SLOVENSKI STANDARD
SIST-TS ETSI/TS 102 234 V1.1.1:2005

01-maj-2005

Telekomunikacijska varnost ï Zakonito prestrezanje (LI) ï Storitveno-specifiļne podrobnosti za storitve internetnega dostopa

Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: TS 102 234 Version 1.1.1

SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

ICS:

33.020	Telekomunikacije na splošno	Telecommunications in general

SIST-TS ETSI/TS 102 234 V1.1.1:2005 en

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST-TS ETSI/TS 102 234 V1.1.1:2005

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

SIST-TS ETSI/TS 102 234 V1.1.1:2005

ETSI TS 102 234 V1.1.1 (2004-02)

Technical Specification

Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

SIST-TS ETSI/TS 102 234 V1.1.1:2005

Reference
DTS/LI-00005

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1.1.1-2005

Important notice

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

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

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

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

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

© European Telecommunications Standards Institute 2004.
All rights reserved.

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

SIST-TS ETSI/TS 102 234 V1.1.1:2005

Contents

Intellectual Property Rights 5
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 General 8
4.1 Internet Access Service (IAS) 8
4.2 Target identity and IP address 8
4.3 Lawful Interception requirements 9
4.3.1 Target identity 9
4.3.2 Result of interception 9
4.3.3 Intercept related information messages 10
4.3.4 Time constraints 10
4.3.5 Preventing over and under collection of intercept data 10
5 System model 11
5.1 Reference network topologies 11
5.1.1 Dial-up access 11
5.1.2 xDSL access 12
5.1.3 Cable Modem Access 13
5.1.4 IEEE 802.11B Access (with WiFi profile) 14
5.2 Reference scenarios 14
5.2.1 Logon 14
5.2.2 Multi Logon 14
5.2.3 Multilink Logon 14
5.2.4 IP transport 14
5.2.5 Logoff 14
5.2.6 Connection loss 15
6 Intercept Related Information (IRI) 15
6.1 IRI events 15
6.2 HI2 attributes 16
7 Content of Communication (CC) 16
7.1 CC events 16
7.2 HI3 attributes 16
8 ASN.1 for IRI and CC 17
Annex A (informative): Stage 1 - RADIUS characteristics 21
A.1 Network topology 21
A.1.1 RADIUS server 21
A.1.2 RADIUS proxy 21
A.2 RADIUS service 22
A.2.1 Authentication service 22
A.2.2 Accounting service 23
A.3 RADIUS protocol 24
A.3.1 Authentication protocol 24
A.3.2 Accounting protocol 24

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1.1.1-2005

SIST-TS ETSI/TS 102 234 V1.1.1:2005

A.4 RADIUS main attributes 25
A.5 RADIUS interception 26
A.5.1 Collecting RADIUS packets 26
A.5.2 Processing RADIUS Packets 26
A.5.2.1 Mapping events to RADIUS packets 26
A.5.2.2 Functional model 27
A.5.2.3 RADIUS Spoofing 30
A.5.3 Mapping RADIUS on the IRI structure 30
Annex B (informative): Stage 1 - DHCP characteristics 31
B.1 Network topology 31
B.2 DHCP service 31
B.3 BOOTP protocol 32
B.4 DHCP protocol 32
B.4.1 Address assignment 34
B.4.2 Message transmission and relay agents 34
B.4.3 Security and authentication 34
B.5 DHCP main attributes 35
B.6 DHCP interception 35
B.6.1 Introduction 35
B.6.2 DHCP packets 36
B.6.3 State machine 36
B.6.3.1 Mapping DHCP packets to events 37
B.6.3.2 Timers and administrative events 37
B.6.3.3 State information 37
B.6.3.4 State machine diagram 38
B.6.4 Mapping DHCP on the IRI structure 38
Annex C (informative): IP IRI Interception 40
C.1 Introduction 40
C.2 Requirements 40
C.3 Proposed implementation 40
Annex D (informative): TCP and UDP IRI interception 41
D.1 Introduction 41
D.2 Requirements 41
D.3 HI2 requirements 41
D.4 HI3 requirements 42
D.5 General requirements 42
Annex E (informative): Bibliography 43
History 44

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

SIST-TS ETSI/TS 102 234 V1.1.1:2005

Intellectual Property Rights

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

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

Foreword

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

Introduction

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

The present document focuses on intercepting HI2 data in relation to the use of Internet Access Services and is to be used in conjunction with the TS 102 232 [2]. In the latter document the handing over of the intercepted data is described.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

SIST-TS ETSI/TS 102 234 V1.1.1:2005

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) shall be sent, and what information it shall contain.

The study shall include but not be 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 TS 102 232 [2].

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-26fbdf014615/sist-ts-etsi-ts-102-234-v1.1.1-2005

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

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

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

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

[5] IETF RFC 1990: "The PPP Multilink Protocol (MP)".

[6] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[7] IETF RFC 2486: "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 802.11B: "IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Extension in the 2,4 GHz band".

