case, the interception of IP addresses is done between the RADIUS client and RADIUS Accounting server (see clause A.3.2). Alternatively the RADIUS Accounting server can be extended with a function that will forward the IP address assignment information to the interception function.

A.1.2 RADIUS proxy

In case the Access Network Provider (ANP) is not the same party as the Internet Access Provider (IAP), the Access Network Provider (ANP) 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 the case the Access Network Provider (ANP) provides its services to multiple IAPs, 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.

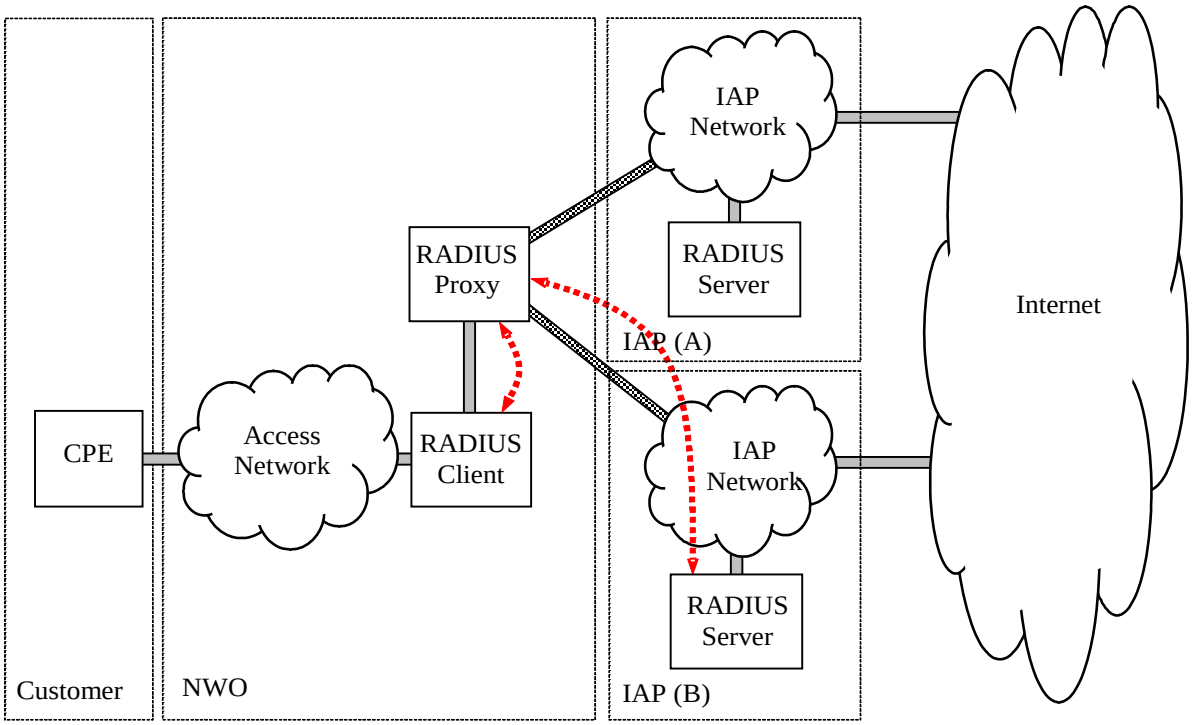


Figure A.2: RADIUS proxy

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 NWO.

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 de 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@example.com" indicates user "foo" at IAP "example.com", the RADIUS Proxy could forward the RADIUS requests to the RADIUS server for IAP "example.com".

If IP address assignment is done by the NAS operated by the NWO, 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.

A.2 RADIUS service

A.2.1 Authentication service

The basic RADIUS service, which provides authentication and authorization, is specified in IETF RFC 2865 [8] and IETF RFC 2869 [17] which defines the relevant key features of the RADIUS service as follows.

Purpose

Managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by managing a single "database" for users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (for example, SLIP, PPP, telnet, rlogin).

Client/Server model

- A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.
- RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.
- A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of Authentication servers.

Network security

- Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

Flexible authentication mechanisms

- The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.

A.2.2 Accounting service

RADIUS Accounting is specified in IETF RFC 2866 [9] and IETF RFC 2869 [17] which define the relevant key features of the Accounting service as follows.

Purpose

IETF RFC 2866 [9] extends the use of the RADIUS protocol to cover delivery of accounting information from the Network Access Server (NAS) to a RADIUS Accounting server.

Client/Server model

- A Network Access Server (NAS) operates as a client of the RADIUS Accounting server. The client is responsible for passing user accounting information to a designated RADIUS Accounting server.
- The RADIUS Accounting server is responsible for receiving the accounting request and returning a response to the client indicating that it has successfully received the request.
- The RADIUS Accounting server can act as a proxy client to other kinds of Accounting servers.

Network security

- Transactions between the client and RADIUS Accounting server are authenticated through the use of a shared secret, which is never sent over the network.

The RADIUS Authentication server and the RADIUS Accounting server may be implemented as a single entity or as separate entities.

A.2.3 IPv6

The IPv6 specific expansion of the RADIUS Authentication and Accounting are specified in the following IETF RFCs:

- IETF RFC 3162 [18].
- IETF RFC 4818 [19].
- IETF RFC 6911 [20].

A.3 RADIUS protocol

A.3.1 Authentication protocol

This clause outlines the basic message exchange for RADIUS authentication. Apart from authentication of plain user-provided credentials, RADIUS supports generic challenge/response authentication as well as the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP). For more detail on these authentication protocols is referred to IETF RFC 2865 [8].

For authentication of users, a RADIUS client exchanges of messages with a RADIUS server over UDP port 1812. Figure A.3 depicts this message exchange.

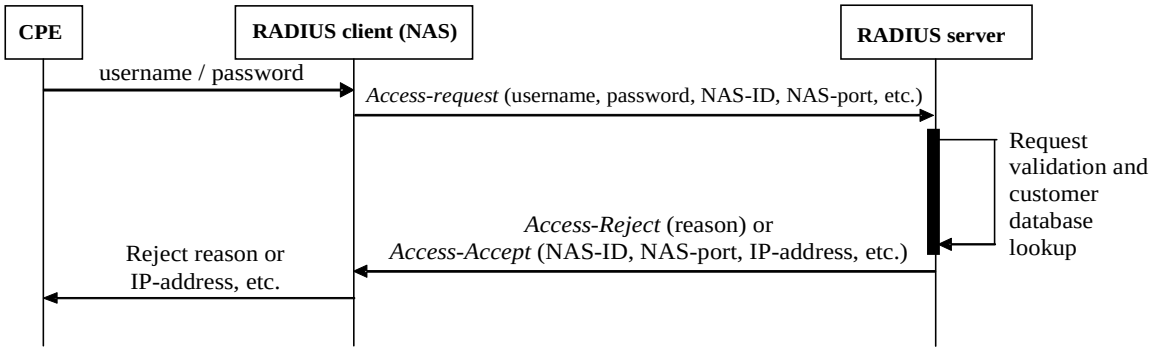


Figure A.3: Basic authentication message exchange

In Figure A.3, the CPE provides the NAS with user credentials, i.e. username and password. The NAS encrypts the password, assembles an Access-Request and sends this to the RADIUS server. The RADIUS server decrypts the password by means of a shared secret, validates the attributes and performs a customer database lookup. If the user is not known, the password is incorrect or the user is not allowed to use the service, the RADIUS server will return an Access-Reject message. If the password is correct and the user is allowed to access the NAS and NAS port in question, the RADIUS server will return an Access-Accept message. In the approach depicted above, the Access-Accept message will contain the IP address for the user as well as other configuration information that will allow the user to set-up the IP stack for proper IP communication.

If communication from the NAS to the RADIUS server is established via a RADIUS proxy, as is described in clause A.1.2, it may be the case that the IP address is assigned by the RADIUS proxy as opposed to the RADIUS server. In other cases, the IP address may be assigned by the NAS from a locally configured address pool and not by a RADIUS server or proxy. In the latter two cases, the IP address will be communicated to the RADIUS server in an Accounting-Request Start message that is described in clause A.3.2.

A.3.2 Accounting protocol

This clause outlines the basic message exchange for RADIUS accounting. For accounting purposes, a RADIUS client exchanges messages with a RADIUS Accounting server over UDP port 1813. Figure A.4 depicts this message exchange.

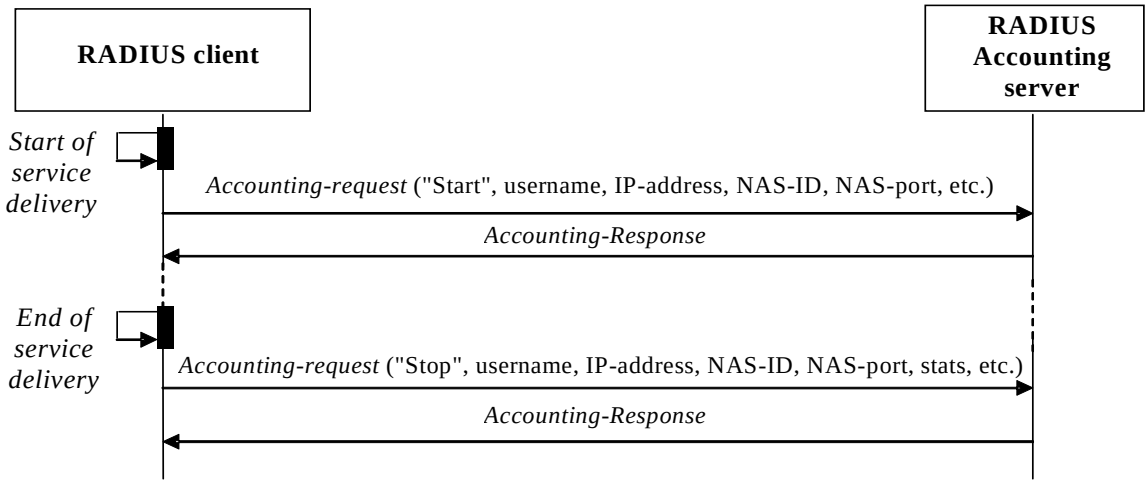


Figure A.4: Accounting message exchange

At the start of service delivery to the user, the RADIUS client sends an Accounting-Request Start message to the RADIUS accounting service. The message will contain various attributes identifying the session. Amongst others, username, IP-address, NAS-ID and NAS-port may be present. The RADIUS Accounting server will acknowledge the Accounting-Request Start by sending an Accounting-Response. If the Accounting-Request and Response are to be used for IRI, near-real-time accounting is required, since batch-accounting would result into unacceptable delays in IRI creation and IP address provision of IP interception equipment.

At the end of service delivery, either because the user logged of or due to accidental disconnection of the user, the RADIUS client sends an Accounting-Request Stop message to the RADIUS Accounting service. The message will contain various attributes identifying the session as well as statistics indicating the duration of the session and the amount of data sent and received. Again the attributes username, IP-address, NAS-ID and NAS-port may be present. The RADIUS Accounting server will acknowledge the Accounting-Request Stop by sending an Accounting-Response.

In some cases, depending on service and configuration, the NAS may send an Accounting-Request Interim-Update message to report the assignment of an IP address. The Interim-Update message can be sent when new information is available or on a periodic basis.

