



1  
2  
3  
4  
5  
6

7

8

# Home Gateway Technical Requirements: Release 1

9

Version 1.0

10

1 July 2006

11

12

13

14

15

16

17

18

19

20

21

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29

PAGE LEFT INTENTIONALLY BLANK

# 1 Table of Contents

2	Table of Contents .....	3
3	1 Important notice, IPR statement, disclaimer and copyright.....	7
4	2 Introduction and scope of the Home Gateway Initiative.....	8
5	2.1 Cooperation with other bodies and initiatives.....	8
6	3 Purpose of this document.....	9
7	3.1 Structure of the document.....	9
8	3.2 Definition of terms .....	9
9	4 HGI Network and Service requirements.....	10
10	4.1 Service support .....	10
11	4.1.1 Brief overview of the Use Case approach and business requirements process.....	10
12	4.1.2 Overview of use cases .....	10
13	4.1.3 Business Requirements Summary.....	12
14	5 HGI Reference Architecture .....	14
15	5.1 End-to-end Network Architecture .....	14
16	5.1.1 Connectivity.....	15
17	5.1.2 QoS .....	15
18	5.1.3 OAM and Management .....	15
19	5.1.4 Encapsulation and session support .....	16
20	5.1.5 IP Addressing .....	16
21	5.1.6 Security.....	16
22	5.1.7 Non Requirements .....	16
23	5.2 Home Network Architecture .....	17
24	5.2.1 HG Architectural Models .....	17
25	5.2.1.1 Basic Considerations.....	17
26	5.2.1.2 Architectural models Supported .....	18
27	5.2.2 Home Network Overview.....	19
28	5.2.2.1 Home Network Connectivity.....	19
29	5.2.2.2 User requirements.....	20
30	5.2.2.3 Service support requirements .....	21
31	5.2.2.4 Home Networking Technologies .....	21
32	5.2.2.5 Home Network Architecture .....	23
33	5.2.2.6 Home Network Technologies Supported .....	24
34	5.3 Home Gateway Functional Overview.....	25
35	5.3.1 Basic Assumptions .....	25
36	5.3.2 Home Gateway Functionalities: block diagram.....	26
37	5.4 Management Architecture .....	28
38	5.4.1 Device Management .....	31
39	5.4.2 QoS Management .....	35
40	5.4.3 Security Management .....	35
41	5.4.4 Software Management and Upgrade .....	36
42	5.4.5 Performance Monitoring and Diagnostics & Troubleshooting.....	36
43	5.4.6 Local Management Application .....	37
44	5.5 QoS Architecture .....	38
45	5.5.1 End-to-end architecture.....	38
46	5.5.2 Potential Congestion Points .....	38
47	5.5.2.1 The Home Gateway upstream .....	38
48	5.5.2.2 The HG Downstream.....	38
49	5.5.2.3 HG Transit Traffic.....	39
50	5.5.3 Bridges and switches in the Home Network.....	39
51	5.5.4 Basic principle of operation .....	39
52	5.5.5 DSCP and VLAN Usage.....	39
53	5.5.6 Traffic Classification .....	40
54	5.5.7 Upstream Classifiers .....	40
55	5.5.7.1 IP Destination Address (IP DA).....	40

1	5.5.7.2	IP Source Address (IP SA).....	40
2	5.5.7.3	Physical port.....	40
3	5.5.7.4	Packet Length.....	40
4	5.5.7.5	MAC Source Address (SA) and Destination Address (DA).....	41
5	5.5.7.6	TCP/UDP Port number.....	41
6	5.5.7.7	Protocol type.....	41
7	5.5.8	Downstream Classifiers.....	41
8	5.5.9	Transit classifiers.....	41
9	5.5.10	QoS Mapping.....	41
10	5.5.11	Upstream Queue structure.....	41
11	5.5.11.1	Downstream and Transit Queue Structure.....	42
12	5.5.12	Class Based QoS, Sessions and Policy.....	42
13	5.6	Security issues.....	42
14	5.6.1	Firewall protection.....	43
15	5.6.2	VPN Capabilities.....	43
16	5.6.3	Encryption algorithms.....	43
17	5.6.4	Code authentication / Signature.....	43
18	5.6.5	Local Configuration Secured Access.....	44
19	5.7	Powering, Safety and EMC.....	44
20	6	Home Gateway Requirements.....	45
21	6.1	WAN Side Interfaces.....	45
22	6.1.1	Type 1 - ATM over DSL Interface.....	45
23	6.1.2	Type 2 - Ethernet over DSL Interface.....	46
24	6.1.3	Type 3 - Ethernet WAN Interface.....	47
25	6.1.4	WAN Interface Combinations.....	47
26	6.1.5	PSTN Interface.....	47
27	6.2	LAN Side Interfaces.....	47
28	6.2.1	Wireless LAN Interface requirements.....	48
29	6.3	Packet processing.....	49
30	6.3.1	Support of routed model and extensions WAN side.....	49
31	6.3.2	Support of routed model and extensions LAN side.....	50
32	6.3.2.1	NAT.....	50
33	6.3.2.2	IP Addressing schemes.....	51
34	6.3.2.3	LAN-side DHCP requirements.....	51
35	6.3.3	Support of Hybrid Model and Extensions.....	53
36	6.3.4	Session Initiation and Support.....	53
37	6.4	Quality of Service.....	54
38	6.4.1	Classification of traffic.....	54
39	6.4.1.1	Requirements for Classification of packets received upon the WAN ingress.....	55
40	6.4.1.2	Requirements for Classification of LAN-LAN traffic.....	56
41	6.4.1.3	Requirements for Multi-field Classification packets received on the LAN ingress ports.....	57
42			
43	6.4.1.3.1	Requirements for Classification of packets received on the LAN ingress using information determined by DHCP Options 60, 61, and 77.....	58
44			
45	6.4.1.4	Requirements for Classification of bridged packets received on the LAN ingress ports.....	59
46			
47	6.4.2	LAN-side VLAN support.....	59
48	6.4.3	Classification Rule Sets.....	60
49	6.4.3.1	Overview.....	60
50	6.4.3.2	Requirements for Classification Rule Sets.....	60
51	6.4.3.3	Requirements for Sequencing Among Classification Rule Sets.....	61
52	6.4.4	Overload Protection Mechanism.....	61
53	6.4.5	QoS Mappings.....	62
54	6.4.5.1	Overall Mappings.....	62
55	6.4.5.1.1	HG Egress Markings.....	62
56	6.4.5.2	Integrated Access Devices.....	63
57	6.4.6	Dropping/Congestion Management.....	63

1	6.4.7	Class Queue structure and Scheduling.....	64
2	6.4.7.1	Queuing into the WAN Egress port.....	64
3	6.4.7.2	Queuing into the LAN Egress ports.....	65
4	6.4.7.3	Example of Queuing Configuration.....	65
5	6.4.8	QoS Management Object.....	66
6	6.4.8.1	Overall Requirements.....	66
7	6.4.8.2	Notation.....	66
8	6.4.8.3	HGI QoS Profile.....	67
9	6.4.8.4	HGI QoS Dynamic Profile.....	69
10	6.4.9	Non-Integrated Device Requirements.....	70
11	6.4.9.1	LAN Infrastructure Devices.....	70
12	6.4.9.2	Non-integrated Ethernet Infrastructure Devices.....	70
13	6.4.9.3	End devices.....	71
14	6.4.9.3.1	Informative notes on Set Top Boxes and VoIP Client Devices.....	71
15	6.5	Management.....	72
16	6.5.1	Northbound Interfaces.....	72
17	6.5.2	RMS Requirements.....	72
18	6.5.3	General HG configuration and management.....	73
19	6.5.4	Definition of the data model supported.....	74
20	6.5.5	Diagnostics, notifications and alarms.....	74
21	6.5.5.1	Notifications and logging.....	75
22	6.5.5.1.1	Mechanisms.....	75
23	6.5.5.1.2	Notification cases.....	75
24	6.5.5.2	Statistics and Diagnostics.....	76
25	6.5.5.2.1	Mechanisms.....	76
26	6.5.5.2.2	Defined diagnostics and statistics.....	76
27	6.5.6	End device management.....	80
28	6.5.6.1	Device Identification.....	80
29	6.5.6.2	Activity discovery and Database management.....	81
30	6.5.7	Local HG management user interface.....	84
31	6.5.7.1	General.....	85
32	6.5.7.2	Design guidelines.....	85
33	6.5.7.3	Operator Portal User Interface link.....	86
34	6.5.7.4	Contents and functionality.....	86
35	6.5.8	Firmware management and updates.....	87
36	6.5.8.1	General.....	88
37	6.5.8.2	Software upgrades.....	88
38	6.5.8.3	Configuration.....	89
39	6.5.8.4	User Interaction.....	90
40	6.5.9	Security management.....	90
41	6.5.9.1	Firewall management.....	90
42	6.5.9.2	Application Layer Gateway Management.....	91
43	6.5.10	End-device recommendations.....	92
44	6.6	Service Support.....	92
45	6.6.1	ALGs.....	93
46	6.6.2	Communication Services Support.....	94
47	6.6.3	Multimedia Services Support.....	96
48	6.7	Security.....	97
49	6.8	Basic System Features.....	98
50	6.8.1	Powering, safety, EMC, and other regulatory requirements.....	98
51	6.8.1.1	Powering.....	98
52	6.8.1.2	Electrical Safety.....	99
53	6.8.1.3	EMC.....	99
54	6.8.1.4	Other considerations (Environmental, reliability).....	99
55	6.8.1.5	Regional regulatory requirements.....	100
56	7	Appendix.....	101

1	7.1	An example of TR-098 configuration to implement the proposed HGI QoS	
2	classification	and queuing .....	101
3	8	HGI Release 2 .....	104
4	9	References .....	105
5	10	Acronyms.....	108
6	11	Definitions.....	111
7			

# 1 Important notice, IPR statement, disclaimer and copyright

3 The Home Gateway Initiative is a non-profit making organization created to define guidelines  
4 and specifications for broadband Home Gateways.

5 This document is the output of the Working Groups of the Home Gateway Initiative (HGI)  
6 and its members as of the date of release. Readers of this document must be aware that it can be  
7 revised, edited or have its status changed according to the Home Gateway Initiative working  
8 procedures.

9 The Home Gateway Initiative makes no representation or warranty on the contents,  
10 completeness and accuracy of this publication.

11 This document, though formally approved by the HGI member companies, is not binding in  
12 any part on the Home Gateway Initiative members.

13 IPRs essential or potentially essential to the present document may have been declared in  
14 conformance to the HGI IPR Policy.

15 Copyright of this document extends to reproduction in all media.

16 Trademarks and copyrights mentioned in this document are the property of their respective owners.

17  
18 The HGI membership list as of the date of the formal review of this document is: 2Wire, Inc.,  
19 ALCATEL, AVM, Belgacom, BeWAN, BridgeCo AG, BT, Conexant, Corinex, Deutsche Telekom,  
20 DS2, Echelon, ECI, Emotum, Ericsson, Fastweb, France Telecom, Fraunhofer ESK, Freescale,  
21 Genesis, Huawei, IBM, Infineon Technologies, Intel, Intellon, Jungo Software Technologies, KPN,  
22 KT Corp., LG- Nortel Inc., LINKSYS, Lucent, Microsoft, Motive, Inc, Motorola, Netopia, NTT,  
23 Passave Inc., Philips, Pirelli, PMC Sierra, Portugal Telecom Inovacao SA, Sagem, Siconnect,  
24 Siemens, STMicroelectronics, Supportsoft, Swisscom AG, Telecom Italia, Telefonica, Telenor,  
25 TeliaSonera, Telkom, Telsey, Telstra, TELUS, Texas Instruments, Thomson, Tilgin, TNO ICT,  
26 Ubicom, ZTE, ZyXEL

## 2 Introduction and scope of the Home Gateway Initiative

Home connectivity has evolved dramatically over recent times. From the initial simple voice service, home services evolved in the 80s to include things such as fax and video text, with the 90s seeing the advent of mass-market Internet access via dial-up modems. At the start of the 21st century, the world has entered the broadband era. Network operators have deployed technology that offers much larger bandwidths, such as DSL, cable or fibre-based access systems.

The Internet has been a major driver for the evolution to broadband, creating a new experience for the customer and offering him new services such as email and Internet browsing, and “online” versions of existing services such as digital photo labs, ticket booking etc.

The next generation of broadband services (triple or even “multiple-play”) has created a set of new requirements for the Home Gateway, namely:

- the need to manage the Home Gateway, and to a lesser extent, the home network and the devices beyond the Home Gateway
- allowing the right device or application to connect to the right service platform with the right service class / Quality of Service
- unifying device capabilities in order to offer customers a better “integrated home environment”.

Due to the lack of suitable off-the-shelf and standardized products to support this new, end-to-end network and service model, several major Telecom Operators have recently worked separately with a very small number of Home Gateway vendors to specify and develop suitable Gateways. However, such custom development is not cost-effective for either operators or vendors.

It became apparent that many operators had similar service aspirations, and so were asking for similar equipment. Therefore in December 2004, nine Telecom Operators founded the Home Gateway Initiative to see if they could agree on a common Gateway specification. The intention was to involve the relevant vendor community (i.e. vendors of gateways, chipsets, software, devices and transmission systems) so that the specifications would also be pragmatic and could be realized in a cost-effective manner.

The aim of HGI is therefore to specify a small range of low cost, high capability Gateways which will provide multi-service communication support for the residential and SOHO environments. While an end-to-end network view has been taken, the specifications mainly focus on the Home Gateway device which sits between the access network and service platforms on one side, and the in-home networked devices and applications on the other.

### 2.1 Cooperation with other bodies and initiatives

The Home Gateway Initiative does not wish to become a new, long-term de facto standardization body. Its initial task is to agree a set of functional requirements for a Home Gateway, wherever possible re-using or referring out to existing specifications. An important aspect of the work is to identify gaps and inconsistencies in or between existing specifications. The HGI will publish its own specifications, but will work alongside other SDOs to ensure that issues are addressed in the most appropriate body, there is no unnecessary duplication of effort, and that the HGI specifications are downstreamed in the most appropriate way.

## 3 Purpose of this document

Starting from a set of business requirements and an end-to-end reference architecture (for networks, services and management) the HGI has derived a homogeneous set of requirements for the Home Gateway. The end-to-end approach ensures that all the requisite functionality is included in the Gateway specification. From the HGI perspective, while the main role of the Home Gateway is to support the premium services provided by Telecom Operators, it must also allow the customer to connect and operate Consumer Electronics equipment and other devices which may have nothing to do with these premium services. The model adopted in HGI release1 implies that the Home Gateway is provided and controlled by the Telecom Operator. All the requirements in this document are related to this scenario. In future releases, additional business models might be supported, and this may have an impact on the technical requirements.

This document presents the entire set of requirements for the Home Gateway and defines mechanisms for the integration of the Gateway with home devices and networks, services, public network interfaces and servers.

This document is intended to be used as a whole, or in part, in tenders and procurement activities, and also provides an important framework for the development and design of HG equipment. The aim has been to produce a specification quickly to avoid further custom Gateway development and to make the requirements as precise as possible, by having very few options.

### 3.1 Structure of the document

The HGI process has to be started with use cases and business requirements (Section 4) along with a set of high level requirements on the end-to-end network functionalities produced by the Architectural Task Force (Section 5.1) Note that these documents are HGI internal documents and thus only available to HGI members. The individual Working Groups then produced detailed sets of formal functional requirements which are amalgamated in Section 6. The contents of Sections 4 and 5 are informative only. Additional details and examples are included in various Appendixes.

### 3.2 Definition of terms

**MUST** A functional requirement which is based on a clear consensus among HGI Service Provider members, and is the base level of required functionality

**MUST NOT** This function is prohibited by the specification

**SHOULD** Functionality which goes beyond the base requirements, which is desirable and for which there is again a clear consensus among HGI Service Provider (SP) members, but which may have a cost/complexity impact. SPs may take a different view on whether the cost of such additional functionality is justified.

**MAY** A functional requirement where there is a significant (i.e. more than one SP), but lesser, level of interest among HGI Service Provider members

Note: These definitions are specific to the HGI and should not be confused with the same or similar terms used by other bodies.

## 4 HGI Network and Service requirements

### 4.1 Service support

#### 4.1.1 Brief overview of the Use Case approach and business requirements process

In order to define the technical specifications, the HGI business group produced use cases and business requirements for the technical groups.

The process has been based on the DLNA use case approach, adapted to HGI needs. The objective is to deliver concrete usage scenarios, which are specific examples of use cases, from which overall business requirements for the gateway are derived.

Each usage scenario has three parts: a Consumer Usage Scenario, a Broadband Service Provider (BSP) Usage Scenario and a Business Requirements List for the Home Gateway. Each usage scenario is further divided into different phases: equipment purchase/service subscription, installation, usage, support, and usage scenario deactivation phases.

Global usage scenarios have also been defined to illustrate simultaneous use of multiple HG-enabled services. These scenarios provide a sense of the performance and feature support levels that are expected from the HG.

Figure 1 details the use case selection and requirement production process.

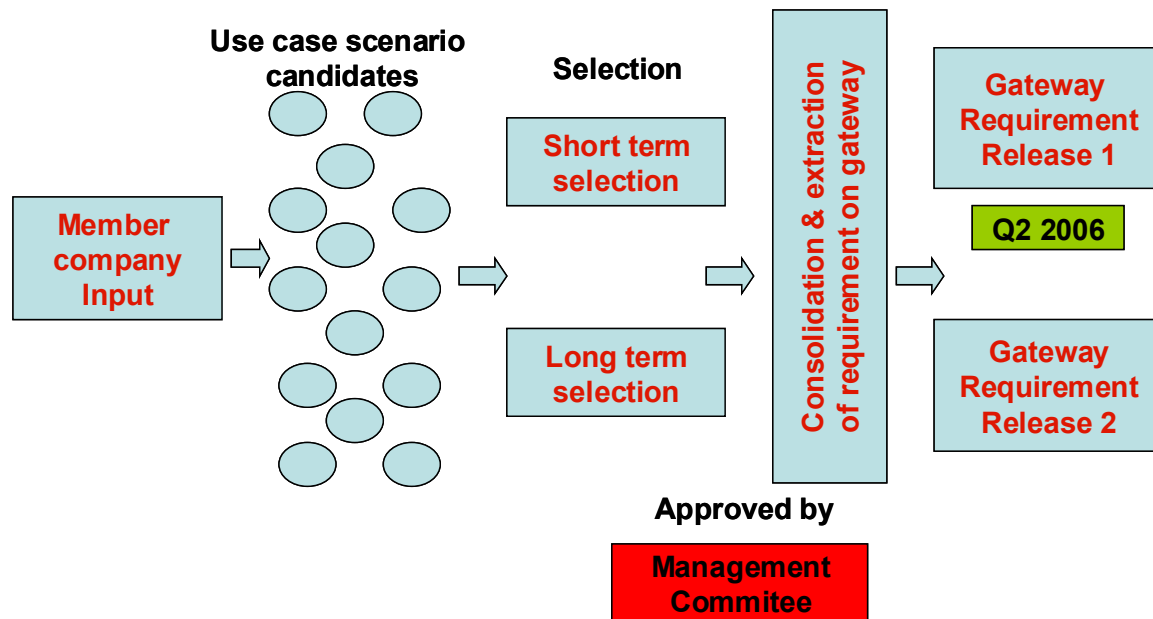


Figure 1 Use case selection and requirement production process

The uses cases and business requirements were then used by the technical working groups to produce the HGI technical requirements.

#### 4.1.2 Overview of use cases

Use cases are based around a typical family of four (2 parents and 2 children) named the Martins. Mr. Martin purchases his broadband service from a Broadband Service Provider (BSP). The BSP is responsible for the operation of the broadband access network and the HG itself. The BSP can offer several services on top of broadband access. Figure 2 illustrates the locations of all the communications devices in Mr. Martin's home.

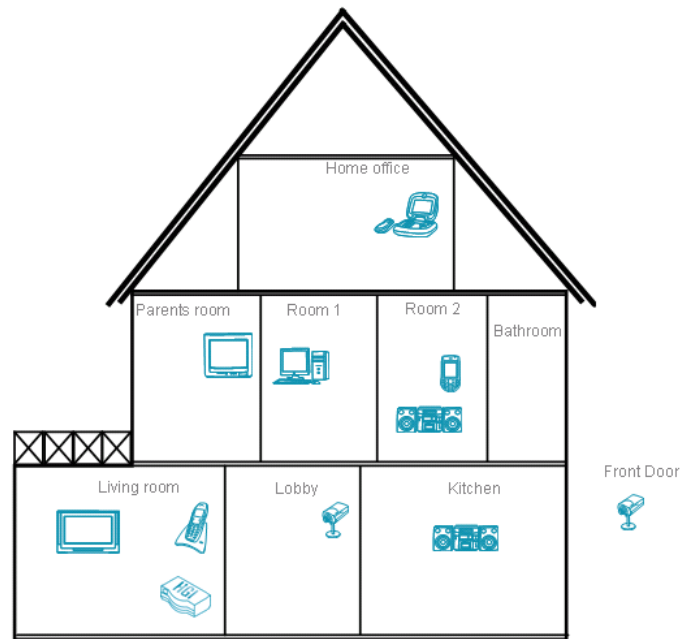


Figure 2 Reference House: The Martins

*Broadband connectivity*

Installing a broadband modem and its associated Internet connection is still a complex experience for most users. Thus, the first usage scenario concerns Mr Martin installing a new broadband connection with Internet service and sharing that connection between several PCs. The second usage scenario concerns Mr Martin purchasing additional services through his BSP which require different versions of HG software.

*Communication*

Voice is still the main communications application. Thus, more and more BSPs are offering voice services as part of their broadband service bundle. Users expect this service to be as easy to configure and use as their current POTS service.

The first communication usage scenario concerns Mr. Martin using an IP phone on his home network to connect to the BSP's VoIP (Voice over IP) service. The second usage scenario is about Mr. Martin using a legacy analogue phone or fax to connect to the voice port of his Home Gateway. The last usage scenario adds a videophone for use of a video communication service.

*Home office*

Working from home is more and more common today with broadband. The Home Office usage scenario describes Mr. Martin using a secure connection to his office and expecting to have a better Quality of Service (QoS) than the other members of the family using their broadband services.

*Home management & security*

Users want to be able to manage their digital home and be in control of their environment. The first usage scenario concerns parental access control to the broadband Internet service. The second usage scenario "personal monitoring with a video camera" details Mrs. Martin being able to check, via a web camera, that her children have returned home while she is still in her corporate office.

*Entertainment & information*

1 Access to entertainment content is one of the largest residential markets and thus is  
2 increasingly being offered as part of the broadband package.

3 The first use case concerns audio content and a new way to distribute audio via broadband.  
4 Mr. Martin expects to be able to listen to a 'personal radio station' (including a generated  
5 compilation based on his musical tastes) with the same quality of service as his current FM radio  
6 service.

7 The second scenario describes IPTV services. Multiple IPTV channels are being  
8 simultaneously accessed by different members of the Martin family from different devices in the  
9 home. The next scenario "IPTV – PVR/DVR – Home Network Storage" describes viewing a  
10 previously recorded movie. The movie was recorded on the main Set Top Box (STB) but is being  
11 viewed on a device other than the TV that is physically connected to that STB.

12 The fourth scenario regards the Home Gateway supporting a media server (a device storing  
13 photos, videos, etc.) by delivering flows to the different devices in the home.

14 The last scenario describes remote access to content stored in the home. Mr Martin's son  
15 wants to be able to access photos stored on his PC at home from his friend's PC in a remote  
16 location. The Home Gateway is expected to protect access to the home.

#### 17 *Fixed mobile convergence*

18 For the first release, the Home Gateway is expected to support fixed mobile technology that  
19 works in a pass-through fashion such as UMA.

### 20 **4.1.3 Business Requirements Summary**

21 The complete business requirements are only available as an internal document for HGI  
22 members but some extracts are given below as a summary. Note that this summary is not an  
23 exhaustive list of the business requirements.

24 Business requirements from the above use cases have been identified in the following  
25 areas:

- 26 • Access network, home network and BSP in general, where the Home Gateway  
27 functions must be access network and home network technology agnostic and be  
28 managed by a single entity;
- 29 • The Home Gateway (including broadband connection provisioning and  
30 management, software maintenance, etc.) and associated devices and services  
31 must be easy to install and configure. They must also be manageable by the BSP;
- 32 • Communication functions including voice/VoIP, VoIP using analogue and video  
33 phones, where these functions and services must be supported by the Home  
34 Gateway;
- 35 • Home-office support functions, where the Home Gateway must support an  
36 appropriate connection to corporate resources;
- 37 • Home management and security functions including access control and personal  
38 monitoring, where the Home Gateway must be secure and should support remote  
39 access to the home;
- 40 • Entertainment and information functions including streaming audio on any device,  
41 BSP-provided IPTV, home network storage, media server access from any terminal  
42 and remote access to content, where services and functions that the HG must  
43 support are identified;
- 44 • QoS support functions:
  - 45 ○ The Home Gateway must provide a mechanism, or mechanisms, that can  
46 support end-to-end QoS, i.e. from the operator's network to the home  
47 network and vice versa. The business group distinguishes two kinds of  
48 services: managed and unmanaged. The BSP has a responsibility for

- 1 managed services to the user; this can include QoS policy. The QoS  
2 mechanism should protect this QoS policy.
- 3 ○ The Home Gateway must support QoS both in the operator network and on  
4 the home network side when different simultaneous broadband services are  
5 used. In addition, the Home Gateway must support QoS on in-home flows.

## 5 HGI Reference Architecture

### 5.1 End-to-end Network Architecture

Although the HGI has largely been driven by the Use Case approach, most Network Providers have some more general architectural requirements, and these also need to be taken into account. Such requirements may arise from a need to continue to support existing network features, or a view of the overall topology and connectivity required. This aspect of the requirements was covered by an Architectural Task Force which produced a consensus view on these issues which was then documented as a set of high-level architecture requirements. This was published as an internal HGI Document used as a guidance document by the Working Groups as they produced their more detailed requirements,

The ATF requirements were categorized under the following headings:

- Connectivity
- QoS
- Management and OAM
- Encapsulation and session support
- IP Addressing
- Security
- Powering

The ATF Requirements Documents are internal working documents, not intended for external release, and they will not be covered in great detail in this Specification. However some of these high-level requirements are mentioned here as they provide background information which may put the detailed requirements in a more understandable context.

The starting point for the ATF work was the overall architectural reference diagram which is shown in Figure 3. The key features of the diagram are:

- Multiple service edges which do not connect to a single service aggregation point e.g. a BRAS. This has implications for L2 connectivity and QoS control
- A single management entity at any one time (RMS) controlling the HG
- QoS control via the RMS system, not directly from a network 'QoS Manager'
- A single Access network connection to the HG
- Allowance for other Access systems to connect directly to end-devices (e.g. satellite input to a STB which is also connected to the HN)
- The HG operating as both a router and a bridge
- Local turnaround of in-home traffic in the HG

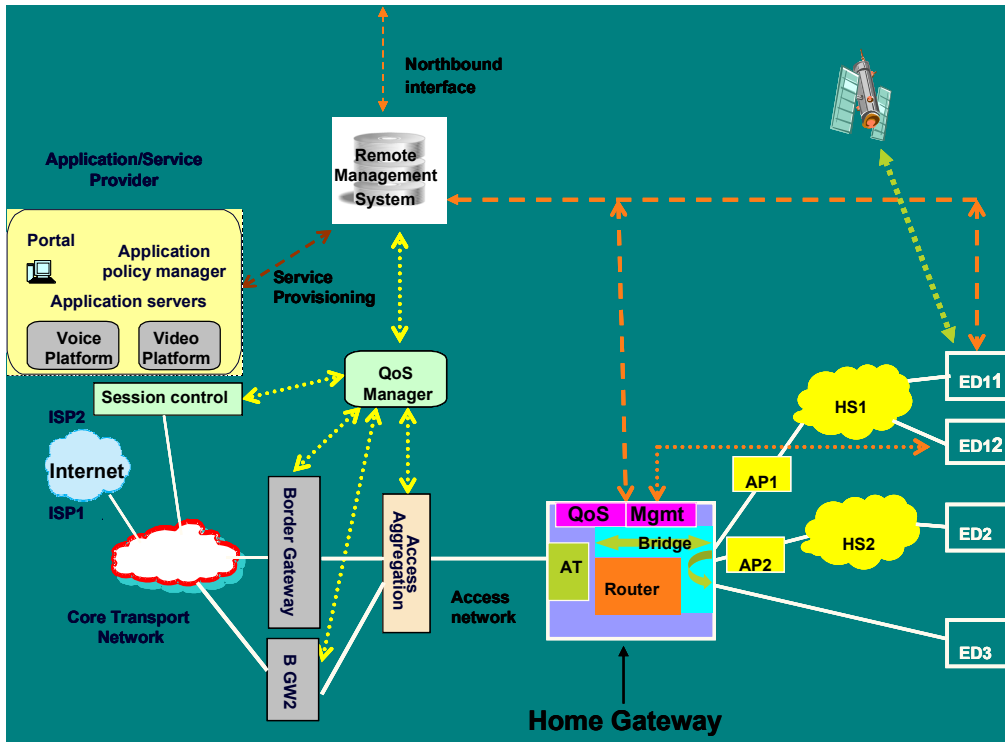


Figure 3 End-to-end Architectural Model

The HGI requirements for release 1 are based on an end-to-end architecture, and are largely access network agnostic; the only exception to this is where there is a specific need to reference a particular access network technology. The high level architectural requirements are given (in an abbreviated form) in the following sections.

### 5.1.1 Connectivity

- Map services into the appropriate L2 pipe to reach the correct service edge node
- Support for multiple BRASs
- Allow direct connection of other access technologies to end-devices
- Simultaneous routing and bridging
- Support direct connectivity (i.e. not via the Access network) between in-home devices.

