

# ETSI TS 183 019 V1.1.1 (2005-12)

---

*Technical Specification*

**Telecommunications and Internet converged Services and  
Protocols for Advanced Networking (TISPAN);  
Network Attachment;  
Network Access xDSL and WLAN Access Networks;  
Interface Protocol Definitions**

---



---

Reference

DTS/TISPAN-03041-NGN-R1

---

Keywords

access, interface, network, xDSL

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chairecor/ETSI\\_support.asp](http://portal.etsi.org/chairecor/ETSI_support.asp)

---

**Copyright Notification**

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

© European Telecommunications Standards Institute 2005.  
All rights reserved.

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

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
1 Scope .....	5
2 References .....	5
3 Definitions and abbreviations.....	6
3.1 Definitions .....	6
3.2 Abbreviations .....	6
4 NGN general architecture.....	7
4.1 Overview of interface e1 .....	8
4.1.1 Authentication.....	8
4.1.2 IP address and network configuration.....	8
5 PPP-based access network configuration .....	9
5.1 Authentication phase .....	9
5.1.1 PPP link establishment phase (LCP) with authentication (PAP/CHAP/EAP) .....	9
5.2 Network Configuration Phase (NCP).....	9
5.2.1 PPP Network Configuration Phase for IP Networks (NCP/IPCP).....	9
5.2.1.1 PPP and ARF .....	9
5.2.1.2 PPP and AMF.....	10
6 Ethernet-based access network configuration .....	11
6.1 Authentication phase .....	11
6.1.1 EAP over Ethernet (802.1X).....	11
6.1.2 802.1X-based WLAN access network functional architecture .....	13
6.2 Network configuration phase .....	13
6.2.1 DHCP procedures .....	13
7 DHCP Support for Interface e1 .....	14
7.1 Access Network based on IPv4 .....	14
7.1.1 DHCP support by the UE.....	14
7.1.2 DHCP support by the ARF .....	15
7.1.3 DHCP support by the NACF .....	15
7.2 Access network based on IPv6 .....	16
8 Applicability to WLAN access networks .....	16
8.1 Requirements of the WLAN access network.....	17
8.2 Requirements of the chosen EAP method .....	17
<b>Annex A (informative): Requirements of the WLAN station.....</b>	<b>19</b>
A.1 Requirements of the WLAN station.....	19
<b>Annex B (informative): Bibliography.....</b>	<b>20</b>
History .....	21

---

## 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 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 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

---

# 1 Scope

The present document describes the protocol specifications and profiles for the interface between the CPE and the access network in the NGN network. The present document will provide specifications for the interface as it pertains to xDSL and WLAN access networks. Other access network types are not precluded, but will not be covered in this version of the present document.

---

# 2 References

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

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

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

- [1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".
- [2] ETSI TS 124 234: "Universal Mobile Telecommunications System (UMTS); 3GPP system to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3 (3GPP TS 24.234 Release 6)".
- [3] Wi-Fi Alliance: "WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks".

NOTE: See: [http://www.wi-fi.org/OpenSection/pdf/WPA\\_for\\_Public\\_Access\\_Final.pdf](http://www.wi-fi.org/OpenSection/pdf/WPA_for_Public_Access_Final.pdf)

- [4] draft-adrangi-eap-network-discovery-12 (March 2005): "Identity selection hints for Extensible Authentication Protocol (EAP)".
- [5] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".
- [6] draft-ietf-radext-rfc2486bis-06 (July 2005): "The Network Access Identifier".
- [7] IEEE 802.1X-2004: "Port Based Network Access Control".
- [8] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".
- [9] DSL Forum TR69.
- [10] IETF RFC 2131: "Dynamic Host Configuration Protocol".
- [11] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".
- [12] IETF RFC 3004: "The User Class Option for DHCP".
- [13] IETF RFC 3825: "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information".
- [14] IETF RFC 3046: "DHCP Relay Agent Information Option".
- [15] IETF RFC 3993: "Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option".
- [16] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

- [17] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".
- [18] IETF RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".
- [19] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".
- [20] draft-ietf-dhc-dhcpv6-remoteid-00.txt (April 2005): "DHCPv6 Relay Agent Remote ID Option".
- [21] draft-ietf-dhc-dhcpv6-subid-00.txt (April 2005): "DHCPv6 Relay Agent Subscriber-ID Option".
- [22] IETF RFC 2516: "A method for transmitting PPP over Ethernet (PPPoE)".
- [23] IETF RFC 3162: "RADIUS and IPv6".
- [24] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS Usage Guidelines)".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**Access Network (AN):** collection of network entities and interfaces that provide the IP transport connectivity between end user devices and NGN entities

**Functional Entity (FE):** entity that comprises a specific set of functions at a given location

NOTE: Functional entities are logical concepts, grouping of functional entities are used to describe practical physical realizations.

**Core Network (CN):** portion of the delivery system composed of networks, systems equipment and infrastructures, connecting the service providers to the access network

**User Equipment (UE):** one or more devices allowing a user to access services delivered by TISPAN NGN networks

NOTE: This includes devices under user control commonly referred to as CPE, IAD, ATA, RGW, TE, etc., but not network controlled entities such as access gateways.