A.4 RADIUS main attributes

This clause outlines some of the RADIUS attributes relevant for binding a "target identity" to an IP address. For a full overview of all attributes and their presence in the various request messages is referred to IETF RFC 2865 [8], IETF RFC 2866 [9], IETF RFC 2869 [17], IETF RFC 3162 [18], IETF RFC 4818 [19] and IETF RFC 6911 [20]. Many NAS vendors have implemented vendor-specific RADIUS attributes. Vendor-specific attributes are not included in the present document.

Table A.1: RADIUS attributes

Field	Description
User-Name	The username provided by the user
NAS-IP-Address	The IP address of the NAS. Usually, either the NAS-IP-Address or the NAS-Identifier is present
NAS-Identifier	A text string identifying the NAS originating the Access-Request
NAS-Port	A unique identifier for the port used by the user on the particular NAS
NAS-Port-Identifier	A text string which identifies the port used in the NAS which is authenticating the user
Framed-IP-Address	The IPv4 address assigned to the user
Framed IPv6 Address	IPv6 Address assigned to the NAS facing interface of the host or Residential Gateway

Field	Description
Framed IPv6 Prefix	IPv6 prefix assigned to the user
Delegated IPv6 Prefix	IPv6 prefix to be delegated to the user
Called-Station-Id	The NAS ISDN/PSTN number as was dialled by the user
Calling-Station-Id	The ISDN/PSTN number the user dialled from
Callback-Number	If call-back is used by the NAS, the ISDN/PSTN number at which the NAS calls the user
Framed Route	IPv4 routing information to be configured for the user on the NAS
Framed IPv6 Route	IPv6 routing information to be configured for the user on the NAS

A.5 RADIUS interception

A.5.0 Introduction

Clause A.5 presents a possible approach to the processing of RADIUS packets in order to obtain dynamic IP addresses as well as to produce IRI messages for LI of Internet Access Services (IASs). The presented approach aims at dealing with the many possible variants of RADIUS implementations in a single generic functional model. There may be room for more sophistication or optimization of the presented model, but in essence it can be implemented as is.

A.5.1 Collecting RADIUS packets

The model is a state machine that requires to be fed with all RADIUS packets that are exchanged between the RADIUS client and the RADIUS server or proxy. As stated in clauses A.1.1 and A.1.2, the collection of the RADIUS packets can be achieved by either a network sniffer function, that sniffs and forwards all RADIUS packets exchanged between the client and server or proxy or by a RADIUS application add-on that forwards the RADIUS packets from the RADIUS platform to the LI platform.

A.5.2 Processing RADIUS packets

A.5.2.1 Mapping events to RADIUS packets

The RADIUS IETF RFC 2865 [8], IETF RFC 2866 [9] , IETF RFC 2869 [17], IETF RFC 3162 [18], IETF RFC 4818 [19] and IETF RFC 6911 [20] specify most of the RADIUS attributes in the various RADIUS packets as optional. On the other hand, depending on the RADIUS implementation, many of the RADIUS attributes may occur multiple times in different RADIUS packets. This unpredictability requires a generic and flexible approach in order to prevent the need for customization of the LI platform for different RADIUS implementations from different vendors.

Processing RADIUS packets has two main objectives; obtaining IP addresses and the creation of IRI.

For obtaining a dynamic IP address, when the IP address is assigned by the RADIUS server, the Access-Request and Access-Accept packet need to be processed. Alternatively, in an architecture where a RADIUS proxy outside the infrastructure of the IAP is handing-out the IP addresses, or when the NAS is allocating IP addresses, the required information may only be available in the Accounting-Request Start or Interim-Update message.

As clause 4.3 lists, creation of IRI is required:

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).

These requirements translate to the events:

a) Logon Attempt.

b) Logon Success.

c) Logon Failed.

d) Interim-Info.

e) Logoff.

f) Silent Logoff.

Table A.2 provides an overview of the Radius packets that, depending on the RADIUS implementation, may contain relevant information for IRI for each of the events.

Table A.2: Mapping events to RADIUS packets

	Access-Request	Access-Accept	Access-Reject	Accounting-Request Start	Accounting-Request Interim-Update	Accounting-Request Stop	Accounting-Response Start	Accounting-Response Stop
Logon Attempt	√							
Logon Success		√		√			√	
Logon Failed			√					
Interim-Info					√	√		√
Logoff						√		√
Silent Logoff		√		√		√	√	√

Typically the Accounting-Request packets will contain all information required for the creation of an IRI record. However, it is advised to wait for the occurrence of the related Accounting-Response record before the IRI message is created. The latter event will not add to the already known information, but waiting for the related Account-Response packet prevents spoofing of the LI system by inserting false Accounting-Request packets into the system.

A.5.2.2 Functional model

From Table A.2, the high-level functional model for the processing of RADIUS packets in Figure A.5 was constructed. The model continuously processes RADIUS packets and acts like a sieve, ensuring that each of the relevant RADIUS packet types is processed by the appropriate function.

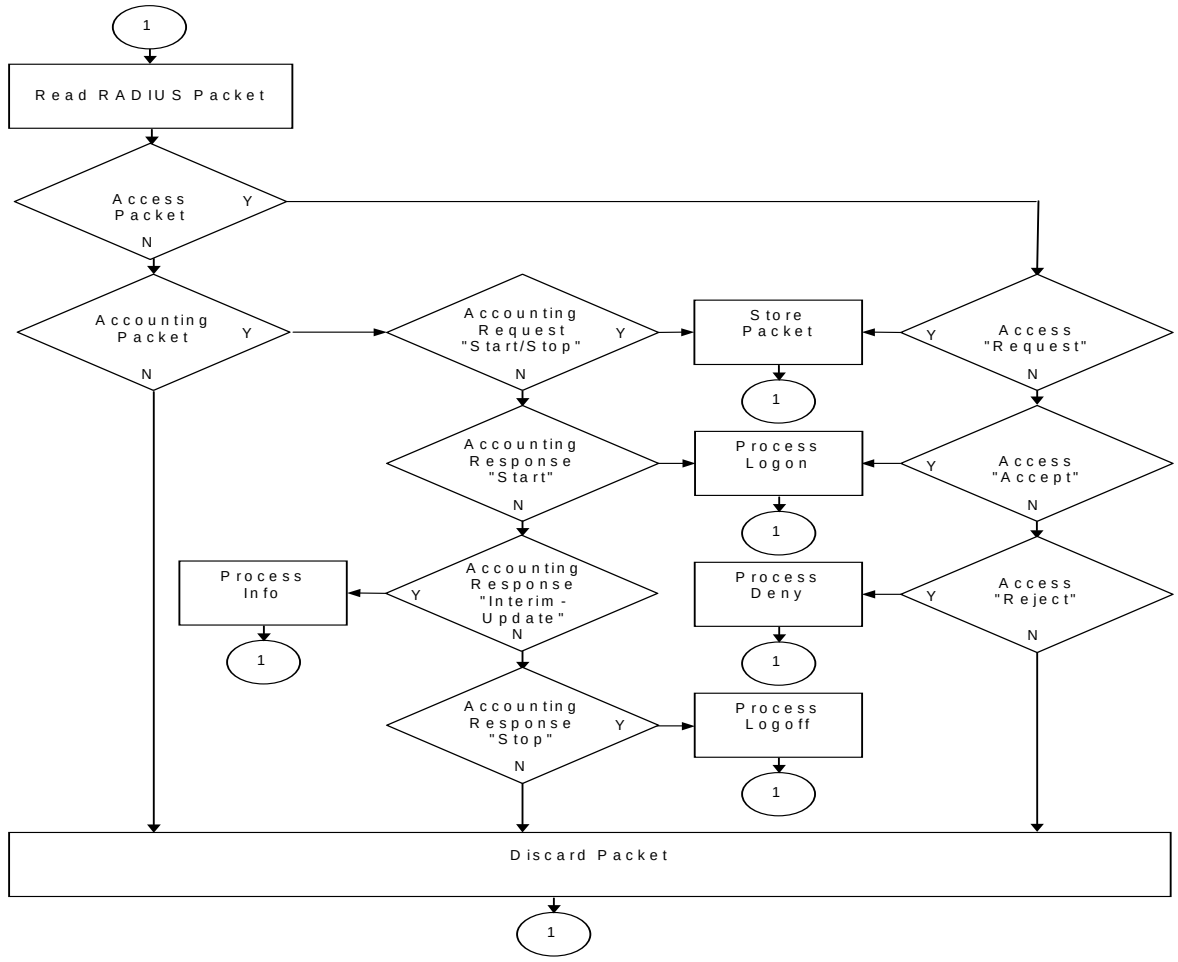


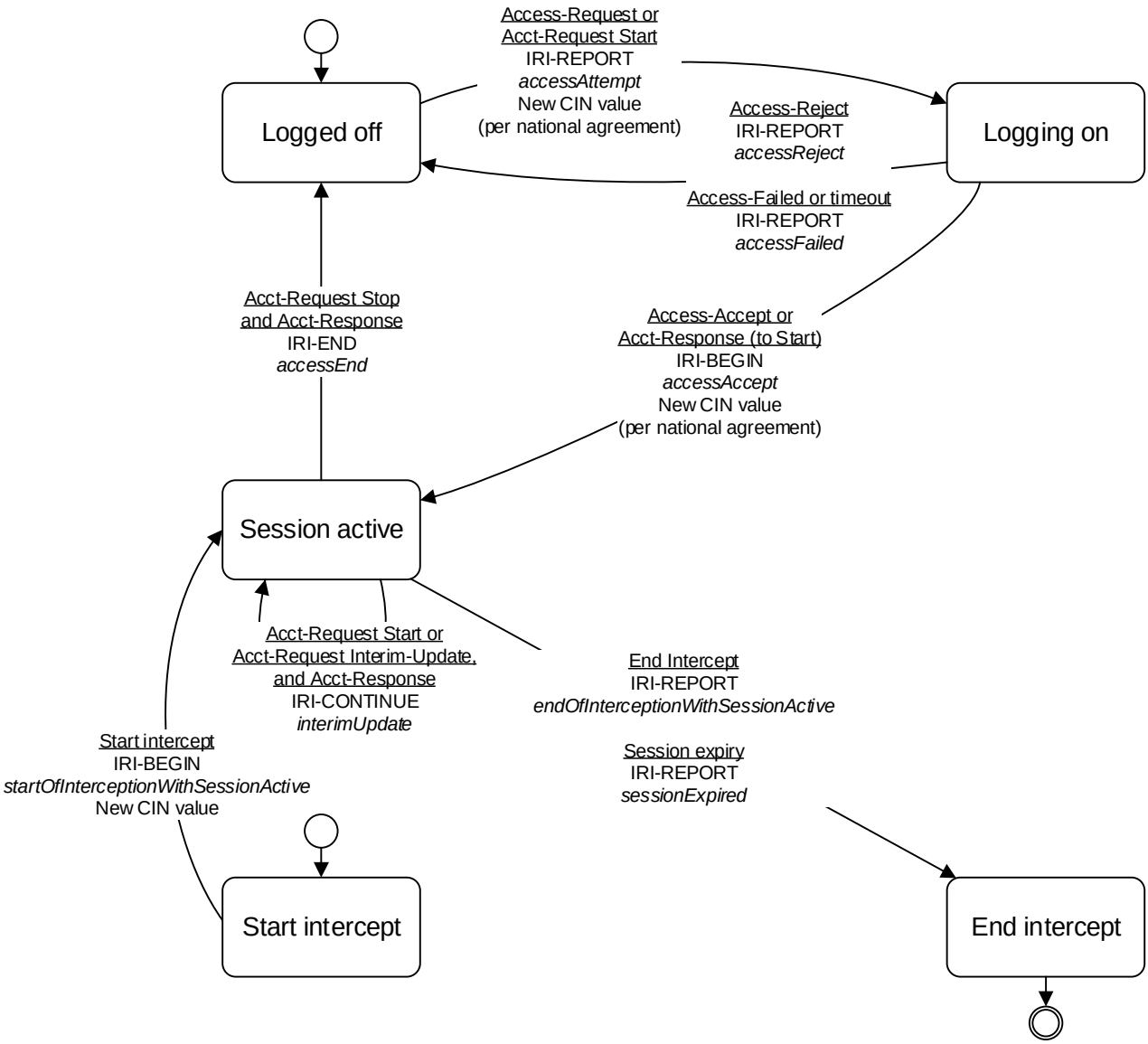
Figure A.5: Functional model for processing RADIUS packets

The following explains each of the processing functions in more detail.