### 5.1.2 QoS

- Include intrahome flows as part of the QoS scheme.
- Support downstream QoS, upstream QoS, and prioritising intrahome traffic with respect to Access Network traffic.
- Support the QoS remarking of LAN-side traffic

### 5.1.3 OAM and Management

- Single WAN-side management entity at any one time. The end devices may or may not be managed by the HG Remote Management Server. If they are managed separately (at the same time), there may be an impact on some services.
- WAN-side IP addresses may be allocated by more than one entity

- 1           • Split between the WAN-side network management system and user management  
2           access (for policy input and status reporting)
- 3           • Data model that allows for different access technologies
- 4           • Manage end-devices as well as the HG itself
- 5           • OAM functionality reactive, i.e. normally off

6

#### 7   **5.1.4           Encapsulation and session support**

- 8           • Terminate, originate and transparently pass PPP sessions
- 9           • Support both PPP encapsulated traffic and non-PPP encapsulated traffic
- 10          • Trigger PPP sessions on the basis of LAN-side activity

11

#### 12   **5.1.5           IP Addressing**

- 13          • Support PPP and DHCP based IP address allocation
- 14          • Support end-devices which have a static, public IP address
- 15          • Different IP address schemes and subnets on the same physical LAN port, and on  
16          different LAN ports,
- 17          • Different IP address schemes and subnets on the WAN port
- 18          • Support NAT and no-NAT simultaneously

19          Note: only IPv4 is supported in Release 1

20

#### 21   **5.1.6           Security**

- 22          • Management system and HG both need to be authenticated
- 23          • Support a specified (and updatable) list of ALGs
- 24          • Provide a Firewall
- 25          • Per service, per user and per device access control
- 26          • Unique (gateway) hardware ID
- 27          • Secure remote (WAN-side) access to appropriate devices (e.g. a security camera)
- 28          • Different classes of user with regard to management access rights

29

#### 30   **5.1.7           Non Requirements**

31   These are features that the HGI community has no significant interest in, and would therefore not  
32   be prepared to pay for. The reason for giving an overview of these here is that it provides some  
33   information on the HGI vision of the kind of device the HG is, and is not.

34

35   The HG is not required to provide the following:

36

- 37          • awareness of non-IP addressable HN devices
- 38          • embedded DRM functionality

- 1 • embedded video codecs
- 2 • local video or audio conference bridging
- 3 • transcoding (except where there is an embedded DECT base-station)
- 4 • back-up batteries
- 5 • in-session handover for non-voice services.
- 6 • upstream multicast support
- 7 • legal intercept capability.

8

## 9 **5.2 Home Network Architecture**

10 This section describes the architectural models covered by HGI release 1 for the HG and the  
11 IP infrastructure. Some extensions to a basic routing/bridging approach were found to be necessary  
12 (in particular for the routed case) to overcome various limitations.

### 13 **5.2.1 HG Architectural Models**

#### 14 **5.2.1.1 Basic Considerations**

15 In principle the HG could be a bridge, a router, or some combination of the two. The  
16 high level features of these different models in this context would be as follows:

- 17 • Bridged model: in this model the HG would be a pure L2 device, and run MAC address  
18 learning between all its WAN and LAN interfaces. Packet forwarding through the HG would  
19 happen at the L2, Ethernet level on the basis of this learnt MAC address to port mapping.  
20 All devices on the home network and on the WAN would need to belong to the same  
21 subnet. LAN side traffic would be sent to the WAN interface when the destination MAC  
22 address was not recognised as being on the LAN. Broadcast traffic on the LAN would also  
23 be sent to the WAN.
- 24 • Routed model: a model in which private IP-addresses would be assigned by a DHCP  
25 server running on the HG, service (Internet, voice, video, etc.) connectivity being realized  
26 through NAT running on the HG. All devices in the HN would need to belong to the same  
27 subnet to ensure connectivity on the HN itself. Some applications (e.g. VPNs) would need  
28 NAT pass-through in the HG in order to work properly across the NAT. The HG could either  
29 run a routing protocol or be configured with (a set of) simple static routes.

30 The choice between these might seem obvious. One of the main drivers behind the  
31 HGI is to provide a highly functional device which separates the HN and Access domains to  
32 provide features such as service support, (some) service termination, security, Firewalling,  
33 QoS and management. These functions are generally much better done at L3 (or above)  
34 which points to the routed model. Further, a full bridge could pose significant issues for the  
35 Access and Home Networks in terms of broadcast traffic and security.

36 However there are certain Service Providers currently implementing direct L2  
37 connectivity to end-devices, so that they can have end-to-end control and can allocate their  
38 own IP addresses. With regard to the routed model, there are also IP addressing  
39 requirements, for instance the need to simultaneously support private and public IP  
40 addresses on the same physical subnet, which call for functionality over and above that of a  
41 basic router.

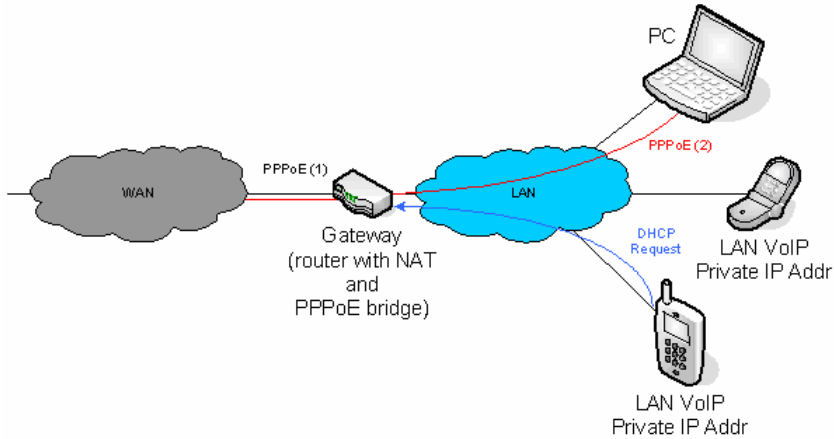
42 The HGI has therefore come up with a small number of hybrid models to address  
43 these issues. Note that the HG is still basically a L3 device, but it can also have some L2  
44 support. This is not a full bridge, as functionality has had to be included to limit the impact of  
45 broadcasts etc.

1 **5.2.1.2 Architectural models Supported**

2 The following architectural models are covered in Release 1. Section 6 contains the related  
 3 list of requirements.

- 4 • Routed model with NAT + PPPoE Passthrough (L2 partial bridge): to support the  
 5 case where a device on the HN needs to be able to directly communicate (at L2)  
 6 with a server on the AN. The L2 connectivity is limited to PPPOE traffic. The  
 7 broadcast PPPoE set-up requests are recognized by the HG, which sets up L2  
 8 bridging for all PPP traffic coming from that device.

9



10

11 Figure 4 Routed model with L2 partial bridge

12

- 13 • Routed model with proxy: for certain services (e.g. SIP) a proxy will be needed in the HG. A  
 14 proxy allows clients to make indirect connections to other network services. The client, residing  
 15 on the home network, connects to the proxy and requests some network service from a server  
 16 on the Access Network. The proxy provides the services by connecting to the specified AN  
 17 server, or possibly by delivering the service from its cache (e.g. in the case of an HTTP proxy).
- 18 • Hybrid model with separate physical networks: this offers two or more physically separated  
 19 home networks, one corresponding to the routed, and the other(s) to the bridged modes of  
 20 operation. The HG has distinct physical interfaces for each network type. Devices can only  
 21 directly communicate with other devices on the same network segment. Communication  
 22 between network segments is only possible via the AN.

23

24

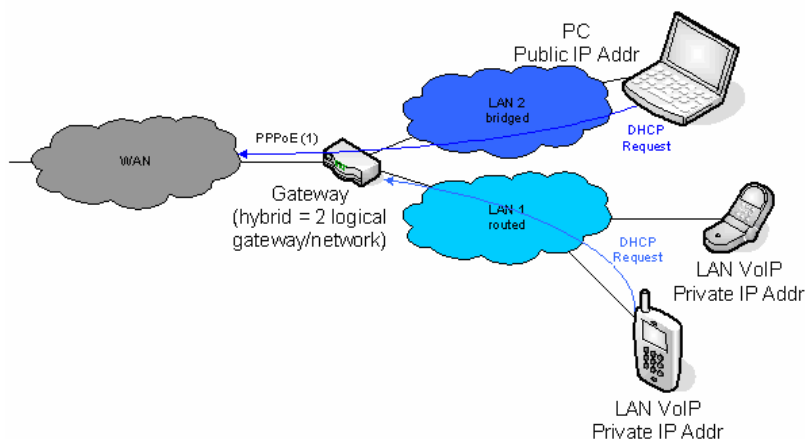


Figure 5 Hybrid model with separate physical networks

## 5.2.2 Home Network Overview

The HG is by definition the gateway between the Access and Home Network. It is therefore essential for the HGI to take a view on the HN technologies, topologies and connectivity it wishes to support so as to be able to:

- Specify which HN technology interface types need to be incorporated into the HG
- Develop a QoS architecture
- Develop a management and monitoring architecture.

This Section briefly outlines the Home Network choices that have been made and the rationale for those choices. It is not an extensive description of, or discussion about, all current home network technologies.

### 5.2.2.1 Home Network Connectivity

The prime purpose of the HG is of course to enable connections to different services via various Service Edge Nodes. However there are other connectivities related to the Home Network which the HG either needs to actively support, or be aware of for the purposes of QoS or Management. While such connectivity may not be directly related a Service Provider's own services, it is in his interests to support them for 2 reasons. Firstly it will avoid some help-desk calls that would have arisen due to interference between Network and in-home traffic, and secondly it will help customer acceptance of the Gateway as it can improve his in-home resource sharing.

The various connectivity are shown in Figure 6 and are as follows:

- 1 and 2 provide connection between EDs and 2 different Service Edge Nodes
- 3 allows two EDs to communicate via the HG, i.e. it acts as a hub. This could for example be to connect two PCs
- 4 connects two devices via an external device such as a switch, but the traffic does not go via the HG
- 5 is a direct ED to ED connection, again with traffic not transiting the HG
- 6 is a combination of 3 and 4, i.e. traffic goes via the Hub and a switch.

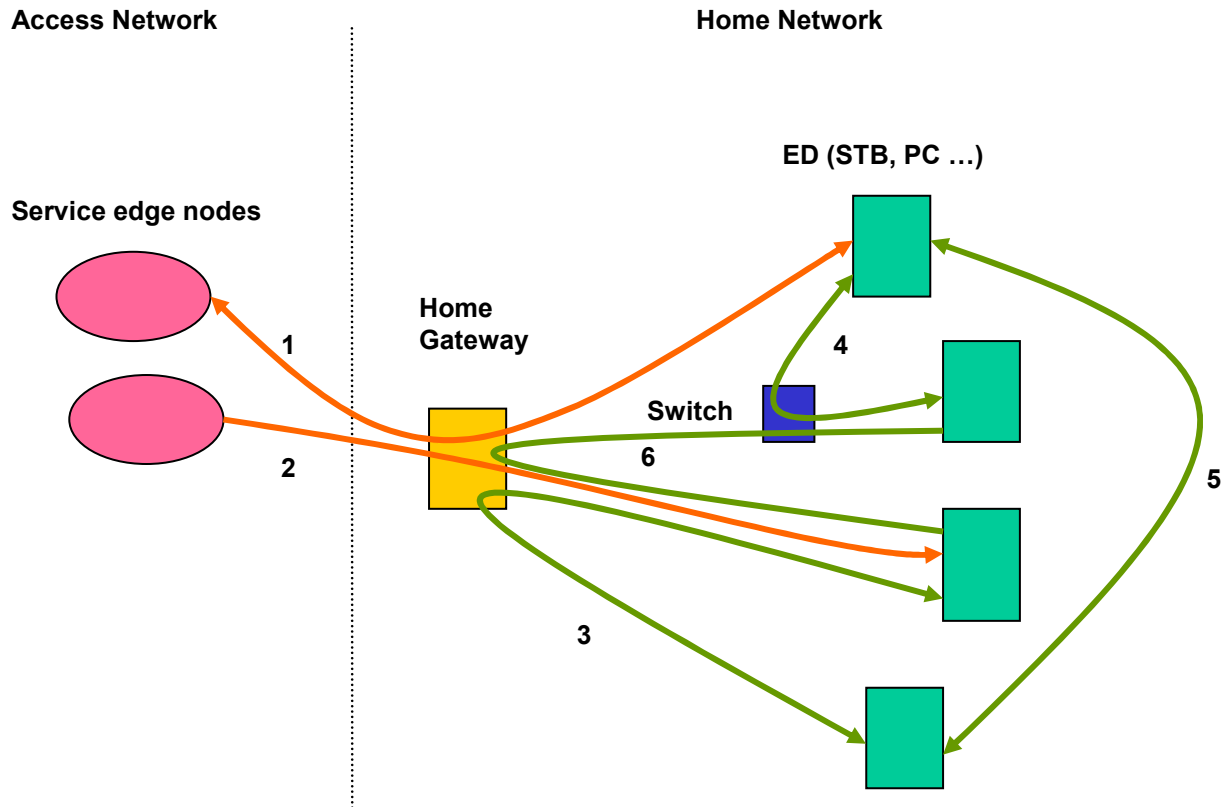


Figure 6 Possible HN connectivity

**5.2.2.2 User requirements**

While the whole purpose of the HGI is to influence and specify the next generation of HGs, it is much harder to influence the Home Networking arena; a number of different industry sectors is involved, there is at least some installed base and there is a wide range of technologies and device types. There are however a number of key end-user Home Network requirements which must be taken into account if the HG is to achieve end-user acceptance and be compatible with the current state of home networking. These are as follows.

The solution must:

- not require the large-scale installation of new wiring in the home; ‘no new-wires’ technologies are therefore preferred (as long as they provide the required performance).
- cover the whole house while providing protection against unauthorized ‘next-door’ access
- support all the end-user’s in-home network needs, i.e. distribute not only those services which are delivered via the access network, but also provide any required intra-home communication (e.g. PC to PC). There should not be any such thing as a home network dedicated only to WAN services.
- allow the end-user to buy (and be able to continue to use existing legacy) infrastructure devices such as in-line technology bridges (e.g. Ethernet to PLT) or switches, which do not need specific HGI functionality, and do not rely on a single vendor (i.e. no proprietary solutions).
- not depend on infrastructure devices (other than the HG itself) or end-devices being managed.

- 1 • not depend on the user having to obey any special rules regarding connectivity or  
2 segmentation, over and above those required by the technology itself.
- 3 • not interfere with the Access network system, or any existing broadcast systems  
4 (TV, radio etc.)
- 5 • appear to behave consistently i.e. any technologies which are subject to interference  
6 must not degrade to the point where they are unable to distribute the required  
7 service set.

### 8 **5.2.2.3 Service support requirements**

9 One of the key parameters of a home network technology is the bit-rate (in terms of the  
10 actual payload) that it supports. However, in order to use this as part of a technology selection  
11 process requires a knowledge of what bit-rates services need, both individually and as a  
12 simultaneous aggregate. The most bandwidth hungry residential applications involve video.  
13 Currently these use rates of ~ 1-3 Mbps, but this is at least partly dictated by the available speeds  
14 on ADSL based Access systems. Live, real-time encoded sport and HDTV require higher  
15 bandwidths. Such access bandwidths will become more available with the deployment of ADSL2+,  
16 VDSL2, Ethernet and fibre-based networks. The deployment of these new technologies will  
17 however depend on a business case and customers' willingness to pay.

18 It is very difficult to come to a definitive view on service rate requirements, as it depends on  
19 the services, the service mixes, the topology and whether a 'shared medium' or dedicated point to  
20 point infrastructure is used. Further complications arise when the intra-home requirements are  
21 added. There is also a trade-off between bit-rate and the complexity of a QoS scheme; while it is  
22 seldom true that overproviding capacity to the point where QoS becomes an irrelevance is practical  
23 or commercially viable, it is true that some overprovisioning may allow a simpler QoS scheme.

24 The only high-level service support requirement is therefore:

- 25 • the HN must support aggregates of 10s of Mbps of actual payload, with at least part  
26 of this payload having very low effective BER and latency.

### 27 **5.2.2.4 Home Networking Technologies**

28 From the above the basic requirements for an ideal HN are:

- 29 • actual throughput of 10s of Mbps with low latency and low packet loss
- 30 • no new wires
- 31 • whole house coverage
- 32 • non-proprietary
- 33 • wide availability and low cost per unit

34 The candidate technologies of interest to the HGI are as follows:

#### 35 **100 Mbps Ethernet (100BaseT)**

36 This is the dominant LAN technology in the business world, and is now so cheap that basic  
37 interfaces and switches are available at consumer prices. The payload is a high percentage of the  
38 line rate, and it is a point to point system which means the aggregate capacity can be made  
39 arbitrarily large. However it needs new wiring to be installed.

#### 40 **PLT (Powerline Technology)**

41 This re-uses the electricity distribution system, and has good (if not quite ubiquitous)  
42 potential coverage. However sending data over mains wiring poses a difficult transmission problem  
43 due to the high noise, time varying environment, and so the true payload is often < 10 Mbps.  
44 Further, this has to be shared between all active devices and in both directions of transmission. The  
45 latency can also be high. Higher rate systems do exist and these could be suitable for many  
46 services (video, Voice, data...), but these are proprietary systems and so not yet Standardised.

1 Doubts persist about whether or not PLT systems can cause interference with other systems.  
2 Guaranteeing performance and therefore service support, on either short or long timescales, for  
3 100% of cases is difficult. However, with QoS Functions or 200Mbps systems, it would be possible  
4 to prioritise services (e.g.: video, voice...) and/or reserve a part of the PLT bandwidth for "Premium  
5 services".

## 6 **HomePNA**

7 Phoneline systems re-use phone extension cabling. Like PLT, this has an arbitrary multipoint  
8 topology, but the noise environment is somewhat less severe. However coverage within a house is  
9 less ubiquitous; there are far fewer phone sockets than power outlets. HPNA 3.0 claims a bit rate of  
10 200 Mbps; the actual throughputs are less than this but the overheads are typically smaller than  
11 with PLT systems. HPNA has had limited market success to date.

## 12 **HomePNA on COAX**

13 HomePNA3.1 defines HPNA operation over coax, as well as adding a significant speed  
14 enhancement (line rate up to 320Mbps while retaining the 3.0 QoS capabilities). In addition, the 3.1  
15 specification solves some issues with the coexistence of VDSL 2 and ADSL, POTS and ISDN on  
16 the same medium. Even though HomePNA 3.1 can operate over coax or phone cabling, the  
17 infrastructure coverage within the home is still not sufficient to make this the ubiquitous solution.

## 18 **Wireless systems**

19 Wireless might appear to be the ideal solution, requiring no wires, and being particularly well  
20 suited to devices which are used at a wide variety of locations within the home (e.g. laptops).  
21 However in spite of the large number of standard solutions that have been developed, so far none  
22 has provided the ideal combination of bit-rate and coverage. Wireless systems are obviously  
23 shared-medium, and therefore need QoS in order to support streaming applications. There is also a  
24 significant security issue with wireless systems that needs to be taken into account.

25 The 2 most promising wireless systems are currently IEEE 802.11b/g and IEEE 802.a/h.  
26 IEEE 802.11b/g operates in the unlicensed 2.4 GHz ISM band, offers a good coverage, but the  
27 typical throughputs are not that high (partly due to interference). IEEE 802.11g provides higher  
28 rates than IEEE 802.11b (in the same band) through more complex encoding. IEEE 802.11a/h uses  
29 a different spectral region (5 GHz) and it provides higher rates, but reduced coverage.

30 IEEE 802.11n may offer more promise in the future, as it uses, rather than suffers from, the  
31 multipath effects which limit conventional systems. However, only pre-standard 802.11n equipment  
32 is currently available.

## 33 **MoCA (Multimedia Over Cable)**

34 Cable TV coax is an intrinsically high bandwidth transmission medium, and it suffers much  
35 less from interference than PLT or HomePNA systems. However a lot of the available spectrum on  
36 the cable is already used for broadcast TV and cable modems, so that in-home cable systems have  
37 to operate at very high frequencies (>~ 900 MHz) where splitter performance may start to  
38 deteriorate, and losses are more significant. Although the HGI aims to be Access technology  
39 agnostic, most of its SP members are Telcos rather than cable companies, and so cannot rely on  
40 there being any coax distribution infrastructure at all for a given customer.

## 41 **USB**

42 USB is a peripheral attachment technology, not a home network technology; it is very short  
43 reach and has very strict master-slave connectivity. It is therefore mainly of interest to connect  
44 peripheral (e.g. mass-storage) devices directly to the HG (using a USB master port).

## 45 **Bluetooth**

46 Bluetooth is a short-reach, low-bit rate Wireless system which is only intended for very local  
47 (e.g. PAN) point to point connectivity. The Bluetooth "cordless profile" interface may be of interest  
48 to support VoIP services from the HG.

1        **DECT**

2        DECT is the widely adopted standard for cordless communications, making use of several  
 3 digital radio techniques to allow reliable connections with a wide coverage and reduced radio  
 4 interference. The upcoming NewDECT standard will support additional features including realtime  
 5 QoS and IP support. For the time being, a DECT interface is only being considered for the HG to  
 6 directly support a VoIP service using the installed base of cordless phones.

7  
 8        **5.2.2.5        Home Network Architecture**

9        In addition to selecting the technologies the HG needs to support, it is also necessary to  
 10 determine the topology. This will depend partly on the required connectivity. The connectivity  
 11 requirements are:

- 12        • any in-home device must be able to communicate with the Access network
- 13        • except for the hybrid mode architecture, any in-home device must be able to  
 14 communicate with any other in-home device without the traffic going via the access  
 15 network (for security, privacy, performance and charging reasons)

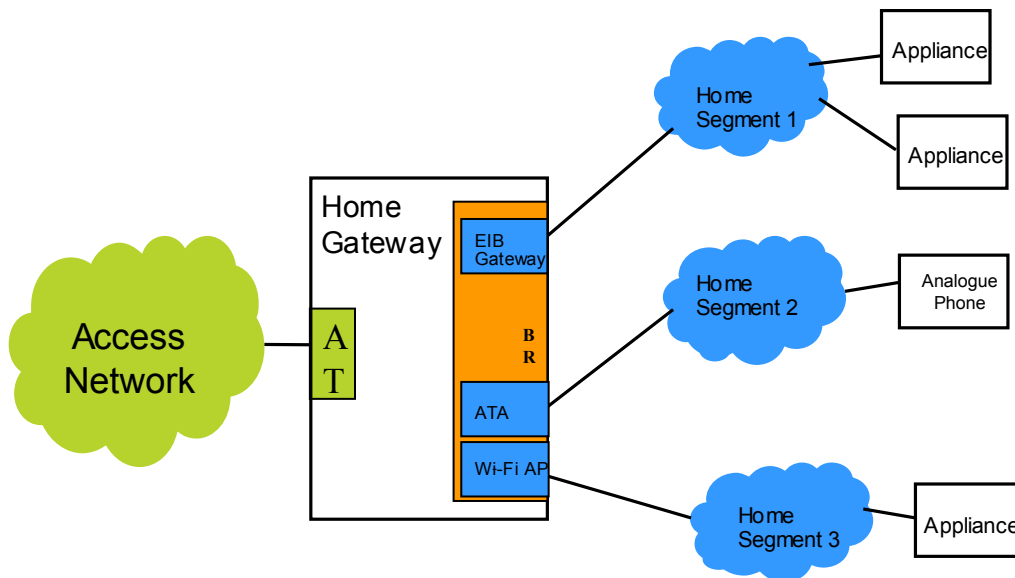
16        There are 2 basic choices in order to achieve the in-home connectivity:

- 17        • force all traffic via the HG
- 18        • allow direct device-device communication without going via the HG

19        There is a further implementation-related choice: whether to incorporate all the supported  
 20 technologies, including service specific interfaces (e.g. ATAs) and infrastructure components (e.g.  
 21 Ethernet switches) in the HG itself (the so-called centralised approach) or use external ATAs,  
 22 technology bridges and switches (distributed approach).

23        The centralised and distributed approaches are shown in next 2 figures.

24



25  
 26        Figure 7 Centralised home network approach  
 27

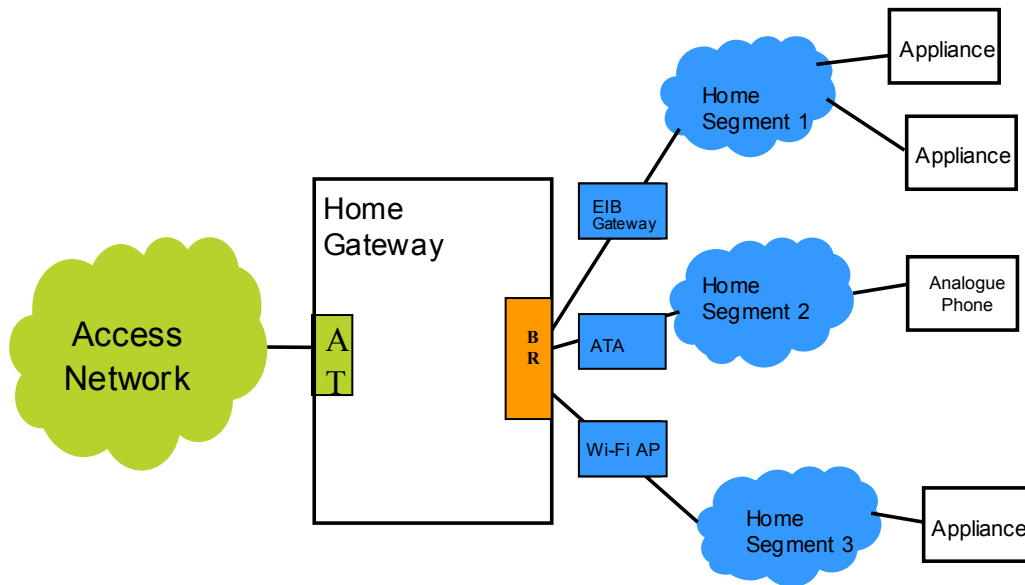


Figure 8 Distributed home network approach

1  
2  
3

4 The main argument in favour of the centralised approach is that it gives the SP more control,  
5 as he can configure and manage all the interfaces. However the downside is that a larger number of  
6 interfaces need to be included in the HG, which will increase cost, and in many cases some of  
7 these will be unused. Further, there is nothing to prevent the end-user adding further bridges or  
8 switches which will result in an incomplete management view. The distributed approach can simplify the  
9 HG, but means the HN will be probably be completely unmanaged, and it places a greater  
10 responsibility on the end-user to implement the HN which may result in more support calls.

11 With regard to connectivity, most of the technologies considered above do not provide a  
12 mechanism for forcing traffic via the HG. Shared medium systems such as PLT or HPNA only  
13 provide direct connectivity between pairs of devices. It might be thought that incorporation of an  
14 Ethernet switch would force all traffic via the HG, but this is only true as long as the end-user does  
15 not add an external switch, in which case there is nothing to prevent local turnaround of traffic.  
16 Therefore the HN solution has to recognise that not all traffic will transit the HG; this must be taken  
17 into account for the purposes of QoS and performance management.

18 **5.2.2.6 Home Network Technologies Supported**

19 Unfortunately none of the existing HN technologies meets all the requirements. The reasons  
20 for this are fairly fundamental, and so there is little prospect of an ideal HN technology emerging.  
21 As no single technology meets the HGI requirements a combination solution is required. The HN  
22 technologies chosen by the HGI for release 1 are:

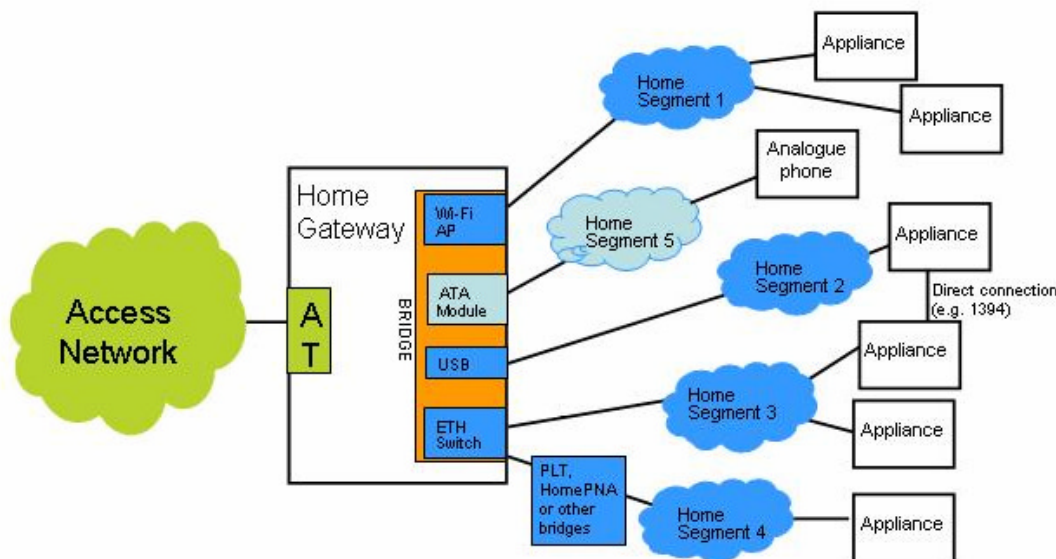
- 23 • IEEE802.11b/g. This will provide connectivity to laptops, PCs and wireless devices  
24 such as PDAs where the key requirement is in-house mobility. It will not necessarily  
25 provide whole house coverage, or QoS such that video streaming applications can  
26 be supported.
- 27 • 100BaseT Ethernet. This will provide high rate, predictable performance, with video  
28 streaming support, but only where it is acceptable to install the required new cabling  
29 i.e. within the room containing the HG, with a small amount of additional inter-room  
30 wiring possible in some cases.
- 31 • USB 1.1. This will provide local peripheral connection.

32 Neither the fully distributed nor the fully centralized approach is ideal. A combination of the  
33 above solutions has been chosen in which the above 3 technologies, and a simple infrastructure  
34 device (Ethernet switch) are incorporated in the HG. Other technologies and further infrastructure

1 devices may be used, but these will be external to the HG. One of the other reasons for choosing  
 2 Ethernet is the availability of Ethernet to other technology bridges e.g. PLT or HPNA. Therefore  
 3 these other technologies can be used to solve the inter-room problem. They can also be used in  
 4 combination (e.g. Ethernet-PLT-Wireless AP) in order to improve the Wireless coverage by allowing  
 5 distributed Access points. The possible existence of these technology bridges is recognized in the  
 6 QoS architecture. Not all in-home traffic will transit the HG, and this is taken account of in the QoS,  
 7 and management schemes.

8 The only additional interface type is an analogue phone socket to provide an analogue  
 9 presented VoIP service which can re-use legacy phones.

10 The following figure illustrates the Release 1 Home Network architecture:



11

12

Figure 9 Home Network Architecture

13

## 14 5.3 Home Gateway Functional Overview

### 15 5.3.1 Basic Assumptions

16 The Home Gateway (HG) is an always on, always connected device, which acts as the  
 17 central point for distributing both LAN-initiated and WAN-initiated services. There is only one HG  
 18 per household which is connected to a single AN.

19 The Home Gateway is able to monitor and perform actions on data flows within the Home  
 20 Network (HN), as well as on bi-directional communication flows between the Home Network and  
 21 the (broadband) Access Network. Given the variety of Access Network technologies, the Home  
 22 Gateway Architecture has to be flexible in terms of providing the support for different WAN side  
 23 interfaces types, although there will only be one WAN connection at a time.