**visited NGN network:** NGN network through which the User Equipment gains network connectivity

NOTE: The NGN Network includes both the Access Network and the Core Network. The User Equipment does not have a service relationship with the business entity that operates this network.

**home NGN network:** NGN network through which the User Equipment gains network connectivity

NOTE: The NGN network includes both the Access Network and the Core Network. The User Equipment has a service relationship with the business entity that operates this network.

### 3.2 Abbreviations

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

3GPP	Third Generation Project Partnership
AMF	Access Management Function
AP	Access Point
ATA	Analog Terminal Adaptor
CLF	Connectivity session Location and repository Function
CNG	Customer Network Gateway
CPECF	CPE Configuration Function

DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
GSMA	Global System for Mobile communications Association
IAD	Integrated Access Device
IETF	Internet Engineering Task Force
IP	Internet Protocol
NACF	Network Access Configuration Function
NAI	Network Access Identifier
NASS	Network Attachment SubSystem
NGN	Next Generation Network
PDBF	Profile Data Base Function
PEAP	Protected EAP
RGW	Residential GateWay
SIM	Subscriber Identity Module
TE	Terminal Equipment
TLS	Transport Layer Security
UAAF	User Access Authorization Function
UAM	Universal Access Method
UE	User Equipment
WLAN	Wireless Local Area Network
xDSL	Digital Subscriber Line

---

## 4 NGN general architecture

ES 282 001 [1] provides a description of the general network architecture of the NGN. The model is depicted in figure 1.



**Figure 1: General NGN network model**

Interface e1 is an access-network-specific interface, and is dependant on the access technology being used (xDSL, WLAN, and so on). Interface e5 is a roaming interface, and is independent of the access technology. Interface e5 is used to provide a consistent method for the visited NGN network to communicate with the home NGN network.

Figure 2 depicts the functional composition of the access network and the NGN core for the roaming scenario, where a UE obtains network access via a visited NGN network and authenticates back with the home NGN network. Details of this model may be found in TS 124 234 [2].

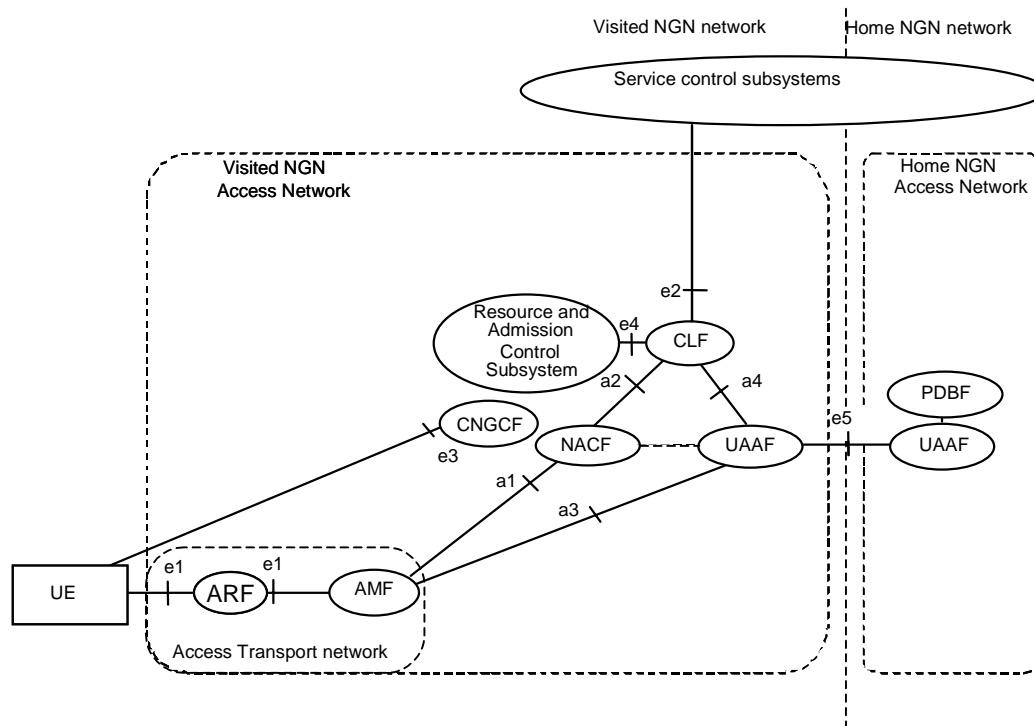


Figure 2: NASS mapped onto functional network roles - roaming scenario

## 4.1 Overview of interface e1

The present document details the protocols and profiles for e1 - the interface for authentication, authorization and IP address allocation. This interface enables the UE to initiate authentication and authorization requests, as well as initiate requests for IP address allocation, DNS allocation, and other network configuration parameters in order to access the network. These requests are received by the AMF (Access Management Function). It is assumed that the IP edge in the transport plane includes an ARF (Access Relay Function), which communicates with the UAAF (User Access Authorization Function) and NACF (Network Access Configuration Function) via the AMF. This interface enables the user equipment to provide user credentials (username/password, token, certificates, etc.) to the Network Attachment Subsystem (NASS) in order to perform network access authentication and authorization. This interface may also enable the NASS to provide authentication parameter to the UE to perform the network authentication when mutual authentication procedure is required. Based on the result of the authentication, the AMF authorises or denies the network access to the user equipment.