Store Packet

In order to track the state of users using the Internet Access Service (IAS), information derived from various types of RADIUS packets needs to be stored to allow correlation with other packets in a later stage of processing. The key used for storing information, and in a later stage retrieving information, needs to be selected as such that all RADIUS packets related to a single Internet session hold the same unique key. Possible combinations are NAS-ID and NAS-Port, NAS-IP-address and NAS-Port, NAS-IP-Address and Accounting-Session-ID or NAS-ID and Accounting-Session-ID. As stated in IETF RFC 2866 [9], if the NAS includes the Accounting-Session-ID in the Access-Request packet it will use the same value in the Accounting-Request messages for that session.

The various states a session can go through is shown in Figure A.6.



NOTE 1: According to IETF RFC 2865 [8], in the case in which the NAS receives an Access-Accept but cannot support the attributes received, it treats the Access-Accept as if it were an Access-Reject. In this case, the RADIUS Accounting server might receive an Accounting-Request Stop without receiving an Accounting-Request Start. If the NAS does not generate a message to the RADIUS server indicating the session has been dropped, the system might consider the session still active. Actions taken for this case are for further study.

NOTE 2: Session expiry may occur from any state for an existing interception session.

Figure A.6: State diagram for a RADIUS session

In order to track the outcome of a logon attempt, the Access-Request packet needs to be stored and later correlated with the appropriate Access-Accept or Access-Reject packet. To prevent spoofing, Accounting-Requests need to be correlated with Accounting-Responses; the Accounting-Requests need therefore to be stored as well.

The Target-Identity used to identify a target session is typically User-name or Calling-station-ID. However, any other user specific attribute or combination of user specific attributes can be used for this purpose.

Logon-attempt: Whenever an Access-Request packet is stored and the Target-identity in the packet is on the target-list, the function for creating and sending of an IRI-REPORT record needs to be invoked in order to signal the access attempt.

Process Login

Logon: Whenever an Access-Accept packet is encountered, the information from the related Access-Request is retrieved and the two records are correlated. If the Target-identity in the packets is on the target-list, the function for creating and sending of an IRI-BEGIN record needs to be invoked in order to signal a successful logon and the value of all assigned IP Addresses and Prefixes needs to be made available to the IP Interception Function of the LI platform in order to start intercepting IP packets for this particular session. After sending of the IRI record, the Access-Accept packet can be deleted from the store.

Alternatively, if an Accounting-Response to an Account-Request-Start packet is encountered and the Target-identity in the packets is on the target-list, the function for creating and sending of an IRI-BEGIN record needs to be invoked in order to signal the start of the session and if the values of all assigned IP Addresses and Prefixes are made available to the IP Interception Function of the LI platform. If an Accounting-Response to an Account-Request-Start packet is encountered while the IP Interception Function was already active for this target session, the function for creating and sending of an IRI-CONTINUE record needs to be invoked. After sending of the IRI record, the Accounting-Request packet can be deleted from the store.

Multi-logon: In case a target user logs on multiple times using the same credentials, a running interception will already exist with an identical Target-identity, but with a different NAS and/or NAS-Port and IP address. Thus, if the same target Target-identity is encountered multiple times but with different IP addresses, each time the functions for creating and sending of IRI records needs to be invoked and the IP Interception Function needs to be provisioned with the IP addresses of the new session.

Multilink-logon: In a straightforward approach to handling Multi-link logon, Access-Accept and/or Account-Request-Start packets that contain an IP address of 0.0.0.0 may be ignored. For all Access-Accept and/or Account-Request-Start packets that may be related to additional channels logging on and that do contain a valid IP address an IRI-REPORT and IRI-BEGIN records can be sent and the IP addresses can be forwarded to the Interception Function. Since all traffic will be sent over the IP address related to the base-channel, the intercepts on the IP addresses related to the additional channels will remain silent. Although the above approach will work, it is a bit crude; by using Multi-link related attributes that may be available in the RADIUS packets, a more sophisticated approach to handling multi-link logon is conceivable.

In some cases, an Accounting-Stop might be detected without first detecting an Accounting-Start (e.g. if the NAS receives an Access-Accept with attributes it does not recognize). This case is handled as described in the Process logoff clause.

Process Deny

Failed logon: Whenever an Access-Reject packet is encountered, the information from the Access-Request is retrieved and the two records are combined. If the Target-identity in the packets is on the target-list, the function for creating and sending of an IRI-REPORT record needs to be invoked in order to signal a failed logon. After sending of the IRI record, the Access-Request packet can be deleted from the store.

Process Logoff

Logoff: If an Accounting-Response to an Account-Request-Stop packet is encountered and if the Target-identity in the packet is on the target-list, the function for creating and sending of an IRI-END record needs to be invoked in order to signal a regular logout and the values of all assigned IP Addresses and Prefixes need to be made available to the IP Interception Function in order to terminate the running interception. After sending of the IRI record, the Accounting-Request packet can be deleted from the store.

Silent Logoff

Silent-Logoff (Exception handling): If in the function Process Login, any of the Access or Account-Request packets contains an IP address that is already associated to a running interception but with a different username, the LI system is about to over collect; due to an anomaly the Accounting-Request Stop packet for the running interception was most likely missed. The function for creating and sending an IRI-END record needs to be invoked in order to signal logoff and the values of all assigned IP Addresses and Prefixes needs to be made available to the IP Interception Function in order to terminate the interception immediately. In the IRI-END there is an attribute that signals the abnormal interception termination condition.

If in the function Process Login, any of the Account-Request packets contains an IP address that is already associated to a running interception with the same username but with a different Accounting Session ID, the LI system has most likely missed the Accounting-Request-Stop packet for the running interception. The function for creating and sending an IRI-END record needs to be invoked in order to signal logoff and afterwards the function for creating and sending IRI-BEGIN has to be invoked in order to signal the start of a new RADIUS session. A new CIN has to be assigned for both IRI and CC data. As this is a new session for the very same target, the interception within the IP Interception Function can remain active. If the IP Interception Function detects that the intercept subject has disconnected via other means than RADIUS messages, it needs to stop the interception immediately and report the event (for further study).

A.5.2.3 RADIUS spoofing

In order to add additional prevention against spoofing of RADIUS packets, the RADIUS processing engine can be provided with a list of valid NAS-IP addresses, so it can verify the origin of RADIUS packets. However, source IP addresses can be spoofed as well. The best protection against spoofing can be achieved by providing the NAS-Secret (the key used for hashing) to the RADIUS processing engine, so it can verify the hash values provided in the RADIUS packets (see IETF RFC 2865 [8]).

A.5.2.4 Mapping of Acct-Terminate-Cause to endReason

Within IETF RFC 2866 [9] a total of 18 causes of session termination are specified. For simplicity reasons the session termination causes are grouped into five end reasons as specified herein. Therefore, by default the following mapping between RADIUS Acct-Terminate-Case attribute and HI2 endReason attribute has to apply. Any other mapping is subject to national regulation.

Table A.3: Mapping of Acct-Terminate-Cause to endReason

Nr	Description termination cause	endReason			
		Undefined	regularLogoff	connectionLoss	connectionTimeout
1	User Request		√		
2	Lost Carrier			√	
3	Lost Service			√	
4	Idle Timeout				√
5	Session Timeout				√
6	Admin Reset	√			
7	Admin Reboot	√			
8	Port Error	√			
9	NAS Error	√			
10	NAS Request	√			
11	NAS Reboot	√			
12	Port Unneeded	√			
13	Port Preempted	√			
14	Port Suspended	√			
15	Service Unavailable	√			
16	Callback	√			
17	User Error	√			
18	Host Request		√		
NOTE: The reason, leaseExpired is only applicable for DHCP.					

A.5.2.5 Use of Event-Time

With IETF RFC 2869 [17] a new RADIUS parameter, Event-Time, has been introduced for Accounting Request messages. It is subject to national agreement to apply the system time stamp of the MF or the Event-Time provided within the Accounting Request message as startTime or endTime within HI2 respectively.

NOTE: Event-Time should be used if the corresponding IRI is based on the Accounting messages.

Therefore, time synchronization between MF and the ISP network is of importance.

A.5.2.6 Use of targetIPAddress, additionalIPAddress and otherTargetIdentifiers fields

As clause 6.2.1 describes the use of targetIPAddress, additionalIPAddress and otherTargetIdentifiers fields in a generic way, below the specific mapping of the IPv6 Addresses and ranges provided within RADIUS is described.

When the iPVersion parameter is set to value iPV6 following should apply for RADIUS:

- The targetIPAddress field will contain the first (or only) target Framed IPv6 address or if this is not available the first Framed IPv6 prefix range or if this is not available as well the first Delegated IPv6 prefix.
- The additionalIPAddress field will not be populated with any value.
- The otherTargetIdentifiers field will contain the second and subsequent IPv6 target addresses (with or without prefix ranges) if any additional address ranges are assigned to the target service.

When the iPVersion parameter is set to value iPV4andV6 (i.e. where the user service is dual-stacked) following should apply for RADIUS:

- The targetIPAddress field will contain the first (or only) target IPv4 address or subnet range.
- The additionalIPAddress field will contain the first (or only) target Framed IPv6 address or if this is not available the first Framed IPv6 prefix range or if this is not available as well the first Delegated IPv6 prefix.
- The otherTargetIdentifiers field will contain the second and subsequent IPv4 or IPv6 target addresses (with or without subnet or prefix ranges) if any additional address ranges are assigned to the target service.

A.5.3 Mapping RADIUS on the IRI structure

Table A.4, Table A.5 and Table A.6 list which attributes of the IRI structure can be assigned a value if a RADIUS server is used for AAA. Table A.4, Table A.5 and Table A.6 show that values for the IRI attributes can be derived from:

1) the Intercept function (for fixed values or timestamps); or
2) the RADIUS Access-packets; or
3) the RADIUS Accounting-packets.