24 The Home Network can support a number of home network technologies, but only one  
 25 Home Gateway manages the whole network.

26 With the exception of analogue presented voice, the HG is not a service end point. Services  
 27 terminate on specific or general purpose devices connected to the Home Gateway through the  
 28 Home Network. However, service-specific parameters and functionalities are needed in the HG, to  
 29 improve efficiency and enable important features related to provisioning and OAM, remote

1 management of the HG, device management, QoS control and security. In addition, the HG may  
 2 include built-in features, in order to offer local services on the home network or to support terminals  
 3 not having the necessary processing and software capabilities to deliver the service (i.e. legacy  
 4 phones used for a VoIP service)

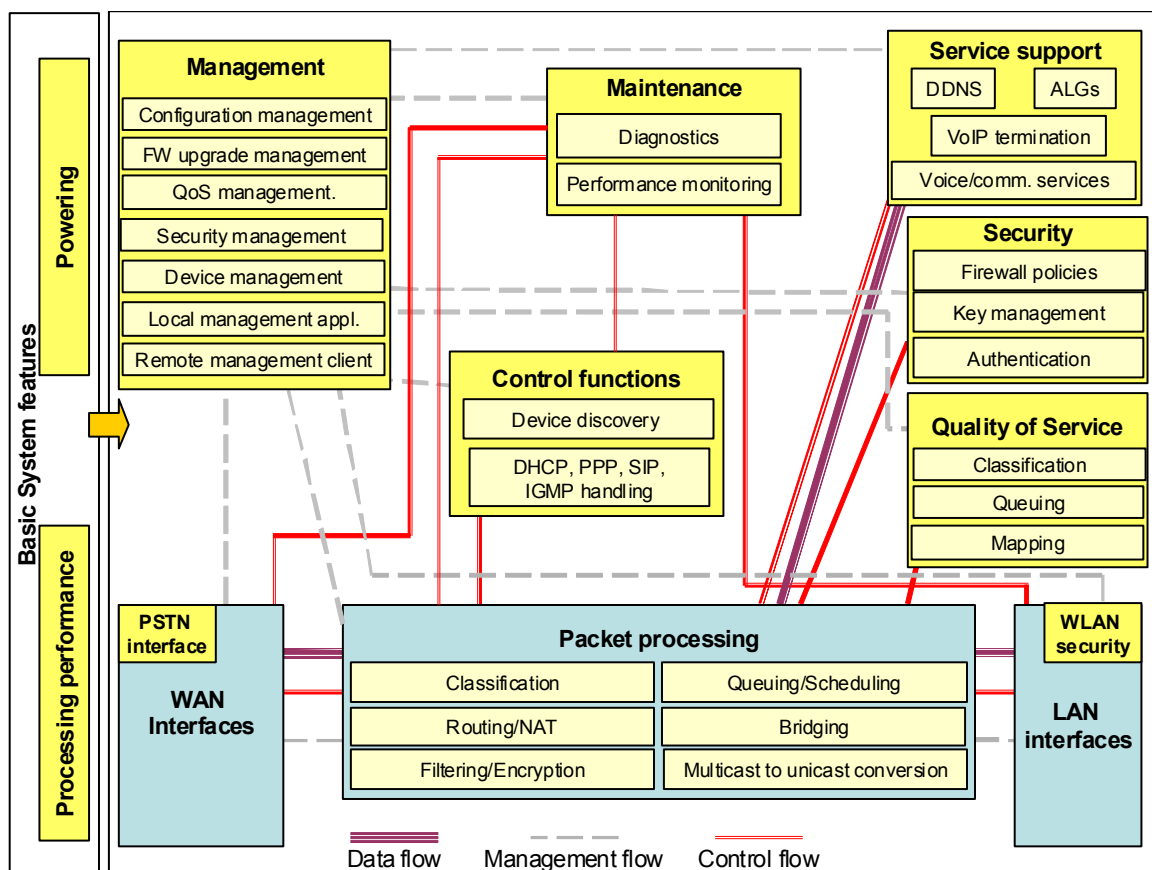
5 The gateway can be regarded as an expandable system, both from the software and  
 6 hardware points of view. However, at least for Release 1, any additional hardware modules will be  
 7 external, and will be connected to the HG via one of the integrated LAN interfaces.

8 **5.3.2 Home Gateway Functionalities: block diagram**

9 The HG architecture is defined as a set of functionalities each of which is a task or a set of  
 10 tasks to be performed through a software program and/or a hardware device/interface/component.  
 11 Figure 10 shows the basic set of functional blocks specified by the HGI Release 1. The actual  
 12 detailed requirements are given in Section 6.

13 The blocks cover a number of functions related to the data plane, the control plane and the  
 14 management plane. The "Packet Processing" block only acts on the header of IP packets, not the  
 15 payload. This process is done on the basis of rules and policies contained in the "Quality of  
 16 Service" and "Security" blocks and is supported by the "Control functions" block for any issue  
 17 related to addressing and device discovery, as well as management or specific protocols such as  
 18 SIP and IGMP.

19



20

21 Figure 10 Home gateway functional blocks for Release 1

22

23 The information flows are defined as follows:

- 24
- Data flows (violet) provide information to the end-user

- Control flows (red) perform the communication session control and connection control functions, dealing with the signalling necessary to set up, supervise and release sessions and connections.
- Management flows (gray) are related to actions setting up parameters of a more permanent nature than just a communication session and can be related to the HG as a whole and to resources and parameters related to the protocols handled by the HG itself. OAM information flows are included here.

The functionality of the blocks is as follows:

WAN interface: This block describes the physical interface towards the access network and the functionalities related to the WAN interface at layers 1 and 2. Different types of WAN interface are possible, but only one interface is supported at a time.

Wired/Wireless LAN interfaces: This block describes the physical interfaces towards the home network and the related functionalities at layer 1 and 2. A number of different interfaces  $I_1 \dots I_n$ , are included. A distinction should be made between the interfaces corresponding to a different LAN technologies (Ethernet, Wi-Fi, USB, ...) and service specific interfaces (DECT, FXS port for VoIP, etc.). The LAN technologies are handled at the lower layers, while any service specific functions are described in the service support block. Wi-Fi security (WEP/WPA keys and ACL management) is included here.

Packet processing: This block describes the interconnection functions at layer 2 and/or layer 3 for LAN-WAN, WAN-LAN and LAN-LAN traffic. This means relaying, forwarding, bridging, and also NA(P)T functions if appropriate. The internal connection functions also include the routing of IP-traffic which is meant for, or coming from, the HG itself (local HG traffic). The block also includes the classification and queuing functions related to QoS management and the filtering and encryption functions related to security, as well as specific service-related functions. These tasks are performed only on the basis of information contained on the Ethernet or IP header; this block does not perform any functions involving an analysis of the packet payload

Control functions: This block consists of the control communication stacks and the control handling. It covers all the functionality needed to control connection addressing and user authentication (via DHCP and/or PPP and signalling protocols) and device discovery inside the home (using DHCP itself or the UPnP protocol). For credentials, it has a relationship with the security block.

Security: All functionalities defining policies related to security are contained in this block. It covers protection for the user from unauthorized attacks and intrusions and for the operators from malicious use of the broadband link. Thus, fire-walling rules, authentication handling functions, key management for encryption are all defined here.

QoS: This block implements the policies for QoS management in the Home Gateway and the home network, as well as any mapping between the LAN side and WAN side. It contains the rules to perform classification and queuing, and priority field mappings.

Service support: This block contains a very limited set of application layer related functions, which allows the support of some terminals which lack the necessary capabilities to provide a service. For HGI release 1, this support is limited to voice/communication services; also, in this block some specific features to ensure the support of specific applications and to manage remote access to the home network are considered.

Management: This block consists of the management communication stacks and the management handling. It contains all the functionality needed to manage the HG itself (configuration, firmware upgrade, QoS and security management etc), the HG services (provisioning, troubleshooting) and also devices (device configuration) and services (service configuration) reachable through the HG. The Web interface is also covered by this block, since it is considered as a basic management tool.

Maintenance: This block contains the processes related to performance control and general diagnostics.

1        Basic system features: This part contains the powering and the processing performance  
2 blocks. These two blocks describe the basic hardware HG resources to be shared between the  
3 various functional blocks with specific reference to available power (and related issues such as  
4 dissipation, reliability etc.) and general capability of the main processor(s) to process traffic flows  
5 (both from a data and a control plane point of view) with a defined level of performance. Note that  
6 processing performance is not covered by this document.

## 7        **5.4                    Management Architecture**

8            Remote management is a key aspect of the specification of the HG in release 1. The first  
9 step was to divide the main remote management functionalities into a list of general management  
10 requirements. These requirements helped to determine the best mechanisms to implement them.  
11 The HGI approach is based on the work of DSL Forum remote management procedures that are  
12 described in DSL Forum TR-069 [1]. Various amendments, additions and the selection of some  
13 options from the DSL Forum specification are detailed in this document.

14            The DSL Forum Technical Reports that are referenced in this document regarding  
15 management features are the following:

16            The Remote Management System (RMS) or Auto Configuration Server (ACS) (in HGI  
17 Release 1 the RMS and ACS definitions coincide, but in future releases the ACS, intended as a  
18 TR-069 capable RMS, might become a part of the overall management system; in this document  
19 the two terms might be used interchangeably) has a TR-069 [1] interface and data model to control  
20 and configure remotely the Home Gateway (HG) and TR-069 [1] enabled devices located in the  
21 home network (HN).

22            The DSL Forum has defined several TR-069-related standards. Some of these relate to the  
23 protocol:

- 24            • TR-069: defines the CPE Remote Management Protocol (CWMP); also defines v1.0  
25 of the Internet Gateway Device data model but HGI specifications are based on v1.1  
26 of this data model, which is defined in TR-098.
- 27            • TR-111 part 1: allows an ACS managing a device to identify the associated HG  
28 through which that device is connected.
- 29            • TR-111 part 2: allows an ACS to initiate a TR-069 session with an ED that is  
30 operating behind a NAT gateway.

31            The others relate to the data model:

- 32            • TR-106: defines baseline data model requirements for all TR-069 HGs and EDs.
- 33            • TR-098: defines v1.1 of the Internet Gateway Device HG data model.
- 34            • TR-104: defines v1.0 of the VoIP ED data model.

35            The HG is under the control of a single RMS. When an end-device is being managed this is  
36 done using the mechanism described in DSL Forum document TR111 part 2 [2] which means that  
37 the HG is transparent to this process.

38            The high level management architecture and the entities involved are shown in Figure 11.

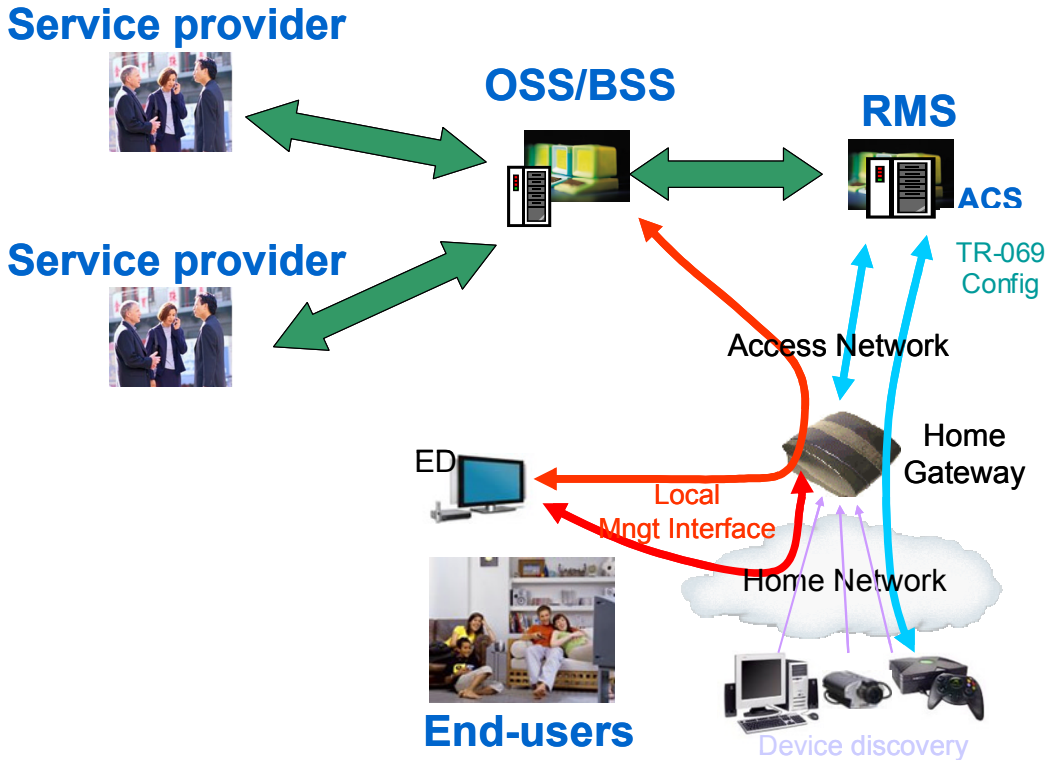


Figure 11 Management entities interactions

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29

The term Remote Management System (RMS) as used in this document is equivalent to the DSL Forum definition of the Auto Configuration Server (ACS). In the future, the HGI RMS might include additional management functionalities. The HGI definition of an Auto Configuration Server (ACS) is a system that has a CPE WAN Management Protocol (CWMP) interface to control and remotely configure the Home Gateway (HG) and TR-069 [1] enabled devices located in the home network (HN). When an end-device is being managed by the RMS this is done using the mechanism described in DSL Forum document TR-111 part 2 [2] which means that the HG is transparent to this process.

The RMS has a northbound interface to the OSS/BSS systems although this is not the main focus of this document. With this interface, the OSS/BSS systems of the operator will be able to establish the policies that the RMS will implement (by applying the required configurations to the HG). Behind the OSS/BSS systems, some service providers may supply configuration requests that may impact the HG (depending on the model of the HG and on the deployed services). These interactions are depicted for completeness of the model and for explanatory purposes but will be defined by each operator and therefore are outside the scope of this document.

The HG and the end devices will also be able to interact autonomously to some degree, performing operations such as device discovery.

Finally, the user may be allowed to have an interface to tune the configuration of the HG to a small degree. Such an interface may have one part based in the HG itself and the other one located in the Operator's portal OSS/BSS.

The management architecture of the Home Gateway is shown in Figure 12 from a functional perspective. The main components and external interfaces are illustrated. The figure also includes the Remote Management System (RMS) and the managed and unmanaged end devices (ED) in the home network. This is done as both the ACS (a TR-069 capable RMS) and the EDs are part of the end-to-end management behaviour.

The HG management architecture can be broken down into these main functions:

- 1           • Device Management
- 2           • QoS Management
- 3           • Security Management
- 4           • Configuration Management
- 5           • Firmware Upgrade Management
- 6           • Performance Monitoring
- 7           • Diagnostics and Troubleshooting (alarms/notifications and log management)

8           Two other components are identified:

- 9           • CWMP Client
- 10          • Local Management Application

11          For both remote and local HG management there is a common Management Abstraction  
12 Layer and a Data Model Management module to allow uniform DB access.

13          ED are either managed devices i.e. devices with a CWMP client communicating directly  
14 (bridged) or indirectly (routed) with the ACS, or unmanaged devices.

15          The main HG management interfaces are:

- 16          •  $I_{HG-LM}$  for local management, is an HTML interface
- 17          •  $I_{HG-ACS}$  for remote management, is a CWMP interface

18          The ED interfaces are:

- 19          •  $I_{ED-ACS}$  for remote management of bridged ED, is a CWMP interface
- 20          •  $I_{ED-HG}$  is a communication ED/HG interface; it can be a DHCP or UPnP interface

21

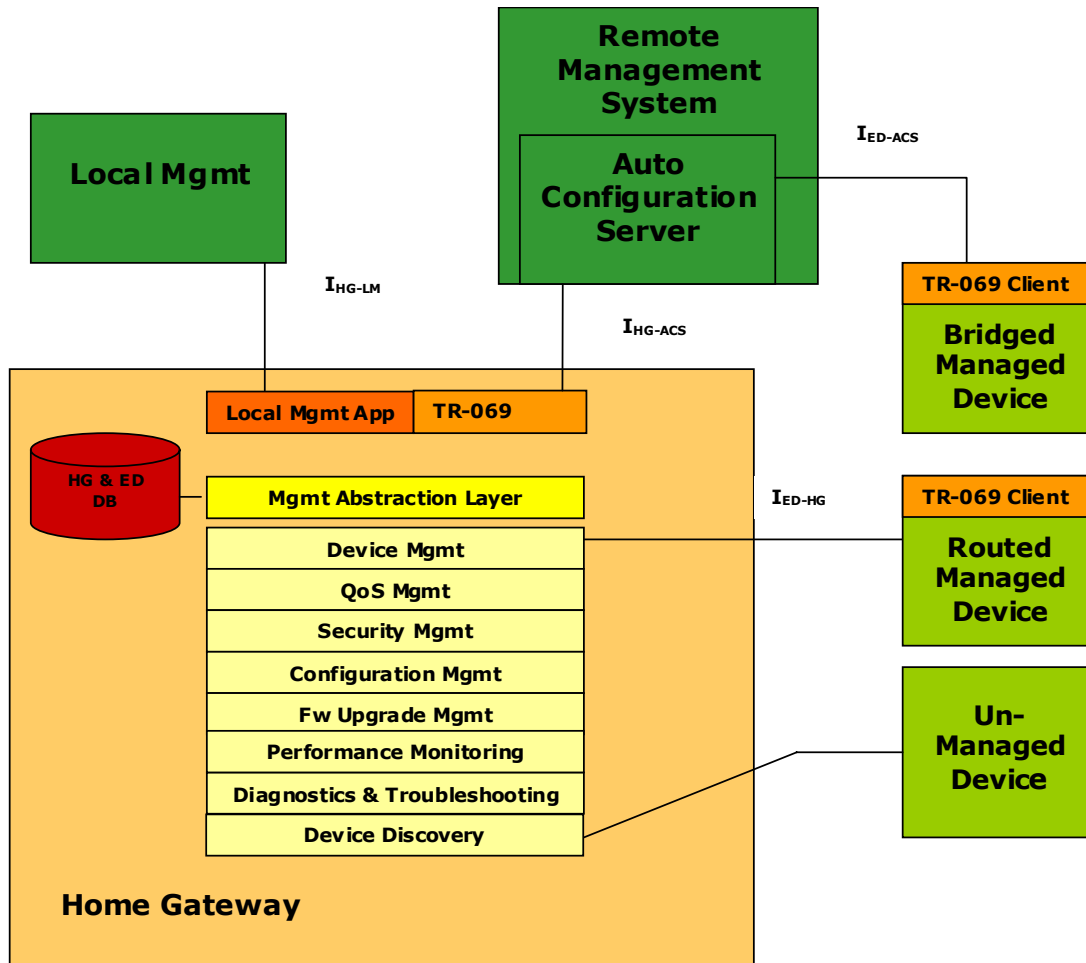


Figure 12 Management Architecture

### 5.4.1 Device Management

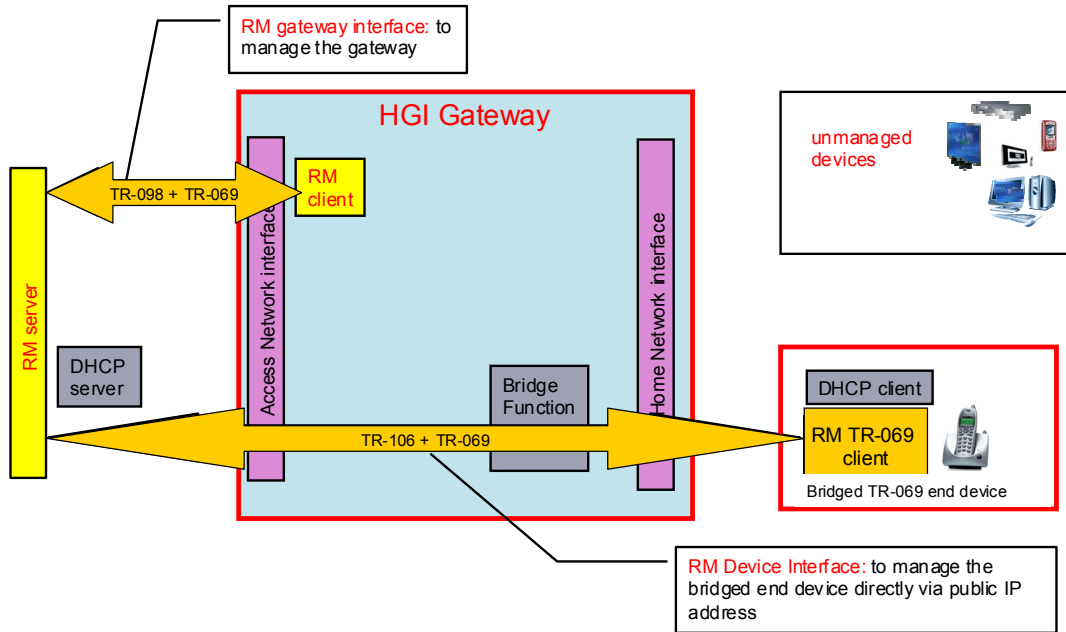
End-device management mechanisms can be divided into two main categories:

- Device Discovery. This task is performed by the HG and will discover end devices (ED) in the home network through DHCP, UPnP and TR-069. This data will be accessible to the RMS.
- Device configuration. The supported mode of operation is the direct configuration of the ED by the RMS. Therefore, the HG supports the pass-through mode (TR-111 part 2 [2]) and the managed ED need to support the TR-069 [1] CWMP protocol.

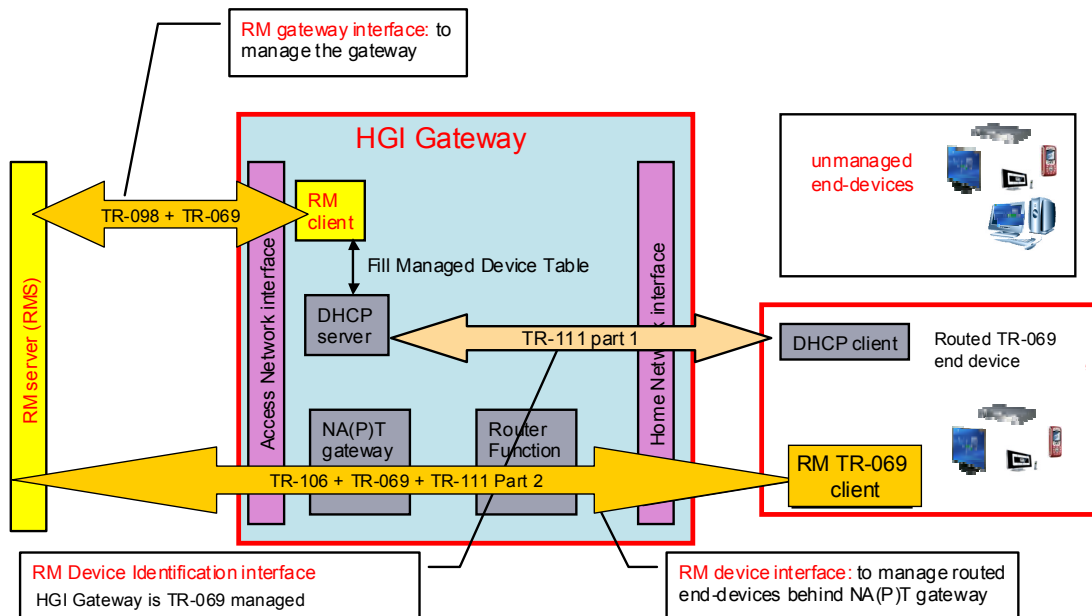
The HG should also enable some remote management of simple end devices that do not support TR-069 [1], but rather UPnP [10] or even only DHCP [8]. Release 1 only deals with the discovery of such non-TR-069 managed devices. The service provider can use this information to optimize the remote management of the (TR-069) managed devices and to optimize customer service. It is assumed that the RMS only communicates with the HN using TR-069, and therefore three remote management models can be distinguished. The models are depicted in Figure 13, Figure 14 and Figure 15. They are:

- the remote management model for TR-069-enabled end devices with the home gateway operating in bridged mode
- the remote management model for TR-069-enabled end devices with the home gateway operating in routed mode

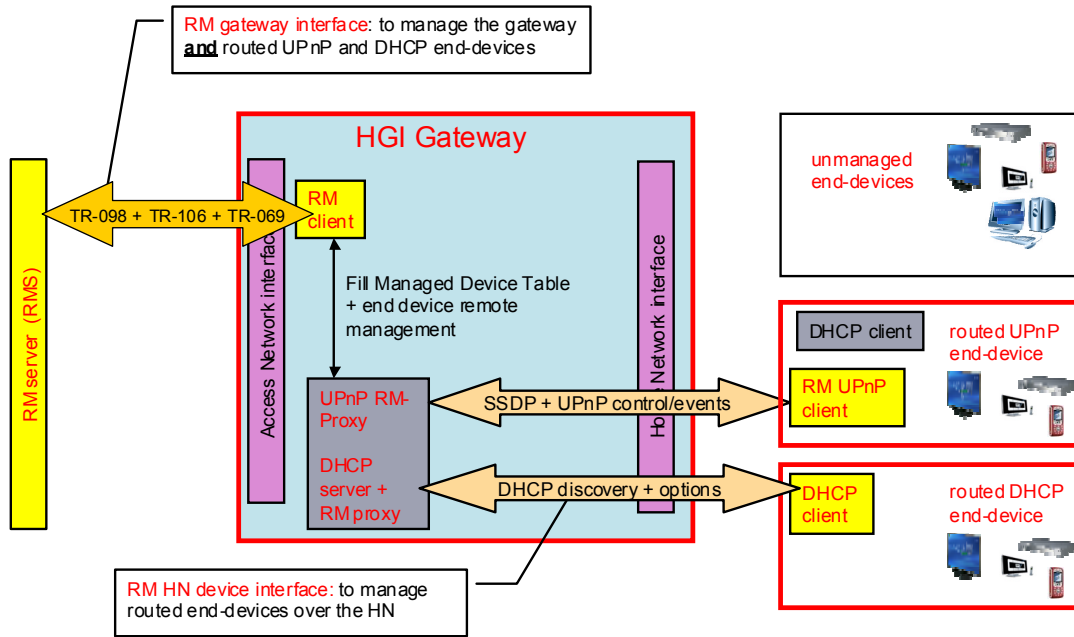
- 1 • the remote management model for UPnP- and DHCP-enabled end devices with the home
- 2 gateway operating in proxy (routed) mode
- 3 The HGI supports all three models.



4  
5 Figure 13 Remote management model for TR-069-enabled end devices with the Home Gateway  
6 operating in bridged mode



7  
8 Figure 14 Remote management model for TR-069-enabled end devices with the Home Gateway  
9 operating in routed mode



1  
2 Figure 15 Remote management model for UPnP and DHCP-enabled end devices with the Home  
3 Gateway operating in proxy mode. Release 1 only deals with discovery of the end devices  
4

5 A distinction is made between managed and unmanaged end devices.

- 6 • A managed device is a device that has a remote management client that
- 7 communicates directly or indirectly (via the Home Gateway) with a remote
- 8 management server.
- 9 • An unmanaged device is a device that does not have a remote management client,
- 10 or that does not communicate directly or indirectly (via the Home Gateway) with a
- 11 remote management server.

12 In the requirements section 6 the terms “manageable device” and “unmanageable device”  
13 are also used. Their definitions are slightly different from the ones above:

- 14 • A manageable device has a remote management client, and may or may not
- 15 communicate with the (service provider’s) remote management server.
- 16 • An unmanageable device is any device without a remote management client.
- 17 Typically, these are user-configured or pre-configured IP devices, including proxies
- 18 to non-IP devices.

19 This is summarized in Table 1:  
20

End device	Has an RM client	Communicates with an RMS
<b>Managed</b>	X	X
<b>Unmanaged</b>	?	-
<b>Manageable</b>	X	?
<b>Unmanageable</b>	-	-

Table 1 Schematic representation of the definitions of (un)managed and (un)manageable devices

The HGI specification requires the HG to discover and identify uniquely the managed devices, and it should discover and identify uniquely the manageable but unmanaged devices connected to the home network. From Table 1 it follows that all end devices with a remote management client should be discovered (or “must” be in the case where they are managed). It is useful to distinguish these devices by way of the remote management client(s) they support. Six types can then be distinguished. These are given in Table 2 and are referred to in the requirements section 6. The columns represent the various device types (HGI nomenclature), and the rows show which remote management client stack is supported by the each device types. This classification is HGI specific.

Client\Type	Z	D	U	CD	CU	C
<b>CWMP</b>				X	X	X
<b>UPnP</b>			X		X	
<b>DHCP</b>		X	X	X	X	

Table 2 HGI types of managed and (manageable) unmanaged devices

Table 2 can be read as follows:

- Type D is managed by DHCP only.
- Type U is a common UPnP device (which includes DHCP by default).
- Type CD is a typical device remotely managed by TR-069 [1], including a DHCP client stack.
- Type CU is a UPnP device that can be remotely managed using TR-069 [1].
- Type C is a device remotely managed by TR-069, but without DHCP client stack.
- User-configured or pre-configured unmanaged IP devices, including proxies to non-IP devices, are classified as Type Z.

Devices of types C, CD and CU can be TR-111 (part 1 and/or part 2) [2] compliant or not.

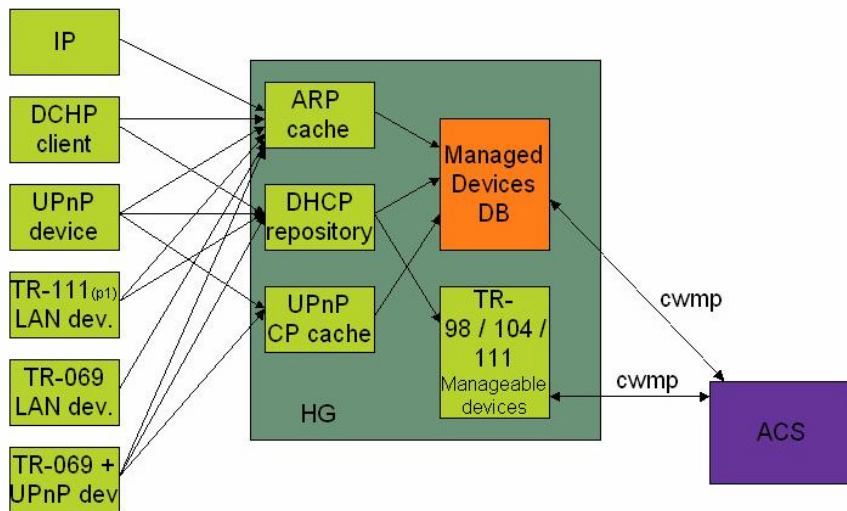
For release 1, the HGI considers managed end devices to be either type C, CD or CU. That qualifies types D and U as manageable but unmanaged devices, and type Z as unmanageable. For release 2, managed devices of types D and U will also be considered.