### 4.1.1 Authentication

This interface specifies the protocols and profiles used for authentication of the UE to the network, and vice-versa. The credentials used for authentication depend on the authentication method used as well as the preferences of the network service provider. Possible credential types include, SIM, certificates, and username/password.

### 4.1.2 IP address and network configuration

Once the UE is authenticated successfully, it shall be able to obtain an IP address in order to access the different services offered by the service provider. This interface also provides a method to transport IP address and network configuration information to the UE to enable IP access.



---

## 5 PPP-based access network configuration

### 5.1 Authentication phase

#### 5.1.1 PPP link establishment phase (LCP) with authentication (PAP/CHAP/EAP)

A generic description of the PPP-based authentication model is provided in TS 124 234 [2], clause 7.2 and annex B. There are currently no specific requirements on PPP-based authentication scenarios. This may be further studied and defined in Release 2 of the TISPAN specifications.

### 5.2 Network Configuration Phase (NCP)

#### 5.2.1 PPP Network Configuration Phase for IP Networks (NCP/IPCP)

##### 5.2.1.1 PPP and ARF

In NASS of WI02021, The Access Relay Function (ARF) acts as a relay between the user equipment and the Network Attachment Subsystem (NASS). It receives network access requests from the user equipment and forwards them to the NASS. Before forwarding a request, the ARF may also insert local configuration information and apply protocol conversion procedures.

In PPPOE case, the ARF should implement a PPPoE intermediate agent function in order to insert access loop identification.

As a PPPoE Intermediate, The ARF intercepts all PPPoE discovery packets, i.e. the PADI, PADO, PADR, PADS and PADT packets, but does not modify the source or destination MAC address of these PPPoE discovery packets. Upon reception of a PADI or PADR packet sent by the PPPoE client, the ARF adds a PPPoE TAG to the packet sent upstream. The TAG contains the identification of the access loop on which the PADI or PADR packet was received in the Access Node where the ARF resides.

If the TAG containing the access loop identification is present in PADO or PADS packets sent by the AMF, the ARF must remove the TAG before sending the packet downstream. If a PADI or PADR packet exceeds 1 500 octets after adding the TAG containing the access loop identification, the ARF must not send the packet to the AMF. The ARF should then return a Generic-Error TAG to the sender in the appropriate PPPoE discovery packet (i.e. PADO or PADS).

The required syntax for access loop identification is depicted in following table defined in RFC 2516 [22].

```

+-----+-----+-----+-----+
| 0x0105 (Vendor-Specific) | TAG_LENGTH |
+-----+-----+-----+-----+
| 0x00000DE9 (3561 decimal, i.e. "ADSL Forum" IANA entry) |
+-----+-----+-----+-----+
| 0x01 | length | Agent Circuit ID value... |
+-----+-----+-----+-----+
| Agent Circuit ID value (cont) |
+-----+-----+-----+-----+
| 0x02 | length | Agent Remote ID value... |
+-----+-----+-----+-----+
| Agent Remote ID value (cont) |
+-----+-----+-----+-----+

```

The first four octets of the TAG\_VALUE contain the vendor id. Specifically, the enterprise code here is that of the DSL Forum, (i.e. 3561 in decimal, corresponding to the IANA "ADSL Forum" entry in the Private Enterprise Numbers registry). The remainder of the TAG\_VALUE is unspecified in RFC 2516 [22]. Note that the sub-options do not have to be aligned on a 32-bit boundary.

"Agent Circuit ID" sub-option (sub-option 1).

This sub-option uniquely identify the Access Node and the access loop on the Access Node on which the PPPoE discovery packet was received.

"Agent Remote ID" sub-option (sub-option 2).

The sub-option contains an string that uniquely identifies the subscriber on the associated access loop on the Access Node on which the PPPoE discovery packet was received.

For encoding the sub-option, the same sub-option based encoding as in DHCP option 82 is used (see clause 7.1.2).

### 5.2.1.2 PPP and AMF

The Access Management Function (AMF) translates network access requests issued by the UE (TISPAN WI 02021). It forwards the requests for allocation of an IP address and possibly additional network configuration parameters to/from the NACF.

In case PPP is applied, the AMF terminates the PPP connection and provides the inter-working with the interface to the network attachment subsystem e.g. using an AAA protocol (RADIUS or Diameter). The AMF acts as a RADIUS client if the UAAF is implemented in a RADIUS server.

When ARF implements a PPPoE Intermediate Agent and adds access loop identification TAG. The AMF should be able to support access loop identification carried over PPPoE.

The AMF shall accept PADI and PADR packets containing a TAG that is used to convey the access loop identification to AMF. The access loop information present in a TAG in the PADI and PADR packets may be used by the AMF to check whether PPPoE discovery is allowed for the identified subscriber line. This procedure is independent of the PPP authentication phase performed later on.