The corresponding RADIUS parameters to be mapped to the IRI attributes are described in:

- IETF RFC 2865 [8].
- IETF RFC 2866 [9].
- IETF RFC 2869 [17].
- IETF RFC 3162 [18].
- IETF RFC 4818 [19].
- IETF RFC 6911 [20].

Table A.4: Mapping RADIUS on the IRI structure

Attribute	Value derived from		
	Interception Function	**Access attribute**	**Accounting attribute**
accessEventType	NA	Code	Code and Acct-Status-Type
targetUsername	NA	User-name (1)	User-name (1)
internetAccessType	Fixed value	NA	NA
iPVersion	Fixed value	NA	NA
targetIPAddress	NA	Framed-IP-Address (8) & Framed IP-Netmask (9)	Framed-IP-Address (8) & Framed IP-Netmask (9)
targetNetworkID	NA	Calling-Station-ID (31)	Calling-Station-ID (31)
targetCPEID	NA	NA	NA
targetLocation	NA	NA	NA
pOPPhoneNumber	NA	Called-Station-ID (30)	Called-Station-ID (30)
pOPIdentifier	NA	NAS-Identifier (32)	NAS-Identifier (32)
pOPIPAddress	NA	NAS-IP-Address (4) or NAS-IPv6-Address (95)	NAS-IP-Address (4) or NAS-IPv6-Address (95)
pOPPortNumber	NA	NAS-Port (5)	NAS-Port (5)
callBackNumber	NA	Callback-Number (19)	Callback-Number (19)
startTime	IF (system clock)	NA	Event-Timestamp (55)
expectedEndTime	NA	NA	NA
endTime	IF (system clock)	NA	Event-Timestamp (55)
endReason	NA	NA	Inferred from Acct-Terminate-Cause (49)
octetsTransmitted	NA	NA	Acct-Output-Octets (43) & Acct-Output-Gigawords (53)
octetsReceived	NA	NA	Acct-Input-Octets (42) Octets & Acct-Input-Gigawords (52)
rawAAAData	<Free to choose>	<Free to choose>	<Free to choose>
nationalIPIRIParameters	Fixed value	NA	NA
additionalIPAddress	NA	NA	NA
authenticationType	Derived from Auth message type	NA	NA
otherTargetIdentifiers	NA	Framed-IP-Address (8) & Framed IP-Netmask (9)	Framed-IP-Address (8) & Framed IP-Netmask (9)
pOPPortId	NA	NAS-Port-ID (87)	NAS-Port-ID (87)
framedRoute	NA	Framed-Route (22)	Framed-Route (22)

NOTE 1: Although most RADIUS implementations support proprietary attributes, the present document only defines attributes from IETF RFC 2865 [8], IETF RFC 2866 [9] and IETF RFC 2869 [17]. Any attributes defined outside the mentioned RFC can be handed over in the RawAAAData attribute.
NOTE 2: Void.
NOTE 3: (x) indicates the RADIUS IETF Attribute number.

Table A.5: Mapping RADIUS on the IRI structure for IPv6

Attribute	Value derived from		
	Interception Function	**Access attribute**	**Accounting attribute**
accessEventType	NA	Code	Code and Acct-Status-Type
targetUsername	NA	User-name (1)	User-name (1)
internetAccessType	Fixed value	NA	NA
iPVersion	Fixed value	NA	NA
targetIPAddress	NA	Framed-IPv6-Address (168) or Framed-IPv6-Prefix (97)	Framed-IPv6-Address (168) or Framed-IPv6-Prefix (97)
targetNetworkID	NA	Calling-Station-ID (31)	Calling-Station-ID (31)
targetCPEID	NA	NA	NA
targetLocation	NA	NA	NA
pOPPhoneNumber	NA	Called-Station-ID (30)	Called-Station-ID (30)
pOPIdentifier	NA	NAS-Identifier (32)	NAS-Identifier (32)
pOPIPAddress	NA	NAS-IP-Address (4) or NAS-IPv6-Address (95)	NAS-IP-Address (4) or NAS-IPv6-Address (95)
pOPPortNumber	NA	NAS-Port (5)	NAS-Port (5)
callBackNumber	NA	Callback-Number (19)	Callback-Number (19)
startTime	IF (system clock)	NA	Event-Timestamp (55)
expectedEndTime	NA	NA	NA
endTime	IF (system clock)	NA	Event-Timestamp (55)
endReason	NA	NA	Inferred from Acct-Terminate-Cause (49)
octetsTransmitted	NA	NA	Acct-Output-Octets (43) & Acct-Output-Gigawords (53)
octetsReceived	NA	NA	Acct-Input-Octets (42) Octets & Acct-Input-Gigawords (52)
rawAAAData	<Free to choose>	<Free to choose>	<Free to choose>
nationalIPIRIParameters	Fixed value	NA	NA
additionalIPAddress	NA	NA	NA
authenticationType	Derived from Auth message type	NA	NA
otherTargetIdentifiers	NA	Target IP Addresses not listed above: Framed-IPv6-Address (168) Framed-IPv6-Prefix (97) Delegated-IPv6-Prefix (123)	Target IP Addresses not listed above: Framed-IPv6-Address (168) Framed-IPv6-Prefix (97) Delegated-IPv6-Prefix (123)
pOPPortId	NA	NAS-Port-ID (87)	NAS-Port-ID (87)
framedRoute	NA	Framed-IPv6-Route (99)	Framed-IPv6-Route (99)

NOTE 1: Although most RADIUS implementations support proprietary attributes, the present document only defines attributes from IETF RFC 2865 [8] IETF RFC 2866 [9], IETF RFC 2869 [17], IETF RFC 3162 [18], IETF RFC 4818 [19] and IETF RFC 6911 [20]. Any attributes defined outside the mentioned RFC can be handed over in the RawAAAData attribute.
NOTE 2: Void.
NOTE 3: (x) indicates the RADIUS IETF Attribute number.

Table A.6: Mapping RADIUS on the IRI structure for IPv4 and IPv6

Attribute	Value derived from		
	Interception Function	**Access attribute**	**Accounting attribute**
accessEventType	NA	Code	Code and Acct-Status-Type
targetUsername	NA	User-name (1)	User-name (1)
internetAccessType	Fixed value	NA	NA
iPVersion	Fixed value	NA	NA
targetIPAddress	NA	Framed-IP-Address (8) & Framed IP-Netmask (9)	Framed-IP-Address (8) & Framed IP-Netmask (9)
targetNetworkID	NA	Calling-Station-ID (31)	Calling-Station-ID (31)
targetCPEID	NA	NA	NA
targetLocation	NA	NA	NA
pOPPhoneNumber	NA	Called-Station-ID (30)	Called-Station-ID (30)
pOPIdentifier	NA	NAS-Identifier (32)	NAS-Identifier (32)
pOPIPAddress	NA	NAS-IP-Address (4) or NAS-IPv6-Address (95)	NAS-IP-Address (4) or NAS-IPv6-Address (95)
pOPPortNumber	NA	NAS-Port (5)	NAS-Port (5)
callBackNumber	NA	Callback-Number (19)	Callback-Number (19)
startTime	IF (system clock)	NA	Event-Timestamp (55)
expectedEndTime	NA	NA	NA
endTime	IF (system clock)	NA	Event-Timestamp (55)
endReason	NA	NA	Inferred from Acct-Terminate-Cause (49)
octetsTransmitted	NA	NA	Acct-Output-Octets (43) & Acct-Output-Gigawords (53)
octetsReceived	NA	NA	Acct-Input-Octets (42) Octets & Acct-Input-Gigawords (52)
rawAAAData	<Free to choose>	<Free to choose>	<Free to choose>
nationalIPIRIParameters	Fixed value	NA	NA
additionalIPAddress	NA	Framed-IPv6-Address (168) or Framed-IPv6-Prefix (97)	Framed-IPv6-Address (168) or Framed-IPv6-Prefix (97)
authenticationType	Derived from Auth message type	NA	NA
otherTargetIdentifiers	NA	Target IP Addresses not listed above: Framed-IP-Address (8) & Framed IP-Netmask (9) Framed-IPv6-Address (168) Framed-IPv6-Prefix (97) Delegated-IPv6-Prefix (123)	Target IP Addresses not listed above: Framed-IP-Address (8) & Framed IP-Netmask (9) Framed-IPv6-Address (168) Framed-IPv6-Prefix (97) Delegated-IPv6-Prefix (123)
pOPPortId	NA	NAS-Port-ID (87)	NAS-Port-ID (87)
framedRoute	NA	Framed-Route (22) and Framed-IPv6-Route (99)	Framed-Route (22) and Framed-IPv6-Route (99)

NOTE 1: Although most RADIUS implementations support proprietary attributes, the present document only defines attributes from IETF RFC 2865 [8], IETF RFC 2866 [9], IETF RFC 2869 [17], IETF RFC 3162 [18], IETF RFC 4818 [19] and IETF RFC 6911 [20]. Any attributes defined outside the mentioned RFC can be handed over in the RawAAAData attribute.
NOTE 2: Void.
NOTE 3: (x) indicates the RADIUS IETF Attribute number.

Annex B (informative): Stage 1 - DHCP characteristics

B.1 Network topology

A DHCP client may be directly connected to the same local area (broadcast) network as the DHCP server, or it may go through a DHCP Relay Agent to access DHCP server on another (IP) network. The ratio of clients to servers is on the order of tens (in a small enterprise LAN environment) to tens of thousands (carrier network).

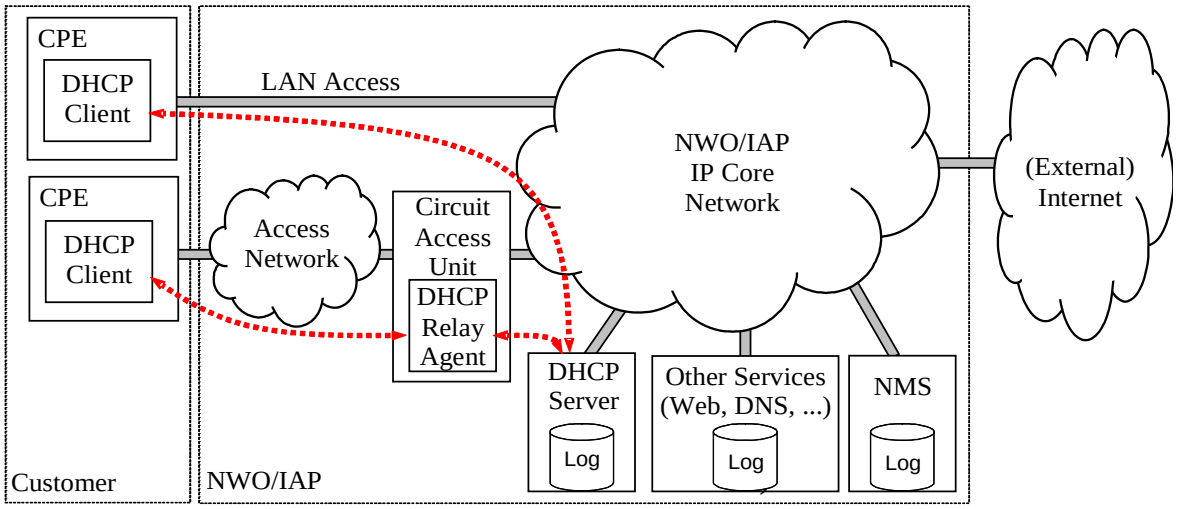


Figure B.1: DHCP Internet access

B.2 DHCP service

DHCP, and BOOTP on which it is based, provide a mechanism by which an Ethernet or Token-ring LAN-attached, TCP/IP host can acquire certain configuration information from a DHCP/BOOTP server. DHCP is typically used in the enterprise and within some carrier networks, particularly cable modem and DSL networks, to temporarily award (lease) IP addresses to attached TCP/IP hosts. This configuration information may also encompass a large number of network and host specific-options, not all of which are necessarily applicable to LI.