1 The HG discovers the ID from connected end devices by retrieving and combining  
 2 information from its ARP [11] cache, DHCP repository, and UPnP Control Point cache. The ARP  
 3 cache, DHCP repository and UPnP CP cache get their information from the various devices  
 4 connected to the HG. To avoid conflicts (arising because a device can be discovered by the ARP  
 5 cache as well as the DHCP repository or the UPnP CP cache), a priority scheme is needed. HGI  
 6 gives priority to the information retrieved from the DHCP repository.

7 A UPnP device (type U or CU) can be an embedded device in a root device, as described by  
 8 the UPnP Device Architecture [10] It is therefore a logical entity, rather than a physical device, A  
 9 root device is usually the physical entity. Not only root devices, but also embedded devices need to  
 10 be discovered to obtain a good overview of the home network. Every UPnP device (root or  
 11 embedded) can be distinguished on UUID [8]. This is therefore used by HGI as the primary ID  
 12 indicator.

13 The discovered ID information is used by the HG to fill a Managed Devices Data Base that  
 14 can be read by the remote management server. In Figure 16 the Managed Devices DB is given as  
 15 a logically separate unit. However, it should be included in the HG data model as defined by the  
 16 DSL Forum, in order to be readable by the ACS with CWMP.

17



18

19

20

Figure 16 Device management and discovery

21

**5.4.2 QoS Management**

22 QoS Management is a critical aspect of ensuring the correct delivery of the services .  
 23 However the definition and mechanisms of QoS management are covered in QoS sections 5.5 and  
 24 6.4.

25

**5.4.3 Security Management**

26 Security and privacy are critical issues in the home environment. Most end users are very  
 27 concerned about unauthorized access 'into' their home and about the privacy of their data.  
 28 Therefore, the HG includes manageable security elements to enhance the confidence of the end  
 29 user about these concerns. This mainly concerns the remote management of the firewall and NAT  
 30 capabilities of the HG. The user may also wish to have the ability to 'hide' some EDs from the SP,  
 31 so that the SP does not have full visibility of the HN, however this is not covered in Release 1.

#### 1 5.4.4 Software Management and Upgrade

2 It must be possible to change or upgrade the system level software remotely and  
3 transparently to the end users. There are two aspects to the firmware / software:

- 4 • The Operating System (OS) itself
- 5 • Service support modules (firewall, service framework, low level driver...) which may  
6 be able to be installed on the gateway without changing the OS

7 There may be HGs that support independent service blocks (modules) on top of the OS.  
8 Other simpler HGs may not support the modular approach because of the lack of resources (power  
9 and memory). In this case the OS already contains the complete set of functionality. When the HG  
10 is very limited on memory, not all the services may be supported at the same time, so for different  
11 services other software versions may be needed.

12 The main operations for the complete OS or for service building blocks are:

- 13 • Installation: (loading, registration, verification, dependency resolution and linking of  
14 software) This covers the installation of software directly to the HG. The ACS must  
15 keep track of the installed modules. A new module will normally be needed when the  
16 capabilities of the gateway are changed (a new feature). The installation  
17 intermediate steps will not be addressed directly in the requirements (Section 6), but  
18 will be addressed in Release 2
- 19 • Version Update: The version of the different software / firmware components is  
20 remotely checked (even the entire HG firmware version) and upgraded as  
21 appropriate.
- 22 • Configuration: The configuration of the various modules can also be done. Each of  
23 these modules has a list of variables (for configuration) that can be queried and  
24 configured remotely.
- 25 • Uninstall: This covers the uninstall of software module from the HG. A track of the  
26 uninstalled modules is maintained (at RMS level). Uninstall is done only when the  
27 module to be erased is not in use.
- 28 • Restore configuration: Restoring of HG configuration data or resetting to factory  
29 default parameters
- 30 • Rescue boot: To recover from HG firmware errors.

#### 31 5.4.5 Performance Monitoring and Diagnostics & Troubleshooting

32 Any HG system level fault (e.g. Hardware, O.S. and SW related) must be detected and  
33 communicated to the RMS. Three scenarios are possible and all are supported:

- 34 • Remote diagnostic tests, to check the state of the different components of the HG.  
35 These tests are either scheduled periodically or launched by system operator  
36 request.
- 37 • Performance monitoring will be also available in order to see statistics (for example  
38 at network level).
- 39 • Events are generated on detection of a possible fault within the system.

40 Some examples of faults which need to be detected are:

- 41 • Malfunction of hardware modules
- 42 • Malfunction of the main software components of the HG, (to detect failures, partial  
43 crashes, etc... that will affect the normal working operation of the HG).

1 **5.4.6 Local Management Application**

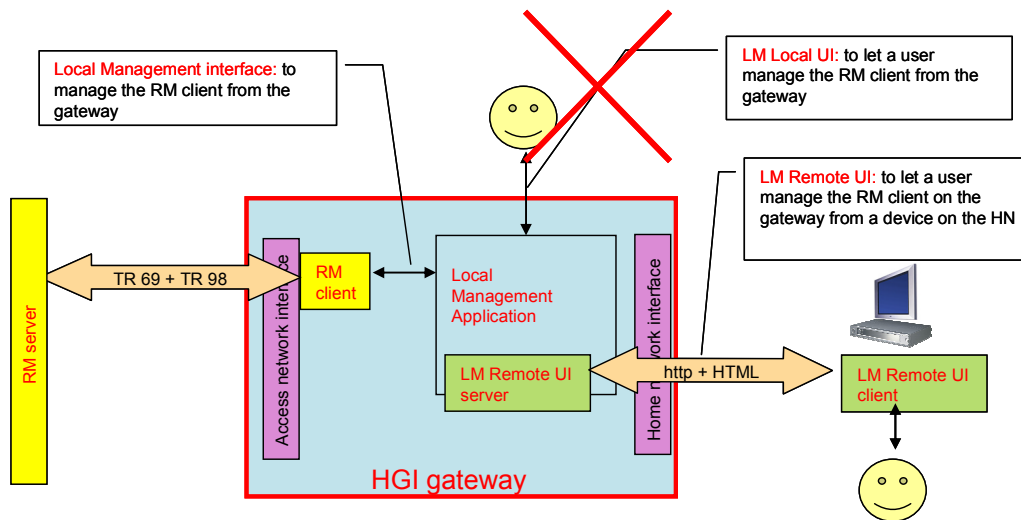
2 In order to provide better support for the HG, a Local Management Interface may be needed  
3 to complement the Remote Management.

4 The Local Management interface is the access method the end user will have to view or  
5 make changes to the HG configuration, user managed services, user managed end devices and  
6 other 'safe' settings.

7 Three levels of management will be present in the HG with the following precedence (high to  
8 low):

- 9 • ACS management (superuser), can manipulate all managed objects in the HG  
10 including lower order user rights
- 11 • Administrator management, can manipulate objects that do not interfere with ACS or  
12 managed service operation. Can manage local user access rights (e.g. additional  
13 firewall rules, specific NAT for unmanaged devices).
- 14 • Users can only manipulate objects when allowed by the Administrator (e.g. url  
15 access)

16 The local user interface access is completely controlled by the HG's firmware itself. This will  
17 require access control to limit this to a local Administrator. This Administrator will have the ability to  
18 change settings for certain managed services or devices, but general users will only have the ability  
19 to view (some of) these managed areas. In Figure 17, an overview of the local management  
20 interface is provided. On the access network side, the RMS or ACS will configure parameters of  
21 this interface through the CWMP management interface as defined in Figure 12.



22  
23 **Figure 17 Local Management Interface overview**  
24

25 In the HG, a Local Management Remote User Interface server (LM Remote UI server) will  
26 host a web based Local Management Remote User Interface, which can be accessed from any end  
27 devices equipped with a browser and located in the HN.

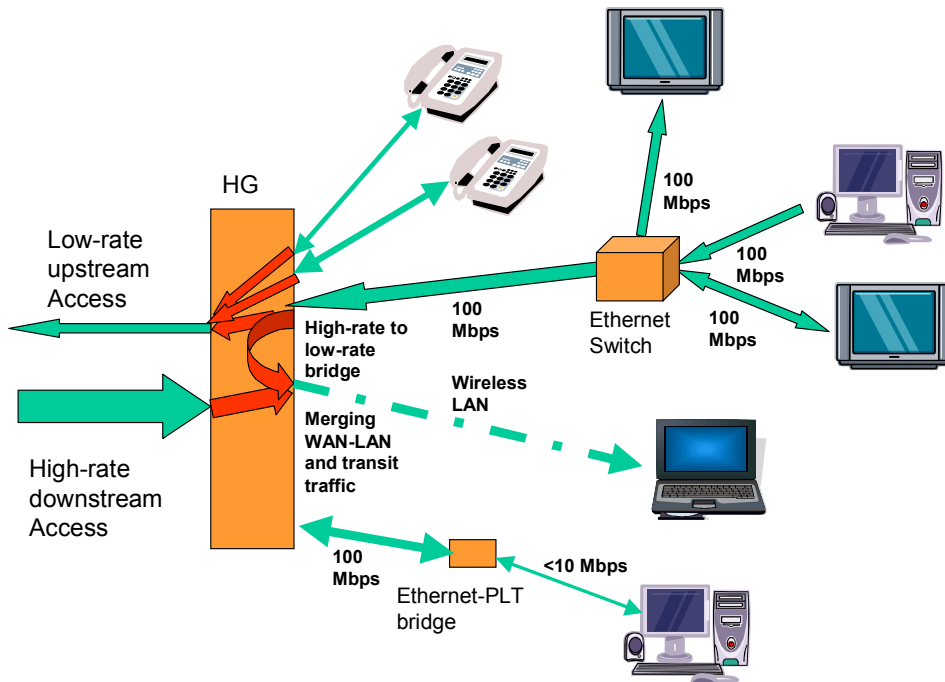
28 The other possible user interface, the Local Management Local User Interface (LM Local  
29 UI), implies that a user interface is directly accessed on the HG and therefore the HG must be able  
30 to connect to a display device and some input device (such as IR remote control). This is not  
31 supported in Release1.

32

1 **5.5 QoS Architecture**

2 **5.5.1 End-to-end architecture**

3 The HGI activity is predicated on the need to provide support for services which require  
 4 Quality of Service. The HGI QoS solution focuses on the Gateway itself, but also takes into account  
 5 both the Home Network and the WAN connections to the various services.



6  
 7 Figure 18 Potential congestion points

8 **5.5.2 Potential Congestion Points**

9 The HGI QoS approach needs to accommodate a variety of both Access and Home Network  
 10 technologies. There are a number of potential congestion points as shown in Figure 18. Note that  
 11 the degree to which these are actual congestion points will depend on the technologies used.

12 **5.5.2.1 The Home Gateway upstream**

13 For certain Access technologies, in particular ADSL, the upstream rate is very much less  
 14 than the rates of the likely home network technologies. Even where the Access physical layer  
 15 capacity is greater than that of the home network technology e.g. for a fibre Access network, there  
 16 may be a need to constrain the service rate to a value which is again less than the home network  
 17 technologies support.

18 There may be a commercial need to allow the end-user to subscribe to more services than  
 19 the upstream rate can simultaneously support.

20 **5.5.2.2 The HG Downstream**

21 The HG QoS solution needs to be access technology agnostic. For faster access  
 22 technologies, e.g. ADSL2+, VDSL/VDSL2, Ethernet or fibre, the HG can become a downstream  
 23 congestion point if the Access Node is not configured to constrain the downstream bandwidth to the  
 24 HG.

### 1 **5.5.2.3 HG Transit Traffic**

2 One of the reasons for congestion is where there is a mismatch between the physical rates  
3 of different technologies. This can occur in the HG itself, for example when it is acting as a bridge  
4 between wired and wireless Ethernet. The other transit problem that can occur is when bridged  
5 intra-home traffic is aggregated with the downstream Access Network traffic, and they are  
6 competing for access to one of the LAN-side ports. The LAN-LAN traffic can burst at very high  
7 rates, and so fill up buffers within the HG thereby significantly delaying lower rate downstream  
8 traffic.

### 9 **5.5.3 Bridges and switches in the Home Network**

10 Rate mismatches can also occur within the Home Network itself, for example in an in-line  
11 bridge device such as a PLT-Ethernet adaptor. Simple aggregation devices which have the same  
12 physical interface type and speed on all links, including the aggregating uplink, can also become  
13 congestion points. A basic Ethernet switch is an example of this type of device. The problem with  
14 dealing with these kinds of mismatches is that the HG may not have any knowledge of the  
15 presence of such devices (which are typically unmanaged), and that at least some of the  
16 technologies will have time varying characteristics. There is no attempt in the Release 1 QoS  
17 scheme to cope with such issues.

### 18 **5.5.4 Basic principle of operation**

19 The HGI QoS approach is mainly concerned with managing QoS through the HG itself. It  
20 works on the basis of a packet by packet, service classification. The service classifiers are  
21 combinations of the ingress packet header fields. LAN-side ingress QoS markings are generally  
22 untrusted, but can be used if trust is established by some other means, and/or in combination with  
23 other service classifiers.

24 The service classification is used to assign the packet to the appropriate queue, and may be  
25 used to set the L2 markings for a particular HN technology. It is also possible to drop packets on  
26 the basis of classification. Service classifiers are downloaded from the ACS as a static policy.  
27 Where service instance classification is used (e.g. for the overload protection mechanism described  
28 below), the additional classifiers are generated within the HG itself. There is no session awareness,  
29 except for that associated with this overload control mechanism. Class-based queuing is used.  
30 LAN-side ingress DSCP markings can be overwritten to zero or a per service configurable value.  
31 There is a QoS mapping table for L2 parameters for LAN-LAN bridged traffic. The HG does not  
32 directly support signalled admission control, but the overload protection mechanism can provide  
33 some features of admission control by limiting the number of service instances to a pre-configured  
34 value.

### 35 **5.5.5 DSCP and VLAN Usage**

36 Some current L3 QoS schemes are based on DSCP markings, with VLANs and Ethernet  
37 priority markings being used in L2 schemes. Although all of these feature to some degree in the  
38 HGI scheme, they are not the main mechanisms. The reasons for this are as follows. There are 2  
39 problems with relying upon DSCP in the LAN to WAN direction. Firstly, all traffic of the same type  
40 would have the same marking but what is required is the ability to differentiate on a service basis.  
41 Secondly, the DSCP markings need to be trusted, but since they can be set by an end-user  
42 application they can be easily spoofed, unless there is a mechanism to establish trust with end  
43 devices

44 In principle VLAN IDs and/or priority tags could be used as a QoS classifier within the Home  
45 Network, however this approach is not part of the HGI Phase 1 QoS strategy. Adding a VLAN  
46 header or priority tags increases the Ethernet frame size; some small, unmanaged Ethernet  
47 switches simply drop such frames. Since there are at least some infrastructure devices which will  
48 drop tagged frames, the HG does not add VLAN headers to any frames. However certain DLNA  
49 devices may send tagged frames. The HG needs to be able to receive such frames and in the case  
50 of bridged traffic, will forward them transparently.

## 1 **5.5.6 Traffic Classification**

2 The key requirement for traffic classification is to be able to classify a service rather than a  
3 traffic type. Queuing, scheduling, and dropping treatments are determined based upon the service  
4 classification. The Service Provider wishes to deliver a quality service, and wants that service to be  
5 treated in a particular way. There may well be other traffic of the same type (e.g. VoIP) which  
6 should not be given any special treatment if it is not a value-added service. Each packet is  
7 classified by inspecting one or more of its header fields. The combination of classifiers used to  
8 identify a service is known as the classification rule for that service.

9 There are in fact rather different requirements for the classification of the three basic  
10 directions of traffic flow through the Gateway i.e. upstream, downstream and transit. The upstream  
11 classification needs to be the most fine-grained, as queuing and scheduling into what is normally  
12 the most significant congestion point needs the greatest degree of control. In the downstream  
13 direction little can be done to improve the QoS of arriving packets, and the main aim is to maintain  
14 this ingress QoS, and ensure that it is not compromised by either transit traffic or the slow operation  
15 of any integrated HN technologies. The downstream and transit classifiers are typically a subset of  
16 the upstream classifiers. The upstream classifiers are briefly described below with a brief rationale  
17 as to when and how they might be used, and the downstream and transit subsets are then noted.

## 18 **5.5.7 Upstream Classifiers**

19 This section describes some of the key upstream classification parameters. A full list of  
20 classification parameters is given in Section 6.4

### 21 **5.5.7.1 IP Destination Address (IP DA)**

22 This is a particularly useful service classifier. Many Managed Services have some kind of  
23 Border Gateway, and so there is a single destination IP address associated with that service. This  
24 has 3 major advantages:

- 25 • It requires a single, initial configuration
- 26 • It cannot be usefully spoofed, as the traffic would go to an inappropriate destination
- 27 • It can be used for an encrypted service as long as the tunnel address is known.

### 28 **5.5.7.2 IP Source Address (IP SA)**

29 This may be appropriate when there is a large number of DAs associated with a service e.g.  
30 if there is a large number of video servers. However the IP SA will often be a locally administered,  
31 private address, but if the device type can be (reliably) identified at the time the address is allocated  
32 (for example via DHCP Option 60), then this can be used to automatically configure the SA as a  
33 service classifier.

### 34 **5.5.7.3 Physical port**

35 Physical port is a useful classifier where a port is dedicated to a service (e.g. an analogue  
36 presented VoIP service).

### 37 **5.5.7.4 Packet Length**

38 Different services from the same physical device may go to the same IP DA; the classic  
39 example of this is voice and packet data from a mobile phone. Packet length can then be a useful  
40 discriminator between voice and data (although the distinction may be less obvious when diverse  
41 speech coding rates are employed). Packet length discrimination allows voice and data to be  
42 queued separately to avoid excessive voice jitter.

### 1 **5.5.7.5 MAC Source Address (SA) and Destination Address (DA)**

2 These can be used to distinguish different physical devices, and therefore different instances  
3 of the same service.

### 4 **5.5.7.6 TCP/UDP Port number**

5 TCP/UDP port number can be used to identify certain applications..

### 6 **5.5.7.7 Protocol type**

7 Distinguishing between TCP and UDP protocols can allow a more general distinction  
8 between different types of service

### 9 **5.5.8 Downstream Classifiers**

10 The main requirement in the downstream direction is to be able to distinguish between  
11 managed and unmanaged services, and this can often be done on the basis of IP SA alone. Some  
12 of the above classifiers are also included in the downstream (DS) scheme, as they may be required  
13 on occasion. However packet length, MAC address, and physical port are not needed in this  
14 direction; there is only 1 WAN port, and so the fact that it is downstream traffic can be taken into  
15 account without there needing to be an explicit classifier.

### 16 **5.5.9 Transit classifiers**

17 The SP is not directly involved with the transit traffic; his main concern is to prevent it  
18 adversely impacting his managed service traffic. This could be done by always separating out DS  
19 and transit traffic, and simply giving absolute priority to the DS traffic. However there may be an  
20 opportunity to distinguish between (transit) streaming and data traffic on the HN, and prioritize the  
21 former. The problem is that if this traffic is simply bridged, then it may not be seen by what is  
22 essentially a L3 classification engine, and indeed if all such traffic was forced via the full classifier,  
23 this would require it to be able to operate at a line rate of up to 100 Mbps. Further, the SP has no  
24 awareness of these LAN-LAN flows as services which makes a service-based classifier hard to  
25 configure. Therefore there is a simple transit priority scheme, which is essentially device-based and  
26 uses MAC address pairs (SA and DA) to identify traffic which can be given higher priority.  
27 Separation between DS and transit traffic is still maintained.

### 28 **5.5.10 QoS Mapping**

29 The HG primarily works on the basis of a packet by packet service classification and  
30 operates largely in isolation from a QoS perspective, therefore mapping between different QoS  
31 regimes is not a key element of the scheme. There are however some mappings which may be  
32 useful, particularly for bridging between different HN technologies and these are defined.

### 33 **5.5.11 Upstream Queue structure**

34 In the upstream direction the main functionality required is to avoid excessive delay for  
35 voice, provide sufficient bandwidth for voice and video, and to prevent best-efforts traffic being  
36 completely starved by higher priority queues. There are 3 fundamentally different types of traffic  
37 with regard to QoS, voice, video and data, This would require 3 queues, However there is a need to  
38 further distinguish between 2 different types of data (e.g. for higher priority control data or to  
39 support a premium data service), Further, the overload protection mechanism requires an  
40 additional queue, making the total number required at least 5.

41 There are 2 types of queue, strict priority and weighted round robin. There are 2 strict priority  
42 queues with the remainder being WRR. The highest priority queue is served to exhaustion. The  
43 second strict priority queue is served when the highest priority queue is empty, and the scheduling  
44 is such that the jitter on the highest priority queue due to all other queues is limited to a single  
45 packet. The highest priority queue would normally be used for voice, which is jitter sensitive, with  
46 the second queue being used for other 'CBR' applications which were less jitter sensitive.

1 Use of 2 strict priority queues mean that all traffic which get puts into these queues will get  
2 transmitted, as long as there is sufficient physical layer capacity. The only additional functional  
3 requirement is to avoid these 2 queues completely starving all other queues. Note that while the  
4 queues are nominally associated with particular traffic types, any service can be mapped to any  
5 queue, and the scheduling behaviour is configurable by means of the round-robin weightings. The  
6 overall aggregate can be shaped to a rate which can be configured to be less than the physical line  
7 rate, and there is also a per queue shaper for the WRR queues which can limit the maximum rate  
8 of the traffic types in those queues. This could be used for example to limit the maximum upstream  
9 rate of an Internet service.

#### 10 **5.5.11.1 Downstream and Transit Queue Structure**

11 In the downstream direction there are 2 concerns, ensuring that WAN traffic is not blocked  
12 by transit traffic, and if there is downstream congestion due to a rate mismatch caused by a slow  
13 HN technology, that the value added traffic gets priority. There may be two different types of transit  
14 traffic, simple data, and streaming e.g. from a media player. The downstream needs a somewhat  
15 simpler queue structure, with 4 queues (LAN Managed Services, WAN Best Effort, LAN Managed  
16 Services, LAN Best Effort) per LAN port.

#### 17 **5.5.12 Class Based QoS, Sessions and Policy**

18 The HGI QoS approach is essentially traffic class-based, i.e. the QoS treatment is the same  
19 for all flows belonging to the same class. This is for reasons of simplicity and scalability. However  
20 there is some limited flow awareness to support an overload protection mechanism. Flows are  
21 closely related to sessions, which have 2 possible uses in a QoS scheme – allowing a different per  
22 session QoS policy to be applied, and preventing new sessions if they would adversely impact  
23 existing ones. The basic requirement here is to provide the appropriate QoS for a service type;  
24 there is no reason to suppose that this should be different on a session by session basis – a given  
25 voice service always needs the same QoS. Therefore a static policy approach has been adopted.  
26 The potential downside of this is that there is no mechanism to prevent a new session overloading  
27 the class so that the entire class suffers.

28 If overload is a genuine concern (as opposed to a theoretical possibility) then some kind of  
29 admission control system is needed. Admission control requires a decision to be made about  
30 resource availability before a session is established, and so involves signalling. The HG is not  
31 involved in signalling (except where the service terminates in the HG itself), and while it could in  
32 principle snoop on signalling, this cannot be done where the signalling is in an encrypted tunnel.  
33 Further, snooping does not provide a graceful means to reject a session request.

34 The HG can support a basic overload protection mechanism which allows a new service  
35 instance to be allowed on a trial basis to see whether or not it can be supported, without impacting  
36 existing traffic. This mechanism works in the following fashion. Within a service class there is the  
37 concept of a recognised and an unrecognised service instance. The simplest way of doing this  
38 would be to classify the instance on the basis of the associated LAN IP or MAC address. Any  
39 packet with the known service class, but unknown instance would be put into a different queue to  
40 recognised instances. Each classification rule has an optional pointer to an Application Layer Logic  
41 (ALL). For overload protection, the ALG would check if this was a known service instance. If not it  
42 would initiate a procedure which would check (over a relatively short period of time) if this new  
43 instance could be accommodated without causing overload as measured by excessive queue  
44 length. Further details of this are given along with the requirements in Section 6.4.

### 45 **5.6 Security issues**

46 It is possible to distinguish three main points where security needs to be enforced: the HG  
47 itself (border element between the Network Access and the Home Network), devices connected to  
48 the Home Network which only access the public network through the Gateway, and devices that  
49 can be connected to the Home Network but have another public network interfaces (e.g. to the  
50 mobile network). In this third case, the HG cannot play any security role if they are using the  
51 alternative connection mode.

1 The overall security approach takes into account the fact that the various functionalities may  
2 need to be implemented in one, or more than one, of these three device types. The following  
3 sections describe only those functions that are implemented in the HG itself. This means that some  
4 important functionality that must be supported somewhere to increase the overall level of protection  
5 for the HN is not covered in this specification.. For example, virus protection is essential, but  
6 Release 1 assumes that the HG will play no direct role in it.

### 7 **5.6.1 Firewall protection**

8 A firewall performs dynamic packet filtering that tracks each connection crossing the firewall  
9 and makes sure it conforms to a defined set of rules. A stateful inspection firewall also monitors the  
10 state of the connection and stores information in a state table. Filtering decisions are also based on  
11 the context that has been established by prior packets that have passed through the firewall. A  
12 stateful firewall can be less efficient with applications that include IP addresses and TCP/UDP port  
13 information in the payload (e.g. FTP, SIP protocols, peer to peer applications). To filter these kinds  
14 of protocols the firewall has to be supported by specific Application Level Gateways that recognizes  
15 the specific packets and analyses the payload in order to obtain the required information.

16 Additional features of interest for Release 1 are:

- 17 • Demilitarized Zone (DMZ): a subnet placed between the public network and the  
18 internal network's line of defence, useful when a user wants to host its own internet  
19 services blocking unauthorized access to the rest of the home network. The point of  
20 a DMZ is that connections from the internal and the external network to the DMZ are  
21 permitted, whereas connections from the DMZ are only permitted to the external  
22 network; hosts in the DMZ may not connect to the internal network.
- 23 • URL filtering: blocking access to a list of URLs and so preventing another person  
24 from sending or receiving information as well as restricting access to objectionable  
25 material for parental control purposes. This function will not be considered in section  
26 6.7, considering that all the parental control features will be managed in Release 1  
27 with a device-centric approach.

### 28 **5.6.2 VPN Capabilities**

29 Different technologies (both standard and proprietary) can be adopted for VPN  
30 implementation. These include Layer 2 solutions like PPTP and L2TP, application level solutions  
31 like SSL and the standard IP Layer solution, IPSEC. An IPSEC-based solution has been selected  
32 for Release 1 because it provides a standard, flexible and network controllable architecture that can  
33 be used irrespective of the application; in contrast SSL cannot be used with applications based on  
34 UDP. A VPN passthrough mechanism is supported by the HG for those cases where the VPN client  
35 is on the terminal. A VPN client should be implemented in the HG to provide support for analogue  
36 presented VoIP only.

37 IPSEC can have coexistence problems with NAT. IPSec NAT Traversal (NAT-T) is a specific  
38 method defined to manage IPSec based communication between two peers, and can be used as  
39 an extension of the IPSec mechanisms in order to overcome this problem.

### 40 **5.6.3 Encryption algorithms**

41 Encryption algorithms can be used for many different purposes, for example key exchange  
42 or authentication. They can be broadly categorized as private (single, shared) key (used for bulk  
43 data encryption and requiring a secret key to be known by both parties, and public (two) key  
44 algorithms (used for key validation & distribution and for signature applications, but limited by their  
45 computational cost). Release 1 addresses the need for storing private/public key pairs inside the  
46 HG, following the RSA protocol, to be used both for authentication and signature purposes.

### 47 **5.6.4 Code authentication / Signature**

48 The digital signature function defines two processes: a process for signing data, and a  
49 process for verifying signed data. The first process uses a private key (i.e. unique and confidential)

1 to produce the signature. The second process uses public key to verify the validity of the signature.  
2 The essential characteristic of the signature function is that the signature can only be produced  
3 using the signatory's private information. Thus when the signature is verified, it can subsequently  
4 be proven to a third party (e.g. a judge or arbitrator) that only the unique holder of the private  
5 information could have produced the signature. For Release 1 this functionality is included to  
6 validate HG firmware updates.

#### 7 **5.6.5 Local Configuration Secured Access**

8 The HG must be accessible locally or remotely to allow access to configuration data in either  
9 a read-only or a read-write fashion. This function must provide an authentication method verifying  
10 the access rights of the entity (user, RMS etc.) attempting to have access to the HG configuration  
11 parameters. Release 1 addresses this need by the use of protocols combined with certificates.

### 12 **5.7 Powering, Safety and EMC**

13 The HG must meet a number of mandatory regulations related to electrical safety and EMC,  
14 and specific related regional requirements. Section 6.8.1 contains a summary of the main directives  
15 and regulations to be taken into account.

16 In addition to these regulatory issues, the HG must be compliant with a number of  
17 requirements related to environmental impact, noise minimisation and reliability; these topics are  
18 also covered in the requirements list.

19

## 6 Home Gateway Requirements

This section contains the requirements related to each of the functional blocks defined in Section 5.3.2.

### 6.1 WAN Side Interfaces

A number of possible interface types are identified below along with some specific requirements. The actual interface to be implemented is dependent on the specific operator's choice.