The AMF shall be able to use the access loop identification to construct the proper RADIUS Attributes (e.g. NAS-Port-Id, NAS-Port or Calling-Station-Id) during the PPP authentication phase. These Attributes are sent in a RADIUS Access-Request packet to the UAAF which is a RADIUS server. This allows the UAAF to take the access loop identification into account when performing authentication, authorization and accounting.

## 6 Ethernet-based access network configuration

### 6.1 Authentication phase

#### 6.1.1 EAP over Ethernet (802.1X)

Figure 3 depicts a typical protocol stack for 802.1X-based [7] authentication. Further details may be obtained from [3]. The EAP messages are carried over EAPOL (EAP over LAN) frames between the UE and the AP and then reencapsulated in RADIUS [8] or Diameter messages when sent from the AP to the home AAA Server (via zero or more AAA proxies). In figure 3, for the WLAN scenario, the UE (mobile station) acts as the 802.1X supplicant, the AP acts as the 802.1X authenticator, and the AAA server (which implements the UAAF functionality) acts as the authentication server.

For security reasons, RADIUS is sometimes also carried over IPsec (RFC 3162 [23] describes use of RADIUS over IPv6-IPsec, and RFC 3580 [24] also recommends use of IPsec to protect RADIUS). Diameter may also be used instead of or in addition to RADIUS.

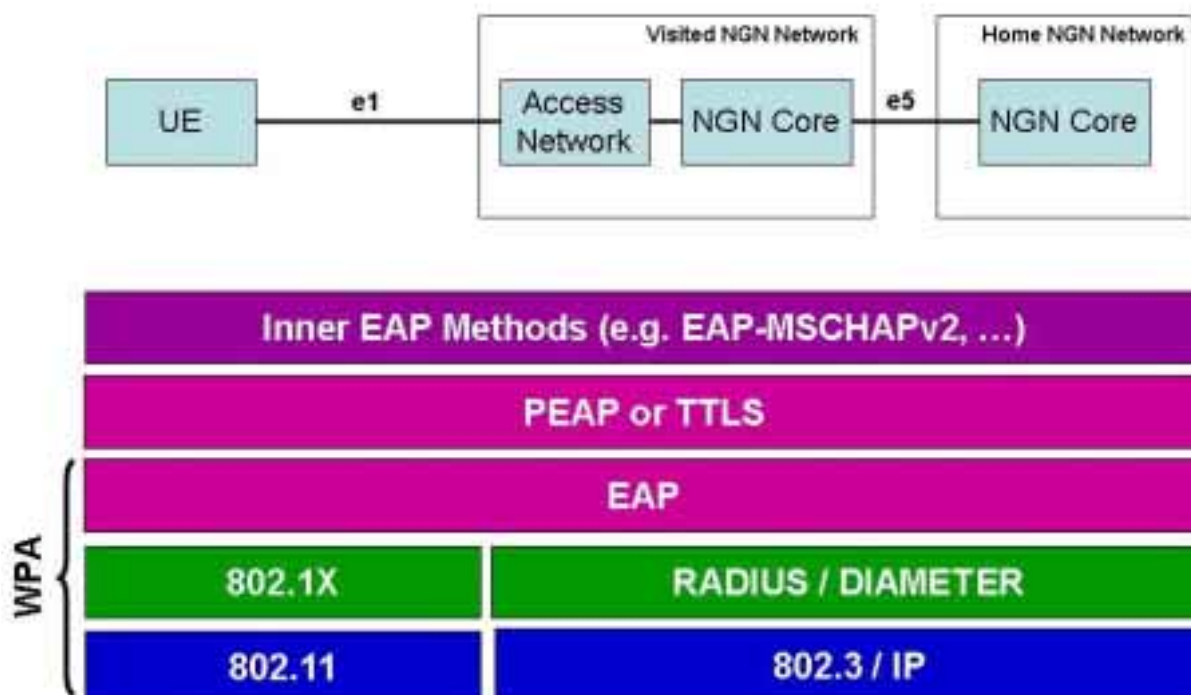
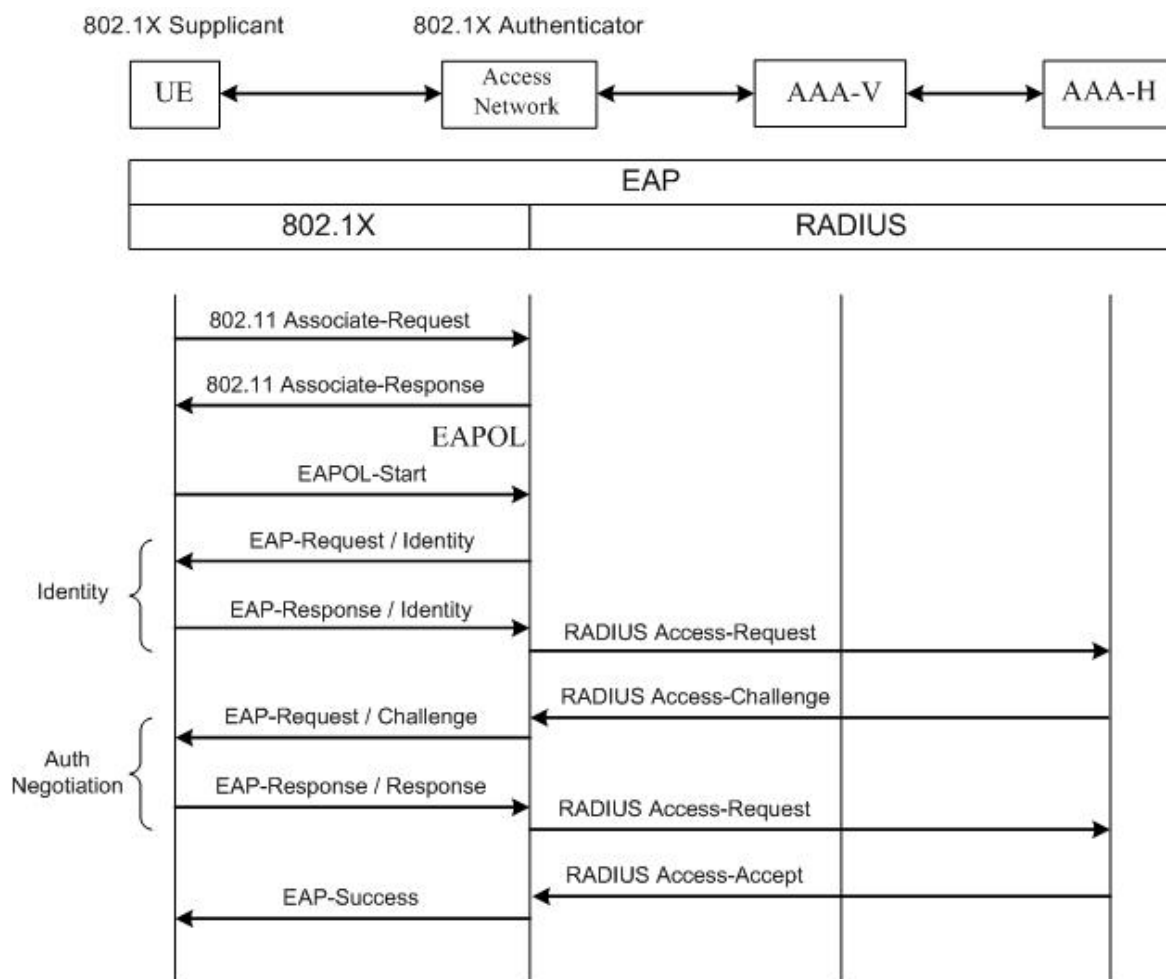


