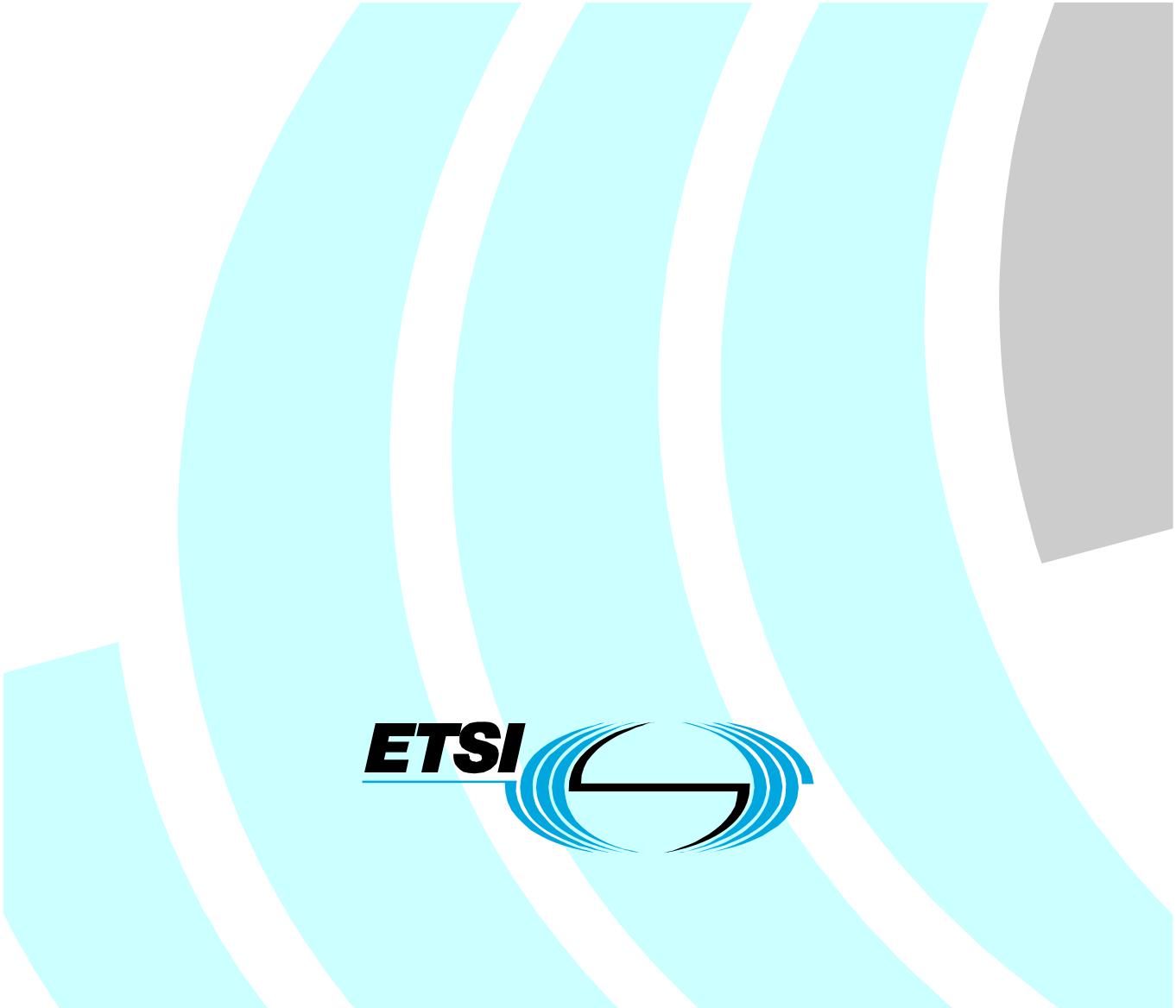
ETSI TR 185 007 V2.0.0 (2008-03)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of protocols for customer networks connected to TISPAN NGN



Reference
DTR/TISPAN-05016-NGN-R2

Keywords
gateway, network, protocol

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/chaircor/ETSI_support.asp

Copyright Notification

Contents

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 Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document contains informative text for analysing the set of protocols that can be used in the Customer Premises Networks (CPN) on the interfaces defined by stage 2 documents TS 185 003 [8] and TS 185 006 [7] related to service and transport layers. It will constitute a basic document produced by WG5, with a strong collaboration with WG3, to be used as the starting point for future technical specifications on that field.

2 References

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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

[1] DSL Forum TR-069 Amendment 1: "CPE WAN Management Protocol".

[2] HGI: "Home Gateway Technical Requirements Release 1".

[3] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[4] IETF RFC 1433: "Directed ARP".

[5] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3".

[6] ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

[7] ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN Customer Devices architecture and interfaces".

[8] ETSI TS 185 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway Architecture and Reference Points".

[9] ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".

[10] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[11] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[12] IETF RFC 4058: "Protocol for Carrying Authentication for Network Access (PANA) Requirements".

[13] IEEE 802.1x: "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control".

[14] IETF RFC 3748: "The Extensible Authentication Protocol (EAP) specification".

[15] ETSI TS 183 065: "Telecommunications and Internet converged Services and Protocols for Advanced Networks(TISPAN); Customer Network Gateway Configuration Function; e_3 Interface based upon CWMP".

[16] DSL Forum TR-098: "DSLHomeTM Internet Gateway Device Version 1.1 Data Model for TR-069".

[17] IEEE 802.11: "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".

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

3 Definitions and abbreviations

3.1 Definitions

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

CPN Device: device physically installed in the CPN allowing user access to network services; this can be a Customer Network Gateway with gateway functionalities towards the NGN, or a Customer Network Device being the end user terminal

Customer Network Device (CND): CPN device enabling the final user to have direct access to services through a specific user interface

NOTE: CNDs can be dedicated to the internet, conversational and audio-video services. But they could be also Consumer Electronics equipment and other devices which may have nothing to do with these premium services (e.g. services performing a content sharing within a CPN, typically between a PC and a music system).

Customer Network Gateway (CNG): CPN device acting as a gateway between the CPN and the NGN

NOTE: CNG is able to perform networking functions from physical connection to bridging and routing capabilities (L1-L3), but also possibly implementing functions related to the service support (up to L7).

Customer Premises Network (CPN): in-house network composed by customer network gateway, customer network devices, network segments, network adapters and nodes

NOTE: Network segments are physical wired or wireless connections between customer premises network elements); network adapters are elements performing a L1/L2 conversion between different network segments; nodes are network adapters with L3 routing capabilities.