EXAMPLE: DNS server address, router address, WINS server address, IP network mask, etc.

Implementations can vary significantly depending on the DHCP implementations in vendor server and client software, as well as the default configurations shipped with the product.

Table B.1 contains parameters of a common open Unix reference implementation.

Table B.1: Common DHCP server configuration options and declarations

Parameter	Description	Data type
Default-lease-time	Default length in seconds that the lease is valid	Numeric
Domain-name	The name of the domain for the specified subnet	Text
Domain-name-servers	A list of name servers for the specified subnet	List of IP addresses
Fixed-address	Static address to assign to a host (supports multiple networks)	List of IP addresses
Group	Starts a group declaration	N/A
Hardware	The type of hardware the network interface has	Hardware-type: text; Hardware
	(currently only Ethernet and token ring are supported)	Address: octets, colon separated
Host	Starts a host declaration	N/A
Host-name	Name to assign to the requesting host	Text
Max-lease-time	Maximum time in seconds the server will grant a lease should the client request a specific lease time	Numeric

Parameter	Description	Data type
Netbios-name-servers	Name of the WINS server	List of IP addresses
Range	Range of IP addresses to assign on the specified network	Low and high IP address
Routers	A list of routers to use	List of IP addresses
Shared-network	Starts a shared-network declaration	N/A
Subnet	Starts a subnet declaration	N/A
Subnet-mask	The subnet-mask of this network, group or host	IP address

When the DHCP server starts, it reads the global configuration parameters from a configuration file, such as the name of the server, the domain for which it is responsible, and so forth. That is, it reads the parameters that will be valid for all the clients (unless they are explicitly changed). DHCP stores the list of addresses in memory for each of the subnets it is serving. When a DHCP client starts, it requests an address from the server. The server looks up an available address and assigns it to the client. Though DHCP is best-known for assigning dynamic IP addresses, it can also assign static addresses to clients if required.

In DHCP terminology, clients "lease" IP addresses. DHCP leases only last a certain amount of time. The default period is typically one day, but can be easily changed. Clients can request leases of a specific duration, but to prevent any machine from holding onto the lease forever, a maximum allowable lease time is usually configured on the server.

B.3 BOOTP protocol

DHCP is carried over BOOTP protocol messages. BOOTP is a client-server protocol, in which the host (also known as client) initiates message exchanges with a server. BOOTP messages are transported in UDP messages using ports 67 (client to server) and 68 (server to client). Each BOOTP message has a fixed format header and a variable format area that contains "options". The header carries information about the operation of BOOTP and the options carry the configuration parameters. There are several DHCP messages that are exchanged between clients and servers; some of those messages will be described in more detail below.

NOTE: In the case of a client using DHCP for initial configuration (before the client's TCP/IP software has been completely configured), DHCP requires creative use of the client's TCP/IP software and liberal interpretation of IETF RFC 1122 [3]. The TCP/IP software SHOULD accept and forward to the IP layer any IP packets delivered to the client's hardware address before the IP address is configured; DHCP servers and BOOTP relay agents may not be able to deliver DHCP messages to clients that cannot accept hardware unicast datagrams before the TCP/IP software is configured.

B.4 DHCP protocol

B.4.0 Overview

DHCP makes use of the BOOTP format, extending the message set by using a BOOTP option to carry the DHCP message type. A client still sends BOOTP REQUESTs, and a server still sends BOOTP REPLYs, but the DHCP message type option indicates what is "really going on". The following sequence serves as a basic example; there are other messages, and many options in the protocol.

When a host connects to a network, it will first locate a DHCP server from which it can obtain configuration information. The host locates a DHCP server by broadcasting a DHCPDISCOVER message, which may include desirable values for parameters (IP address, lease duration, etc.), and a list of requested parameters. Any available DHCP servers receive the DHCPDISCOVER message, and reply to the host with a DHCPOFFER message. The DHCPOFFER message may include the parameters requested by the client, and others the server deems appropriate. The host then selects one of the responding servers to use for subsequent DHCP transactions.

Once the host has selected a DHCP server, it contacts that server with a DHCPREQUEST message, specifying the parameters it requires (including values from the DHCPOFFER, specifically the IP-address). The server determines the appropriate configuration parameters for the host and returns those parameters in a DHCPACK message. Once the host received the DHCPACK message, it configures its TCP/IP stack according to the parameters from the server, and is then ready to use TCP/IP.

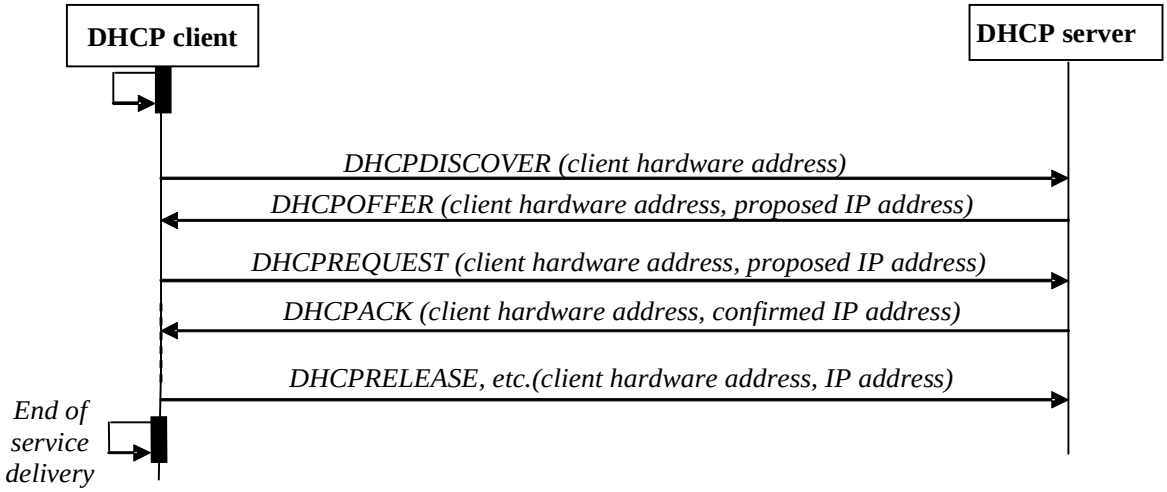


Figure B.2: DHCP exchange

A host that has not been manually configured with an IP address can use DHCP to obtain an address from a server. To allow for reuse of IP addresses, the assignment of an address to a client includes a lease, which represents a period of time in which the host is allowed to use the IP address and in which the server agrees not to reassign the address to another host. Once the lease has expired on an address, the server is free to reassign the address to another host. Address reassignment is useful in conserving IP addresses by reusing addresses from hosts that have left the network.

While a manually configured host may still use DHCP (DHCPINFORM) to acquire other configuration parameters (next hop router, DNS server, etc.) at the beginning of a new service attachment, there would be no explicit DHCP protocol event or time-out associated with service termination, or for that matter anything that distinguishes "start of service". It is presumed that other administrative measures would be applied to detect "start of service" (IRI-BEGIN) and "end of service" (IRI-END).

DHCPREQUEST can be used to "re-confirm" an address assignment upon re-boot of a system.

DHCP can be used to extend the lease on an IP address while the host continues to use the address. Sometime before the lease expires (options specifying the renew interval may be passed in the original DHCPACK), the host sends a DHCPREQUEST message to its DHCP server, requesting the extension of the lease on its IP address. The server records the lease extension and responds with a DHCPACK containing the information about the extended lease. The lease extension process can be completed without interruption of the use of the IP address, so applications using TCP/IP are unaffected.

After a host has left a network, the host no longer requests for extensions on the lease for its assigned IP address, and the lease eventually expires. At this point, the server returns the IP address to its pool of available addresses and can reassign the address to another host. The length of the lease on an IP address and the policy for extending a lease is chosen by the DHCP server administrator.

B.4.1 Address assignment

The DHCP server records the addresses and associated leases that it assigns to hosts. When a host that has been assigned an address is restarted, it first sends a DHCPREQUEST message to confirm that it is still on the correct network for that address. The server compares the address sent by the host in the DHCPREQUEST message to the address the server recorded for the host and sends a DHCPACK to the host to confirm that the client can continue to use the address. If the client has moved to a new network, the server responds with a DHCPNAK, and the client restarts the DHCP process to obtain a new address appropriate to the new network.

A DHCP server identifies a host by its MAC address or (optionally) a client identifier supplied by the host. The address assignments recorded by the DHCP server are indexed by the identifier for the client. Thus, if a host moves from one network to another, its current IP address can be determined by looking in the servers' address assignment records for the most recent address assigned to that host. In the case of an ISP using DHCP for address assignment, the ISP may choose to record other subscriber information such as the subscriber's name or account number with the host MAC address, so that the IP address currently associated with a specific subscriber can be identified.

B.4.2 Message transmission and relay agents

Except when it is extending the lease on an IP address, a host uses link-local broadcast to send DHCP messages. When the server is on the same physical network as the host, the server receives the messages directly from the host. However, this method of message transmission requires that a DHCP server be deployed on every physical network, which can impose significant management overhead. To avoid the requirement for a DHCP server on every network, DHCP relay agents can be used to forward messages between hosts and DHCP servers. A DHCP relay agent, typically implemented in a network element such as a router, forwards the messages broadcast by hosts to a DHCP server, and returns the messages from servers back to hosts. Each DHCP relay agent is configured with the addresses of the available DHCP servers, usually at the same time as the hosting network element.

IETF RFC 3046 [10] defines an extension to DHCP called "relay agent options", which are additional options that can be added to a DHCP message by a relay agent. The purpose of these options is to allow a relay agent to include additional information in the DHCP message that may be used by the server or the relay agent. For example, a relay agent can include information about the port on which it received a DHCP message from a client, so the relay agent can forward the response from the server to the correct port.

There is a proposed relay agent option (draft-ietf-dhc-agentopt-radius-04.txt [i.3]) that combines IEEE 802.1X [i.2] (Port based network access protocol), RADIUS and DHCP to provide authenticated identity information to a DHCP server. This option carries RADIUS authentication information from the network element on which the relay agent is implemented to the DHCP server. In a typical scenario, a network subscriber first gains authenticated access through an IEEE 802.1X [i.2] protocol exchange with the network access device. The network access device uses RADIUS to authenticate the identity of the user attempting to gain access through IEEE 802.1X [i.2]. This access device then caches identity information about the subscriber, obtained through the exchange with the RADIUS server. When the subscriber's host initiates a DHCP exchange, the access device includes the identity information in the message forwarded to the DHCP server. The DHCP server then assigns an IP address to the host and records the identity of the subscriber along with the assigned address.