Figure 3: EAP authentication protocol stack

Figure 4 depicts a typical 802.1X-based authentication scenario. The UE (in this case, the wireless station) attempts to associate with an AP and is challenged to authenticate. At this point, the wireless station needs to indicate its user identity. There are usually two parts to this identity: the user name and the realm. Typically, these are combined into a Network Access Identifier (NAI) of the form user@realm. The realm part of the NAI is used to establish a connection with the appropriate AAA-H for that user. This presumes that the visited network recognises that realm name. If this is not the case, then the visited network will signal an authentication failure back to the wireless station. The wireless station can then either try a different NAI (with a different realm) or can try to establish a new NAI on the visited network. If those alternatives also fail, the wireless station will be denied access or will be granted only limited guest access.



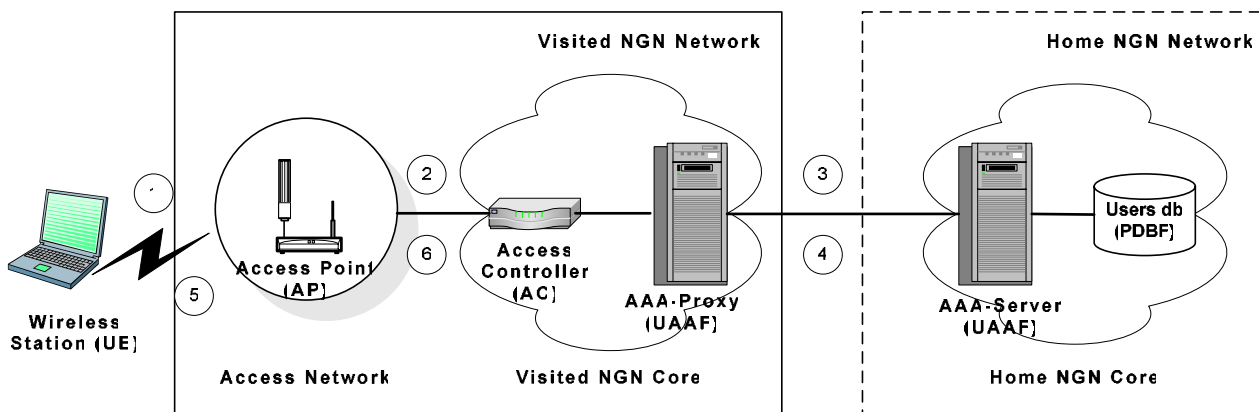
**Figure 4: 802.1X-based authentication with RADIUS as AAA protocol**