"Multiple" Play Services (can be: double, triple, quadruple etc.): Delivery by a single service provider of different types of concurrent services to one or multiple users within the same CPN. Services can be categorized in the following way: data (e.g. Web browsing, best effort traffic etc.), person(s) to person(s) communication, entertainment.

3.2 Abbreviations

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

ACS	AutoConfiguration Server
ARF	Access Relay Function
ARP	Address Resolution Protocol
CND	Customer Network Device
CND-A	CND-Client Application
CND-AtF	CND Attachment Function
CND-CMF	CND Configuration and Maintenance Function
CND-CSMF	CND-Communication Services Media Function
CND-LAF	CND-Local Authentication Function
CND-NTF	CND-NAPT Traversal Function
CND-SIP UA	CND-SIP User Agent
CNG	Customer Network Gateway
CNG-ACF	CNG-Admission Control Function
CNG-AtF	CNG-Attachment Function
CNG-AuF	CNG-Authentication Function
CNGCF	Customer Network Gateway Configuration Function
CNG-CMF	CNG-Configuration and Maintenance Function
CNG-LF	CNG-Location Function
CNG-NFF	CNG-NAPT and Firewall Function
CNG-PCF	CNG Policy Control Function
CNG-PPF	CNG Plug and Play Function
CNG-UIF	CNG User reference point Function
CPN	Customer Premises Network
DB	DataBase
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
GUI	Graphic User Interface
HG	Home Gateway
IMS	IP Multimedia Subsystem
NAPT	Network Address and Port Translation
NTF	NAPT Traversal Function
PANA	Protocol for carrying Authentication for Network Access
P-CSCF	Proxy Call Session Control Function
PPP	Point-to-Point Protocol
RM	Remote Management
SIP	Session Initiation Protocol
WAN	Wide Area Network

4 Reference Architecture

The present document is based on the architecture defined in TS 185 003 [8] and TS 185 006 [7]. Figure 4.1 shows all the interfaces analysed in the present document.

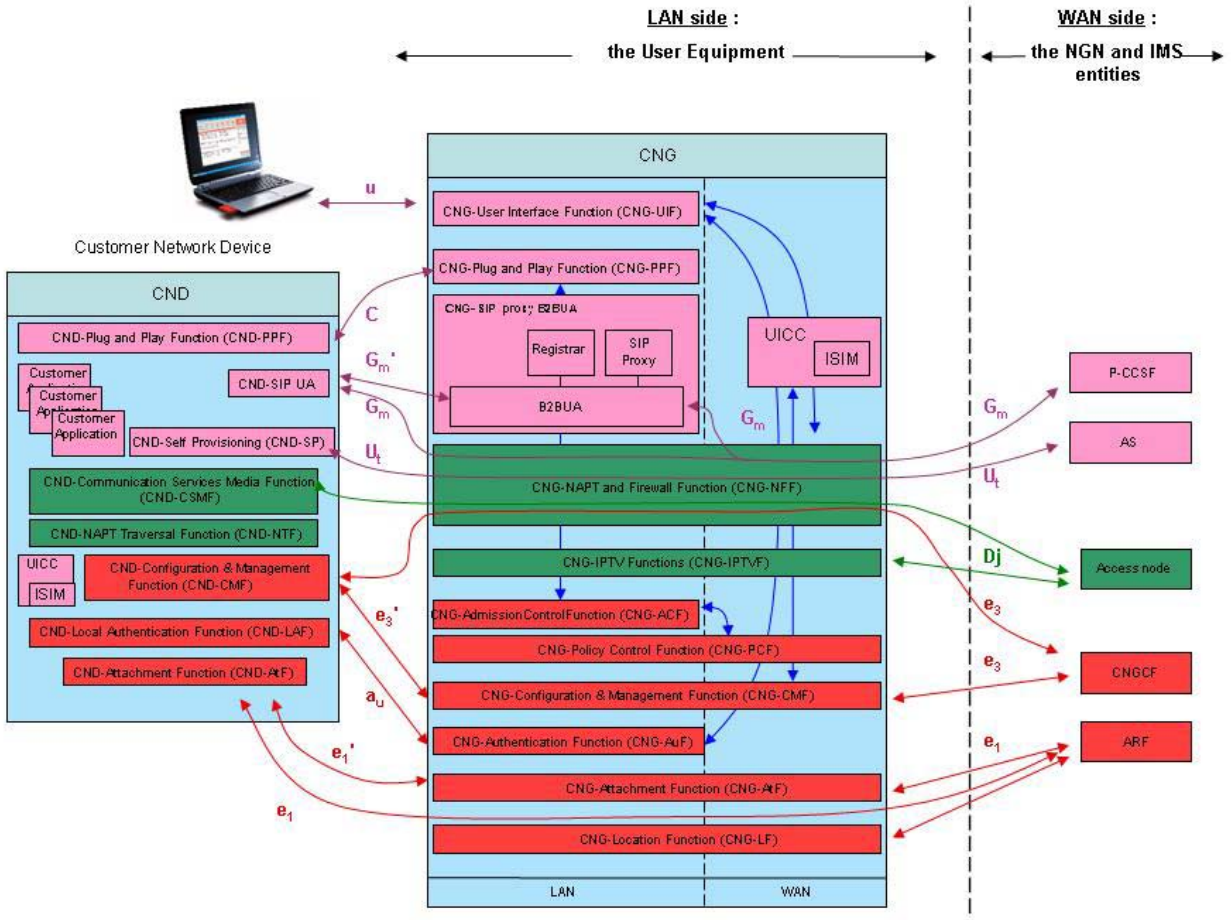


Figure 4.1: IMS CND connected to the NGN-IMS network through a CNG

5 Transport Layer

5.1 Attachment

5.1.1 Protocols on e_1' Interface

The e_1' interface is defined between the CND and the CNG-AtF. In comparison with e_1 interface, the e_1' may implement only a subset of functionalities and due to the fact that e_1' is inside the CPN some implementations can be excluded. In the following clause some examples of e_1' usage are given.

The CNG-AtF provides IP addresses (IPv4 or IPv6 format) to the CND through the CND-AtF, it may also send some configuration information for the CND (typically through DHCP options).

The CNG-AtF gives private IP addresses to the CNDs if the CNG support NAT/NA(p)T function.

5.1.1.1 Hardware identities exchange

In order to mutually exchange hardware identities between a CND and the CNG, it is strongly recommended to implement the DSL Forum specification TR-069 Amendment-1 [1], Annex F (previously TR-111). This specification indicates the usage of the DHCP option 125 to exchange identities. If the CND support the TR-069 that means the CND implement the e_3 reference point also, it is possible apply the following implementation.