B.4.3 Security and authentication

The original DHCP protocol specification includes no mechanisms for security or authentication. IETF RFC 3118 [11] specifies an authentication framework and one specific authentication mechanism for DHCP. Using this authentication mechanism, hosts and servers can authenticate the identity of the source of DHCP messages, so that rogue hosts and servers can be ignored. Also, the integrity of the contents of DHCP messages can be guaranteed, so that hosts and clients cannot be attacked by modifying the contents of DHCP messages in transit.

B.5 DHCP main attributes

This clause outlines some of the DHCP attributes relevant for binding a "target identity" to an IP address. DHCP attributes, usually described as options, are encoded as type-length-value tuples. The type enumerations are defined by IANA [i.4], in many cases, the lengths are fixed by the type, but included anyway.

As indicated earlier, the DHCP messages are encoded as BOOTP requests and replies. BOOTP was created to provide minimal configuration to boot a processor, typically something like a router or X-terminal. The BOOTP configuration typically included a filename and server name from which a device could download a boot image. As most client equipment now includes adequate non-volatile storage, DHCP has extended and modified the fields in the BOOTP messages for its own purposes. It still uses the address fields, but DHCP may now use the "filename" and "server name" fields as extensions of the "options" field.

As the encoding of the individual option lengths are limited to 8-bits, some options have to be segmented into multiple instances of the same option, for re-assembly at the receiver (according to IETF RFC 3396 [12]).

Some options have sub-options, further encoded as Type-Length-Value (TLV) within the "value" portion of the option TLV.

Table B.2: Specific attributes of interest

IP Address	The IP address leased by the DHCP server to the client is one of the few identifiers of client traffic which are exposed to the Internet. As it is dynamically assigned, capturing and expeditious dissemination this information about a target is significant. The IP address is encoded as the "yiaddr" ("your IP address") or "ciaddr" ("client IP address") field in the BOOTP header. Non-TLV, fixed length (4 bytes), at a fixed offset in the BOOTP header.
MAC address	The client's MAC address (CHADDR) is specified in the BOOTP header, which encapsulates the DHCP messages. Presumably this is acquired by the client from its LAN MAC interface, although this is by no means fixed: many network interface cards and client operating systems support the capability of setting the MAC address. Devices (network switches) also exist which automatically map the MAC address specified by the client to another presented to the external world. The MAC address is encoded as the "chaddr" ("client hardware address") field in the BOOTP header. Non-TLV, fixed length (16 bytes), at a fixed offset in the BOOTP header. Qualified by the BOOTP-hlen and BOOTP-htype fields.
Lease Time	An IP address is usually leased to the client for a specific period of time (Address Lease Time option 51), often hours or days, after which the lease needs to be renewed by a client DHCP REQUEST (usually unicast to the same server). The Lease Time is TLV-encoded, option 51 (decimal), 32-bits, seconds.
Relay Agent Information	In cable modem (and other) networks, the customer premise equipment acts as a DHCP proxy, and modifies the client DHCP messages to include a unique identifier belonging to the CPE, as distinct from the Ethernet MAC of the customer computer. Presumably this identifier, unlike the customer computer MAC address would not be as easily modified, and may be used by the DHCP server, and other directly connected equipment, for identification purposes. The Relay Agent Information is TLV-encoded, option 82 (decimal), variable length. Agent Remote ID sub-option 2: TLV encoded, variable length (sometimes the MAC address of the cable modem, sometimes an operator-assigned identifier).

B.6 DHCP interception

B.6.1 Introduction

It is believed that an intrusive application add-on to the DHCP server can authoritatively determine when a target has been assigned an IP-address (entry into the BOUND state), the length of the lease, and when the assignment is voided.

A probe-based implementation, however, requires the maintenance of client/server state based on monitored exchanges between the client(s) and server(s) or relay-agent(s). The simple state machine presented here is believed to be sufficient to LI purposes. Note that because there is no authentication of DHCP packets any host could inject falsified packets in an undetectable manner (a fair DoS attack on the DHCP service). A single target specification may yield multiple DHCP clients, for example in a cable modem deployment where there are multiple PCs at the target site.

B.6.2 DHCP packets

DHCP is moderately complex and the sequence and contents of packets may vary considerably depending on the client and server state and configuration, network environment and location in the network. DHCP is a request/response protocol where requests and responses are linked by the xid and client identifier (usually hardware address or *chaddr*):

- DHCPDISCOVER: This BOOTP-Request is the client's attempt to discover DHCP servers. This is usually the initial message in the process, when the client has no record of a previous assignment or address preference.
- DHCPOFFER: This BOOTP-Reply is the server response to the client DHCPDISCOVER message. This contains a *proposed* IP address assignment for the client. It may be appropriate to observe these messages even when not addressed to the target, in the event that the IP-Address assumed to be bound to the target is now offered to some other client (noted below as *conflict*).
- DHCPREQUEST: This BOOTP-Request is the client request for parameters OFFER'ed by one server, and rejecting offers from all other servers, OR extending a lease, OR confirming a previous assignment.

- DHCPACK: This BOOTP-Reply is the server response to DHCPREQUEST (or DHCPINFORM, see below), containing confirmed configuration parameters for client. The response to a DHCPREQUEST includes the IP address assignment, and lease duration. Nominally, this signal is a successful assignment. There is, however, some ambiguity as the client may subsequently respond with a DHCPDECLINE, invalidating the assignment. It may be appropriate to inspect DHCPACKs for clients other than the target in order to detect address conflicts (see DHCPOFFER, above).
- DHCPNAK: This BOOTP-Reply is used when the server rejects a DHCPREQUEST (most likely because of address conflicts).
- DHCPDECLINE: This BOOTP-Request is the client response to DHCPACK, when it knows the address assignment is unsuitable (e.g. ARP request for the same address is answered by another host).
- DHCPRELEASE: This BOOTP-Request is used when the client releases previously assigned address.
- DHCPFORCERENEW: This BOOTP-Reply is used when the server forces the client to attempt to renew the address assignment. This may not be a transparent action from the client's perspective.
- DHCPINFORM: This BOOTP-Request is used when the client attempts to acquire additional local configuration that is not relevant to the IP address assignment. This is usually employed when the client has acquired an IP address assignment through other means (fixed configuration). Note that like a DHCPREQUEST, the server will respond with a DHCPACK to this request, however the DHCP ACK will not include a *yiaddr* or lease-time option.

B.6.3 State machine

B.6.3.0 Overview

As intimated above, a simplified state machine may be adequate for LI purposes. In particular, the distinctions between INIT, INIT-BOOT and SELECTING, REBOOTING and REQUESTING, and RENEWING and REBINDING seem to be of finer granularity than is useful to the LI function. A renaming and combining of like states results in:

- INIT: no address assigned, no (observed) DHCPREQUEST outstanding.
- REQUESTING: a DHCPREQUEST for a target without an assignment has been observed, awaiting a server response.
- BOUND: a DHCPACK has assigned an address to the target - this would also be the "initial state" in the event of a "preload" (see below). Because of the ambiguity introduced by "preload" (see below), one should be prepared to receive DHCPACK and DHCPNAK, and respond appropriately.
- RENEWING: collapses the RENEWING/REBINDING states of IETF RFC 2131 [6] an address has been assigned, but the client's lease is expiring and the client is attempting to renew the lease by sending DHCPREQUEST (DHCPDISCOVER) messages.

B.6.3.1 Mapping DHCP packets to events

DHCP requests and responses are linked via a client-assigned transaction-identifier (xid). It is not immediately obvious whether the LI function needs to track xids to validate requests/responses. As provisioning of targets is asynchronous to the exercise of DHCP by those targets, and probing may be lossy, the LI function should be prepared to receive any DHCP message in any state, and act appropriately.

DHCPDISCOVER and DHCPOFFER: While these are part of the initial client/server handshake they do not of themselves distinguish an "assignment event" for LI. A DHCPOFFER may, however, invalidate a previous assignment by indicating an address assignment conflict. In the BOUND state, receipt of these messages for a target should trigger a transition into RENEWING.

DHCPREQUEST: marks the start of an assignment.

DHCPACK contains all the information necessary to detect and report the assignment of an IP address. Receipt of this message for a target would normally cause a transition into the BOUND state, however in the event that the confirmed IP address (yiaddr) matched one assumed to be assigned to a target, but given to another client, it should mark a transition into the INIT state and an IRI-END.

DHCPNAK: as DHCP does not do any authentication, an "assignment failure" may not have the same significance as a RADIUS "Logon Failure". This message would invalidate a previous target IP address assignment in the process of being RENEW'ed, and transition into the INIT state.

DHCPDECLINE: invalidates a presumed IP address assignment. This is an unfortunate side-effect of the ambiguity of the DHCPACK, transition into INIT state.

DHCPRELEASE: invalidates a previous IP address assignment - transition into the INIT state.

DHCPFORCERENEW: forces client into renew cycle (RENEWING).

B.6.3.2 Timers and administrative events

Lease-timeout: there are several timers associated with DHCP, governing re-transmissions, when to start the renewal process, etc. The one that is relevant to LI is the lease time-out, provided in the DHCPACK (one of several features that distinguishes a response to a DHCPREQUEST and a DHCPINFORM; the former DHCPACK has a lease time, the latter would not).

"Preload": an administrative action to provide the assignment information for a target which would normally be discovered by monitoring the DHCP exchange. This is used when provisioning a target after the target obtains an IP address assignment. This event would affect an immediate transition from "INIT" into "BOUND" state.