To avoid revealing the true user identity to an entity other than the home service provider, especially across the WLAN radio link, the wireless station can use a generic user name like "anonymous" or "user" in the NAI given in the initial identity exchange. The realm part of the NAI is the only information the visited network needs to know at this point. If PEAP or TTLS are used to establish a secure tunnel between the STA and the AAA-H, then the protected identity exchange will not be visible to the visited network or to any eavesdroppers. The visited network will eventually need to obtain some identity value for charging and billing purposes if the authentication is successful. The home network can provide the identity that identifies the account for charging. This account is used between the visited network and the home network for inter-operator charging purposes only. This account need not be the same as that used by the home network to bill the subscriber. Furthermore, this identity can be an alias specified by the home provider rather than information that might compromise the true identity of the wireless user. The identity used for charging can be shared only with the AAA infrastructure and never needs to be sent unprotected across the WLAN radio link.

## 6.1.2 802.1X-based WLAN access network functional architecture

The WLAN Access Network will physically consist of at least one Access Point (AP), which will provide the radio connectivity for the WLAN UE devices. The Access Network or the core network may also contain an Access Controller (AC), that may manage a number of APs.

A generic model for access of WLAN to NGN networks is depicted in figure 5.



**Figure 5: Generic model for WLAN access to NGN**

The numbers shown in figure 5 correspond to the following steps of a typical 802.1X-based authentication scenario.

- 1) The wireless station (UE) discovers an 802.11 access point (AP) and initiates a connection request. The AP (or a network authenticator) responds with a request for the UE identity.
- 2) The AP in the access network forwards the UE identity as an authentication request message to the local authentication server/proxy (AAA-Proxy) that implements the UAAF functionality. This may be forwarded via an Access Controller (AC). Either the AP, or the AC, or a combination of the two could implement the AMF functionality.
- 3) If the AAA-Proxy is able to authenticate the user credentials, it does so locally. If the AAA-Proxy examines the wireless station identity and decides that this is a roaming user, it forwards the authentication request on to the AAA server of the home provider of that user (AAA-Server) based on the realm name specified in the wireless station identity.
- 4) The AAA-Server (which also implements the UAAF functionality) authenticates the user via an EAP-based challenge-response method that runs end-to-end between the AAA-Server and the wireless station. A local user database (PDBF) is consulted by AAA-Server to verify the credentials provided by the wireless station. The result of the authentication and session key material are communicated back to the AAA-V and AP respectively.
- 5) The AP configures link-layer session keys and signals that the wireless station has been successfully authenticated. Prior to this time, the AP blocks any attempt by the wireless station to obtain an address or access the Internet.
- 6) The AP, through the AAA-Proxy, sends accounting messages to the AAA-Server. When the wireless station disconnects, an accounting stop message is sent as the last message for that session. The AAA-V and AAA-H generate charging records. The AAA-H sends these record to a billing center.

## 6.2 Network configuration phase

### 6.2.1 DHCP procedures

The Network Access Configuration Function (NACF) is responsible for the IP address allocation to the UE. IT may also distribute other network configuration parameters such as address of DNS server(s) and address of signalling proxies for specific protocols. A NACF may be realised as a DHCP server.

Once the UE has been authenticated as described above, it may use DHCP to request an IP address. A local DHCP server that functions as a NACF may respond to this request and assign an IP address with a local subnet prefix to the UE. It maintains a mapping between the UE and the IP address that has been assigned to it, and may forward this information to the CLF. Further specifications are provided in clause 7.

---

## 7 DHCP Support for Interface e1

### 7.1 Access Network based on IPv4

#### 7.1.1 DHCP support by the UE

The User Equipment (UE) shall behave as an RFC 2131 [10] compliant DHCP v4 client. The UE shall be able to send DHCP messages that support the following options:

- Option 55 "Parameter List" RFC 2132 [11].
- Option 60 "Vendor Class Identifier" RFC 2132 [11].
- Option 61 "Client Identifier" RFC 2132 [11].

Option 55 shall be set to request the following options: 6, 43, 66, 67, 120 and 123.

A UE supporting the autoconfiguration protocol defined by the DSL forum shall identify itself by including the string "dslforum.org" anywhere in the Vendor Class Identifier option (60). This will ensure that the name of the ACS will be sent back in the DHCP offer in the Vendor Specific Information option (43), as described in DSL Forum TR69 [9].

It is also recommended that the UE send the following options:

- Option 12 "Host Name" RFC 2132 [11].
- Option 77 "User Class" RFC 3004 [12].

The UE shall be able to receive and process DHCP messages that include the following options:

- Option 6 "Domain Server" RFC 2132 [11].
- Option 15 "Domain Name" RFC 2132 [11].
- Option 43 "Vendor Specific" RFC 2132 [11].
- Option 51 "IP Address Lease Time" RFC 2132 [11].
- Option 58 "Timer T1" RFC 2132 [11].
- Option 59 "Timer T2" RFC 2132 [11].
- Option 120 "SIP Servers DHCP Option" RFC 3361 [16]

Support of the following options is also recommended:

- Option 1 "Subnet Mask" RFC 2132 [11].
- Option 3 "Router" RFC 2132 [11].
- Option 5 "Name Server" RFC 2132 [11].
- Option 33 "Static Route" RFC 2132 [11].
- Option 42 ""NTP servers" RFC 2132 [11].
- Option 66 "TFTP Server Name" RFC 2132 [11].
- Option 67 "Bootfile-Name" RFC 2132 [11].