#### General statements:

N°	Requirement
R1.	The HG WAN interface <b>MUST</b> be easily identifiable and separated from the LAN interface(s)
R2.	The HG <b>MUST</b> support only one of the 3 WAN interfaces described in sections 6.1.1, 6.1.2, 6.1.3 or a combination of them as described in 6.1.4
R3.	The HG <b>SHOULD</b> be equipped with an additional separate PSTN (FXO) interface
R4.	If a DSL WAN is connected, the PSTN (FXO) port <b>SHOULD</b> 'break-over' to the WAN port in the event of power failure

#### 6.1.1 Type 1 - ATM over DSL Interface

N°	Requirement
R5.	The HG <b>MUST</b> support ADSL2+ access network technology (ITU-T 992.5 [21])
R6.	The HG <b>MUST</b> support backward compatibility with ADSL (ITU-T G.992.1 [19]) and ADSL2 with Annex L (ITU-T G.992.3 [20])
R7.	The HG <b>MUST</b> support the handshake procedure for digital subscriber line transceivers (ITU-T G 994.1 [22])
R8.	The HG <b>MUST</b> support regional PSD-masks relevant to each market (Annex A, B or C) (ITU-T G.992.1 [19], G.992.3 [20] and G.992.5 [21])
R9.	The <b>SHOULD</b> support PSD-Mask (Annex M) (ITU-T G.992.3 [20] and G.992.5 [21])
R10.	The HG <b>MAY</b> support PSD-Mask (Annex I, J) (ITU-T G.992.3 [20] and G.992.5 [21])
R11.	Upgradeability from ADSL2+ to VDSL2 ITU-T G.993.2 [23] (profile 8a,b,c,d) <b>SHOULD</b> be provided by the HG.
R12.	The HG <b>MUST</b> support ATM over ADSL2+, ADSL2 and ADSL (ITU-T I.361/365 [24] [25] recommendations and RFC2684 [42]) with PVC management
R13.	The HG <b>MUST</b> be preconfigured either with a "search list" of possible VPI/VCI values (at least 0/35, 0/38, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 1/32, /32, 8/48) or the HG <b>MUST</b> be preconfigured with a set of VPI/VCI default values specified by the operator

R14.	The HG <b>SHOULD</b> support ILMI (Integrated Local Management Interface protocol) to configure ATM and encapsulation parameters, following the guidelines in DSL Forum TR-062 [3] and ILMI ATM Forum 4.0 specification [4]
R15.	If both the HG and the network support ILMI, then ILMI <b>MUST</b> override the ATM and encapsulation parameters
R16.	The HG <b>MAY</b> support auto-discovery of other VPI/VCI sets (Note: auto-discovery should only be used when all other ATM mechanisms have failed)
R17.	The HG <b>MUST</b> be capable of supporting at least 8 PVCs in order to manage multiple service provisioning to LAN attached End Devices
R18.	Dual bearer/Dual Latency (interleaved and fast channels) <b>MAY</b> be supported.
R19.	If Dual Bearer/Dual latency is supported, the related parameters such as min rate, max rate and bandwidth ratio between interleaved and fast <b>MUST</b> be configurable per PVC.
R20.	The following ATM traffic classes <b>MUST</b> be supported: CBR, VBR-rt, VBR-nrt, UBR
R21.	The HG <b>MUST</b> be able to reply to OAM F5 cells conforming to ITU-T I.610
R22.	The HG <b>MUST</b> reply to F5 VC-AIS cells with VC-RDI.

1

 2 **6.1.2 Type 2 - Ethernet over DSL Interface**

N°	Requirement
R23.	The HG <b>MUST</b> support VDSL2 ITU-T G.993.2 [23] (profile 8a, 8b, 8c and 8d) access technology for Central Office deployments with co-existence with ADSL2+
R24.	The HG <b>MUST</b> support VDSL2 ITU-T G.993.2 [23] (profile 12a, 12b, 17a and 30a) access technology for MDU deployments with short loop lengths and no co-existence with ADSL2+
R25.	The HG <b>MUST</b> support backward compatibility with ADSL, ADSL2 and ADSL2+
R26.	The HG <b>MUST</b> support the relevant regional PSD-Mask (Annex A, B, C of ITU-T G.993.2 [23])
R27.	The HG <b>MUST</b> support PTM-TC (Packet Transfer Mode – Transmission Convergence) for Ethernet packets (IEEE EFM 802.3ah standard [28])
R28.	The HG <b>SHOULD</b> support Dual Bearer for PTM-TC
R29.	The HG <b>SHOULD</b> support Dual Latency for PTM-TC
R30.	The HG <b>MUST</b> support Pre-emption for PTM-TC
R31.	The HG <b>MUST</b> support the related Ethernet protocols at layer 2, with VLAN management (support for untagged frames and 802.1Q [29] tagged frames containing priority-tagged information (IEEE 802.1p [5] and VLAN-ID information) on the WAN side.

1 **6.1.3 Type 3 - Ethernet WAN Interface**

N°	Requirement
R32.	The HG <b>MUST</b> support Ethernet 100Base-TX [5] technology for twisted pair (Cat-5 or Cat-6)
R33.	The HG <b>MUST</b> support the related Ethernet protocols at layer 2, with VLAN management (support for untagged frames and 802.1Q [29] tagged frames containing priority-tagged information (IEEE 802.1p [5]) and VLAN-ID information) on the WAN side.

2

 3 **6.1.4 WAN Interface Combinations**

N°	Requirement
R34.	An HG <b>MAY</b> be equipped with a combination of Type 1 & Type 3 or Type 2 & Type 3 interfaces.
R35.	In the above case the Type 3 interface <b>MUST</b> be separate from the Type 1 or Type 2 interface and presented on a dedicated physical connector.
R36.	Only one of these interfaces <b>MUST</b> be active at any time

4

 5 **6.1.5 PSTN Interface**

N°	Requirement
R37.	If a DSL-connected HG supports an analogue telephony service, then it <b>SHOULD</b> provide a relay to automatically connect this output directly to a PSTN input socket under local mains power failure. (FXO port).
R38.	If the HG has an FXO port it <b>MUST</b> use either a RJ-11 or RJ-45 connector (see Req R4).

6

 7 **6.2 LAN Side Interfaces**

8 The requirements in this section are related to the physical interfaces and MAC layers of the  
 9 Home Network technologies supported in the Gateway. These include both wired and wireless  
 10 standards for device connectivity. Any higher layer protocols are not covered in this Section,.

N°	Requirement
R39.	The HG <b>MUST</b> contain a 10/100BaseTX Ethernet1 switch on the LAN side, with at least 2 ports. These ports <b>MUST</b> support auto sense between full or half duplex and auto sense between 10 and 100 Mbps and auto sense between MDI and MDI-X.

---

<sup>1</sup> IEEE 802.3 and ISO-IEC 8802-1

N°	Requirement
R40.	The HG <b>SHOULD</b> support a 10/100BaseTX Ethernet switch on the LAN side, with at least 4 ports
R41.	The HG <b>MUST</b> support a MAC frame format which complies with 802.3 [5] (length/type formats) and 802.1q [29] (VLAN).
R42.	The HG <b>SHOULD</b> include an USB 1.1 or 2.0 slave interface to connect a PC
R43.	The HG <b>MAY</b> include an USB 2.0 host [30] interface in order to connect mass storage devices and printers.
R44.	Every USB host interface port <b>MUST</b> provide local power as indicated in the USB 2.0 specifications [30].
R45.	The HG <b>MAY</b> include a Bluetooth (1.2 or higher [31]) interface - Cordless Telephony Profile, with support of EDR (Extended Data Rate).
R46.	The HG <b>MAY</b> include an internal DECT interface.
R47.	If the HG is equipped with Wi-Fi and Bluetooth, then it <b>MUST</b> include a hardware synchronization mechanism, to avoid mutual interference.
R48.	The HG <b>SHOULD</b> include one FXS port to connect an analogue telephone.

### 1 6.2.1 Wireless LAN Interface requirements

N°	Requirement
R49.	The HG <b>MUST</b> include a Wi-Fi™ certified IEEE 802.11b/g access point.
R50.	The HG <b>MAY</b> include a Wi-Fi certified IEEE 802.11a interface with the extension (IEEE 802.11h) for European countries.
R51.	The HG <b>MUST</b> radiate at least 50 mW E.I.R.P. from the antenna measured at the minimum antenna gain.
R52.	The HG <b>MUST</b> not exceed the maximum limits for radiated power according to the regional regulations.
R53.	The HG <b>MUST</b> be equipped with a minimum of two (internal or external) antennas with a diversity system
R54.	The HG <b>MUST</b> be Wi-Fi Alliance WPA2 Personal certified [6].
R55.	The HG including a Wi-Fi interface <b>MUST</b> be WMM™ certified [6], on the basis of Wi-Fi Alliance requirements for interoperability [6]
R56.	The procedure for device registration and authentication of Wi-Fi terminals <b>MUST</b> be triggered using a “push button” method

N°	Requirement
R57.	To ensure compatibility with all possible devices, the push button mechanism <b>SHOULD</b> be triggered using a “PIN insertion” method.
R58.	The HG <b>MUST</b> be configurable either to broadcast or hide every single SSID it supports.
R59.	By default, the HG <b>SHOULD</b> hide SSIDs
R60.	The HG <b>MUST</b> implement an automatic radio channel selection mechanism to choose the channel with least interference on power up or following a manual request
R61.	Periodic channel selection <b>MAY</b> be performed provided that service is not affected.
R62.	Automatic radio channel selection <b>MUST</b> be able to be enabled/disabled from the local configuration interface as well as from the ACS.
R63.	The HG <b>MUST</b> support at least 32 wireless clients, of which at least 8 are WPA encrypted, simultaneously.

## 1 **6.3 Packet processing**

### 2 **6.3.1 Support of routed model and extensions WAN side**

N°	Requirement
R64.	The HG <b>MUST</b> support at least 1 IP interface per WAN logical interface.
R65.	The HG <b>MUST</b> acquire from its WAN side using DHCP or PPP IPCP all the information needed to support the routed mode of operation (i.e. DNS primary & secondary address, IP address, subnet mask, gateway address).
R66.	The HG <b>MUST</b> also support static provisioning of the above information, via local configuration.
R67.	The HG <b>MUST</b> support a method to make its WAN-side IP address known to the ACS, for remote access and configuration purposes
R68.	<p>The following DHCP options [8][12] <b>MUST</b> be supported by a DHCP client residing in the HGW:</p> <ul style="list-style-type: none"> <li>1 Subnet Mask</li> <li>3 Default Gateway</li> <li>6 Domain Server</li> <li>50 Requested IP Address</li> <li>51 Lease Time</li> <li>60 Vendor Class Identifier</li> <li>61 Client Identifier</li> <li>125 Vendor Specific Information</li> </ul>

N°	Requirement
R69.	The following DHCP options [8][12] <b>SHOULD</b> be supported by a DHCP client residing in the HGW: 7 SysLog Servers 77 User Class
R70.	The following DHCP options [8][12] <b>MAY</b> be supported by a DHCP client residing in the HGW: 0 Padding 2 Timer Offset 12 Host Name 15 Domain Name 33 Classful Static Route 42 NTP Server 43 Vendor Specific Information 53 DHCP Message Type 54 DHCP Server Identifier 55 Parameter Request List 56 DHCP Notification Message 58 Renewal time 59 rebind time 66 TFTP Server Name 67 Boot Filename 121 Classless Static Route 255 End Option

1

## 2 6.3.2 Support of routed model and extensions LAN side

### 3 6.3.2.1 NAT

N°	Requirement
R71.	The HG <b>MUST</b> support NAT/NAPT as described in RFC 2663, RFC 3022, RFC 3027 & RFC 3489 [42][43][44][45].
R72.	The HG <b>MUST</b> support either “full cone” or “restricted cone” or “port restricted cone” NAT implementation as described in RFC 3489.
R73.	The HG <b>MUST</b> support configurable port forwarding for access to devices on the HN.
R74.	HG NAT tables <b>MUST</b> be filled either by the remote management system or by the user

N°	Requirement
R75.	Rules defined by the Remote Management System <b>MUST</b> have a higher priority than rules defined by the user.

1

2 **6.3.2.2 IP Addressing schemes**

N°	Requirement
R76.	The HG <b>MUST</b> support partial L2 bridging from its LAN to its WAN interface for PPPoE recognizing the related broadcast messages and creating appropriate bridging for correct MAC addresses.
R77.	The HG <b>MUST</b> allocate a private IP address to its LAN side interface.
R78.	The HG LAN side IP address <b>MUST</b> be on the same subnet as the devices on the Home Network
R79.	The HG LAN side IP address <b>MUST</b> be used as the Default Gateway in DHCP replies. Note: as all LAN interfaces are bridged, only one IP address is needed, which is used by all interfaces
R80.	The HG <b>MUST</b> allow LAN bridging between different interfaces, enabling intra-LAN connectivity

3 **6.3.2.3 LAN-side DHCP requirements**

N°	Requirement
R81.	A LAN side DHCP server <b>MUST</b> be available on the HG.
R82.	The HG <b>MUST</b> support a means to remotely configure its own DHCP server

N°	Requirement
R83.	<p>The following DHCP options <b>MUST</b> be supported by a DHCP server [8][12] residing in the HG:</p> <ul style="list-style-type: none"> <li>0 Padding</li> <li>1 Subnet Mask</li> <li>3 Default Gateway (Router)</li> <li>6 Domain Name Server</li> <li>12 Host Name</li> <li>15 Domain Name</li> <li>42 NTP Server</li> <li>43 Vendor Specific Information</li> <li>50 Requested IP Address</li> <li>51 Lease Time</li> <li>53 DHCP Message Type</li> <li>54 DHCP Server Identifier</li> <li>55 Parameter Request List</li> <li>56 DHCP Notification Message</li> <li>58 Renewal Time</li> <li>59 Rebinding Time</li> <li>60 Vendor Class-identifier</li> <li>61 Client Identifier</li> <li>77 User Class</li> <li>125 Vendor specific information</li> <li>255 End Option</li> </ul>
R84.	<p>The following DHCP options <b>SHOULD</b> be supported by a DHCP server residing in the HG:</p> <ul style="list-style-type: none"> <li>66 TFTP server name</li> </ul>
R85.	<p>The DHCP server <b>MUST</b> support fixed IP address allocation to specific device name or MAC addresses to be used in combination with port forwarding/DMZ host.</p>
R86.	<p>The DHCP server <b>MUST</b> provide the same IP address to each device so long as the device has not been absent from the network for a period greater than 60-90 days</p>
R87.	<p>Where the DHCP server assigns private IP addresses to requesting devices on the home network, they <b>MUST</b> be on the same subnet (RFC 1918 [42]).</p>
R88.	<p>The HG <b>MUST</b> support use of public IP addresses (that are within the proper subnet mask defined for the gateway WAN IP connection) on the LAN and properly route the device traffic. Note: it is assumed that devices with public IP addresses will be manually configured.</p>

1 **6.3.3 Support of Hybrid Model and Extensions**

N°	Requirement
R89.	If the HG has an ATM WAN interface, it <b>MUST</b> support RFC 2684 [42] for multi protocol Ethernet bridged encapsulation over AAL5
R90.	The HG <b>MUST</b> support configuring and enabling multiple instances of bridging between WAN side logical interfaces (PVC, VLAN ...) and LAN side physical (Ethernet Port, SSID ...) interfaces
R91.	The HG <b>MUST</b> support configuring and enabling one or more WAN logical interfaces and one or more physical LAN interfaces, to be routed (as described in sections 6.3.1 and 6.3.2)
R92.	The HG <b>MUST</b> run both bridging and routing simultaneously
R93.	The HG <b>MUST</b> be able to forward traffic over the right connection (in the case of multiple PVCs, multiple PPPoE sessions, multiple VLANs etc), on the basis of a number of parameters to be used as classifiers, and defined by DSL Forum TR-068.

2

3 **6.3.4 Session Initiation and Support**

N°	Requirement
R94.	The HG <b>MUST</b> support a "connect on demand" option for connections. In this mode the connection to the DSL network is initiated when outbound traffic is encountered from the local LAN, and terminated after a timeout period in which no traffic has occurred.
R95.	The device <b>MUST</b> support a "manual connect" option for connections. In this mode the connection to the DSL network is initiated manually through the GUI or an XML request and, by default, terminates only when explicitly requested to do so by the user, or due to a power loss or when the connection is lost.
R96.	The HG <b>MUST</b> support an "always on" mode for connections. In this mode the device <b>MUST NOT</b> time out DSL sessions (ATM, IP and PPP) and <b>MUST</b> automatically re-establish any sessions after disconnection, lease expiration or loss and restoration of power. This feature can be enabled/disabled through the GUI or following an ACS request.
R97.	The connection timeout interval <b>MUST</b> be configurable.
R98.	A manual disconnection method (i.e. without waiting for a connection timeout) <b>MUST</b> be provided.
R99.	A default of 20 minutes <b>SHOULD</b> be used for connection timeouts.

4

5

## 6.4 Quality of Service

This section specifies the QoS datapath functions which must be supported by the HG, and the QoS management objects which are used to configure QoS policy within the HG. Core QoS traffic management functions include classification, marking, congestion management, queuing, shaping, and egress scheduling.

Figure 19 shows a conceptual view of the core QoS traffic management functions as packets are received from the LAN ingress ports or from internal HG sources. This diagram is not meant to determine the implementation structure of the QoS functions nor those of the related datapath functions.

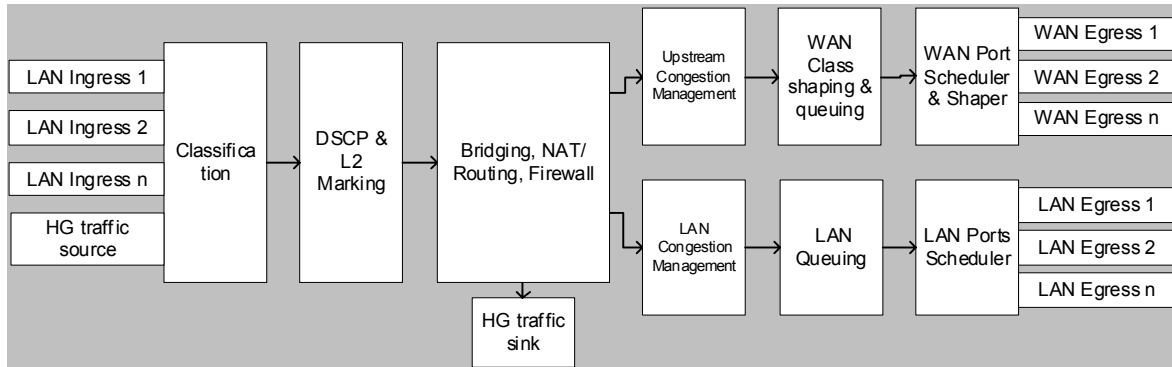


Figure 19 QoS Functions from LAN Ingress

Figure 20 shows a conceptual view of the core QoS traffic management functions as packets are received from the WAN ingress ports. Note that while these are logical WAN ports, there is only one Physical WAN port. This diagram is not meant to determine the implementation structure of the QoS functions nor those of the related datapath functions.

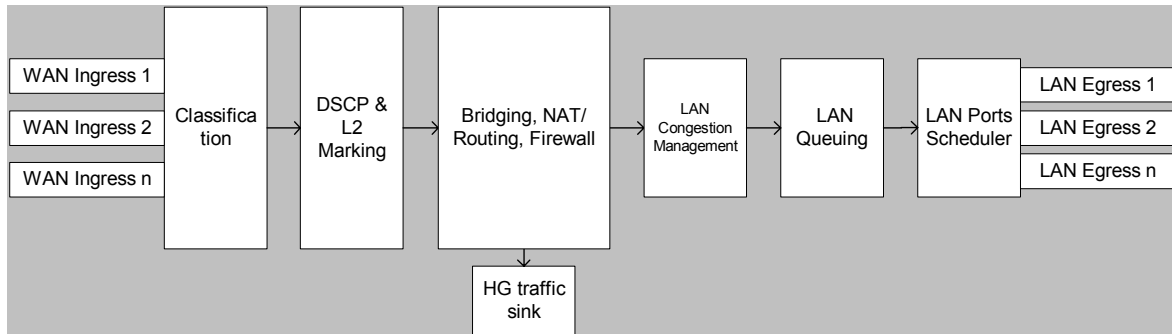


Figure 20 QoS Functions from WAN Ingress

These functions are described in turn below.

### 6.4.1 Classification of traffic

The Classifier treats packets on the basis of the ingress interface, layer 2 header fields (VC or VLAN), IP header fields, layer 4 fields, and packet length. The output of the classification process is a set of decisions about the subsequent handling of that packet. The classification process determines the layer 3 and layer 2 egress marking, handling by the congestion

1 management function, and (in combination with the forwarding decision) the allocation of the packet  
2 to an egress queue.

3 **6.4.1.1 Requirements for Classification of packets received upon the WAN**  
4 **ingress**

5 The requirements in this subsection pertain to packets received upon the WAN ingress port.

N°	Requirement
R100.	The HG <b>MUST</b> classify all packets received on the WAN ingress port.
R101.	The HG <b>MUST</b> be able to set the home network priority level for each packet by setting the DSCP bits on the basis of the classification result.
R102.	The HG <b>MUST</b> assign each packet to the appropriate egress queue, drop the packet, or deliver it to an internal sink, on the basis of the classification result combined with the forwarding decision. NOTE: the packet drop in this context refers to an ingress security function where packets may be dropped as a direct result of classification.
R103.	The HG <b>MUST</b> be able to classify packets based upon IP destination address.
R104.	The HG <b>MUST</b> provide a configurable IP destination subnet mask, so that classification is performed only upon the network prefix bits of the IP destination address.
R105.	The HG <b>MUST</b> be able to classify packets based upon IP source address.
R106.	The HG <b>MUST</b> provide a configurable IP source subnet mask, so that classification is performed only upon the network prefix bits of the IP source address.
R107.	The HG <b>MUST</b> be able to classify packets based upon the DSCP field.
R108.	The HG <b>MUST</b> be able to classify packets based upon the Protocol field in the IP header (e.g. ICMP, IGMP, TCP, UDP, ...).
R109.	The HG <b>MUST</b> be able to classify packets based upon source TCP/UDP port number or range of port numbers. Port numbers may be either statically configured or determined dynamically within the HG. This specification does not specify methods for dynamic determination of port number. This could be done, for example, by use of application layer logic.
R110.	The HG <b>MUST</b> be able to classify packets based upon destination TCP/UDP port number or range of port numbers. Port numbers may be either statically configured or determined dynamically within the HG <sup>2</sup> . This specification does not specify methods for dynamic determination of port number. This could be done, for example, by use of application layer logic.
R111.	The HG <b>SHOULD</b> be able to classify packets based upon IP packet size.
R112.	The HG <b>MUST</b> be able to classify packets based upon any combination of up to 5 of the WAN ingress classification parameters

<sup>2</sup> This specification does not specify methods for dynamic determination of port number. This could be done, for example, by use of an ALG.

N°	Requirement
R113.	The HG <b>SHOULD</b> be able to classify packets on any combination of the WAN ingress classification parameters.

1

2

For ATM based access systems, the following requirements also apply

N°	Requirement
R114.	The HG <b>MUST</b> be able to classify packets based upon ATM VPI/VCI

3

4

Where Ethernet is present on the access link, the following requirements also apply

N°	Requirement
R115.	The HG <b>MUST</b> be able to classify packets based upon Ethernet priority, as defined in IEEE 802.1D
R116.	The HG <b>MUST</b> be able to classify packets based upon VLAN ID, as defined in IEEE 802.1Q
R117.	The HG <b>MUST</b> be able to classify packets based upon MAC source address
R118.	The HG <b>MUST</b> provide a configurable MAC source address mask, so that classification is performed only upon bit fields within the MAC source address determined by this source address mask.
R119.	The HG <b>MUST</b> be able to classify packets based upon MAC destination address
R120.	The HG <b>MUST</b> provide a configurable MAC destination address mask, so that classification is performed only upon bit fields within the MAC destination address determined by this destination address mask.
R121.	The HG <b>MUST</b> be able to classify based upon the Ethernet Length/Type field.

5

6

#### 6.4.1.2 Requirements for Classification of LAN-LAN traffic

7

8

9

10

11

Normally, traffic which enters the gateway on an Ethernet port and leaves from another Ethernet port is subject to the simple classification described in Section 6.4.1.4. In some cases such traffic may require deeper classification. For example, traffic destined to a particular Ethernet port may require deeper classification. The following requirements pertain to the handling of traffic received on the LAN Ethernet ports.

N°	Requirement
R122.	The HG <b>MUST</b> support the simple classification of bridged packets as described in section 6.4.1.4

N°	Requirement
R123.	The HG <b>SHOULD</b> be able to classify packets received on LAN ingress ports and destined to designated LAN Ethernet egress ports according to the multi-field classification described in Section 6.4.1.3. These designated LAN Ethernet egress ports <b>MUST</b> be configurable from the ACS. Note that multi-field classification of LAN-LAN traffic may have performance implications.

1

2 **6.4.1.3 Requirements for Multi-field Classification packets received on the**

3 **LAN ingress ports**

4 The following requirements pertain to the classification of packets received on the LAN

5 ingress ports which are destined for the WAN or are bridged to the LAN after multi-field

6 classification. There is an alternative, simpler classification set for locally bridged, LAN-LAN traffic.

N°	Requirement
R124.	The HG <b>MUST</b> classify all packets received on the LAN ingress ports
R125.	For packets bridged to the LAN, the HG <b>MUST</b> be able to set the home network priority level for each packet by setting the DSCP bits on the basis of the classification result. Note: at the classification stage, the means of determining whether the packet will be bridged to the LAN is beyond the scope of this specification.
R126.	For packets sent to the WAN, the HG <b>MUST</b> be able to set DSCP and L2 egress markings including VLAN QTAG including priority field, for each packet on the basis of the classification result. Note: at the classification stage, the means of determining whether the packet will be sent to the WAN is beyond the scope of this specification
R127.	The HG <b>MUST</b> assign each packet to the appropriate egress queue, drop the packet, deliver it to application layer logic, or deliver it to internal sink, on the basis of the classification result combined with the forwarding decision.
R128.	The HG <b>MUST</b> be able to classify packets based upon the LAN type (Ethernet, Wi-Fi, etc.)
R129.	The HG <b>SHOULD</b> be able to classify packets based upon physical port.
R130.	The HG <b>MUST</b> be able to classify packets based upon MAC source address
R131.	The HG <b>MUST</b> have a configurable MAC source address mask, so that classification is performed only upon bit fields within the MAC source address determined by this source address mask.
R132.	The HG <b>MUST</b> be able to classify packets based upon Wi-Fi SSID
R133.	The HG <b>MUST</b> be able to classify packets based upon MAC destination address
R134.	The HG <b>MUST</b> have a configurable MAC destination address mask, so that classification is performed only upon bit fields within the MAC destination address determined by this destination address mask.

N°	Requirement
R135.	The HG <b>MUST</b> be able to classify packets based upon IP destination address
R136.	The HG <b>MUST</b> provide a configurable IP destination subnet mask, so that classification is performed only upon the network bit field within the IP destination address as determined by this destination subnet mask.
R137.	The HG <b>MUST</b> be able to classify packets based upon IP source address
R138.	The HG <b>MUST</b> provide a configurable IP source subnet mask, so that classification is performed only upon the network bit field within the IP source address as determined by this source subnet mask.
R139.	The HG <b>MUST</b> be able to classify packets based upon DSCP.
R140.	The HG <b>MUST</b> be able to classify packets based upon the Protocol field in the IP Header (e.g. ICMP, IGMP, TCP, UDP,...).
R141.	The HG <b>MUST</b> be able to classify packets based upon source TCP/UDP port number or range of port numbers. Port numbers may be either statically configured or determined dynamically Within the HG. This specification does not specify methods for dynamic determination of port number. This could be done, for example, by use of an application layer logic.
R142.	The HG <b>MUST</b> be able to classify packets based upon destination TCP/UDP port number or range of port numbers. Port numbers may be either statically configured or determined dynamically within the HG. This specification does not specify methods for dynamic determination of port number. This could be done, for example, by use of an application layer logic.
R143.	The HG <b>SHOULD</b> be able to classify packets based upon IP packet size
R144.	The HG <b>MUST</b> be able to classify packets based upon any combination of up to 5 of the LAN ingress classification parameters
R145.	The HG <b>SHOULD</b> be able to classify packets on any combination of the LAN ingress classification parameters.

1 **6.4.1.3.1 Requirements for Classification of packets received on the LAN**  
 2 **ingress using information determined by DHCP Options 60, 61, and 77**

3 The classifier can use several LAN-side fields as classification keys. In addition to other  
 4 means, the HG can learn classification keys through DHCP client requests that it services. In this  
 5 case, the HG associates information conveyed to the HG in a DHCP client request with a  
 6 corresponding MAC or IP address. The following sets out requirements for support of classification  
 7 using keys learned in DHCP client requests.

N°	Requirement
R146.	The HG <b>MUST</b> be able to interpret DHCP option 60 messages received on LAN ports and associate a vendor class ID with a source IP address so that the source IP address can be used as a classification parameter.

N°	Requirement
R147.	The HG <b>MUST</b> be able to interpret DHCP option 60 messages received on LAN ports and associate a vendor class ID with a source MAC address so that the source MAC address can be used as a classification parameter.
R148.	The HG <b>MUST</b> be able to interpret DHCP option 61 messages received on LAN ports and associate a client identifier with a source IP address so that the source IP address can be used as a classification parameter.
R149.	The HG <b>MUST</b> be able to interpret DHCP option 61 messages received on LAN ports and associate a client identifier with a source MAC address so that the source MAC address can be used as a classification parameter.
R150.	The HG <b>MUST</b> be able to interpret DHCP option 77 messages received on LAN ports and associate a user class ID with a source IP address so that the source IP address can be used as a classification parameter.
R151.	The HG <b>MUST</b> be able to interpret DHCP option 77 messages received on LAN ports and associate a user class ID with a source MAC address so that the source MAC address can be used as a classification parameter.

1

2 **6.4.1.4 Requirements for Classification of bridged packets received on the**

3 **LAN ingress ports**

4 The following requirements pertain to the classification of packets received on the LAN

5 ingress ports which are destined for the LAN, i.e. simply bridged in the HG.

N°	Requirement
R152.	The HG <b>MUST</b> classify all packets received on the LAN ingress ports
R153.	The HG <b>MUST</b> assign each packet to the appropriate egress queues on the basis of the classification result combined with the forwarding decision
R154.	The HG <b>MUST</b> be able to classify packets based upon MAC source address
R155.	The HG <b>MUST</b> be able to classify packets based upon MAC destination address
R156.	The HG <b>MUST</b> be able to classify packets based upon a combination of the classification parameters described in this section.

6

7 **6.4.2 LAN-side VLAN support**

N°	Requirement
R157.	The HG <b>MUST NOT</b> add VLAN headers to any frames which are transmitted on a LAN side port

N°	Requirement
R158.	The HG <b>MUST</b> be able to receive VLAN tagged or priority tagged frames on any of its LAN ports. Where these frames are locally bridged to the LAN, the VLAN ID and priority tag <b>MUST</b> be forwarded unchanged.
R159.	Where VLAN or priority tagged frames received on the WAN are bridged to the LAN, the VLAN ID and priority tag <b>SHOULD</b> either be forwarded unchanged or removed. This <b>MUST</b> be configurable from the remote management server.

1

## 2 6.4.3 Classification Rule Sets

### 3 6.4.3.1 Overview

4 This section describes requirements in the HG for classification rule sets, which are sets of  
5 individual classification rules. This section also describes requirements for sequencing among the  
6 classification rule sets.