As defined in TR-069 [1] (Table 36) the hardware identity of any device, either CNG or CND, is represented by the DeviceId, that is composed by the following three parameters:

OUI	Organizationally Unique Identifier of the device manufacturer. Represented as a six hexdecimal-digit value.
ProductClass	Identifier of the class of product for which the serial number applies. That is, for a given manufacturer, this parameter is used to identify the product or class of product over which the SerialNumber parameter is unique.
SerialNumber	Identifier of the particular device that is unique for the indicated class of product and manufacturer.

As specified in TR-069 (Annex-F Table 78):

- the CND provides its DeviceId to the CNG by using DHCP Option 125, Sub-Option codes 1 (OUI), 2 (SerialNumber), 3 (ProductClass);
- the CNG provides its DeviceId to the CND by using DHCP Option 125, Sub-Option codes 4 (OUI), 5 (SerialNumber), 6 (ProductClass).

5.1.1.2 Discovery of local SIP server within B2BUA

The CND device can discover the SIP server using DHCP option 120 "SIP Server DHCP Option" in case of IPv4 [3].

The CND device can discover the SIP server using DHCP option 21 "SIP Servers Domain Name List" or DHCP option 22 "SIP Servers IPv6 Address List" if using IPv6.

5.1.1.3 CND discovery

The CND discovery task is performed by the CNG and will discover CNDs in the CPN (for example through DHCP, UPnP). This data should be accessible to the CNGCF.

The following introduction to the CND discovery is coherent with the general architectural approach to management activities described in HGI Home Gateway Technical Requirements Release 1 [2] with some terminology modification in coherence with TISPAN terminology.

The CNG discovers the ID from connected CNDs by retrieving and combining information from its ARP [4] cache, DHCP repository, and UPnP Control Point cache. The ARP cache, DHCP repository and UPnP CP cache get their information from the various devices connected to the CNG. To avoid conflicts (arising because a device can be discovered by the ARP cache as well as the DHCP repository or the UPnP CP cache), a priority scheme is needed. HGI gives priority to the information retrieved from the DHCP repository.

The discovered ID information is used by the CNG to fill a Managed Devices Data Base that can be read by the CNGCF. In figure 5.1 the Managed Devices DB is given as a logically separate unit. However, it should be included in the CNG as an extension of the data model, for example extending the DSL Forum data model defined in TR-098 [16] specification as already proposed by HGI.

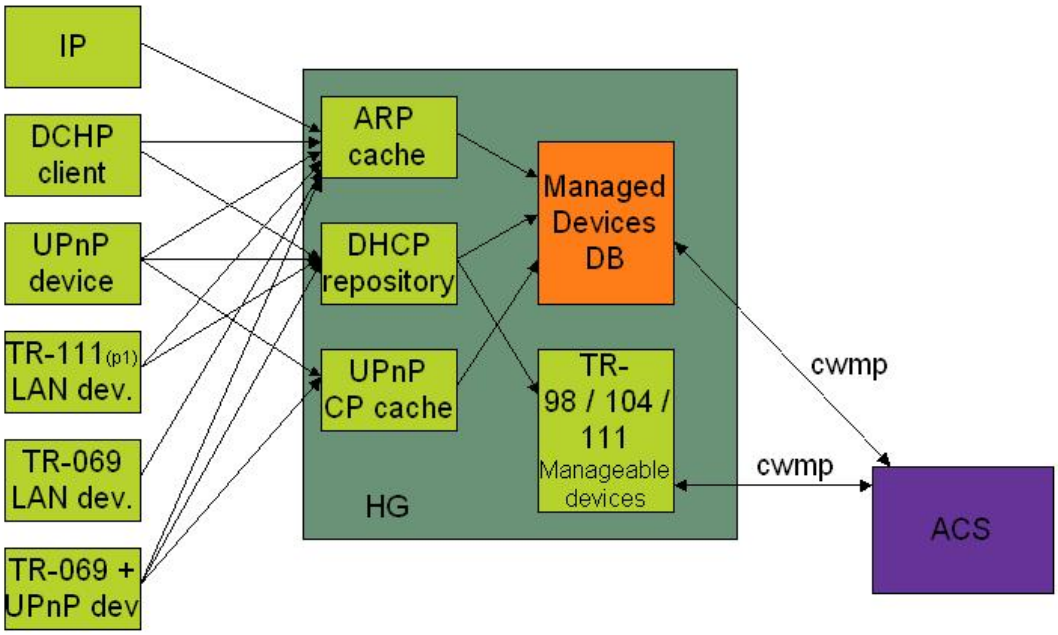


Figure 5.1: From HGI R1 spec - Device management and Discovery

The Managed Devices DB defined in HGI can be mapped in the CNG-CMF defined in TS 185 003 [8]. Note that in figure 5.1 HGI terminology is used. In this case ACS corresponds to CNGCF in TISPAN terminology and HG corresponds to CNG.

5.1.2 Protocols on a_u Interface

The $\mathbf{a_u}$ reference point is defined between the Customer Network Device and the CNG-AuF. There may be two types of authentication/authorization, according to:

- CPN pairing based on specific CPN technologies (e.g. Wifi SSID, PLC technology).
- Access rights for some LAN services like the CNG Configuration (through the CNG-UIF).

In both cases the authenticated entity is a customer network device, while the authenticator is the CNG.

The following details are referred to the CNDs pairing procedures.

A typical scenario for mutual local authentication is shown on figure 5.2.

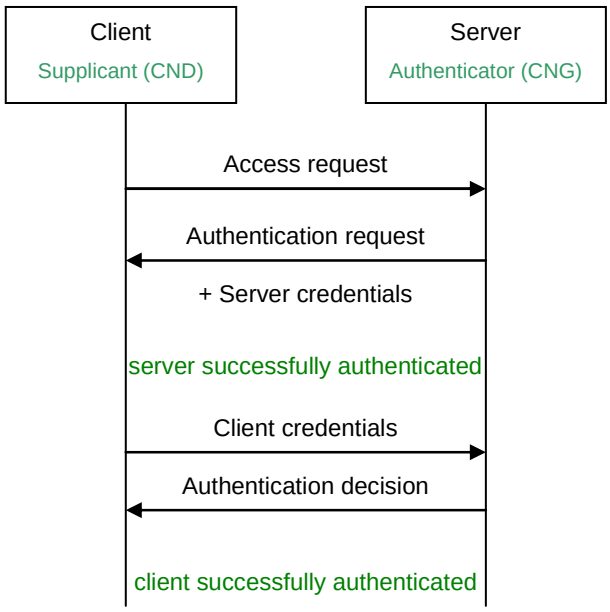


Figure 5.2: Mutual authentication scenario

The first couple of messages allows the server to be authenticated by the client, while the second pair is allowing the supplicant authentication.