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

SIST-TS ETSI/TS 102 234 V1.1.1:2005

3 Definitions and abbreviations

3.1 Definitions

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

access provider: Communication 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

3.2 Abbreviations

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

AAA	Authentication, Authorization and Accounting
AP	Access Provider
ASN.1	Abstract Syntax Notation 1
ATM	Asynchronous Transfer Mode
BOOTP	BOOTstrap Protocol
CC	Content of Communication
CHAP	Challenge Handshake Authentication Protocol
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
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
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)
IAP	Internet Access Provider
IAS	Internet Access Service
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LCP	Link Control Protocol
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAC	Media Access Control
NAS	Network Access Server
NWO	NetWork Operator
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet

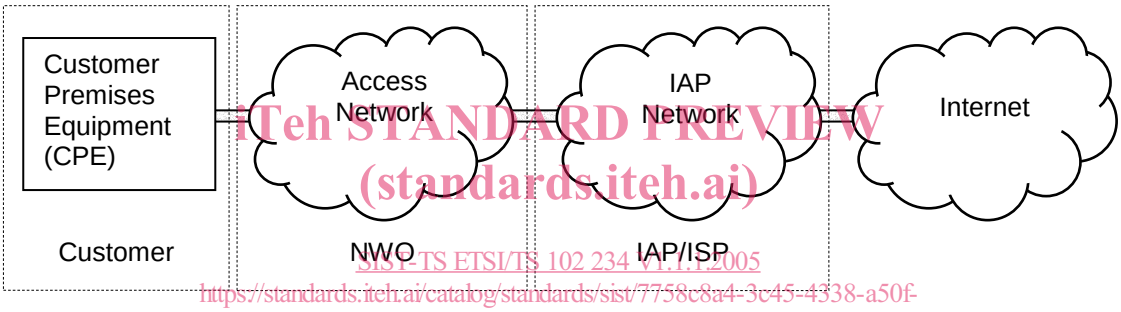
SIST-TS ETSI/TS 102 234 V1.1.1:2005

PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SLIP	Serial Line Interface Protocol
SvP	Service Provider
TCP	Transmission Control Protocol
TLV	Type-Length-Value
UDP	User Datagram Protocol

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 Internet Access Service 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 document, the provider of the Internet Access Service 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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014ed5/sist-ts-etsi-ts-102-234-v1.1.1-2005

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 802.11B [13] wireless network for WiFi access.

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.

SIST-TS ETSI/TS 102 234 V1.1.1:2005

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 must stop immediately, since the IP address may be handed out to another user shortly after.

4.3 Lawful Interception requirements

This clause lists the requirements for Lawful Interception. These requirements are derived from higher-level requirements listed in ES 201 671 [1] and TS 102 232 [2] and are specific to Internet Access Services. These requirements focus on both the administrative part of Internet Access for delivery over HI2 as well as capturing traffic for delivery over HI3.

4.3.1 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 dependant 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 RFC 2486 [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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

The target identity must 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). Further study may yield more types of target identity.

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;

SIST-TS ETSI/TS 102 234 V1.1.1:2005

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 Content of communication 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 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

For a description of the use and purpose of the various IRI records refer to TS 102 232 [2].

SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf014615/sist-ts-etsi-ts-102-234-v1-1-1-2005

4.3.4 Time constraints

The delays for generating the Intercept Related Information 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 must 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 must be stopped and the situation must 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 must be stopped and the situation must be reported upon.

SIST-TS ETSI/TS 102 234 V1.1.1:2005

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.

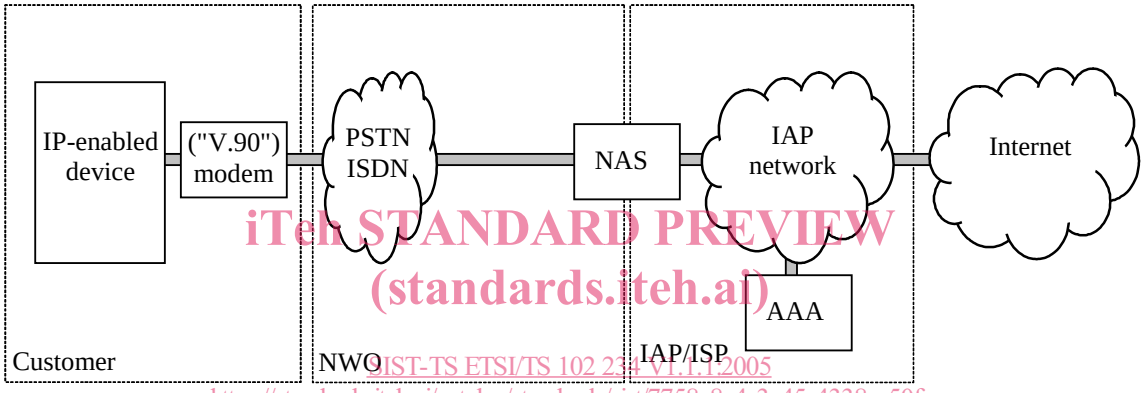
5 System model

5.1 Reference network topologies

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TS ETSI/TS 102 234 V1.1.1:2005
https://standards.iteh.ai/catalog/standards/sist/7758c8a4-3c45-4338-a50f-2fdbdf0146f5/sist-ts-etsi-ts-102-234-v1.1.1-2005

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. 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 address 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 address, 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 address 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.