ETSI TS 102 232-3 V3.12.1 (2023-08)

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-00242-3

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 Web server (https://ipr.etsi.org/).

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

Trademarks

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

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

Foreword

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

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

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

Modal verbs terminology

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

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

Introduction

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

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

1 Scope

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

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

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

2 References

2.1 Normative references

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

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

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

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

[1] ETSI TS 101 671: "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™a, -b or -g (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".

2.2 Informative references

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

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

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

[i.1] ETSI TR 102 205: "Methods for Testing and Specification (MTS); UML 2.0 action syntax feasibility study".

[i.2] IEEE 802.1X-2001™: "IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control".

[i.3] draft-ietf-dhc-agentopt-radius-04.txt: "RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option".

[i.4] IANA bootp parameters.

[i.5] ETSI TS 102 232-3 (V3.4.1): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".

[i.6] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations".

[i.7] IETF RFC 6264: "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition".

[i.8] IETF RFC 6888: "Common Requirements for Carrier-Grade NATs (CGNs)".

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

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

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

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

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

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

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

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

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

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

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

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

3.2 Symbols

Void.

3.3 Abbreviations

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

AAA	Authentication, Authorization and Accounting
ACK	Acknowledge
ADSL	Asymmetric Digital Subscriber Line
ANP	Access Network Provider
AP	Access Provider
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BOOTP	BOOTstrap Protocol
CC	Content of Communication
CGN	Carrier-Grade NAT
CHAP	Challenge Handshake Authentication Protocol
CIN	Communication Identity Number
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CSP	Communications Service Provider (covers all AP/NWO/SvP)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service

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

4 General

4.1 Internet Access Service (IAS)

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

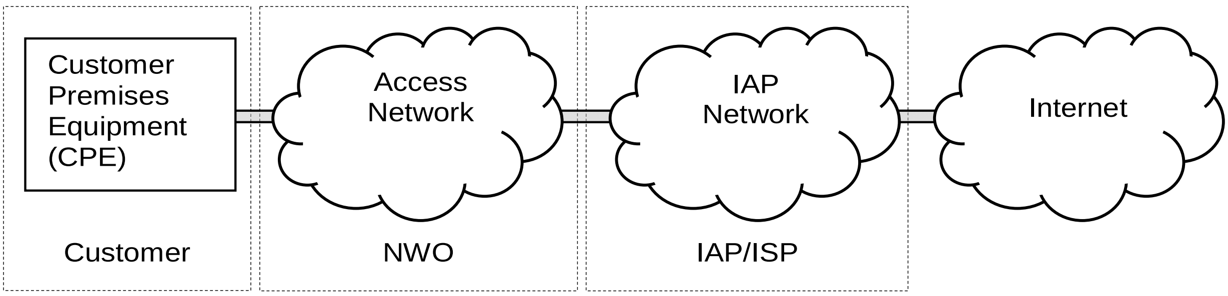

Figure 1: Internet access

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

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

4.2 Target identity and IP address

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

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

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

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

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

4.3 Lawful Interception requirements

4.3.0 Introduction

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

4.3.1 Target identity

Where the special properties of a given service, and the justified requirements of the LEAs, necessitate the use of various identifying characteristics for determination of the traffic to be intercepted, the provider (CSP) shall ensure that the traffic can be intercepted on the basis of these characteristics.

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

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

a) Username or Network Access Identifier (as defined in IETF RFC 7542 [7]).

b) IP address (IPv4 or IPv6).

c) Ethernet address.

d) Dial-in number calling line identity.

e) Cable modem identifier.

f) Other unique identifier agreed between AP and LEA.

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

4.3.2 Result of interception

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

a) When an attempt is made to access the access network.

b) When an access to the access network is permitted.

c) When an access to the access network is not permitted.

d) On change of status (e.g. in the access network).

e) On change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on).

The IRI shall contain:

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

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.

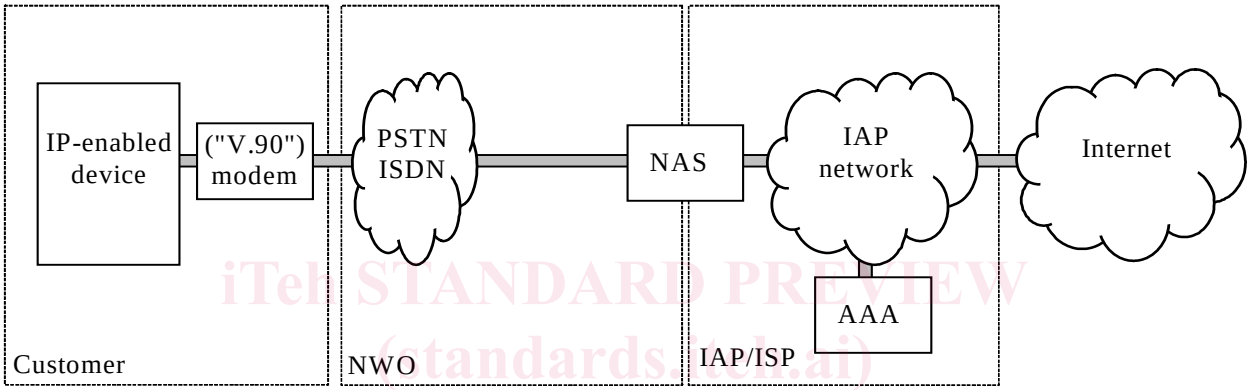

Figure 2: Dial-up access

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.

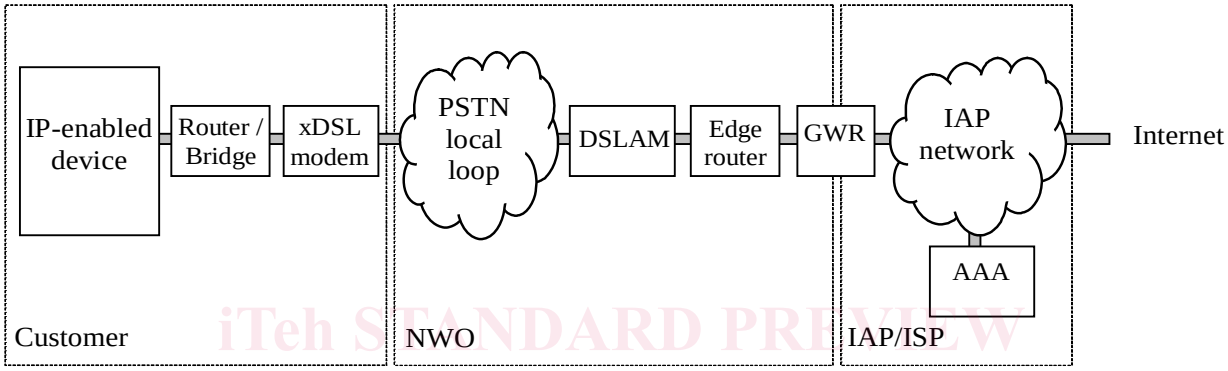

Figure 3: xDSL access

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.