In the case of the a_u interface usage, the CND acts as supplicant while the CNG, acting as wireless Access Point, is the authenticator (there is no involvement of any network server). The scenario applies mainly to the wireless CNDs but can be theoretically valid for every possible CND.

There are two possible ways to authenticate the entity: using shared secrets (passwords or symmetric cryptography) or PKI certificates (asymmetric cryptography).

5.1.2.1 Local authentication protocol

A Supplicant and Authenticator conversation uses PPP [11], PANA [12] or IEEE 802.1X [13] encapsulation for EAP. The base authentication protocol is EAP [14].

EAP (Extensible Authentication Protocol) should be considered as the basic authentication protocol, but several methods and variants may be used for authentication. In the table 1 some examples of EAP methods are indicated, with reference to the type of credentials they utilize.

Table 5.1: Examples of EAP methods

Method	Type of method	Server authentication	Client Authentication
EAP-TLS	direct	certificates	certificates
EAP-TLS with TLS-PSK	direct	certificates shared secret	shared secret
EAP-PSK	direct	shared secret	shared secret
EAP-Double-TLS	direct	shared secret	shared secret

The protocol stack for a Supplicant and Authenticator conversation is shown on the figure below. The lower layer with respect to EAP could be PPP, PANA, IEEE 802.1X [13], IEEE 802.11 [17] and so on. The EAP method layer implements authentication algorithm, sends and receives EAP messages and handles fragmentation if needed.

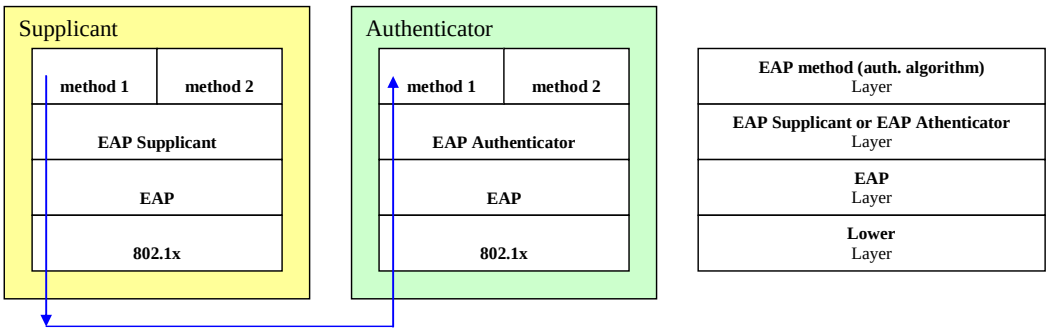


Figure 5.3: EAP entities layers

CNG is an Access Point (AP, IEEE 802.1X [13] authenticator) and Access Controller (AC), granting access to the residential network based on an access list of authorized users.

- Authentication protocol: IEEE 802.1X [13] (EAP) (WPA (Wi-Fi Protected Access)).
- Authentication method: any EAP-compliant method.

An example of the packets exchange of EAP messages encapsulated in IEEE 802.1X [13] is shown on figure 5.4. This diagram is referred to the Wi-Fi Alliance WPA Personal solution, which provides the usage of that protocol (802.1X can be in any case used on its own, independently from WPA).

In the figure two "layers" of entities are shown: two that communicate using 802.1X protocol, that is the so-called supplicant Port Access Entity (PAE, in wireless device) and the authenticator entity (PAE in Access Point), and another two that are using EAP above 802.1X (EAP peer and EAP authentication server).

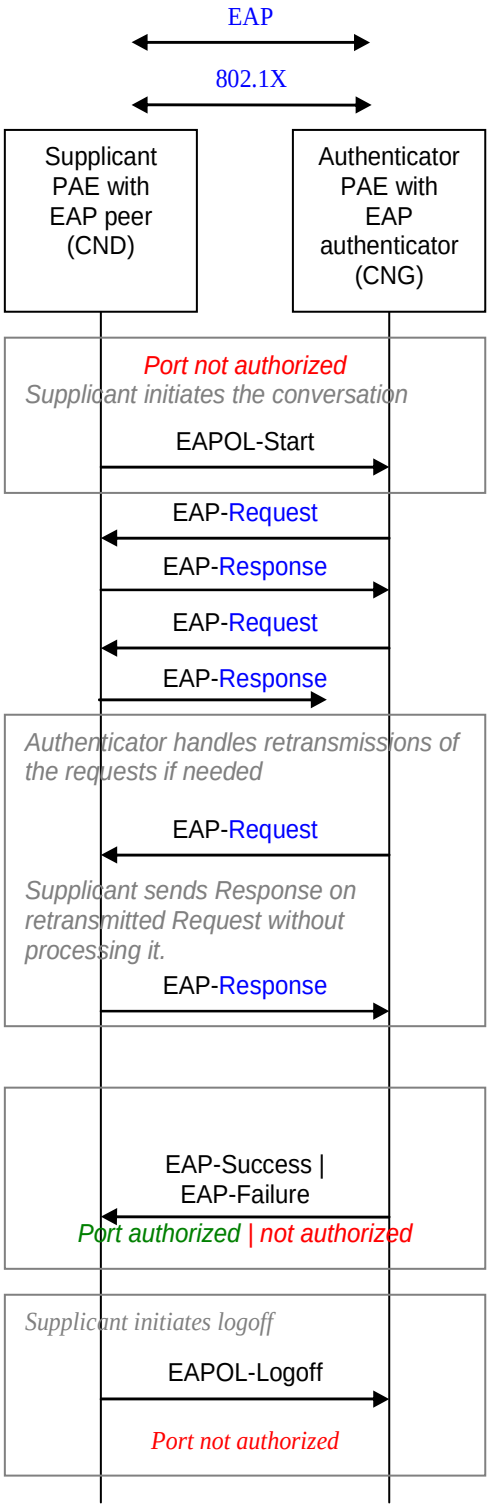


Figure 5.4: EAP messages encapsulated in 802.1X packets exchange

5.2 Management

The following introduction to the CND management is coherent with the general architectural approach to management activities described in HGI Home Gateway Technical Requirements Release 1 [2] with some terminology modification in coherence with TISPAN terminology.

The CND configuration can be done in direct or indirect mode:

- If the supported mode of operation is the direct configuration of the CND by the CNGCF, therefore, the CNG supports the pass-through mode (TR-69) and the managed CND needs to support the TR-069 CWMP protocol as defined for the e_3 interface in TS 183 065 [15].
- If the supported mode of operation is the indirect configuration of CND, a possible solution is given in clause 4.2.2.1.