7 During classification, individual classification rules are checked for a match with the  
8 corresponding fields in each packet. A rule-match occurs when all the individual classifiers within  
9 that rule match. A rule set is an associated collection of rules.

10 The internal representation of the classification rules and rule sets is not specified.

11 There are four distinct classification rule sets which are present in the HG. They are:

- 12 • WAN\_Rule\_Set, which embodies the classification rules for packets arriving on the  
13 WAN ingress.
- 14 • LAN\_Rule\_Set\_1, which embodies the classification rules for LAN-WAN traffic, and  
15 LAN-LAN traffic which is multi-field classified
- 16 • LAN\_Rule\_Set\_2, which embodies the classification rules which are used to identify  
17 LAN-WAN service instances as part of the overload protection mechanism
- 18 • LAN\_Rule\_Set\_3, which embodies the classification rules for LAN-LAN traffic which  
19 is bridged through the HG with no multifield classification.

### 20 6.4.3.2 Requirements for Classification Rule Sets

N°	Requirement
R160.	The HG <b>MUST</b> support a classification rule set for WAN ingress (WAN_Rule_Set)
R161.	The classification rules associated with WAN_Rule_Set <b>MUST</b> only be able to be configured by remote download from the ACS.
R162.	The HG <b>MUST</b> support 3 classification rule sets for LAN ingress: LAN_Rule_Set_1, LAN_Rule_Set_2, and LAN_Rule_Set_3
R163.	The classification rules associated with LAN_Rule_Set_1 <b>MUST</b> be able to be configured by remote download from the ACS and <b>MUST</b> be able to be modified by the local Application Layer Logic (e.g. the DHCP options). Individual rules associated with LAN_Rule_Set_1 are formed according to requirements in Section 6.4.1.3

N°	Requirement
R164.	Individual rules associated with LAN_Rule_Set_2 <b>MUST</b> only be created internally in the HG.
R165.	LAN_Rule_Set_3 contains additional rules for bridged, LAN-LAN traffic. Individual rules associated with LAN_Rule_Set_3 are formed according to requirements in Section 6.4.1.4. These <b>MUST</b> be able to be downloaded from the ACS, and <b>SHOULD</b> be able to be entered locally by the user.
R166.	For each rule in LAN tables 1 and 2 it <b>MUST</b> be possible to configure a pointer to an additional, per packet operation (e.g., application layer logic).
R167.	The HG <b>MUST</b> support a minimum of 32 concurrent rules for WAN_Rule_Set_1
R168.	The HG <b>MUST</b> support a minimum of 32 concurrent rules for LAN_Rule_Set_1
R169.	The HG <b>MUST</b> support a minimum of 16 concurrent rules for LAN_Rule_Set_2
R170.	The HG <b>MUST</b> support a minimum of 16 concurrent rules for LAN_Rule_Set_3

### 1 6.4.3.3 Requirements for Sequencing Among Classification Rule Sets

N°	Requirement
R171.	For routed LAN-WAN traffic, the rules in LAN_Rule_Set_2 <b>MUST</b> be tested <sup>3</sup> first (i.e. before the rules in LAN_Rule_Set_1).
R172.	The first rule match in any Rule_Set <b>MUST</b> terminate the classification process for that packet. Note; that if more than one rule match is possible for a given packet, the terminating match will depend on the order in which the rules are specified
R173.	The gateway <b>MUST</b> process the rules in the sequence in which they are configured
R174.	If there is no rule match in LAN_Rule_Set_2, then the rules in LAN_Rule_Set_1 <b>MUST</b> be tested
R175.	For WAN-LAN traffic, the rules in the WAN_Rule_Set <b>MUST</b> be tested
R176.	It <b>MUST</b> be possible to configure a default classification in the event of no rule match

### 2 6.4.4 Overload Protection Mechanism

3 The following requirements relate to the overload protection mechanism which is described  
 4 in Section 5.5. This description is an example of a protection mechanism; alternative protection  
 5 mechanisms may be employed.

6 The protection mechanism utilizes an Instance Table within the HG. The Instance Table is  
 7 used by the HG to record instances of services which have been recognized by the classification  
 8 using the LAN\_Rule\_Set\_2. The formulation of the Instance Table is vendor-specific.

<sup>3</sup> Testing means that all the classifiers in a rule are checked for a match with the corresponding field in each packet. A rule-match occurs when all the classifiers match.

N°	Requirement
R177.	<p>The HG <b>SHOULD</b> support a mechanism (e.g. an ALG) which :</p> <ul style="list-style-type: none"> <li>i. differentiates instances of a service on the basis of one or more single, configured parameters (e.g. IP SA)</li> <li>ii. creates a service instance Table entry, for each newly recognised instance of the specified service, subject to a configurable limit. This allows the maximum number of service instances to be constrained if required. There needs to be a Table for each service for which this technique is used</li> <li>iii. increments a packet count every time a recognised service instance packet is classified</li> <li>iv. performs a real time check of each service instance packet count against a configurable upper and lower limit (i.e. &lt; InactivePackets per SampleInterval, &gt; ActivePackets per SampleInterval)</li> <li>v. checks whether a configurable queue length threshold (QueueThreshold) has been exceeded during the same SampleInterval time period</li> <li>vi. when the upper limit is exceeded without the queue length threshold being exceeded, a new classification rule is added to the Rules Table. This rule which is a copy of the non-instance specific rule, with the appropriate instance identifier added, and the queue changed to that appropriate for an established flow.</li> <li>vii. when the lower limit is not met, the instance specific rule is deleted from the Rules Table</li> <li>viii. marks the most recently established flow in some way. This would be typically used by a separate process to delete this service instance rule in the event of subsequent congestion</li> </ul>

1

## 2 6.4.5 QoS Mappings

3 Note: This section is informative and not normative except where specific requirements are  
4 listed and it provides guidance on the use of QoS Markings in the home LAN.

### 5 6.4.5.1 Overall Mappings

#### 6 6.4.5.1.1 HG Egress Markings

7 Table 3 shows the correspondence between HGI service classes and the default DSCP or  
8 layer 2 markings applied by the HG to packets as they are emitted onto the LAN side.

HGI	Layer 3	Layer 2		
	Diffserv	WMM/ 802.11e	PLC (4 Level)	PLC (8 Level)
Class Service	DSCP	Access Category	Channel Access Priority	Channel Access Priority
Transit BE Data	0x00	AC_BE (AC1)	Priority 1 (CA 1)	CA0
Downstream BE Data	0x18	AC_BE (AC1)	Priority 1 (CA 1)	CA3
Transit VAS	0x20	AC_VI (AC2)	Priority 2 (CA2)	CA4
Downstream Video	0x28	AC_VI (AC2)	Priority 2 (CA2)	CA5
Downstream Voice	0x38	AC_VO (AC3)	Priority 3 (CA3)	CA7

Table 3 Correspondence between Service Classes and HG Egress Markings

#### 6.4.5.2 Integrated Access Devices

The following requirements pertain to the use of priority markings for integrated wireless or powerline access devices within the HG.

N°	Requirement
R178.	If both layer 2 and layer 3 egress markings are used, the marking action associated with the classification rules <b>SHOULD</b> be configured so that layer 2 and layer 3 markings follow the correspondence with service classes as shown in Table 3.

#### 6.4.6 Dropping/Congestion Management

The congestion manager monitors the buffer resource consumption by tracking the depth of each class queue for each out-going port. The congestion manager will either permit or deny the packet from being enqueued into the class queue based on the Random Early Discard algorithm.

The following requirements pertain to congestion management functions in the HG.

N°	Requirement
R179.	The HG <b>MUST</b> support Random Early Discard (RED) [47] for the upstream queues and the LAN egress queues
R180.	The operation of the RED function in either direction <b>MUST</b> be configurable from the ACS for each queue
R181.	The HG <b>MUST</b> support the RED function to be disabled in either direction.
R182.	The HG <b>MUST</b> allow independent configuration of the maximum threshold parameter for RED in each direction
R183.	The HG <b>MUST</b> allow independent configuration of the minimum threshold parameter for RED in each direction

N°	Requirement
R184.	The HG <b>MUST</b> allow independent configuration of the w_q (weighting factor) parameter for RED in each direction
R185.	The HG <b>MUST</b> allow independent configuration of the maximum probability parameter for RED in each direction

1 **6.4.7 Class Queue structure and Scheduling**

2 **6.4.7.1 Queuing into the WAN Egress port**

3 The following requirements apply to the HG's upstream queues and scheduling those  
4 queues into the WAN.

N°	Requirement
R186.	The HG <b>MUST</b> support at least five class queues at the WAN egress interface
R187.	The HG <b>SHOULD</b> support at least eight class queues at the WAN egress interface
R188.	The HG <b>MUST</b> provide a configurable mapping between WAN egress queues and logical layer 2 WAN ports (i.e. ATM VC or VLAN)
R189.	The HG <b>MUST</b> support configurable shaping per WAN class queue
R190.	The HG <b>SHOULD</b> be able to configure each queue for strict priority or Weighted Round Robin scheduling
R191.	The HG <b>MUST</b> support at least 2 strict priority queues
R192.	The HG <b>MUST</b> support at least 3 queues which use Weighted Round Robin scheduling
R193.	The HG <b>MUST</b> provide a mechanism to prevent starvation of the WRR queues by the strict priority queues. The starvation prevention mechanism is vendor-specific but it <b>MUST</b> be able to be configured in terms of an average, absolute minimum bandwidth (in kbps) which is available to the WRR queues if they need it. If this bandwidth is not required then it <b>MUST</b> be available to the strict priority queues.
R194.	The Round Robin weights <b>MUST</b> be individually configurable
R195.	The first strict priority queue <b>MUST</b> be given priority over all other queues i.e. served until exhaustion except when subjected to the starvation prevention mechanism for lower priority queues. Note: this queue would typically be used for voice.
R196.	The second strict priority queue <b>MUST</b> be given priority over all other queues except the first strict priority queue, except when subjected to the starvation prevention mechanism for lower priority queues. Note: this queue would typically be used for video
R197.	The first strict priority queue <b>MUST</b> provide very low jitter for voice packets. The first strict priority queue <b>MUST</b> be serviced straight after every single packet is scheduled from any other queue.

N°	Requirement
R198.	When all strict priority queues are empty, the WRR queues <b>MUST</b> be serviced according to their weighting priority and subject to any per queue shaping limit.
R199.	The HG <b>MUST</b> support aggregate shaping into each WAN egress logical layer 2 port, i.e. the overall rate at which all queues are serviced is dependent on this shaping value.

1

#### 2 **6.4.7.2 Queuing into the LAN Egress ports**

3 The following requirements pertain to the HG's LAN egress class queue structures and  
4 scheduling from those queues into the port level.

N°	Requirement
R200.	The HG <b>SHOULD</b> support queuing of data from any source into the LAN egress queues (as a result of the classifier)
R201.	The HG <b>MUST</b> implement at least four class queues for each LAN egress port
R202.	The HG <b>MUST</b> support at least 2 strict priority queues per LAN egress port
R203.	The HG <b>MUST</b> support at least 2 queues which use Weighted Round Robin scheduling per LAN egress port
R204.	The Round Robin weights <b>MUST</b> be individually configurable
R205.	The first strict priority queue <sup>4</sup> <b>MUST</b> be given priority over all other queues i.e. served until exhaustion
R206.	The second strict priority queue <sup>5</sup> <b>MUST</b> be given priority over all other queues except the first strict priority queue, but might not be served to exhaustion
R207.	When all strict priority queues are empty, the WRR queues <sup>6</sup> <b>MUST</b> be serviced according to their weighting priority.

#### 5 **6.4.7.3 Example of Queuing Configuration**

6 Table 4 provides an example of a queuing configuration that may be configured in the HG.  
7

---

<sup>4</sup> This queue would typically be used for WAN ingress Managed Services

<sup>5</sup> This queue would typically be used for transit streaming (audio/video/voice) traffic

<sup>6</sup> One of the WRR queues would typically be used for WAN ingress best efforts traffic, and the other for transit best efforts traffic.

Direction	Purpose	Scheduling into Port
Upstream	Voice	Strict Priority (highest)
Upstream	Video	Strict Priority (next)
Upstream	Temporary Voice	W1 Weighted Round Robin
Upstream	Premium Data, GPRS Data, Game Data	W2 Weighted Round Robin
Upstream	Best Effort Data	W3 Weighted Round Robin
Downstream	Managed Services	Strict Priority (highest)
Transit	LAN streaming	Strict Priority (next)
Downstream	Best Effort Data	W2 Weighted Round Robin

Table 4 Example of Queuing Configuration

#### 6.4.8 QoS Management Object

This section describes the managed objects which allow the service provider to provision policy on QoS handling within the HG.

This is derived from the TR-098 QoS and QoSDynamicFlow profiles [41], with an extra HGI column for detailed requirements. It is intended to map the QoS requirements of the preceding sections to TR-098, and not to add new QoS requirements. Where appropriate, the HGI column includes a reference to the corresponding requirement(s).

##### 6.4.8.1 Overall Requirements

N°	Requirement
R208.	The HG <b>MUST</b> support the X_HGI_QoS:1 profile as defined in Table 5.
R209.	The HG <b>MAY</b> support the X_HGI_QoSDynamic:1 profile as defined in Table 6.
R210.	The HG <b>MUST</b> announce support for the X_HGI_QoS:1 profile and, if supported, the X_HGI_QoSDynamic:1 profile via the TR-106 [40] DeviceSummary parameter.

##### 6.4.8.2 Notation

The following abbreviations are used to specify profile requirements:

Abbreviation	Description
R	Read support is REQUIRED.
W	Both Read and Write support is REQUIRED.
P	The object is REQUIRED to be present.
C	Creation and deletion of the object via AddObject and DeleteObject is REQUIRED.

1 **6.4.8.3 HGI QoS Profile**

2 Table 5 defines the HGIQoS:1 profile for the InternetGatewayDevice:1 object. The minimum  
 3 required version for this profile is InternetGatewayDevice:1.1.

4 This profile does not provide any support for the optional overload protection mechanism.

5

Name	Req	HGI
InternetGatewayDevice.QueueManagement.	P	
Enable	W	
MaxQueues	R	R186: WAN egress: must be at least 5 plus... R201: LAN egress: ...4 per LAN egress interface R187: WAN egress: should be at least 8 plus... R201: LAN egress: 4 per LAN egress interface.
MaxClassificationEntries	R	R167: WAN ingress: must be at least 32 plus... R168: LAN ingress: ...32, i.e. 64.
ClassificationNumberOfEntries	R	
MaxQueueEntries	R	R191, R202: must be at least 2 SP queues R192: WAN egress: must be at least 3 WRR queues (so must be at least 5 WAN queues per egress interface) R203: LAN egress: must be at least 2 WRR queues (so must be at least 4 LAN queues per egress interface)
QueueNumberOfEntries	R	
DefaultQueue	W	R176
DefaultDSCPMark	R	
DefaultEthernetPriorityMark	R	
InternetGatewayDevice.QueueManagement.Classification.{i}.	PC	
ClassificationEnable	W	
ClassificationStatus	R	
ClassificationOrder	W	
ClassInterface	W	R110: WANConnectionDevice instance: VPI/VCI R128: LANxxxInterfaceConfig instance: physical port <b>(SHOULD)</b> R132: WLANConfiguration instance: WLAN SSID
DestIP	W	R103: WAN ingress R135: LAN ingress
DestMask	W	R104: WAN ingress R136: LAN ingress
SourceIP	W	R105: WAN ingress R137: LAN ingress
SourceMask	W	R106: WAN ingress R138: LAN ingress
Protocol	W	R108: WAN ingress R140: LAN ingress
DestPort	W	R110, R142: will be used only when the port can be statically configured. If application layer logic is required in order to determine the port number, the HG will presumably support the standard TR-098 QoSDynamicFlow:1 profile.
DestPortRangeMax	W	R110, R142
SourcePort	W	R109, R141: WAN ingress: will be used only when the port can be statically configured. If application layer logic is required in order to determine the port number, the HG will presumably support the standard TR-098 QoSDynamicFlow:1 profile.

Name	Req	HGI
SourcePortRangeMax	W	R109, R141
SourceMACAddress	W	R130: LAN ingress R154: transit
SourceMACMask	W	R131: LAN ingress
DestMACAddress	W	R133: WAN ingress R154: transit
DestMACMask	W	R134: WAN ingress
Ethertype	W	
SourceVendorClassID	W	R146, R147: LAN ingress
SourceClientID	W	R148, R149: LAN ingress
SourceUserClassID	W	R150, R151: LAN ingress
IPLengthMin	W	R111, R143: <b>(SHOULD)</b>
DSCPCheck	W	R107, R139
DSCPMark	W	R101, R125, R126
EthernetPriorityCheck	W	R110: Only for WAN ingress.
EthernetPriorityMark	W	R126
VLANIDCheck	W	R112: Only for WAN ingress.
ClassQueue	W	
InternetGatewayDevice.QueueManagement.Queue.{i}.	PC	
QueueEnable	W	
QueueStatus	R	
QueueInterface	W	
QueueBufferLength	R	
QueueWeight	W	R194 WAN egress
QueuePrecedence	W	R195, R196
REDThreshold	W	R180, R182, R183: RED parameters are not well modelled in TR-098
REDPercentage	W	R180, R184, R185: RED parameters are not well modelled in TR-098
DropAlgorithm	W	R179: "RED" R181: "DT"
SchedulerAlgorithm	W	R190: "SP. "WRR" (SHOULD)
ShapingRate	W	R189
ShapingBurstSize	W	R189
InternetGatewayDevice.WANDevice.{i}.WANConnection-Device.{i}.WANDSLLinkConfig.	P	
ATMQoS	W	R199
ATMPeakCellRate	W	R199
ATMMaximumBurstSize	W	R199
ATMSustainableCellRate	W	R199
InternetGatewayDevice.WANDevice.{i}.WANConnection-Device.{i}.WANIPConnection.{i}.	-	
ShapingRate	W	R189
ShapingBurstSize	W	R189
InternetGatewayDevice.WANDevice.{i}.WANConnection-Device.{i}.WANPPPConnection.{i}.	-	
ShapingRate	W	R189
ShapingBurstSize	W	R189

Table 5 QoS:1 profile definition for InternetGatewayDevice:1.x

 1  
2

1 **6.4.8.4 HGI QoS Dynamic Profile**

2 Table 6 defines the X\_HGI\_QoSDynamic:1 profile for the InternetGatewayDevice:1.x object.  
 3 The minimum required version for this profile is InternetGatewayDevice:1.1.

4 This profile defines additional requirements for the optional overload protection mechanism,  
 5 which is described in requirement R177.

6

Name	Req	HGI												
InternetGatewayDevice.QueueManagement.	P													
MaxAppEntries	R	Must be at least 1.												
AppNumberOfEntries	R													
MaxFlowEntries	R	Must be at least 1.												
FlowNumberOfEntries	R													
AvailableAppList	R	Must include "urn:homegatewayinitiative-org:qos:overload-protection1".												
InternetGatewayDevice.QueueManagement.Classification.{i}.	PC													
ClassApp	W	Must be instance number of the App entry that handles overload protection.												
InternetGatewayDevice.QueueManagement.App.{i}.	PC	These requirements relate to the App entry that handles overload protection.												
AppEnable	W													
AppStatus	R													
ProtocolIdentifier	W	Must be "urn:homegatewayinitiative-org:qos:overload-protection:1".												
AppName	W													
AppDefaultQueue	W	Must be the instance number of the queue that is used for flows that are not yet established (i.e. the temporary queue).												
AppDefaultDSCPMark	W													
AppDefaultEthernetPriorityMark	W													
InternetGatewayDevice.QueueManagement.Flow.{i}.	PC	These requirements relate to the Flow entry that handles overload protection.												
FlowEnable	W													
FlowStatus	R													
FlowType	W	Must be "urn:homegatewayinitiative-org:qos:overload-protection:1".												
FlowTypeParameters	W	<p>Must encode the overload protection algorithm parameters as specified in TR-098, i.e. (loosely) in the form "name1=value1&amp;name2=value2". The following parameter names and values Must be supported:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>MaxInstances</td> <td>Maximum number of instances of this service (whether established or not)</td> </tr> <tr> <td>SampleInterval</td> <td>Interval (in ms) between executions of the state machine algorithm</td> </tr> <tr> <td>InactivePackets</td> <td>If number of packets in sample interval is less than this, service instance is considered inactive</td> </tr> <tr> <td>ActivePackets</td> <td>If number of packets in sample interval is greater than this, service instance is considered active</td> </tr> <tr> <td>QueueThreshold</td> <td>If "established flow" queue depth exceeds this within sample interval, no new service instances will be allowed to become established</td> </tr> </tbody> </table>	Name	Value	MaxInstances	Maximum number of instances of this service (whether established or not)	SampleInterval	Interval (in ms) between executions of the state machine algorithm	InactivePackets	If number of packets in sample interval is less than this, service instance is considered inactive	ActivePackets	If number of packets in sample interval is greater than this, service instance is considered active	QueueThreshold	If "established flow" queue depth exceeds this within sample interval, no new service instances will be allowed to become established
Name	Value													
MaxInstances	Maximum number of instances of this service (whether established or not)													
SampleInterval	Interval (in ms) between executions of the state machine algorithm													
InactivePackets	If number of packets in sample interval is less than this, service instance is considered inactive													
ActivePackets	If number of packets in sample interval is greater than this, service instance is considered active													
QueueThreshold	If "established flow" queue depth exceeds this within sample interval, no new service instances will be allowed to become established													

Name	Req	HGI
FlowName	W	
AppIdentifier	W	Must be instance number of the App entry that handles overload protection.
FlowQueue	W	Must be the instance number of the queue that is used for established flows.
FlowDSCPMark	W	
FlowEthernetPriorityMark	W	

1  
2 Table 6 X\_HGI\_QoSDynamic:1 profile definition for InternetGatewayDevice:1  
3

4 The example in Section 7.1 outlines a TR-098 configuration to implement the proposed HGI  
5 QoS classification and queuing.

#### 6 7 **6.4.9 Non-Integrated Device Requirements**

8 The following requirements pertain to the use of priority markings for non-integrated wireless  
9 or powerline access devices that are connected via Ethernet.

##### 10 11 **6.4.9.1 LAN Infrastructure Devices**

12 The following requirements pertain to the use of priority markings for non-integrated wireless  
13 or power line access devices and Ethernet LAN devices.

N°	Requirement
R211.	The non-integrated wireless or power line device <b>SHOULD</b> set its native layer 2 markings for packets it receives from wired or wireless Ethernet by translating the received DSCP value to the native layer 2 markings using the translation shown in Table 7.
R212.	For packets it sends to the Ethernet, the non-integrated wireless or power line device <b>SHOULD</b> translate its native layer 2 marking to DSCP using the correspondence between DSCP and native layer 2 markings shown in Table 7.

##### 14 **6.4.9.2 Non-integrated Ethernet Infrastructure Devices**

15 The following requirements pertain to the interpretation of priority markings for non-  
16 integrated Ethernet infrastructure devices such as bridges and switches.

N°	Requirement
R213.	The non-integrated Ethernet Infrastructure Device <b>SHOULD</b> determine the QoS treatment accorded to packets by internally translating the received DSCP value to User Priority as shown in Table 7., without the addition of an 802.1Q tag.

17  
18

Layer 3	Layer 2			
Diffserv	802.1D	WMM/ 802.11e	FLC (4 Level)	FLC (8 Level)
DSCP	User Priority	Access Category	Channel Access Priority	Channel Access Priority
0x08	1	AC_BK (AC0)	Priority 0 (CA0)	CA1
0x10	2	AC_BK (AC0)	Priority 0 (CA0)	CA2
0x00	0	AC_BE (AC1)	Priority 1 (CA1)	CA0
0x18	3	AC_BE (AC1)	Priority 1 (CA1)	CA3
0x20	4	AC_VI (AC2)	Priority 2 (CA2)	CA4
0x28	5	AC_VI (AC2)	Priority 2 (CA2)	CA5
0x30	6	AC_VO (AC3)	Priority 3 (CA3)	CA6
0x38	7	AC_VO (AC3)	Priority 3 (CA3)	CA7

Table 7 Correspondence between Service Classes and Infrastructure Device Markings

#### 6.4.9.3 End devices

Table 8 shows the correspondence between HGI service classes and the default DSCP and layer 2 markings applied to packets by end devices within the LAN.

HGI	Layer 3	Layer 2		
	Diffserv	WMM/ 802.11e	FLC (4 Level)	FLC (8 Level)
Class Service	DSCP	Access Category	Channel Access Priority	Channel Access Priority
Upstream BE Data Transit BE Data	0x00	AC_BE (AC1)	Priority 1 (CA1)	CA0
Upstream Premium Data	0x18	AC_BE (AC1)	Priority 1 (CA1)	CA3
Upstream Video Transit VAS	0x20	AC_VI (AC2)	Priority 2 (CA2)	CA4
Upstream Voice	0x38	AC_VO (AC3)	Priority 3 (CA3)	CA7

Table 8 Correspondence between Service Classes and End Device Markings

#### 6.4.9.3.1 Informative notes on Set Top Boxes and VoIP Client Devices

The following notes pertain to Set Top Box (STB) deployed within the home network and not integrated within the HG.

- The outgoing packets from the STB should have their DSCP bits configurable to conform to the "Upstream Video" category in.
- The default DSCP markings for outgoing packets from the STB should conform to the "Upstream Video" category in Table 8.

1 The following notes pertain to VoIP client devices deployed within the home network and not  
2 integrated within the HG.

- 3 • The outgoing packets from the VoIP Client Device should have their DSCP bits  
4 configurable.
- 5 • The default DSCP marking for outgoing voice packets from the VoIP client device should  
6 conform to the “Upstream Voice” category in Table 8

## 7 **6.5 Management**

8 This section is compliant with DSL Forum TR-069, TR-098, TR-104, TR-106 and TR-111  
9 [49] except where this is explicitly mentioned. If there are still any ambiguities or conflicts in the  
10 text, it must be assumed that compliance with the above mentioned TR documents supersedes any  
11 other requirements.

### 12 **6.5.1 Northbound Interfaces**

N°	Requirement
R214.	The HG/ACS communication interface <b>MUST</b> comply with all the mandatory requirements of the CWMP protocol v1 as defined in TR-069 [1].
R215.	The HG <b>MUST</b> include the following profile name: “X_HGI_ManagementProfile:1” in the DeviceSummary parameter, if the device complies with all the mandatory requirements of this specification. This profile follows the definition and usage conventions described in TR-106.

13

### 14 **6.5.2 RMS Requirements**

N°	Requirement
R216.	The RMS <b>MUST</b> be able to manage the Home Gateway using the CWMP protocol as described in TR-069 (the ACS referenced there is a TR-069 capable RMS in this specification), including device configuration, software updates, and device diagnostics
R217.	The RMS <b>MUST</b> be able to support DSL Forum and HG devices, and thus support TR-098, TR-104, and TR-106 data models and their extensions as defined by HGI
R218.	The RMS <b>SHOULD</b> support extensibility for vendor-specific data model extensions.
R219.	The RMS <b>SHOULD</b> be able to manage end user devices behind the Home Gateway using CWMP.
R220.	The RMS <b>MUST</b> implement a Northbound Interface (NBI) that allows it to integrate into service provider backend operational support systems (OSS), such as billing applications, call centre and support tools, subscriber management systems, and policy management systems.
R221.	The RMS <b>MUST</b> provide an administrator GUI for the use of the service provider. It <b>MUST</b> be possible to provide secure access to this GUI.
R222.	The RMS <b>SHOULD</b> be able to scale to manage millions of devices of multiple types (e.g. gateways, IP STBs, VoIP ATAs, etc.)

N°	Requirement
R223.	The RMS <b>MUST</b> provide high availability of service.
R224.	The RMS <b>MUST</b> provide for RMS database backup/restore

1

### 2 6.5.3 General HG configuration and management

N°	Requirement
R225.	The HG <b>MUST</b> support and implement a local management graphical user interface. The details of this interface are defined in section 6.5.7
R226.	<p>The HG <b>MUST</b> automatically establish a CWMP management session with the ACS in the following cases, as defined in DSL Forum TR-069 [1]:</p> <ul style="list-style-type: none"> <li>• Each time the IP address of the HG changes</li> <li>• On power-up or reset</li> <li>• After a time-out following management session period expiration</li> <li>• After configuration changes in the HG and the related notifications are activated and the related Active Notification attributes are set.</li> <li>• After a connection Request from the RMS (or ACS).</li> </ul>
R227.	The data exchanged between the HG and the ACS <b>MUST</b> be encrypted, except for the firmware images for in-band management <sup>7</sup> . It <b>SHOULD</b> be encrypted for out-of-band management <sup>8</sup> . The level of encryption of the exchanged data is the one defined in DSLForum TR-069 (SSL or TLS level) <sup>9</sup> .
R228.	All authentication and configuration traffic from local clients to HG and vice-versa <b>MAY</b> be encrypted.
R229.	The firmware image file <b>MUST</b> be signed to ensure its correctness and integrity during the transmission.
R230.	Service provider or customer specific data, such as password or personal information, <b>MUST NOT</b> be located in any software file image or software module file image. Therefore software that is transferred between RMS and HG <b>MAY</b> be encrypted
R231.	<p>In order to be able to start communication with the ACS, the HG <b>MUST</b> be able to discover its address by one of the following mechanisms:</p> <ul style="list-style-type: none"> <li>• The ACS URL is preconfigured</li> <li>• The ACS URL is locally inserted in a secure way through the LM Remote UI</li> </ul>

<sup>7</sup> In-band management: The management session is established in the same communication channel as the data (same VC, VLAN...)

<sup>8</sup> Out-of-band management: The management session is established in a separate communication channel from the rest of data (dedicated VC, VLAN...)

<sup>9</sup> Out-of-band management: The management session is established in a separate communication channel from the rest of data (dedicated VC, VLAN...)