B.6.3.3 State information

At minimum, once an assignment is made, either via the DHCP negotiation or administrative command - preload, the LI function should maintain enough information to uniquely identify:

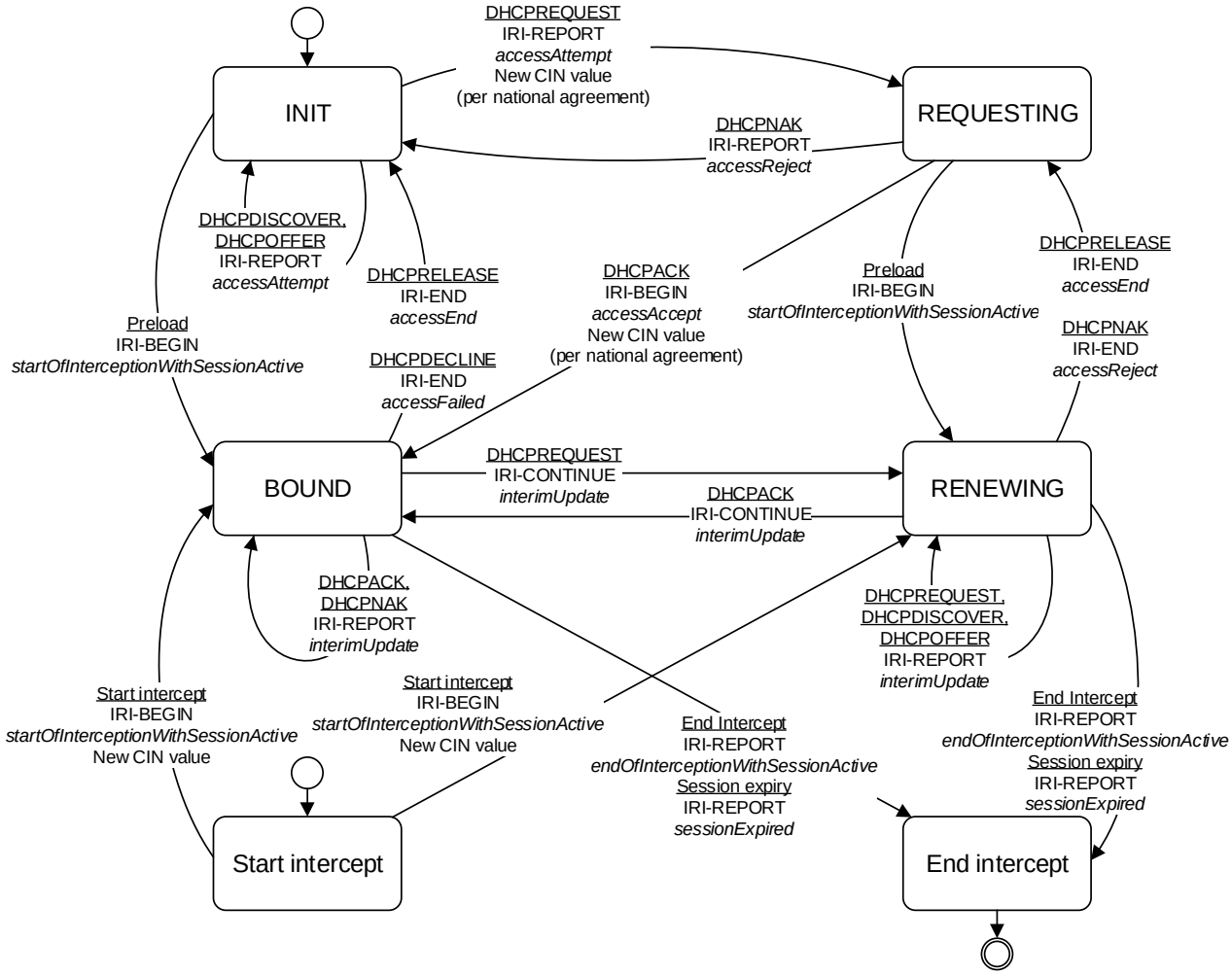
- the client in the case of a renegotiation;
- the allocated address in the case of a re-assignment.

The following information is likely to be necessary information, although it may not be sufficient:

- one or more client identifiers used for targeting and renegotiation. The obvious example of a target identifier is the client MAC address, however there may be two or more ways to identify a single target;
- client IP address;
- remaining lease time;
- associated DHCP server address;
- current state.

NOTE: Not all information is present in all messages, or even in all exchanges.

B.6.3.4 State machine diagram



NOTE 1: Figure B.3 is by no means complete or authoritative.
NOTE 2: Session expiry may occur from any state for an existing interception session.

Figure B.3: State diagram for a DHCP session

B.6.4 Mapping DHCP on the IRI structure

An event which signals a new assignment (DHCPACK) will be reported as an IRI-BEGIN, a renewed lease will be forwarded as an IRI-CONTINUE, and any event that signalled the termination of an assignment, including a conflicting DHCPOFFER, will be forwarded as an IRI-END.

IRI-BEGIN should include at least the target identifier, the IP address assigned, the client-identifier(s), the server IP address and the lease timeout.

IRI-CONTINUE should include at least the target identifier, the IP address assigned, the client-identifier(s), the server IP address and the lease timeout.

IRI-END should include at least the target identifier, the IP address assigned, the client-identifier(s) and the server IP address.

Table B.3: Mapping DHCP on the IRI structure

Attribute	Option [RFC defined in]
accessEventType	Inferred
targetUsername	Option 82, sub-option 2 (IETF RFC 3046 [10]) or chaddr (IETF RFC 2131 [6])
internetAccessType	Fixed value
iPVersion	Fixed value
targetIPAddress	yiaddr (IETF RFC 2131 [6])
targetNetworkID	chaddr (IETF RFC 2131 [6])
targetCPEID	DHCP Relay Agent Information (for further study)
targetLocation	NA
pOPPhoneNumber	NA
pOPIdentifier	NA
pOPIPAddress	giaddr (IETF RFC 2131 [6]) or DHCP server IP-address
pOPPortNumber	Option 82, sub-option 1 (IETF RFC 3046 [10])
callBackNumber	NA
startTime	IF System clock
expectedEndTime	Current time (upon receipt of DHCP-ACK) plus IP Address Lease Time (IETF RFC 2131 [6])
endTime	IF System clock
endReason	Inferred
octetsTransmitted	-
octetsReceived	-
rawAAAData	<Free to choose>
nationalIPIRIParameters	Inferred
additionalIPAddress	yiaddr (IETF RFC 2131 [6])
authenticationType	Derived from Auth message type
otherTargetIdentifiers	yiaddr (IETF RFC 2131 [6])

NOTE 1: Depending upon the network configuration, Option-82 may not be present, in which case chaddr may be a more appropriate TargetUserName. Sub-option2 of Option 82 may contain various kinds of information, depending on the particular DHCP implementation. In a DHCP environment, TargetUsername is unlikely to be a user name, however, it is the piece of information that uniquely identifies the Target access point. It is more likely to be a MAC address or a serial number from the cable-modem.

NOTE 2: POPIPAddress (giaddr (IETF RFC 2131 [6]) or DHCP server IP-address): In cable networks, the DHCP servers are often centrally located, and service a very large network of cable headends (CMTS) and customer modems. In these networks, giaddr (IETF RFC 2131 [6]) may be a more accurate identifier as it may in fact identify the CMTS (cable headend). In smaller, non-cable networks, where the DHCP server is within the same broadcast domain as the client, the DHCP-server IPAddress itself may be the closest approximation to the POPIPAddress.

NOTE 3: TargetIPAddress (yiaddr (IETF RFC 2131 [6])): It is important to note that yiaddr should only be considered "bound" to the client when it appears in a DHCP-ACK message. For example, yiaddr is also set in the DHCP-OFFER, in which case it is only a "possible" IP address, and in the DHCP-DISCOVER, it would be zero.

NOTE 4: TargetNetworkID (chaddr (IETF RFC 2131 [6])): For the non-cable case, this may be the "targeting" information (that is the client's fixed MAC address). In a cable network it may be the MAC address of the customer's router or PC NIC card, and discovered only by matching the option 82 information.

NOTE 5: Void.

Annex C (informative): IP IRI interception

C.1 Introduction

Concepts of what constitutes IRI may differ, resulting in alternative IP interception requirements and implementations. This annex contains an alternative specification that limits IP IRI handover to signalling information based on individual IP frames, and excludes signalling in any encapsulated frames such as TCP or UDP, where such exclusion may be required. This annex describes an approach for implementing this option.

C.2 Requirements

[C.2.1] If IP IRI is delivered, the CC from which the IRI is derived will not be delivered.

[C.2.2] IP IRI will only contain information derived from IP header; and no data from any encapsulated layer headers such as UDP or TCP, or higher layers will be included.

[C.2.3] The IP IRI PDU may contain values derived from all IP layer Header fields, both IPv4 and IPv6 headers.

[C.2.4] Depending on implementation requirements, different IP layer header fields may be included in the IP IRI PDU. The implementing parties effect selection of the fields.

C.3 Proposed implementation

Since the optional IP layer header fields are subject to possible exclusion from the IP IRI PDU, it is recommended to implement a configuration option in the Interception Function that allows for flagging individual header-fields for in - or exclusion.

If the LI implementation derives the IP IRI from network statistics, such as those being defined in IETF's IPFIX Working Group, in agreement between CSP and the authorities, IP IRI may be delivered as aggregated records as opposed to "per packet IRI". In this approach the number of packets and the number of bytes included in the aggregated IRI record is provided in the iPAggregatedNbrOfPackets and iPAggregatedNbrOfBytes fields of the ASN.1.

Annex D (informative): TCP and UDP IRI interception

D.1 Introduction

If IRI were to be provided for transport layer traffic (e.g. UDP, TCP), i.e. above the IP layer, the requirements listed in this annex provide a guideline for designing and implementing a solution for unicast traffic. Support for multicast traffic is for further study.

Depending on national legislation, it would not be appropriate for IAPs to deliver IRI based on information above layer 3, since the communication on level 4 and up are not provided by the IAP, it is considered User data and should therefore be considered CC.

However, some CSPs use TCP and UDP port information for support of services (e.g. traffic analysis, filtering, QoS, billing). In this case, the TCP or UDP information may be considered IRI.

In this context "IP layer 4" is a reference to the attempt to squeeze TCP/IP into the OSI reference model, in which case all protocols that run directly on top of IP are considered "layer 4". No information above layer 4 is known or interpreted.

If encryption such as IPSEC is used between the intercept subject and the associate, then IRI will not be available for TCP or UDP.

D.2 Requirements

Requirement Definitions

TCP Flow	A TCP flow can be identified by the socket pair (IP source address, TCP source port, IP destination address, TCP destination port). A TCP flow begin can be identified from the detection of a SYN. A TCP flow end can be identified by the FIN or RST bits in a TCP session.
UDP Flow	An UDP flow can be identified by the socket pair (IP source address, UDP source port, IP destination address, UDP destination port). An UDP flow begin can be identified from the recognition of a previously unknown socket pair. An UDP flow end can be identified by a time interval with no traffic over the socket pair.
IP Flow	An IP flow can be identified as a non-UDP Flow, non-TCP Flow and the IP-tuple (IP source address, IP destination address, Protocol Type). An IP flow begin can be identified from the recognition of an unknown IP-tuple. An IP flow end can be identified by a time interval with no traffic over the IP-tuple.

D.3 HI2 requirements

[D.3.1] When present, the TCP source and destination port may be considered IRI.

NOTE 1: This information is control information that can be used to identify applications running over TCP and traffic analysis.

[D.3.2] When present, the UDP source and destination port may be considered IRI.

NOTE 2: This information is control information that can be used to identify applications running over TCP and in traffic analysis.

[D.3.3] The HI2 interface should support the ability to deliver an IRI-Begin-record whenever a Flow has begun without delivering the contents of the TCP or UDP segments.

NOTE 3: This begin event is, to a degree, required by the delivery protocol and can be used as a trigger to the LEA or the LEA collector that a communication is beginning.

[D.3.4] The HI2 interface should support the ability to deliver an iRI-End-record whenever a Flow has ended without delivering the contents of the TCP or UDP segments.

NOTE 4: This end event is, to a degree, required by the delivery protocol and can be used as a trigger to the LEA or the LEA collector that a communication is ended or can provide gross level information about the communication.

[D.3.5] The HI2 iRI-Begin-record should contain the IP addresses involved in an intercepted flow.

NOTE 5: This information is necessary for the LEA to identify the communicating parties.

[D.3.6] The HI2 iRI-Begin-record should contain the TCP ports involved in an intercepted TCP flow.

NOTE 6: This information is necessary to assist the LEAs in identify the communicating applications.

[D.3.7] The HI2 iRI-Begin-record should contain the UDP ports involved in an intercepted UDP flow.

NOTE 7: This information is necessary to assist the LEAs in identify the communicating applications.