The CNG can also enable some remote management of simple CNDs that do not support TR-069 [1]. The service provider can use this information to optimize the remote management of the (TR-069) managed devices and to optimize customer service. It is assumed that the CNGCF only communicates with the CPN using TR-069 as defined for the e_3 interface in TS 183 065 [15], and therefore three remote management models can be distinguished. The models are depicted in figures 5.5, 5.6 and 5.7. They are:

- the remote management model for a TR-069-enabled CND with the CNG operating in bridged mode;
- the remote management model for a TR-069-enabled CND with the CNG operating in routed mode;
- the remote management model for a CND that does not support TR-069, but is locally managed by the CNG acting as remote management proxy.

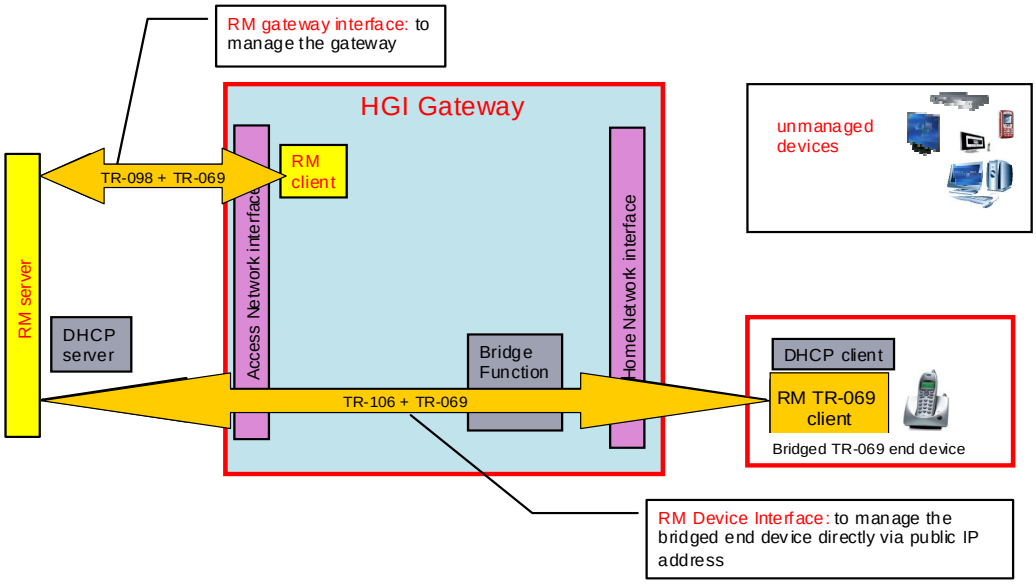


Figure 5.5: From HGI R1: Remote management model for TR-069-enabled end devices with the Home Gateway operating in bridged mode

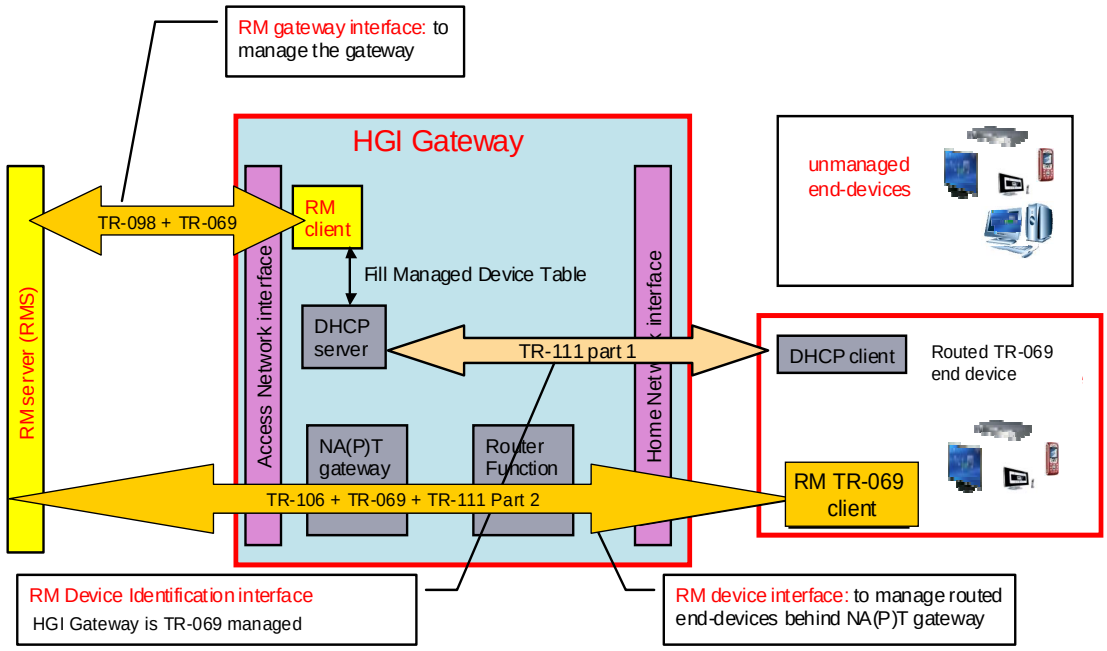


Figure 5.6: From HGI R1: Remote management model for TR-069-enabled end devices with the Home Gateway operating in routed mode