N°	Requirement
R232.	The HG <b>MUST</b> allow the ACS to modify the ACS URL remotely
R233.	The HG <b>MUST</b> identify itself to the ACS with its serial number and OUI, as defined in TR-069. If the serial number is not unique across the product line, the product class <b>MUST</b> also be provided
R234.	<p>The HG <b>MUST</b> support auto-provisioning of basic L2 and L3 connectivity for the management communication channel:</p> <ul style="list-style-type: none"> <li>• When using DHCP, authentication <b>MUST</b> be based on the hardware address of the HG WAN interface or the line identification.</li> <li>• When using PPP, authentication <b>MUST</b> be based on a generic username/password burnt in the firmware of the HG or provided locally in a secure way.</li> <li>• When using ATM networks, the HG <b>MUST</b> be preconfigured with ATM VC configuration. Nevertheless it <b>SHOULD</b> support ILMI to configure automatically ATM connectivity.</li> </ul>

#### 1 6.5.4 Definition of the data model supported

N°	Requirement
R235.	The use of profiles for HGI data model <b>MUST</b> follows the definition and usage conventions described in the TR-106 [47]
R236.	<p>The HG <b>MUST</b> support the “Baseline:1” profile definition for InternetGateway:1.1 defined in DSLForum TR-098 [41]. This profile defines objects regarding:</p> <ul style="list-style-type: none"> <li>• DeviceInfo</li> <li>• ManagementServer</li> <li>• Layer3Forwarding</li> <li>• LANConfigSecurity (password of the local management interface)</li> <li>• LANDevice</li> <li>• WANDevice</li> </ul>
R237.	The HG <b>MUST</b> support the related objects of the WAN Interfaces defined in the following profiles: ADSLWAN:1, EthernetWAN:1, Bridging:1. These profiles are defined in the DSLForum TR-098.
R238.	The HG <b>MUST</b> support the related objects of the LAN Interfaces defined in the following profiles: EthernetLAN:1, USBLAN:1, WiFiLAN:1. These profiles are defined in the DSLForum TR-098.

#### 2 6.5.5 Diagnostics, notifications and alarms

3 This section specifies the notification and diagnostic capabilities of the HG. The mechanisms  
4 and notification cases are described in some detail.

5

1 **6.5.5.1 Notifications and logging**

 2 For notifications, the TR-069 definition is adopted. Log management is only outlined in Release 1,  
 3 whereas the full specification of management features for the log will be detailed in Release 2.

 4 **6.5.5.1.1 Mechanisms**

N°	Requirement
R239.	The HG <b>MUST</b> be able to issue notifications and alarms to the RMS. Two operating methods <b>MUST</b> be supported (not simultaneously): <ul style="list-style-type: none"> <li>• Active Notification: The HG notifies the RMS of the alarm as soon as it is produced. This mechanism <b>MUST</b> be implemented using the proactive notification mechanisms as defined in TR-06910.</li> <li>• Passive notification: The HG stores the notification internally and sends it to the RMS only on request from the latter. This mode <b>MUST</b> be implemented using TR-069.</li> </ul>
R240.	The HG stores the log information internally and sends it periodically to the RMS using a log file. This mode <b>MUST</b> be implemented using the "Upload" method, using the option "2 Vendor Log File", as defined in TR-069.
R241.	The log file <b>MUST</b> be an XML file that is based on the log information stored in the HG

5

 6 **6.5.5.1.2 Notification cases**

 7 Those cases where it is required to issue an event in the HG to be communicated to the  
 8 RMS are now listed and the default behaviour is described.

- 9
- Active notifications

N°	Requirement
R242.	The HG <b>MUST</b> issue a notification to inform the RMS about its status, when finishing the booting procedure, as defined in TR-069.
R243.	The HG <b>MUST</b> issue a notification to inform the RMS that its WAN side IP address has changed. By default, this event is actively notified as defined in TR-069

10

- 11
- Passive notifications

N°	Requirement
R244.	The HG <b>MUST</b> issue an event if its QoS queues are full or if congestion is suspected in the CPE . By default, this event is notified be request of the RMS, using the "passive notification" mechanism

---

<sup>10</sup> This mode can flood the network with management data, so it should be treated very carefully, as defined TR-098 section 2.4.1

N°	Requirement
R245.	The HG <b>MUST</b> issue an event if a software module of the HG has been added, deleted or upgraded .

1

2 **6.5.5.2 Statistics and Diagnostics**

3 **6.5.5.2.1 Mechanisms**

N°	Requirement
R246.	The RMS <b>MUST</b> be able to run diagnostic tests on different parts of the HG.
R247.	This diagnostics <b>MUST</b> be integrated in the data model as defined in TR-069 (appendix B).

4 **6.5.5.2.2 Defined diagnostics and statistics**

5 For diagnostics and statistics, TR-069 and TR-098 are adopted. This section specifies the  
 6 objects and attributes required (**MUST**) and desirable (**SHOULD**) that are included in the profiles of  
 7 the above mentioned reports. Objects and attributes of these profiles that are not explicitly  
 8 mentioned are considered to be optional (low priority).

N°	Requirement
R248.	<p>Diagnostics and reporting of WAN side parameters <b>MUST</b> be supported. The mechanisms are the ones included in TR-069 [1] and TR-098 [41] using the following objects (note: the objects listed here are linked to specific WAN side technologies and therefore they will be only present in the WAN access technology is present).</p> <p>The statistical data are:</p> <ul style="list-style-type: none"> <li>• WANCommonInterfaceConfig (attributes: WANAccessType, Layer1UpstreamMaxBitRate, Layer1DownstreamMaxBitRate, PhysicalLinkStatus, WANAccessProvider, TotalBytesSent, TotalBytesReceived, TotalPacketsSent, TotalPacketsReceived, MaximumActiveConnections, NumberOfActiveConnections)</li> <li>• WANDSLInterfaceConfig (attributes: all except enable)</li> <li>• WANDSLInterfaceConfig.Stats.Total</li> <li>• WANDSLInterfaceConfig.Stats.Showtime</li> <li>• WANDSLLinkConfig (attributes: LinkStatus, AutoConfig, ATMTransmittedBlocks, ATMReceivedBlocks, AAL5CRCERrors, ATMCRCErrors)</li> <li>• WANEthernetInterfaceConfig (attributes: Status, MACAddress)</li> <li>• WANEthernetInterfaceConfig.Stats</li> <li>• WANEthernetLinkConfig</li> <li>• WANDSLLinkConfig (attributes: LinkStatus, LinkType, AutoConfig, ModulationType, ATMTransmittedBlocks, unsignedInt, ATMReceivedBlocks, AAL5CRCERrors, ATMCRCErrors, ATMHECErrors)</li> <li>• WANIPConnection (attributes: ConnectionStatus, PossibleConnectionTypes, Uptime, LastConnectionError)</li> <li>• WANIPConnection.Stats</li> <li>• WANPPPConnection (attributes: ConnectionStatus, PossibleConnectionTypes, Uptime, LastConnectionError, PPPEncryptionProtocol, PPPCompressionProtocol, PPPAuthenticationProtocol, CurrentMRUSize, TransportType)</li> <li>• WANPPPConnection.Stats</li> </ul> <p>The diagnostics are:</p> <ul style="list-style-type: none"> <li>• WAN-DSL Diagnostics</li> <li>• WANATMLoopbackF5Diagnostics</li> </ul>
R249.	<p>The following WAN side parameters <b>SHOULD</b> be supported. The mechanisms for diagnostics are the ones included in TR-069 and TR-098 using the following objects:</p> <ul style="list-style-type: none"> <li>• WANDSLInterfaceConfig.Stats.CurrentDay</li> <li>• WANDSLInterfaceConfig.Stats.QuarterHour</li> <li>• WANIPConnection (attribute: RSIPAvailable)</li> <li>• WANPPPConnection (attribute: RSIPAvailable, ExternalIPAddress, RemoteIPAddress, PPPLCPEcho, PPPLCPEchoRetry)</li> </ul>

N°	Requirement
R250.	Diagnostics and reporting of LAN side parameters, performance and devices (network level) <b>MUST</b> be supported. The mechanisms for diagnostics are the ones included in TR-069 and TR-098 in the following objects: <ul style="list-style-type: none"> <li>• LANEthernetInterfaceConfig (attributes: Status, MACAddress)</li> <li>• LANEthernetInterfaceConfig.{i}.Stats</li> <li>• LANUSBInterfaceConfig (attributes: all except enable)</li> <li>• LANUSBInterfaceConfig.{i}.Stats</li> <li>• WLANConfiguration (attributes: Status, Standard, PossibleChannels, PossibleDataTransmitRates, TotalBytesSent, TotalBytesReceived, TotalPacketsSent, TotalPacketsReceived, TotalAssociations)</li> </ul>
R251.	Ping and traceroute diagnostic tools <b>MUST</b> be included in the HG to test connectivity in the WAN and LAN interfaces. The mechanisms for diagnostics are the ones included in TR-098 and TR-106, in the following profile: <ul style="list-style-type: none"> <li>• IPPing:1</li> <li>• IPTraceroute:1</li> </ul>
R252.	Diagnostics of hardware and module tests <b>MUST</b> be included: CPU, memory, running processes, etc... Mechanisms for diagnostics are the ones included in TR-069. The extension to the data model is located in the "InternetGatewayDevice" object. The following table gives its definition

1

Argument	Type	Write	Read	Description
InternetGatewayDevice.X_HGI_DeviceDiagnostics.{i}	Object	-	R	Object containing general diagnostics for the CPE.
DiagnosticsState	String	-	R	Indicates availability of diagnostic data. One of: <ul style="list-style-type: none"> <li>• "None"</li> <li>• "Requested"</li> <li>• "Complete"</li> </ul> Value may be set to Requested to initiate the diagnostic test. When writing, the only allowed value is Requested. To ensure the use of the proper test parameters (the writable parameters in this object), the test parameters <b>MUST</b> be set either prior to or at the same time as (in the same SetParameterValues) setting the DiagnosticState to Requested. When requested, the CPE <b>SHOULD</b> wait until after completion of the communication session with the RMS before starting the diagnostic. When the diagnostic initiated by the RMS is completed (successfully or not), the CPE <b>MUST</b> establish a new connection to the RMS to allow the RMS to view the results, indicating the Event code "8 DIAGNOSTICS COMPLETE" in the Inform message.

Argument	Type	Write	Read	Description
Description	String(256)	-	R	Short description of the diagnostics. Normally a list of modules tested: CPU, memory, Routing daemons...
IsOK	Boolean	-	R	Whether the test results were positive (everything is OK) or errors were encountered.
DeviceDiagnostic.Errorlist	Object	-	R	Object containing the errors, encapsulated with the event object
DeviceDiagnostic.Errorlist.NumberError	unsignedInt	-	R	Number of events (errors) contained in the Errorlist.
InternetGatewayDevice.X_HGI_DeviceDiagnostic.Errorlist.Event.{i}	Object	-	R	Object used to encapsulate the errors happened during the diagnostics procedure.
Date	dateTime	-	R	Date and time of occurrence of the event.
Type	String(64)	-	R	Type of the event. This is used to classify the events. The precise types of events to be supported depends on the capabilities of the CPE and the involved diagnostic
Severity	String(32)	-	R	Define the seriousness of the event: Information: An event produced that can be used to track problems, collect statistics but that is not an error. Error: Error that will prevent that the CPE can perform some of its functions, but the main ones will continue to work. Critical: Error that affects the normal operation of the CPE: Some core functions of the CPE will not be available.
Description	String(256)	-	R	Short message describing / identifying the event.

1

N°	Requirement
R253.	Diagnostics of specific hardware and firmware modules installed in the HG, <b>SHOULD</b> be included to test whether the modules are working properly . Mechanisms for diagnostics are the ones included in TR-069. The extension to the data model is the same as the one already described. The only change consists of the name of the root object (X_HGI_DeviceDiagnostics) which has been changed to reflect the modules to be tested. Extension to the data model are reported in the following table

2

Argument	Type	Write	Read	Description
InternetGatewayDevice.X_HGI_ModulesDiagnostics	Object	-	R	Object containing module diagnostics for the CPE.
InternetGatewayDevice.X_HGI_ModulesDiagnostics.ListTestableModules	String[]	-	R	List of the modules that can be tested remotely (comma-separated list of the names of the modules)
InternetGatewayDevice.X_HGI_ModulesDiagnostics.SIPDiagnostics	Object	-	R	Test SIP functionality in the HG. This object is identical to DeviceDiagnostics
InternetGatewayDevice.X_HGI_ModulesDiagnostics.FirewallDiagnostics	Object	-	R	Test the firewall and port mapping functionality in the HG. This object is identical to DeviceDiagnostics

Argument	Type	Write	Read	Description
InternetGatewayDevice .X_HGI_ModulesDiagnostics. ATA	Object	-	R	Test the integrated ATA module (if present). This object is identical to DeviceDiagnostics

1

2 **6.5.6 End device management**3 **6.5.6.1 Device Identification**

N°	Requirement
R254.	The HG <b>MUST</b> discover and identify uniquely the managed devices connected to the home network
R255.	The HG <b>SHOULD</b> discover and identify uniquely the unmanaged devices connected to the home network
R256.	The HG <b>MAY</b> discover and identify uniquely the unmanageable devices connected to the home network
R257.	A database of devices (device repository) <b>MUST</b> be held in the HG. This database contains the results of the device discovery and capabilities detection mechanisms.
R258.	<p>In the above mentioned database, the HG <b>MUST</b> record per device the following identity information:</p> <ul style="list-style-type: none"> <li>• LAN side Private IP address and management port number.</li> <li>• WAN side Public IP address and management port number (NA(P)T binding)</li> <li>• Hardware (MAC) address</li> <li>• ManufacturerOUI</li> <li>• SerialNumber</li> <li>• UUID (Universally Unique IDentity)</li> <li>• ProductClass</li> <li>• Device Type</li> <li>• Friendly name</li> <li>• Manufacturer</li> <li>• Model name</li> <li>• Type of physical interface through which the host is connected to the HG.</li> </ul>
R259.	From every device, at least the hardware address should be available. The values that are not available to the HG <b>MUST</b> be left blank in the database.
R260.	Devices <b>MUST</b> be distinguished based on UUID. If the UUID is not available, then the devices <b>MUST</b> be distinguished on {ManufacturerOUI, SerialNumber} or, if this is not globally unique, {ManufacturerOUI, ProductClass, SerialNumber}.
R261.	If the combinations of the above UUID are not available, then the devices <b>MUST</b> be distinguished on hardware (e.g. MAC) address.

N°	Requirement
R262.	The HG <b>MUST</b> update the database or req. R257 with the IP- and hardware addresses provided by the DHCP clients on the network.
R263.	For every ED (managed and unmanaged), the HG <b>MUST</b> determine the IP address and hardware address from its ARP cache [11], if not obtained via DHCP.
R264.	The HG <b>MUST</b> read additional ID information provided by managed EDs of type D (see Table 2) and TR-111 enabled managed EDs of type CD by means of DHCP option 125 [13], and update its database accordingly.
R265.	The HG <b>SHOULD</b> also read ID information provided by the DHCP options 60 (vendor class identifier) [12], 61 (client identifier) [12], 77 (User Class) [17], 124 (V-I vendor class) [13] or 125 for other managed and unmanaged devices, and update its database accordingly.
R266.	The HG <b>MUST</b> contain the SSDP stack as defined in [10] for discovery of the ID information of managed EDs of type U and CU (see Table 2) and unmanaged UPnP devices.
R267.	The HG <b>MUST</b> be able to interpret all standardized UPnP Device Descriptions (XML schemas), and extract the mandatory device ID information from it.
R268.	When the ID-information is retrieved, the HG <b>MUST</b> update its database accordingly.
R269.	The HG <b>MUST</b> discover embedded UPnP devices in UPnP root devices.
R270.	A number of values in the database might be provided by the clients by means of DHCP as well as UPnP (Friendly Name, MAC and OUI). In case of inconsistency, the HG <b>MUST</b> choose the DHCP values.
R271.	The discovery mechanism <b>MUST</b> apply to any new managed device that is connected to the HN.
R272.	The discovery mechanism <b>SHOULD</b> also apply to unmanaged devices.
R273.	The HG <b>MUST</b> discover the managed devices placed behind an access point or a bridge in the same way as those directly connected to the HG.
R274.	The HG <b>MUST</b> determine if the newly discovered ED supports DHCP, and/or UPnP, and/or CWMP, and if the ED is following the HGI recommendations (see section 5.4.1).
R275.	EDs that follow the TR-069 specs can be discovered as such, if they also use TR-111 [39]. Therefore, the HG <b>MUST</b> follow the TR-111 specifications.
R276.	The HG <b>MUST</b> discover if an end device is still present in the home network or not.

#### 1 6.5.6.2 Activity discovery and Database management

N°	Requirement
R277.	The database <b>MUST</b> be accessible by the ACS by means of CWMP.

N°	Requirement
R278.	The database (device repository) in the HG <b>MUST</b> be a modification and extension of the InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i} object of the HG data model of TR-069 as given at the end of this section and named (following HGI profile conventions) InternetGatewayDevice.LANDevice.{i}.Hosts.X_HGI_Host.{i}
R279.	The value of the HostNumberOfEntries parameter in the InternetGatewayDevice.LANDevice.{i}.Hosts object <b>MUST</b> be equal to the number of uniquely defined devices discovered on the network.
R280.	The entries in the device database <b>MUST</b> be kept even if the device is disconnected from the HN, unless the discovery mechanism (DHCP or UPnP) provides explicit information about the presence of the device in the HN.
R281.	The maximum number of UUID of a UPnP device in the database <b>MUST</b> be 32
R282.	If a 33rd UUID of a UPnP device has to be added then the oldest entry <b>MUST</b> be removed from the database.
R283.	The UPnP discovery mechanism automatically detects if a device is present in the network or not. The active flag <b>MUST</b> be automatically set to false if the UPnP device is removed from the UPnP cache.
R284.	If the device requests a DHCP lease time from the HG, the HG <b>MUST</b> put this value to $T_1$ seconds
R285.	$T_1$ <b>MUST</b> be configurable by the ACS.
R286.	The default value of $T_1$ <b>SHOULD</b> be 10000. In the TR-069 data model (CPE parameter list for an Internet Gateway Device) $T_1$ is the value of the parameter DHCPLeaseTime in the object InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.
R287.	If a device is present in the database, but has not been active (i.e. discovered by Gratuitous ARP or DHCP Inform) for $T_1$ seconds, the “active” flag <b>MUST</b> automatically be set to “False”.
R288.	The “active” flag <b>MUST</b> be automatically set to “False” by end of DHCP lease time (DHCP option 51).
R289.	If a device has not returned to activity $T_2$ days after the “active” flag is set to “False”, the HG <b>MUST</b> inform the ACS about this, if the notification attribute of the Active parameter is set to Active. The ACS <b>SHOULD</b> subsequently delete the device from the database.
R290.	$T_2$ <b>MUST</b> be remotely configurable by the ACS.
R291.	Therefore the InternetGatewayDevice.LANDevice.{i} host objects of the TR-069 data model of the HG <b>MUST</b> be extended with a writeable parameter named ActivityLossTimeOut that contains the value of $T_2$ . This parameter gives the minimum time that the “active” flag of an end device must be “false” before the ACS should delete it from the database.
R292.	The default value ActivityLossTimeOut <b>SHOULD</b> be 1209600.

1 The modifications and extension to the InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i} object  
2 of the HG data model of TR-069 as referred to in the following table.

- 3 • Objects and Parameters not currently present in the TR-069 model but which are  
4 (or may be) required by HGI are underlined.
- 5 • Objects and Parameters that are not required by HGI are ~~struck through~~.

Name	Type	Write	Read	Description
InternetGatewayDevice.LANDevice.{i}.Hosts.X_HGI_Host.{i}	object	-	R	Host table. Each entry in this table corresponds to a distinct LAN Device (managed or unmanaged, manageable or unmanageable) that is discovered by the Home Gateway, either by TR-111 Gateway-Device association, DHCP discovery, UPnP discovery, or ARP discovery..
<u>UUID</u>	<u>unsignedInt(16)</u>	-	R	Universally Unique Identifier, as defined by RFC4122 [8] and given by the UDN in the UPnP Device Description
<u>LANIPAddressPort</u>	string	-	R	IPv4 address of the end device and its management port number, given as a dotted decimal, followed by a semicolon, followed by the port number. The port number is 68 for devices of types D and CD, and given by the UPnP Control URL for devices of types U and CU. If the port number is not known, than 80 should be assumed.
<u>IPAddress</u>	string			Current IP Address of the host.
<u>AddressSource</u>	string			Indicates whether the IP address of the host was allocated by the CPE using DHCP, was assigned to the host statically, or was assigned using automatic IP address allocation. Enumeration of: "DHCP" "Static" "AutoIP"
<u>LeaseTimeRemaining</u>	int[-1:]			DHCP lease time remaining in seconds. A value of -1 indicates an infinite lease. The value must be 0 (zero) if the AddressSource is not DHCP.
<u>MACAddress</u>	string			MAC address of the host
<u>HardwareAddress1</u>	string	-	R	Hardware address 1 of the end device, e.g. Ethernet MAC address.
<u>HardwareAddress2</u>	string	-	R	Hardware address 2 of the end device, e.g. Ethernet MAC address.
<u>HardwareAddress3</u>	string	-	R	Hardware address 3 of the end device, e.g. Ethernet MAC address.
<u>ManufacturerOUI</u>	<u>string(6)</u>	-	R	Organizationally unique identifier of the Device manufacturer as provided to the Gateway by the Device. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros. The value <b>MUST</b> be a valid OUI as defined by [38]. In case of a TR-111 device this value <b>MUST</b> be taken from the InternetGatewayDevice.ManagementServer.ManageableDevice.{i} object.
<u>SerialNumber</u>	<u>string(64)</u>	-	R	Serial number of the Device as provided to the Gateway by the Device. In case of a TR-111 device this value <b>MUST</b> be taken from the InternetGatewayDevice.ManagementServer.ManageableDevice.{i} object.
<u>ProductClass</u>	<u>string(64)</u>	-	R	Identifier of the class of product for which the Device's serial number applies as provided to the Gateway by the Device. If the Device does not provide a Product Class, then this parameter <b>MUST</b> be left empty. In case of a TR-111 device this value <b>MUST</b> be taken from the InternetGatewayDevice.ManagementServer.ManageableDevice.{i} object.

Name	Type	Write	Read	Description
<u>DeviceType</u>	string(64)	=	R	Specified by the vendor, except for UPnP devices, when it is the device type suffix as defined by UPnP Forum [16]
HostName	string(64)	=	R	The device's host name or empty sting if unknown. <u>Short description for the end user.</u> Specified by vendor. For devices of type U and CU this value <b>MUST</b> be equal to the FriendlyName of a UPnP Device.
<u>Manufacturer</u>	string(64)	=	R	<u>Manufacturer's name. Specified by vendor.</u>
<u>ModelName</u>	string(64)	=	R	<u>Model Name. Specified by vendor</u>
InterfaceType	string	=	R	Type of physical interface through which this host is connected to the CPE (i.e. the Home Gateway). Enumeration of: "Ethernet" "USB" "802.11" "HomePNA" "HomePlug" "Other"
Active	Boolean	=	R	Whether or not the host is currently present on the LAN. If "true", then the end device is active. If "false", then the end device is not active..  The method of presence detection is a local matter to the CPE.  The ability to list inactive hosts is Optional. If the CPE includes inactive hosts in this table, this variable <b>MUST</b> be set to zero for each inactive host. The length of time an inactive host remains listed in this table is a local matter to the CPE.
<u>ManagementProtocol</u>	string	=	R	"Z" for unmanageable devices (type Z, only known from the ARP cache) "D" for devices of type D (managed and unmanaged, known from DHCP repository) "U" for devices of type U (managed and unmanaged, known from UPnP CP cache) "CD" for devices of type CD (only managed, known from DHCP repository and ACS) "CU" for devices of type CU (only managed, known from DHCP repository, UPnP CP cache, and ACS) "C" for devices of type C (only managed, known from ACS).  CWMP managed devices of other service providers will appear as devices of types Z, D or U..

1

## 2 6.5.7 Local HG management user interface

3 There also needs to be a Local Management Interface to complement the Remote  
4 Management of the HG. This interface is called the Local Management Remote User Interface (LM  
5 Remote UI).

1 **6.5.7.1 General**

N°	Requirement
R293.	The HG <b>MUST</b> provide a LM Remote UI which allows a human (via a browser in an ED) to interact with it. This interface is based on web technologies (http protocol).
R294.	It <b>MUST</b> be possible for the RMS to disable the LM Remote UI of the HG.
R295.	The HG <b>MAY</b> allow secure remote access to the LM Remote UI (from the AN), using https.
R296.	If the above requirement is supported, the user <b>MUST</b> be able to limit or disable the above functionality.
R297.	LM Remote UI <b>MUST</b> implement standard 'Keyboard & Mouse' input & navigation interaction paradigms for Administrator and General User, as defined by PC based user interfaces
R298.	LM Remote UI <b>SHOULD</b> implement standard 'Remote control' input & navigation: Up, Down, Left, Right and Enter interaction paradigms for Administrator & General User, as defined by TV based user interfaces (e.g. CEA-2014 <sup>11</sup> [50])
R299.	The HG <b>MAY</b> provide another UI, based on command line interface as telnet or serial cable connection. This interface <b>MUST</b> be password protected

2

3 **6.5.7.2 Design guidelines**

N°	Requirement
R300.	LM Remote UI <b>MUST</b> conform to HTML standard as defined in W3C specification (HTML 4.0 conforming to ISO 8879)
R301.	LM Remote UI <b>SHOULD</b> conform to CE-HTML standard (XHTML based standard provided as part of Web4CE CEA-2014 <sup>11</sup> [50])
R302.	LM Remote UI <b>MUST</b> be designed for standard resolution of 1024 x 768 (4:3 aspect ratio) and 1366 x 768 (16:9 aspect ratio)
R303.	LM Remote UI <b>SHOULD</b> be scalable to support minimum SDTV resolutions (NTSC / VGA 640 x 480)
R304.	LM Remote UI <b>SHOULD</b> be scalable for small resolutions in 4:3 aspect ratio (as 320 x 240) for small display devices as PDA or smart-phones.

4

---

<sup>11</sup> The reference to CEA-2014 is limited to the sections of that document that do not require UPnP (or other) features that are either not part of HGI release 1 or that are in contrast with other mandatory or optional requirements of HGI rel1.

1 **6.5.7.3 Operator Portal User Interface link**

N°	Requirement
R305.	The LM Remote UI <b>MUST</b> contain a link to a portal hosted by the operator, where the user can access additional functionalities related to the management of the HG that are not directly supported in the LM Remote UI. For example, this mechanism can be used to give information to the users about the events that happened in the HG.
R306.	The link <b>MUST</b> be coded as a URL that can be remotely configurable. Therefore a new attribute, "OperatorPortalURL" <b>MUST</b> be supported in the "InternetGatewayDevice.UserInterface" object of the TR-069 data model for Internet Gateways.
R307.	The LM Remote UI and the operator end user portal <b>SHOULD</b> be designed using similar design paradigms and look and feel.

2

3 **6.5.7.4 Contents and functionality**

N°	Requirement
R308.	<p>The LM Remote UI <b>MUST</b> support at least 2 user profiles: Administrator and General User including password authentication.</p> <ul style="list-style-type: none"> <li>• Administrator. This profile can perform all the operations supported by the LM Remote UI, regardless of whether it affects managed services. A display warning message, reminding the user that the actions done with this profile may affect the managed services, <b>SHOULD</b> be presented whenever the end user logs in with this profile.</li> <li>• General User. All the operations that can be performed <b>MUST NOT</b> affect managed services. Therefore some restrictions may apply in accessing the interface pages</li> </ul>
R309.	The HG <b>MUST</b> support the ability to perform reset to factory default or boot safe profile (configuration and firmware) from the LM Remote UI.

N°	Requirement
R310.	<p>The LM Remote UI <b>MUST</b> include the following information:</p> <ul style="list-style-type: none"> <li>• Simple HG Device Information <ul style="list-style-type: none"> <li>○ Manufacturer Name</li> <li>○ HG Name (Friendly)</li> <li>○ HG Model</li> <li>○ Firmware Version</li> </ul> </li> <li>• Simple HG Network Information <ul style="list-style-type: none"> <li>○ HG Hardware Address</li> <li>○ HG IP Address</li> </ul> </li> <li>• Device Information (per device) <ul style="list-style-type: none"> <li>○ Device Name</li> <li>○ IP Address</li> <li>○ Hardware Address</li> <li>○ Device Status</li> </ul> </li> </ul>
R311.	<p>The LM Remote UI <b>MUST</b> allow configuration of the following items:</p> <ul style="list-style-type: none"> <li>• Firewall rules port forwarding and NAT functionalities. Some abstractions, so as to define general security levels, <b>MAY</b> be offered to simplify this task.</li> <li>• The general user actions <b>MUST NOT</b> interfere with existing RMS configuration.</li> <li>• User names and passwords of the profiles for the LM Remote UI.</li> </ul>

1

2 **6.5.8 Firmware management and updates**

N°	Requirement
R312.	<p>The RMS <b>MUST</b> support software and firmware upgrades of the HG. The main components to be updated are:</p> <ul style="list-style-type: none"> <li>• Operating system and gateway firmware. This includes complete firmware updates or upgradeable modules.</li> <li>• Module additions or removals, in the case of a modular gateway. For example, when a new hardware module is added or removed, the drivers and associated services enablers are included.</li> </ul>

3

4 Standards as DSL-Forum TR-069 already provide mechanisms for firmware upgrades.  
5 However, some additional mechanisms and specifications are needed. These add-ons are  
6 described in the following sections.

1 **6.5.8.1 General**

N°	Requirement
R313.	TR-069 Appendix A [1] <b>MUST</b> be supported for software management and updates. This applies to the firmware of the HG
R314.	It <b>MUST</b> be possible to support software modules that can be upgraded remotely. This object is located under the “InternetGatewayDevice” object. Therefore, TR-069 data model should be extended with the information included in the following table

2

Argument	Type	Write	Read	Description
InternetGatewayDevice.X_HGI_Module.{}	Object	-	R	Installed module description.
Identifier	String(16)	-	R	Description / Identification of the modules, which <b>MUST</b> consistent with the list of modules attribute.
SoftwareVersion	String(64)	-	R	A string identifying the software module version currently installed in the CPE. To allow version comparisons, this element <b>SHOULD</b> be in the form of dot-delimited integers, where each successive integer represents a more minor category of variation. For example, a version number can be 3.0.21 where the components mean: Major.Minor.Build.
EnabledOptions	String(1024)	R	R	Comma-separated list of the option names of each. Option that is currently enabled in the CPE. The mechanism is identical to the one defined for CPE firmware in the DSL Forum TR-069

3

N°	Requirement
R315.	If software modules are supported, the TR-069 firmware upgrading mechanism <b>MUST</b> also be fully supported for software management and updates: The “DOWNLOAD” procedure will include a “filetype” that specifies the vendor and the module upgrade.

4

 5 **6.5.8.2 Software upgrades**

N°	Requirement
R316.	The HG <b>MUST</b> support RMS initiated firmware upgrades according to TR-069
R317.	It <b>MUST</b> be possible to read the current firmware version from the RMS at any time. DSL Forum TR-069 data model is used to perform this operation. (See the “InternetGatewayDevice.DeviceInfo” object from TR-069 Appendix B).
R318.	The HG <b>SHOULD</b> control the firmware integrity (for example MD5 checksum) and authenticate the signature prior to the flashing procedure
R319.	The normal operation (last good state of network provisioning and configuration) of the HG <b>MUST</b> be re-established in terms of provisioning and configuration when the HG itself comes back after a power failure.