- Option 72 "WWW Server"
- Option 123 "GeoConf Option" RFC 3825 [13].
- Option 114 "URL option"
- Option TBD "PANA Authentication Agent"
- Option TBD "Civic Location"

### 7.1.2 DHCP support by the ARF

The Access Relay Function (ARF) shall behave as an RFC 2131 [10] compliant DHCP v4 Relay Agent. It shall support the DHCP Relay Agent Information option (Option 82) and insert the following sub-options:

- Sub-option 1 "Agent Circuit ID" RFC 3046 [14].
- Sub-option 2 "Agent Remote ID" RFC 3046 [14].
- Sub-option 6 "Subscriber-ID" RFC 3993 [15].

The following encoding is recommended for the Agent Circuit ID:

```

AgentCircuit-ID = AccessNodeId AggregationType slot/port ":" Layer2Id
AccessNodeId = NAME
AggregationType = "atm" | "eth"
Slot = *DIGIT
Port = *DIGIT
Layer2Id = ATM_Id | Ethernet_Id
ATM_Id = vpi "." vci
Ethernet_Id = vlan_tag
vpi = *DIGIT ; VP Identifier
vci = *DIGIT ; VC Identifier
vlan_tag = DIGIT ; VLAN tag
DIGIT = %x30-39 ; 0-9
ALPHA = %x41-5A / %x61-7A ; A-Z / a-z
NAME = ALPHA *63(ALPHA / DIGIT / "_")

```

The Agent Remote ID shall be in the form of an ASCII string that identifies the subscriber line with regards to the Network Attachment Subsystem.

The Subscriber ID shall be in the form of an ASCII string that identifies the subscriber with regards to the Network Attachment Subsystem, independently from the access technology used.

### 7.1.3 DHCP support by the NACF

The Network Access Configuration Function (NACF) shall behave as an RFC 2131 [10] compliant DHCP v4 server. The NACF shall support all options defined in RFC 2132 [11] and RFC 3004 [12], RFC 3046 [14], RFC 3361 [16], RFC 3825 [13] and RFC 3993 [15].

The NACF shall insert the following options in a DHCP Offer:

- Option 6 "Domain Server": The domain name server option specifies a list of Domain Name System name servers available to the client.
- Option 15 "Domain Name": specifies the domain name that client should use when resolving hostnames via the Domain Name System.
- Option 51 "IP Address Lease Time": It is recommended that a long lease time be used.
- Option 58 "Timer T1": This timer should be set to a value that is less than the default value described in RCF 2131.
- Option 59 "Timer T2": This timer should be set to a value that is less than the default value described in RCF 2131.

- Option 120 "SIP Server": This option shall contain the P-CSCF identity. The SIP server DHCP option carries either a 32-bit (binary) IPv4 address or, preferably, a DNS name to be used by the SIP client to locate a SIP server.

The NACF may also insert the following options in a DHCP Offer:

- Option 42 "Network Time Protocol Servers".
- Option 43 "Vendor Specific": Vendor Specific Information option used by clients and servers to exchange vendor- specific information. If a vendor potentially may encode more than one item of information using "Encapsulated vendor-specific options" (e.g. name of the CPECF).

NOTE: If the CPECF is a TR69, the DHCP server shall include the two encapsulated Vendor-Specific options (URL of ACS, Provisioning Code) defined in TR69.

- Option 66 "TFTP Server Name": TFTP server address.
- Option 67 "Bootfile Name": Identifies a bootfile to be retrieved by the user equipment.
- Option 72 "WWW server": The WWW server option specifies a list of WWW available to the client.
- Option 123 "GeoConf Option": Coordinate-based Location Configuration Information option provides the coordinate-based geographic location of the client.
- Option 114 "URL option" : May be used for authentication
- Option TBD "PANA Authentication Agent" the PANA Authentication Agent Option carries either a 32-bit (binary) IPv4 address list or, preferably, a domain name list to be used by the PANA client to locate a PANA authentication Agent
- Option TBD "Civic Location": Dynamic Host Configuration Protocol option containing the civic location of the client or the DHCP server.

## 7.2 Access network based on IPv6

The UE, the ARF and the NACF shall behave as an RFC 3315 [17] compliant DHCPv6 client, DHCPv6 relay agent and DHCP Server (respectively). All options defined in RFC 3315 [17] shall be supported.

The following options shall also be supported:

- DHCPv6 options 21 and 22 for SIP server.
- OPTION\_SIP\_SERVER\_D (21) defined in RFC 3319 [18].
- OPTION\_SIP\_SERVER\_A (21) defined in RFC 3319 [18].
- OPTION\_DNS\_SERVERS (23) defined in RFC 3646 [19].