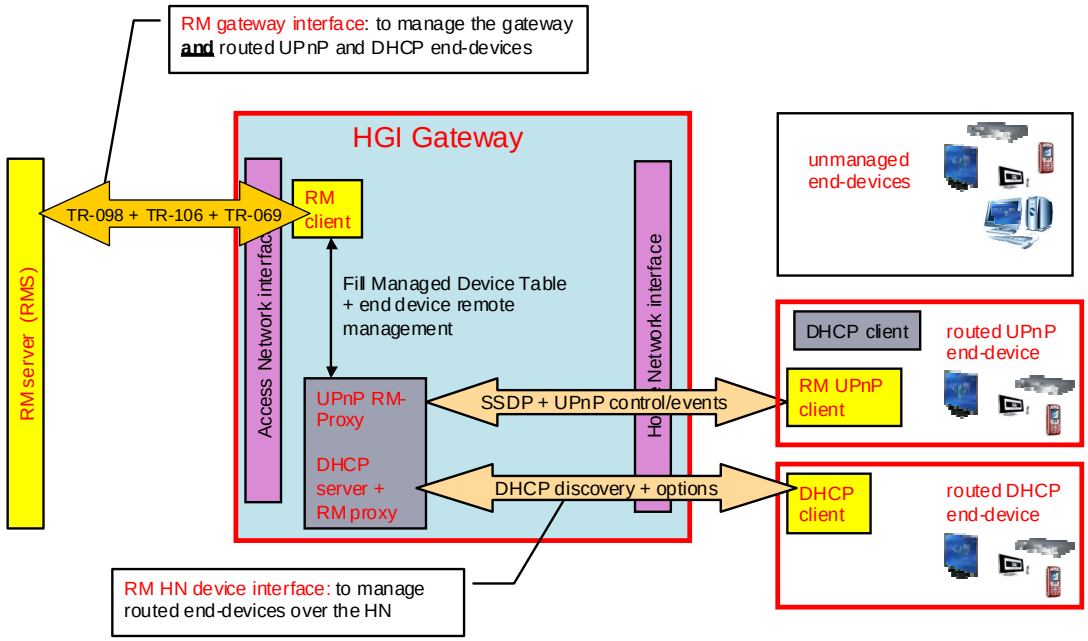


Figure 5.7: From HGI R1: Remote management model for UPnP and DHCP-enabled end devices with the Home Gateway operating in proxy mode. HGI Release 1 only deals with discovery of the end devices

From figure 5.5 to 5.7 HGI terminology is used, in order to map this terminology with TISPAN terminology the following mapping can be applied:

- HGI Gateway corresponds to CNG.
- Access Network Interface corresponds to WAN side interface.

- Home Network Interface corresponds to CPN side interface.
- RM server corresponds to CNGCF.
- RM client corresponds to CNG-CMF defined in TS 185 003 [8].

A distinction is made between managed and unmanaged end devices.

- A managed device is a device that has a remote management client that communicates directly or indirectly (via the CNG) with a remote management server (CNGCF).
- An unmanaged device is a device that does not have a remote management client, or that does not communicate directly or indirectly (via the CNG) with a remote management server (CNGCF).

From management point of view is possible to distinguish the following type of CND:

- CND that support TR-069 remote management as specified for e_3 reference point (TS 183 065 [15]).
- CND that support local management protocols on the e_3' reference point (as described in clause 4.2.2.1).
- User-configured or pre-configured unmanaged IP devices, including proxies to non-IP devices.

5.2.1 Protocols on e_3 Interface

In order to manage the CNG from the CNGCF on the e_3 interface, as defined in TS 183 065 [15], it is strongly recommended to implement the CWMP protocol as described in DSL Forum TR-069. The CWMP remote management protocol is based on the candidate protocols recommended in ES 282 004 [18].

In order to manage the CND from the CNGCF on the e_3 interface it is strongly recommended to implement the CWMP as described in TR-069 (including previous TR-111) [1]. In this case the CND can support a protocol for NAT/NA(p)T traversal. The STUN protocol is a possible solution to implement the NAT/NA(p)T traversal.

5.2.2 Protocols on e_3' Interface

5.2.2.1 Provisioning on CND with parameters enabling NGN services usage

This clause describes how to deliver the identities and credentials, needed to access the NGN, on CND from CNG through the e_3' interface. Starting from the assumption that these identities and credentials are already delivered on the CNG, through the e_3 interface from CNGCF using TR-069, or are stored in an ISIM on UICC in the CNG; this clause describes how to communicate these information to the CNDs.

The identities and credentials stored in CNG are based on the following parameters: IMPU, IMPI, Shared keys, Home Network Domain, outbound proxy (P-CSCF IP Address) and authentication realm.

The protocol is based on HTTP, so an HTTP server on CNG and a browser on CND are required.

The CND requests are sent through an HTTP GET to the CNG and the CNG will reply with configuration messages or error messages in XML format.

The CND is able to send three types of request:

1) request for available identities on CNG;
2) request for choosing an identity;
3) request for removing an associated identity.

The CNG is able to produce three corresponding types of response:

1) sending a list with all identities available;
2) confirming if the selected identity is associated;
3) confirming if the selected identity is deallocated.

EXAMPLE: The CND is plugged on the CNG and switched on for the first time:

- through the e_1' interface the CND obtains a private IP address and exchanges hardware identities with CNG;
- through the e_3' interface the CND sends the request for available NGN identities to the CNG;
- the CNG sends the list in XML format;
- the user select an identity (or a default identity is automatically selected by the CND) and the CND sends the request for choosing identity to the CNG;
- than the CNG associates the NGN identity with hardware identity and sends a confirmation to the CND;
- now the CND is ready to send a REGISTER message to the NGN.

5.2.2.2 Provisioning Information Flow

A CND may be provisioned using the e_3 protocols, the e_3' protocol or manually.

If the CNG supports the e_3' protocol, a CND supporting e_3' protocol will be successfully provisioned.

If the CNG does not support the e_3' protocol, a CND not supporting e_3' protocol may be provisioned only with e_3 protocol or manually.

In case a CND supports both e_3 and e_3', and assuming that CNG does not support e_3', then, in order to choose a reference point between e_3 and e_3', it is necessary to distinguish two cases:

- Case 1: Configuration parameters are provisioned by CNGCF to CND indirectly (trough the CNG).
- Case 2: Configuration parameters are provisioned by CNGCF to CND directly.

A possible CND's behaviour can be the following:

- the CND sends the identities request message, on e_3', to the CNG;
- if the CNG answer with the list of configuration parameters (see 4.2.2.1), then Case1;
- if the CNG answers with an error message, then Case2 and the CND can therefore send a notification (by means of the Inform RPC), on e_3 (CWMP), to the CNGCF in order to request the necessary configuration data (it is up to the CNGCF to provision the appropriate configuration data to the managed CNDs).