[D.3.8] The HI2 iRI-Begin-record may contain a timestamp indicating the time a flow start was detected.

[D.3.9] The iRI should be able to contain the number of bytes transferred from the identified target and the number of bytes transferred to the identified target. This byte count should include all Layer 3 and above bytes seen by the interception equipment for the targeted flow including retransmissions by higher level protocols such as TCP.

NOTE 8: This information provides the LEA will an indication of the amount of information transferred between the endpoints.

[D.3.10] The HI2 iRI-End-record may contain a timestamp indicating the time a flow end was detected.

D.4 HI3 requirements

[D.4.1] HI3 delivery should be identical to IP content delivery.

NOTE: Anything less would be incomplete data.

D.5 General requirements

[D.5.1] All timeout intervals are set via HI1 and are outside the scope of the delivery function.

Annex E (informative): Considerations regarding publicly exposed IP addresses

As of clause 6.2.1.2 a publicly exposed IP address that is known to be associated with the target via NAT translation might be available at the MF. Besides the requirement that the respective IP address is available, clause 6.2.1.2 also requires that the respective mapping between the exposed IP address and the IP address being not exposed is valid.

The aforementioned conditions regarding availability and validity may for example be fulfilled when a static one-to-one mapping between non-exposed and the respective publicly exposed IP address is used by the IAP or if the respective lookup of any publicly exposed IP address can be executed in reasonable time, e.g. in near real-time, by the MF. Furthermore, these conditions may also be partially fulfillable in scenarios where the mapping is not static, but the respective IP address assignment rate is dynamic, but rather low in average.

There might be situations where a valid mapping might not be available for the LI system at all. This might for example be the case if the assignment of target IP addresses changes with such a high frequency, i.e. the sessions are that short, that the correlation between the target IP address and any publicly exposed IP address cannot be performed by reasonable technical means, which might in particular be likely in situations where IP address assignment rate is high and where the involved clocks within the IAP's network functions / elements (including the MF) are not well synchronized. Also in this respect, "time synchronization between MF and the ISP network is of importance", as already pointed out in clause A.5.2.5. On the other hand, and especially in large IT networks, which sometimes consist of a wide variety of subnetworks or IT systems, it is quite common for each subnetwork or system to be time synchronous in itself, but the subnetworks or systems are not (regularly) synchronized with each other, as this may not be required from an operational perspective regarding the IAP's main objective, i.e. offering internet access to their users.

Depending on the IAP's IT infrastructure and network topology, time synchronization between in particular the IAP's network functions involved in IP address assignment and the IAP's LI systems involved in the respective delivery of IP address information might be technically feasible and may also be required to some extent to comply with national regulations.

Other scenarios where the correlation might be challenging to perform within reasonable time may include situations where the geolocation of the involved network functions / elements are at a distance, that the respective roundtrip time has an impact and might also vary over time due to dynamic routing within the IAP's network, e.g. due to QoS settings, etc.

Annex F (informative): Bibliography

- IANA Private Enterprise Numbers (PENs).

Annex G (informative): Change history

Status of the present document Service-specific details for Internet access services		
TC LI approval date	**Version**	**Remarks**
January 2004	V1.1.1	First publication of the TS after approval by ETSI/TC LI#04 (14-16 October 2003, Moscow) Version 1.1.1 published as ETSI TS 102 234
September 2004	V1.2.1	Included Change Requests: TS102234CR002 (cat F) Alignment of form of ASN.1 version TS102234CR003 (cat D) Editorial in Introduction These CRs were approved by TC LI#06 (22-23 July 2004, Póvoa de Varzim) TC LI#07 (28-30 September 2004, Bremen) decided to publish v1.2.1
July 2005	V1.3.1	Included Change Requests: TS102234CR005r1 (cat C) Definition of "nASPortNumber" and ASN.1 specification: Modification of parameter length TS102234CR006 (cat C) Create an own ASN.1 box for IPCCContents for different data streams These CRs were approved by TC LI#09 (28-30 July 2005, Rovaniemi)
October 2005	V1.4.1	Included Change Requests: TS102234CR007r1 (cat C) LI activation during an active internet session TS102234CR008r1 (cat C) Additions and changes for interception of wireless LAN These CRs were approved by TC LI#10 (4-6 October 2005, Sorrento)
February 2006	V1.5.1	Included Change Request: TS102234CR009 (cat C) on Clarification of session-numbering for IP-Access This CR was approved by TC LI#11 (31 January – 2 February 2006, Saint Martin) Correction of mistakes performed during ETSI publication process of v1.4.1 Version 1.5.1 only distributed for internal use in TC LI#12 and not officially published by ETSI
May 2006	V1.6.1	Included Change Requests: TS102234CR010 (cat F) on Changes to Figure A.6 TS102234CR011r2 (cat F) on Additions to ASN.1 TS102234CR012 (cat F) on Changes to Table B.2 TS102234CR013r1 (cat F) on Simplification of Figure 6 TS102234CR014r1 (cat F) on Changes to Table 2 TS102234CR015 (cat F) on Changes to Table A.3 All CRs resulting from the LI Plugtest were approved by TC LI#12 (9 – 11 May 2006, Limassol)
September 2006	V2.1.1	Included Change Request: TS102234CR016r1 (cat F) IRI Events and ASN.1 correction This CR was approved by TC LI#13 (6-8 September 2006, Stockholm) **ETSI TS 102 234 is converted to part 03 of the multi part specification ETSI TS 102 232**
October 2008	V2.2.1	Included Change Requests: TS102232-03CR017r1 (cat C) on Inclusion of NationalIPIRIParameters field in IPIRIContents TS102232-03CR018r2 (cat B) New values to be added to InternetAccessType These CRs were approved by TC LI#19 (30 September - 2 October 2008, Prague)
June 2011	V2.3.1	Included Change Request: TS102232-03CR019r5 (cat B) on Dual StackIPv6 Sequence-Of-IP-Addresses This CR was approved by TC LI#27, 28-30 June 2011, Mariehamn The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver7.txt) which accompanies the present document

Status of the present document Service-specific details for Internet access services		
TC LI approval date	**Version**	**Remarks**
January 2012	V3.1.1	Included Change Requests: TS102232-03CR022 (cat B) on New IPIRIContents field to identify authentication type & profile This CR was approved by TC LI#28, 13-15 September 2011, Otranto TS102232-03CR026r2 (cat B) on New values to be added to InternetAccessType in order to describe new type internet access services This CR was approved by TC LI#29, 24-26 January 2012 in Dun Laoghaire The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver8.txt) which accompanies the present document
May 2012	V3.2.1	Included Change Request: TS102232-03CR024r2 (cat B) on Changes to expand Target Identifiers This CR was approved by TC LI#30 (14-16 May 2012, Amsterdam) The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver9.txt) which accompanies the present document
September 2013	V3.3.1	Included Change Request: CR027 (Change to IRI-REPORT to signal end of intercept whilst session remains active) This CR was approved by TC LI#34 The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver10.txt) which accompanies the present document
July 2016	V3.4.1	Included Change Requests: CR028 (Fix header issue in Table A.1) CR029 (Adding common Location parameter to ETSI TS 102 232-3) These CRs were approved in TC LI#38 and TC LI#42, respectively The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver11.txt) which accompanies the present document
February 2017	V3.5.1	Included Change Request: CR030 (Improve state diagrams) This CR was approved by TCLI#43 The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver11.txt) which accompanies the present document
June 2017	V3.6.1	Included Change Request: CR033 (Improve state diagrams) This CR was approved by TCLI#45 The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver12.txt) which accompanies the present document
October 2017	V3.7.1	Included Change Requests: CR034 (IPv6 RADIUS updates) CR035 (Adjust imports in preparation of making ETSI TS 101 671 historical) The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver13.txt) which accompanies the present document
July 2020	V3.8.1	Included Change Requests: CR037 (Fix ASN.1 syntax error) The accompanying ASN.1 file has been fixed without version bump. The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver13.txt) which accompanies the present document

Status of the present document Service-specific details for Internet access services		
TC LI approval date	**Version**	**Remarks**
October 2020	V3.9.1	Included Change Request: CR038 (Addition of PDSR/PDHR to enable use with Broadband) The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver14.txt) which accompanies the present document
November 2022	V3.10.1	Included Change Requests agreed by ETSI TC LI#61: CR039 (Minor corrections) CR041 (Moving ASN.1 to attachment) The ASN.1 definitions are contained in a .txt file (IPAccessPDU,ver14.txt) which accompanies the present document
March 2023	V3.11.1	Included Change Requests agreed by ETSI TC LI#62: CR 042 (Fully qualify ASN.1 imports) The ASN.1 definitions are contained in a .asn file (IPAccessPDU,ver15.asn) which accompanies the present document
June 2023	V3.12.1	Included Change Requests agreed by ETSI TC LI#63: CR 043 (Provision of NAT translated IP addresses) CR 044 (Support for CC without a session context) The ASN.1 definitions are contained in a .asn file (IPAccessPDU,ver16.asn) which accompanies the present document
December 2023	V3.13.1	Included Change Request agreed by ETSI TC LI#64: CR 045r2 Truncated packets in IPCCContents The ASN.1 definitions are contained in a .asn file (IPAccessPDU,ver17.asn) which accompanies the present document
July 2024	V3.14.1	Included Change Request agreed by ETSI TC LI#66: CR 046r1 Next generation IP packet reporting The ASN.1 definitions are contained in a .asn file (IPAccessPDU,ver18.asn) which accompanies the present document
February 2025	V3.15.1	Included Change Request agreed by ETSI TC LI#68: CR 047r1 CPEProvidedLocationAttributes statement of use The ASN.1 definitions are contained in a .asn file (IPAccessPDU,ver19.asn) which accompanies the present document
June 2025	V3.16.1	Included Change Request agreed by ETSI TC LI#69: CR 048r1 IRI without network sessions, and session expiry The ASN.1 definitions are contained in a .asn file (IPAccessPDU,ver20.asn) which accompanies the present document

History

Document history		
V1.1.1	February 2004	Publication as ETSI TS 102 234 (Historical)
V1.2.1	October 2004	Publication as ETSI TS 102 234 (Historical)
V1.3.1	August 2005	Publication as ETSI TS 102 234 (Historical)
V1.4.1	January 2006	Publication as ETSI TS 102 234 (Historical)
V1.6.1	July 2006	Publication as ETSI TS 102 234 (Historical)
V2.1.1	December 2006	Publication (Historical)
V2.2.1	January 2009	Publication (Historical)
V2.3.1	August 2011	Publication (Historical)
V3.1.1	February 2012	Publication
V3.2.1	June 2012	Publication
V3.3.1	October 2013	Publication
V3.4.1	September 2016	Publication
V3.5.1	March 2017	Publication
V3.6.1	August 2017	Publication
V3.7.1	November 2017	Publication
V3.8.1	August 2020	Publication
V3.9.1	November 2020	Publication
V3.10.1	November 2022	Publication
V3.11.1	March 2023	Publication
V3.12.1	August 2023	Publication
V3.13.1	January 2024	Publication
V3.14.1	July 2024	Publication
V3.15.1	April 2025	Publication
V3.16.1	August 2025	Publication