The ARF shall insert the following information:

- OPTION\_REMOTE\_ID (tbd) defined in draft-ietf-dhc-dhcpv6-remoteid-00.txt [20].
- OPTION\_SUBSCRIBER\_ID (tbd) defined in draft-ietf-dhc-dhcpv6-subid-00.txt [21].

---

## 8 Applicability to WLAN access networks

This certification of WLAN devices by the Wi-Fi Alliance may only be applicable to WLAN devices that are deployed by a service provider, and may not be necessary or enforceable for devices that may be deployed in the customer premises - for example, a wireless AP that is connected to a DSL line coming in to a home.



## 8.1 Requirements of the WLAN access network

- 1) The WLAN device in the WLAN access network shall be Wi-Fi Alliance certified, and:
  - a) The WLAN device shall support either 802.11b or 802.11g.
- 2) The access network shall support WPA/802.1X.
  - a) The SSID used for WPA/802.1X in the beacon shall be broadcast by the WLAN device in strict accordance with the 802.11 specification. The beacon shall contain the WPA Information Element.
  - b) The access network shall support EAPOL messages, and shall be able to transport at a minimum EAP messages of the EAP method types defined in clause 8.2.
  - c) The access network shall provide a DHCP service, with assignment of wireless station IP address, netmask, gateway IP address and DNS server address. Specific requirements are described in clause 7 of the present document.
  - d) The access network shall support login with username (NAI) as defined in RFC 2486bis [6].
- 3) The access network may support WPA2.
- 4) The access network may also support UAM. In this case, the access network shall meet the following requirements simultaneously.
  - a) The SSID used for WPA in the beacon shall be broadcast by the WLAN device in strict accordance with the 802.11 specification. The beacon shall contain the WPA Information Element.
  - b) The SSID used for open authentication in the beacon shall be broadcast by the AP in strict accordance with the 802.11 specification. The beacon shall indicate open authentication by not requiring WEP or 802.1X.
- 5) If the access network supports UAM method of authentication, it shall also meet the following requirements:
  - a) It may provide a DHCP service, with assignment of wireless station IP address, netmask, gateway IP address and DNS server address.
  - b) It may support redirection of HTTP requests to a login webpage while in unauthenticated mode.
  - c) It shall support login with username (NAI) as defined in RFC 2486bis [6].
  - d) It shall secure authentication of credentials over HTTPS.
- 6) The access network may support intermediary network discovery and selection to allow a wireless station to select an intermediary when in a visited network.
  - a) If a user's service provider does not have a service agreement with a visited network provider, it may still be possible to obtain service via a roaming intermediary or exchange. If more than one intermediary is available, the choice of intermediary may affect charges, service, QoS, and other issues. In this case, it is important for the user to have an opportunity to influence that choice.
  - b) Work in this area is being done in the IETF. Work items that should be tracked include the NAI format standard defined by RFC 2486bis [6], and the EAP Network Discovery proposal (draft-adrangi-eap-network-discovery-12 [4]).

## 8.2 Requirements of the chosen EAP method

- 1) The EAP method used shall support:
  - a) Mutual authentication.
  - b) Key-derivation.
- 2) TS 124 234 [2], clause 6, shall be supported when EAP-SIM and EAP-AKA are used by the WLAN UE and the WLAN access network.

NOTE: Requirement 1 of clause 6.5 is satisfied by the following EAP methods. It should be noted that the list below is not restrictive.

- EAP-SIM.
- PEAP/EAP-MSCHAPv2.
- TTLS/MS-CHAPv2.
- EAP-AKA.
- EAP-TLS.

---

## Annex A (informative): Requirements of the WLAN station

### A.1 Requirements of the WLAN station

- 1) The wireless interface on the WLAN station shall be Wi-Fi Alliance certified, and:
  - a) The WLAN station shall support either 802.11b or 802.11g.
- 2) The WLAN station shall be able to operate in Wi-Fi Protected Access (WPA)/802.1X mode, and:
  - b) WLAN authentication signalling shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 3748 [5]. The EAP method chosen shall follow the EAP method requirements noted in clause 8.2.
  - c) The wireless station shall use an NAI as defined in RFC 2486bis [6] and TS 124 234 [2].
- 3) The wireless station may operate in UAM mode.
  - d) The wireless station shall be able to successfully associate to the open SSID and be 802.11 authenticated (as per 802.11-1999 specification).
- 4) The wireless station shall be able to differentiate between multiple BSSID capability information elements, which have the same SSID name.
- 5) The wireless station may operate in WPA2 mode.
- 6) The wireless station may support intermediary network discovery and selection to allow a wireless station to select an intermediary when in a visited network.
  - e) If a user's service provider does not have a service agreement with a visited network provider, it may still be possible to obtain service via a roaming intermediary or exchange. If more than one intermediary is available, the choice of intermediary may affect charges, service, QoS, and other issues. In this case, it is important for the user to have an opportunity to influence that choice.
  - f) Work in this area is being done in the IETF. Work items that should be tracked include the NAI format standard defined by RFC 2486bis [6], and the EAP Network Discovery proposal (draft-adrangi-eap-network-discovery-12 [4]).

---

## Annex B (informative): Bibliography

- ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

---

## History

<b>Document history</b>		
V1.1.1	December 2005	Publication