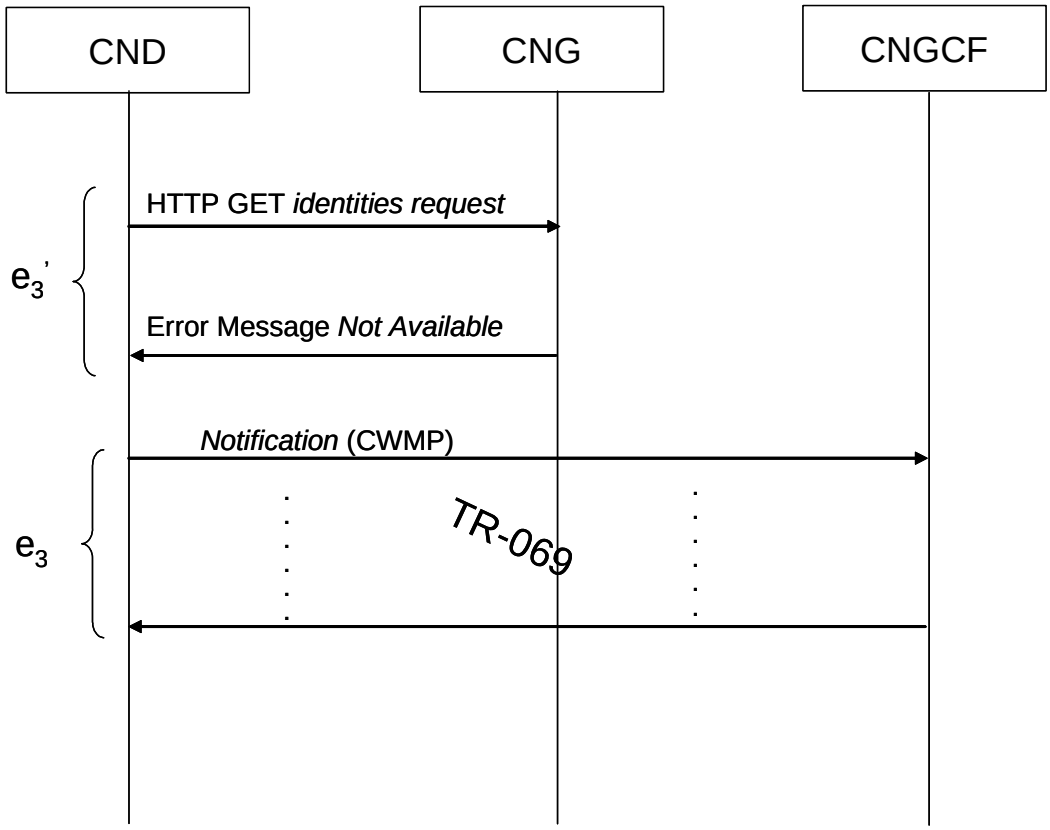


Figure 5.8: Case 2 Provisioning base on e_3

Summarizing:

- in Case 1, the solution described in clause 4.2.2.1 will be used;
- in Case 2, the CND tries to use the solution described in 4.2.2.1, but the CNG answers with an error message and then the CND sends a notification (CWMP) to the CNGCF trough the e_3 reference point.

5.2.3 Protocols on U Interface

The U interface [8] gives the possibility to one or several users authorized (via the CNG-AuF) to have access to the CNG Configuration, through the CNG-UIF. The connection should be as secure as possible (using HTTPs for instance).

An authorized user can access to the CNG Configuration by a GUI. This clause describes the GUI accessible through the u reference point.

The CNG GUI gives information and status of the different services provided through the CNG to the user. The u reference point is also used to configure the CNG, that means to set up NGN and CPN connections, services, security, etc., and to allow a remote configuration of the CPN by the operator.

Figure 5.9 presents a possible structure of the GUI.

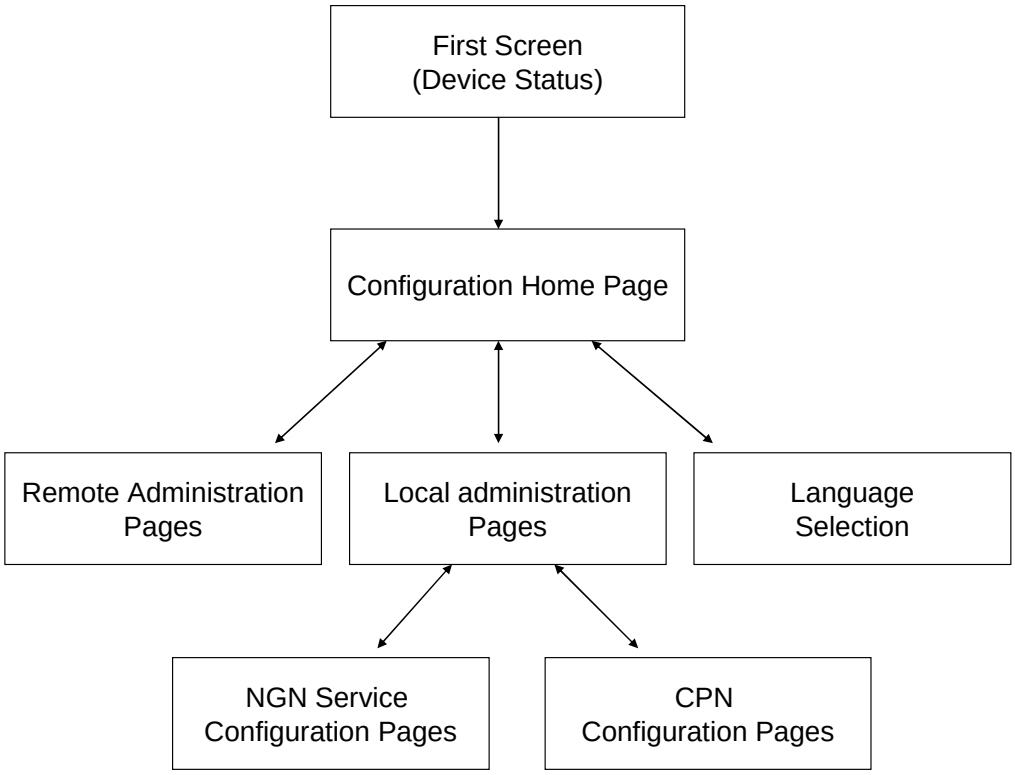


Figure 5.9: GUI structure

Possible protocols for the GUI page are the following:

- HTML, XML for the webpage language.
- HTTP for the Webpage access.

5.2.3.1 Presentation (First page)

To access to the GUI, the user should click on the CNG icon which he should find on his computer desktop. This shortcut may be created during the installation process. Otherwise, he should directly go to the CNG GUI from a Web browser, for instance at the following address: http://192.168.1.1, or http://CNG-alias (IP address locally resolved by the CNG).

The user arrives then at the first screen of the GUI.

5.2.3.2 Configuration pages

If the user wants to access to the configuration pages, he should click on one hyperlink. He should be prompted then to enter the CNG username and password.

The CNG administration interface should be protected by a username/password. Operator should provide the default username and password.

- The default username may be: admin.
- The default password may be: admin.

The administrator user should be able to change those parameters through the configuration pages.

If the configuration password is incorrect, a pop up should appear and notice that the password is incorrect by the following message "The 2 passwords do not match" for instance.

5.2.3.2.1 Languages

The GUI should offer several languages, and the user should be able to switch from one to another.

5.2.3.2.2 Local administration

Some CPN parameters may be configured by the user locally.

After changing any setting on the CNG GUI:

- If the changes do not require rebooting the CNG, a page should appear with the following message: "Configuration successful" and the GUI returns automatically to the Welcome page.
- If the changes require rebooting the CNG or restarting a critical service, a new GUI page should appear. It should contain a message, for instance "configuration successful", and also a button ("Apply the configuration now"), which should be used to apply changes. If the user does not click on the button, changes are not applied.

5.2.3.2.3 Remote administration

The CPN is remotely configured using TR-069 through the e_3 reference point.

If the remote administration is not active, the following message should be displayed on the GUI page "The remote administration mode is currently inactive".

If the CNG is not connected to the internet, it is not possible to activate the remote administration. Moreover, the following message should be displayed: "You do need to be connected to the Internet in order to activate the remote management function".

5.2.3.3 Examples for the GUI implementation

5.2.3.3.1 Presentation (First page)

The following parameters should be considered as examples for the GUI presentation page content.

Menu path	**First page**	
Description	**Field**	**Default**
Name of the CNG (=SSID)	Name: text info	factory setting
ADSL and PPP connection status (Link down, Synchronization in progress, etc. invalid ADSL authentication, if the CNG is connected to the internet, the NGN IP@ (or private IP@ allocated to the CNDs by the CNG) is also displayed	ADSL status text info	Current status
Hypertext link used to directly access to the GUI configuration pages	Configuration pages access (restricted access, protected by password). Hyperlink	N/A

5.2.3.3.2 Configuration

The configuration pages summarize all the services carried by the CNG: the following examples are given underneath for the Internet, VoIP, IPTV, videophony services.

Menu path	**Welcome on my services**	
Description	**Field**	**Default**
Name of the CNG (=SSID)	Name: text info	factory setting
Internet service status (activated: enable or deactivated: disable)	status text info	Enable
Hypertext link used to directly access to the Internet setup and status page	Change hyperlink	N/A
Telephony over ADSL service status (activated: enable or deactivated: disable)	status text info	Disable
Hypertext link used to directly access to the Telephony over ADSL setup and status page	Change hyperlink	N/A
TV over ADSL service status (activated: enable or deactivated: disable)	status text info	Enable
Hypertext link used to directly access to the TV over ADSL setup and status page	Change hyperlink	N/A
Videophony over ADSL service status (activated: enable or deactivated: disable)	status text info	Disable
Hypertext link used to directly access to the Videophony over ADSL setup and status page	Change hyperlink	N/A

5.2.3.3.2.1 Language selection

Examples are given hereafter for the parameters related to language configuration.

Menu path	**Configuration/Languages**	
Description	**Field**	**Default**
Button used to select the administration interface language	French button English button	French
Button used to apply the new language	Submit button	N/A

5.2.3.3.2.2 Local administration

Some examples for local administration parameters are given hereafter:

Menu path	**Configuration/Administrator**	
Description	**Field**	**Default**
Administrator name (admin compulsory)	Login text field	admin
Administrator password (limited to 20 characters)	Password encrypted text field	Current password (factory setting: admin)
Confirmation of the administrator password (limited to 20 characters)	Confirm encrypted text field	Current password (factory setting: admin)
Button used to apply the new password	Submit button	N/A
NAPT configuration	NAPT configuration rules	Default NAPT behaviour
Port forwarding	Port forwarding rules	None
MAC@ authorized for WiFi connection	MAC@ text field	MAC@ of the CPN
Service activation	Service text field	Disable
Security level (firewall)	Security text field	medium

5.2.3.3.2.3 Remote administration

The authorized user should be able to activate the remote administration.

Menu path	Configuration/Assistance	
Description	**Field**	**Default**
Button used to activate the remote administration	Activate button	N/A

5.3 Transfer Layer

This layer is based on Dj interface for media transfer [10].

6 Service Layer

6.1 Protocols on U_t Interface

This interface is specified in TS 183 038.

6.2 Protocols on G_m Interface

This interface is specified in ES 283 003 [5].

6.3 Protocols on C Interface

The C interface is defined in [8]. The protocols to be used on C interface are for further study.

6.4 Protocols on G_m' Interface

In comparison with G_m interface, the G_m' may implement only a subset of functionalities specified in [5]. In the following clause some examples of G_m' usage are given.

6.4.1 Procedures for registering non-IMS SIP IETF devices in CNG over G_m'

There are two alternatives when registering non-IMS SIP IETF devices in the CNG

- Non-IMS SIP IETF device registers a local SIP URI.
- Non-IMS SIP IETF device registers a public SIP URI (IMPU).

6.4.1.1 Registration of local SIP URI

The non-IMS SIP IETF device registers a local SIP URI (terminal-id@myhome) to the local SIP registrar. The terminal-id part of the SIP URI is an arbitrary text string that might be preconfigured in the device. The domain name part of the SIP URI is the address of the local SIP server. Pre-configuring of devices enables "plug and play" functionality i.e. the user does not need to configure the device. The B2BUA can handle the case where two SIP devices register the same local SIP URI.

The CNG is provisioned with public IMPUs and maps between public IMPUs and local SIP identities:

- If a device registers a local SIP URI then the B2BUA registers the associated public IMPUs in IMS, if not already registered.

NOTE: If there is a built-in Analogue Telephone Adapter (ATA) associated with a public IMPU then this IMPU should always be registered.

- If a device de-registers a local SIP URI then the B2BUA de-registers the associated public IMPUs if no other device requires this IMPU.

- If a device is associated with multiple public IMPUs the preferred IPMU for outgoing calls is configurable in the CNG.

It should also be possible to configure an alias for a local SIP URI that can be used locally to address the device in the CPN.

6.4.1.2 Registration of public SIP URI

The non-IMS SIP IETF device is configured with a public IMPU either by the user or by CND Configuration Management function.

The non-IMS SIP IETF device sends a SIP Register. The B2BUA can distinguish between the following two cases:

- The public SIP URI (IMPU) is not pre-configured in the CNG but exists in CND.

If the non-IMS SIP IETF device registers a public SIP URI (IMPU) that not is pre-configured in the CNG then the B2BUA can forward the IMPU together with other related parameters (e.g. authentication header) added by the CNG to the WAN.

- The public SIP URI (IMPU) is preconfigured in the CNG but not in CND.

If a non-IMS SIP IETF device registers a public SIP URI (IMPU) that is pre-configured in the CNG then the B2BUA registers the IMPU in NGN-IMS and handles authentication on behalf of the device. The B2BUA then acts as an outbound proxy. The B2BUA adds authorization header and forwards the request to the NGN-IMS. The CNG handles authentication on behalf of the non-IMS SIP IETF device. In case of HTTP Digest Authentication is used then the B2BUA can add the Authorization header.

History

Document history		
V2.0.0	March 2008	Publication