N°	Requirement
R320.	There <b>MUST</b> be a mechanism that guarantees that the basic functionality and connectivity to the RMS can be recovered in case of a failure of a software upgrade or installation of new software.
R321.	<p>At least, a bootloader that works independently of the rest of the software <b>MUST</b> be present. For recovery the following mechanisms are possible (one or the other):</p> <ul style="list-style-type: none"> <li>• There is always (but maybe limited) default software together with a default configuration stored on the HG. If software upgrade fails (e.g. the HG is not booting anymore, incompatibilities with hardware are found, mismatch between software and configuration, etc.), the HG automatically loads his default software and configuration. Active notification to the RMS is necessary.</li> <li>• The HG has enough resources to always keep the latest running software and configuration. If a software upgrade fails the HG automatically reboots with the last good software and configuration. Notification to the RMS is necessary.</li> </ul>
R322.	When upgrading the safe boot loader, the old version <b>MUST NOT</b> be overwritten but maintained in the HG memory until the integrity check of the new version has been completed.

1

2 **6.5.8.3 Configuration**

N°	Requirement
R323.	There <b>MUST</b> be a factory-default configuration (or initial provisioning configuration) stored on the HG.
R324.	The above configuration <b>MUST</b> always work (with any software/firmware and hardware) and in particular <b>MUST</b> be able to establish the connectivity to the RMS.
R325.	<p>There <b>MUST</b> be the ability to reset the gateway locally to factory default (either by the Local Management User Interfaces or by a factory reset button that <b>SHOULD</b> be present). There <b>MUST</b> be two levels for the reset:</p> <ul style="list-style-type: none"> <li>• Reset to factory default configuration</li> <li>• Reset to last running software and configuration</li> </ul> <p>Note: this requirement is for the exceptional case when the HG is not accessible from the RMS</p>
R326.	It <b>MUST</b> be possible for the RMS to periodically fetch current configuration parameters to store in a remote database. Note: This can be implemented using the TR-069 UPLOAD method and the configuration file will be coded in a vendor specific format.
R327.	It <b>MUST</b> be possible to restore configuration parameters stored in the RMS. Such events are RMS initiated. This is implemented using the TR-069 DOWNLOAD method, using the "FileType" attribute to "3 Vendor Configuration File"

1 **6.5.8.4 User Interaction**

N°	Requirement
R328.	<p>It <b>SHOULD</b> be possible to allow the end-user to determine the software upgrade method in a limited way. The following parameters <b>SHOULD</b> be accessible by the user:</p> <ul style="list-style-type: none"> <li>• Always newest software: software upgrades done by the RMS without any constraint and as soon as they become available</li> <li>• Only when needed: software upgrades only occur when needed for specific service features that the user has subscribed to.</li> <li>• User defined time windows: software upgrades are SP initiated, but occur only in the user-specified time window.</li> </ul>
R329.	<p>The above functionalities and interface <b>MUST NOT</b> be located on the HG but on the Operators Portal User Interface (see section 6.5.7.3), as it defines policies about upgrades to be implemented mainly by the RMS.</p>

2 **6.5.9 Security management**

3 The RMS has to support the remote management of the main security functionalities of the  
4 HG: the stateful firewall and the ALG

5 **6.5.9.1 Firewall management**

6 The RMS has to manage remotely the internal firewall of the HG. To implement this  
7 operation, the RMS downloads to the HG an xml file to configure the firewall. This file integrates the  
8 basic firewall configuration that includes the HIGH and LOW configurations (see Security Section  
9 for more details)

10 DSL Forum TR-069 provides mechanisms for configuration file downloads. However, some  
11 additional mechanisms and specifications are needed to fully support the HGI requirements.

N°	Requirement
R330.	<p>The HG supports a stateful firewall, which <b>MUST</b> be remotely manageable by the RMS using a firewall rules configuration file. The file name is "X_HGI_FWConfiguration" and <b>SHOULD</b> be signed</p>
R331.	<p>NAT/PAT mechanisms, like port mapping capability to enable remote access to home based devices or servers (HTTP, FTP, SFTP, SSH, TELNET), <b>MUST</b> be remotely manageable as defined in the WANPPPCConnection or WANPPPCConnection objects of DSL Forum TR-098 define in the Baseline:1 profile. The RMS via the management abstraction layer has the capability to enable/disable the port mapping of the usual protocols.</p>
R332.	<p>The integrated firewall module of the HG <b>MUST</b> be manageable and <b>MUST</b> support the remote download by RMS request through the download RPC defined in the DSL Forum TR-069.</p>
R333.	<p>The above mentioned file <b>MUST</b> contain the both configuration HIGH and configuration LOW, if present (configurations are defined in 7.11 and 7.12)</p>

N°	Requirement
R334.	The version of the firewall <b>MUST</b> be also accessible by the RMS to help to determine if an update is necessary. The HG <b>MUST</b> support the VendorConfigFile objects defined in the TR-069, indicating the name and the version of the basic firewall configuration. (Note: This VendorConfigFile is not included in the Baseline:1 profile)
R335.	The status (HIGH, LOW) of the integrated firewall module of the HG <b>MUST</b> be remotely accessible by the RMS.
R336.	The HG <b>MUST</b> support the vendor specific parameters described in the following table

1

Name	Type	Write	Read	Description
InternetGatewayDevice-X_HGI_FWConfig	object	-	R	Vendor specific objects about the firewall
Status	String	R	R	Indicates the status of the firewall. Enumeration of: "LOW" "HIGH"
Date	dateTime	-	R	Date and time when the status of the firewall was modified

2

### 3 6.5.9.2 Application Layer Gateway Management

N°	Requirement
R337.	The ALG list (see ALG section 6.6.1) stored in the HG <b>MUST</b> be remotely accessible by the RMS.
R338.	The HG <b>MUST</b> allow the RMS to enable or disable the ALG. These changes can be made either by the RMS or by the user through the local management interface (some restrictions may apply to the latter case).
R339.	The HG <b>MUST</b> support the vendor specific objects required for the ALG management as defined in the table below.

4

Name	Type	Write	Read	Description
InternetGatewayDevice.X_HGI_ALG	Object	-	R	ALG table
ALGNumberOfEntries	unsignedint	-	R	Number of ALG entries
InternetGatewayDevice.X_HGI_ALG.Info.{i}	Object	-	R	Each instance contains objects associated a given ALG
Enable	Boolean	R	R	Enables or disables this ALG
Status	string	R	R	Indicates the status of the ALG entry. Enumeration of: "Enabled" "Disabled"
Name	String(64)	-	R	Name of the ALG
Version	String(16)	-	R	A string identifying the ALG version currently used in the CPE

Name	Type	Write	Read	Description
Description	String(256)	-	R	A description of the ALG

Table 9 ALG vendor specific objects

 1  
2

### 3 6.5.10 End-device recommendations

N°	Requirement
R340.	End devices <b>MUST</b> support the use of DHCP to configure IP connectivity during the start-up phase.
R341.	Managed EDs <b>MUST</b> provide IP and hardware address information by broadcasting a gratuitous ARP whenever their IP stack is initialized.
R342.	DHCP messages of managed EDs <b>MUST</b> include the IANA Enterprise Number [14] for the HGI in option 125. This number is 25812
R343.	The DHCP messages of managed EDs <b>MUST</b> also contain the following Encapsulated Vendor-Specific Option-Data fields in option 125, as defined in TR-111 and TR-106 [15] <ul style="list-style-type: none"> <li>• DeviceManufacturerOUI</li> <li>• DeviceSerialNumber</li> <li>• DeviceProductClass</li> </ul>
R344.	Managed EDs of type D <b>MUST</b> also include “DeviceType” in the Encapsulated Vendor-Specific Option-Data fields of DHCP option 125. The contents and format of this value are identical to the device type suffices as defined by the UPnP forum [16] (i.e.: “urn:uuid”).
R345.	Managed EDs of types U and CU <b>MUST</b> include “UUID” (Universally Unique Identifier) in the Encapsulated Vendor-Specific Option-Data fields of DHCP option 125. The contents and format of this value are given by RFC 4122 [7]
R346.	Managed end devices that are directly configurable by the ACS (interface IACS_ED) <b>MUST</b> follow the TR-069 and TR-106 [40] specifications.
R347.	Managed end devices directly configurable by the ACS <b>SHOULD</b> also follow the TR-111 part 1 and part 2 specifications [39].

4

### 5 6.6 Service Support

N°	Requirement
R348.	A dynamic DNS client <b>SHOULD</b> to be provided on the HG, to associate the HG IP address to a user chosen domain in the DNS system.
R349.	As an alternative to the above requirement, the dynamic DNS client <b>MAY</b> be implemented in the ACS

N°	Requirement
R350.	The HG <b>MUST</b> have a unique hardware ID for authentication and remote management purposes, composed of an OUI (Organizationally Unique Identifier) + serial number
R351.	The HG <b>MUST</b> support a time server client to obtain the time and date.
R352.	A NTP (RFC 1305 [42]) or SNTP (RFC 2030 [42]) client <b>MUST</b> be implemented to allow synchronization with the provider's NTP server.
R353.	The HG <b>MUST</b> advertise all the information related to the network NTP or SNTP server towards the home devices.
R354.	Information related to the network NTP or SNTP server towards the home devices <b>MUST</b> be retrieved using DHCP option 42 (or 4 in case of SNTP).
R355.	The HG <b>MUST NOT</b> implement any explicit function to reset time and date.

1

 2 **6.6.1 ALGs**

N°	Requirement
R356.	<p>The HG <b>MUST</b> support an Application Layer Gateway to support the interoperability with NAT mechanisms for the protocols listed in RFC 3027 [42]:</p> <ul style="list-style-type: none"> <li>• FTP</li> <li>• RSVP</li> <li>• DNS</li> <li>• SMTP</li> <li>• SIP</li> <li>• H.323</li> <li>• SNMP</li> <li>• RealAudio</li> </ul>

N°	Requirement
R357.	The HG <b>MUST</b> provide an additional set of ALGs to support the following protocols: <ul style="list-style-type: none"> <li>• PPTP</li> <li>• L2TP passthrough</li> <li>• IPSec passthrough single and multiple</li> <li>• ICMP</li> <li>• TELNET</li> <li>• HTTP</li> <li>• HTTPs</li> <li>• POP3</li> <li>• NTTP</li> <li>• RTSP</li> <li>• PPTP passthrough</li> <li>• GRE tunnelling</li> <li>• MSN Messenger</li> <li>• Yahoo Messenger</li> <li>• MSN Gaming Zone</li> <li>• Windows Media Player</li> <li>• Directplay (DirectX)</li> </ul>
R358.	ALGs <b>MUST</b> be able to be switched off in case of conflicts with external devices using STUN for NAT traversal

1

## 2 6.6.2 Communication Services Support

N°	Requirement
R359.	If the HG implements a SIP protocol stack (in the case of an embedded ATA), this <b>MUST</b> be according to RFC 3261 [42]
R360.	When an FXS port is supported, the HG <b>MUST</b> support SIP termination for VoIP communication on FXS.
R361.	When an integrated DECT port is supported, the HG <b>MUST</b> support SIP termination for VoIP communication to DECT.

N°	Requirement
R362.	If implemented, the SIP UA embedded in the HG, representing FXS or DECT, <b>MUST</b> support <ul style="list-style-type: none"> <li>• CLIP and CLIR</li> <li>• Call Hold and Retrieve</li> <li>• Call waiting</li> <li>• Call forwarding (CFU, CFB, CFNR)</li> <li>• CCBS.</li> <li>• Call transfer</li> <li>• Message Waiting Indication</li> </ul>
R363.	If the HG offers, through the SIP UA's on the LAN, a local calling service (without any signalling traffic on the WAN), a residential SIP proxy <b>MAY</b> be integrated in the HG supporting the following features: <ul style="list-style-type: none"> <li>• Local SIP forking (stateful proxy)</li> <li>• direct routing for internal calls</li> <li>• CLIP (e.g. copy P-Asserted-ID to From)</li> <li>• Click 2 call (B2BUA)</li> </ul>
R364.	If implemented, the residential SIP proxy <b>MUST</b> support a location database of SIP UAs on the LAN, built up by proxying REGISTER messages.
R365.	The HGW <b>MUST</b> support internal calling between the FXS and DECT terminations (if supported)
R366.	The HG <b>MUST</b> be the repository of SIP URI, username and password assigned to the embedded SIP UA(s) during the subscription procedure.
R367.	In case neither FXS nor DECT ports are in use, the internal SIP termination <b>MUST</b> be able to be switched off by the user or by the ACS
R368.	The ATA function in the HG <b>MUST</b> support the following features: VAD (Voice Activity Detection), CNG (Comfort Noise Generation) and PLC (Packet Loss Concealment)
R369.	The ATA function in the HG <b>MUST</b> support Line Echo Cancellation on all FXS and FXO ports
R370.	The HG <b>MUST</b> support the following Narrow-band codecs: G711 Mu-Law, G711 A-Law
R371.	The HG <b>SHOULD</b> support the following Narrow-band codecs: G729A, G729AB
R372.	HG <b>SHOULD</b> support the following Wide-band codecs: G722, G729EV, L16 and PCMA/16
R373.	Voice codecs <b>SHOULD</b> be resident in the gateway HW, but <b>MAY</b> also be downloadable
R374.	The HG <b>MUST</b> support an analogue fax service.

N°	Requirement
R375.	In the case of an xDSL connection with an associated PSTN service, the HG <b>SHOULD</b> support specific regional dialling plans to allow certain numbers (including emergency calls) to be routed to the FXO port (if service availability is detected on the PSTN line) instead of being routed to the VoIP outbound proxy.
R376.	In the case of xDSL connection with an associated PSTN service, the HG <b>MUST</b> support both a fallback (WAN connection or VoIP servers down) through an FXO port and a failover (power down) feature through a relay.
R377.	The HG <b>MAY</b> support H.323 [52]
R378.	If H,322 is supported, the following specifications <b>MUST</b> be used as a reference: ITU-T H.323 v4 [52]; H.225.0 v4 [53]; H.245 v7 [54]
R379.	The HG <b>MAY</b> support MGCP
R380.	If MGCP is supported, the following specifications <b>MUST</b> be used as a reference: RFC3660, RFC3435 [42]
R381.	An IPSEC VPN client in the gateway <b>SHOULD</b> be present, in order to establish and terminate a VPN (but only for devices connected to the analogue phone ports of the gateway)
R382.	The HG <b>SHOULD</b> support Secure RTP to protect VoIP data streams terminating in the embedded ATA
R383.	TLS or IPSEC <b>SHOULD</b> be supported to protect the signalling traffic for VoIP data streams terminating in the embedded AG.

1

 2 **6.6.3 Multimedia Services Support**

N°	Requirement
R384.	The HG <b>MUST</b> support IGMP v1/v2 (according to RFC2236 [42])
R385.	The HG <b>SHOULD</b> support v3 Querier function (according to RFC3376 [42])
R386.	If a multicast stream data flow coming from the WAN is NOT terminated in the HG, the HG <b>MUST</b> keep a record of which devices are subscribed to which multicast group. This can be done via IGMP snooping or RTSP ALG techniques.
R387.	If a multicast stream data flow coming from the WAN is NOT terminated in the HG, the HG <b>MUST</b> forward inbound multicast packets only to those physical interfaces which are connected to devices that have joined the specific multicast group.
R388.	If a multicast stream data flow coming from the WAN is terminated in the HG, the HG <b>MUST</b> implement a proxy mechanism, which subscribes to appropriate the multicast groups on the AN on behalf of devices on the HN, and realizes a mapping between the AN multicast stream format to the HN defined stream format

N°	Requirement
R389.	Where this is a multicast stream in the home network, the Home Gateway <b>MUST</b> perform a link layer multicast to unicast translation.

1

## 2 6.7 Security

N°	Requirement
R390.	Local access: the end user <b>MUST</b> be able to locally modify high level configuration parameters of his residential gateway (DSL login and password, LAN and WLAN configuration etc....) through a web interface.
R391.	A Local Configuration Secured Access (see 5.6.5) mechanism <b>MUST</b> be supported to authenticate the user (at least login password access control).
R392.	Web based remote access: the ACS or an accredited administrator <b>MUST</b> be authenticated by the gateway in order to remotely access management functionalities (configuration, firmware download, Management Information Base access...) <sup>12</sup> .
R393.	The gateway <b>MAY</b> be pre-configured with a unique certificate by vendors or a trusted Certificate Authority. In order to fulfil the strong authentication for remote management requirement, only Service Provider's or Manufacturer's Certification Authority <b>MUST</b> be trusted.
R394.	The gateway <b>SHOULD</b> be able to store and use cryptographic keys such as A private/public RSA pair.
R395.	Sensitive data service authentication keys, login PPP, VoIP data for instance <b>SHOULD</b> be stored in protected data storage areas or hardware containers
R396.	The HG <b>MUST</b> support a pass-through mechanism for any kind of VPN including VPNs based on IPSEC flows terminated on terminals.
R397.	At least 8 VPN pass-through sessions <b>MUST</b> be supported for different private networks and/or for different services having specific security requirements.
R398.	The HG <b>MUST</b> support NAT traversal techniques for VPN.
R399.	A stateful firewall <b>MUST</b> be implemented performing security control of any incoming flow entering the HN through the HG (note: this does not apply to bridged traffic). The basic policies are described in the security section (see section 6.7).

<sup>12</sup> The remote access **SHOULD** be based on cryptography like in standards SSL/TLS, SSH combined with the use of certificates, or IPSEC

N°	Requirement
R400.	At least the following basic firewall configuration <b>MUST</b> be supported by the HG: <ul style="list-style-type: none"> <li>• Configuration HIGH: DROP by default</li> <li>• WAN --&gt; LAN: to refuse TCP SYN, to refuse connections INVALID, NEW, RELATED in TCP, UDP and ICMP; to authorize already established connections (and known by the stateful firewall)</li> <li>• LAN --&gt; WAN: to authorize known ports:               <ul style="list-style-type: none"> <li>○ 25 – SMTP</li> <li>○ 80 – HTTP</li> <li>○ 109 (TCP) - POP2</li> <li>○ 443 – SSL</li> <li>○ 587 – ESMTP</li> <li>○ 995 (TCP) - POP3</li> <li>○ 123 - NTP</li> <li>○ 587 - ESMTP</li> </ul> </li> <li>• to refuse ports 109/UDP, 110/UDP and WINS</li> </ul>
R401.	A second basic firewall configuration <b>MAY</b> be supported by the HG <ul style="list-style-type: none"> <li>• Configuration LOW: ACCEPT by default               <ul style="list-style-type: none"> <li>○ WAN --&gt; LAN: to refuse ports 137, 138, 139 (NETBIOS)</li> <li>○ LAN --&gt; WAN: all authorized</li> </ul> </li> </ul>
R402.	DMZ support <b>MAY</b> be provided by the firewall in cooperation with the routing and address translation (NAT) or port address translation (PAT) capabilities of the HG
R403.	The HG <b>MUST</b> reject packets from the WAN with MAC addresses of devices on the local LAN or invalid IP addresses (e.g., broadcast addresses, private IP addresses or IP Addresses matching those assigned to the LAN Segment).
R404.	The HG <b>MUST</b> reject any unidentified Ethernet packets (i.e. any packet that is not associated with IP or PPPoE protocols).

1

## 2 6.8 Basic System Features

### 3 6.8.1 Powering, safety, EMC, and other regulatory requirements

4 *Note: Only requirements considered mandatory by national regulations are included in*  
 5 *sections 6.8.1.2, 6.8.1.3, 6.8.1.4 and 6.8.1.5.*

#### 6 6.8.1.1 Powering

N°	Requirement
R405.	The HG <b>SHOULD</b> run on DC power, provided by an external power supply module

N°	Requirement
R406.	The use of a fan is not recommended for reliability and noise reasons. If a fan is used, the noise <b>MUST</b> NOT exceed 25 dBA
R407.	The HG <b>MAY</b> be remotely powered from the access network, in the case of power failure
R408.	The HG <b>MAY</b> provide Power over Ethernet (according to IEEE802.3af) on its Ethernet (LAN side) outlets
R409.	The HG <b>MAY</b> provide dying gasp to send a message to the WAN remote management system in case of power failure

1 **6.8.1.2 Electrical Safety**

N°	Requirement
R410.	The HG and its power supply module <b>MUST</b> meet IEC 60950-1 [57] and its applicable regional and national variations
R411.	If remote powering is provided, the HG <b>MUST</b> meet IEC-60950-21 [58]
R412.	The power module <b>MUST</b> connect to the mains by means of a built-in (moulded) plug or a detachable power cord, suitable for the target country.

2 **6.8.1.3 EMC**

N°	Requirement
R413.	For the United States, the HG and its power module <b>MUST</b> meet FCC part 15
R414.	For all other countries, the HG and its power module <b>MUST</b> meet CISPR 22 (class B) and CISPR 24 or their local equivalent
R415.	Any HG with a built-in 802.11x wireless LAN <b>MUST</b> comply with the relevant requirements of EN 300 328 (2.4 GHz), EN 301 893 (5GHz), EN 301 489-1 and EN 300 489-17 [71][74][72][73]

3 **6.8.1.4 Other considerations (Environmental, reliability)**

N°	Requirement
R416.	The HG <b>MUST</b> meet WEEE and RoHS Directives (Europe) and/or similar requirements for other countries
R417.	The HG <b>MUST</b> comply with the reference levels related to human exposure to electromagnetic fields (EN 50371 [70], EN 50385 and/or similar requirements for other countries).
R418.	The HG and its power module <b>MUST</b> have a calculated MTBF > 100,000 hours.

1 **6.8.1.5 Regional regulatory requirements**

N°	Requirement
R419.	For Europe, the HG and its power module <b>MUST</b> carry the “CE mark”, and be declared in conformity with the essential requirements of the R&TTE Directive (99/05/EC)
R420.	For Europe, the HG and its power module <b>SHOULD</b> be declared in conformity with the Low Voltage Directive (73/23/EEC), the EMC Directive (86/336/EEC or 2004/108/EC)
R421.	For Japan, the HG and its power module <b>SHOULD</b> have VCCI registration
R422.	For the United States, the HG and its power module <b>MUST</b> be National Recognized Test Labs listed.

# 7 Appendix

## 7.1 An example of TR-098 configuration to implement the proposed HGI QoS classification and queuing

This outlines an example TR-098 [41] configuration that uses only the parameters in the X\_HGI\_QoS:1 and X\_HGI\_QoSDynamicFlow:1 profiles.

A shell-like \$VAR syntax is used to refer to configurable values. The following values would need to be supplied:

- \$VOICE\_SERVER\_IP: IP address(es) of voice server(s)
- \$GPRS\_LENGTH\_MIN: packet length threshold to distinguish between voice and data packets
- \$VIDEO\_CLIENT\_ID: DHCP option 61 value(s) for identifying trusted LAN video sources
- \$VPN\_SERVER\_ID: IP address(es) of VPN server(s)
- \$GAME\_PORT: destination port number(s) that identify gaming traffic
- \$VAS\_SOURCE\_IP: IP address(es) of WAN sources of managed services data (some overlap with \$VOICE\_SERVER\_IP and \$VPN\_SERVER\_IP)

There may also be other scheduling parameters, e.g. for the anti-starvation algorithm.

```

InternetGatewayDevice.QueueManagement. =
  Enable = true
  #####
  # Queues #
  #####
  # VAS = Value Added Services
  # scheduling parameter values are for illustration only
  # note that queues are assumed to be instantiated on all egress interfaces
  # that require them, i.e. need only define one queue object per set of
  # queuing parameters
  # SP1 strict priority queue (Upstream Voice, Downstream VAS)
  Queue.1. =
    QueueEnable = true
    QueuePrecedence = 1
    SchedulerAlgorithm = "SP"
  # SP2 strict priority queue (Upstream Video, Transit VAS)
  Queue.2. =
    QueueEnable = true
    QueuePrecedence = 2
    SchedulerAlgorithm = "SP"
  # WRR1 weighted round robin queue (Upstream Temporary Voice)
  Queue.3. =
    QueueEnable = true
    QueueWeight = 3
    QueuePrecedence = 3
    SchedulerAlgorithm = "WRR"
  
```

```

1  # WRR2 weighted round robin queue (Upstream Premium Data, Upstream GPRS
2  # Data, Upstream Game Data, Downstream Best Effort Data)
3  Queue.4. =
4      QueueEnable = true
5      QueueWeight = 2
6      QueuePrecedence = 3
7      SchedulerAlgorithm = "WRR"
8
9  # WRR3 weighted round robin queue (Best Effort Data)
10 Queue.5. =
11     QueueEnable = true
12     QueueWeight = 1
13     QueuePrecedence = 3
14     SchedulerAlgorithm = "WRR"
15
16 # Default queue is WRR3 (this is used if a packet doesn't match any
17 # classifiers)
18 DefaultQueue = 5
19
20 #####
21 # Apps and Flows #
22 #####
23
24 # Voice App (temporary voice queue logic)
25 App.1. =
26     AppEnable = true
27     ProtocolIdentifier = "urn:homegatewayinitiative-org:qos:overload-
28         protection:1"
29     AppDefaultQueue = 3 # WRR1
30
31 # Voice App Flow (if matches this flow, goes to the voice queue)
32 Flow.1. =
33     FlowEnable = true
34     FlowType = "urn:homegatewayinitiative-org:qos:overload-protection:1"
35     FlowParameters = "MaxInstances=10&SampleInterval=10..."
36     AppIdentifier = 1
37     FlowQueue = 1 # SP1
38
39 #####
40 # Classifiers (for most, there could be several instances) #
41 #####
42
43 # lower values of ClassificationOrder have precedence
44
45 # Upstream GPRS (IP DA + packet length)
46 Classification.1. =
47     ClassificationEnable = true
48     ClassificationOrder = 1
49     ClassInterface = "LAN"
50     DestIP = $VOICE_SERVER_IP
51     IPLengthMin = $GPRS_LENGTH_MIN
52     ClassQueue = 4 # WRR2
53
54 # Upstream Voice (IP DA + voice ALG)
55 Classification.2. =
56     ClassificationEnable = true
57     ClassificationOrder = 2
58     ClassInterface = "LAN"
59     DestIP = $VOICE_SERVER_IP
60     ClassApp = 1 # voice
61
62 # Upstream Video (IP SA or DHCP option 60, 61, 77)
63 Classification.3. =
64     ClassificationEnable = true
65     ClassificationOrder = 3

```

```
1      ClassInterface = "LAN"
2      SourceClientID = $VIDEO_CLIENT_ID
3      ClassQueue = 2 # SP1
4
5      # Upstream Premium Data (IP DA)
6      Classification.4. =
7          ClassificationEnable = true
8          ClassificationOrder = 4
9          ClassInterface = "LAN"
10         DestIP = $VPN_SERVER_IP
11         ClassQueue = 4 # WRR2
12
13         # Upstream Games (destination port(s); maybe protocol too?)
14         Classification.5. =
15             ClassificationEnable = true
16             ClassificationOrder = 5
17             ClassInterface = "LAN"
18             Protocol = 17 # UDP
19             DestPort = $GAME_PORT
20             ClassQueue = 4 # WRR2
21
22         # Downstream VAS traffic (IP SA)
23         Classification.6. =
24             ClassificationEnable = true
25             ClassificationOrder = 6
26             ClassInterface = "WAN"
27             SourceIP = $VAS_SOURCE_IP
28             DSCPMark = 0x28 # VO
29             ClassQueue = 1 # SP1
30
31         # could also define classifier for Transit traffic identified by IP SA,
32         # DHCP option or other classifiers
33
34         # Downstream Best Effort traffic (ingress port)
35         Classification.7. =
36             ClassificationEnable = true
37             ClassificationOrder = 7
38             ClassInterface = "WAN"
39             DSCPMark = 0x08 # EE
40             ClassQueue = 4 # WRR2
```

## 1 **8 HGI Release 2**

2 This document does not conclude the work of the HGI. Release 1 defines the set of  
3 requirements needed to support services, networks and devices that have already been deployed  
4 or that will be deployed by 2007. However both services and technology continue to evolve and  
5 emerging technologies and related business opportunities need to be taken into consideration to  
6 understand their impact on the Home Gateway architecture and functionalities. Further service-  
7 driven requirements are being considered for a Release 2 Document. This will build on, and be fully  
8 backward compatible with, the Release 1 requirements.

## 9 References

- 1 [1] DSL Forum TR-069 "CPE WAN Management Protocol"
- 2 [2] DSL Forum TR-111 "Applying TR-069 to Remote Management of Home Networking
- 3 Device"
- 4 [3] DSL Forum TR-062 "Auto-Config for the Connection Between the DSL Broadband
- 5 Network Termination (B-NT) and the Network using ATM (TR-037 update)"
- 6 [4] ATM Forum ILMI 4.0, [http://www.mfaforum.org/ftp/pub/approved-specs/af-ilmi-](http://www.mfaforum.org/ftp/pub/approved-specs/af-ilmi-0065.000.pdf)
- 7 [0065.000.pdf](http://www.mfaforum.org/ftp/pub/approved-specs/af-ilmi-0065.000.pdf)
- 8 [5] <http://standards.ieee.org/getieee802/>
- 9 [6] [http://www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php)
- 10 [7] ITU-T H.610 "Full services VDSL – System architecture and customer premises
- 11 equipment"
- 12 [8] RFC 4122 (UUID URN Namespace) <http://www.ietf.org/rfc/rfc4122.txt>
- 13 [9] RFC 2131 (DHCP) <http://www.ietf.org/rfc/rfc2131.txt>
- 14 [10] UPnP Device Architecture 1.1; <http://www.upnp.org>
- 15 [11] RFC 826 (ARP) <http://www.ietf.org/rfc/rfc826.txt>
- 16 [12] RFC 2132 (DHCP Options and BOOTP vendor extensions)
- 17 <http://www.ietf.org/rfc/rfc2132.txt>
- 18 [13] RFC 3925 (V-I Vendor Options for DHCPv4) <http://www.ietf.org/rfc/rfc3925.txt>
- 19 [14] IANA Private Enterprise Numbers registry. <http://www.iana.org>
- 20 [15] DSL Forum TR-106 "Data Model template for TR-069 enabled devices"
- 21 <http://www.upnp.org>
- 22 [16] RFC 3004 (User Class option). <http://www.ietf.org/rfc/rfc3004.txt>
- 23 [17] Organizationally Unique Identifiers (OUIs), <http://standards.ieee.org/faqs/OUI.html>
- 24 [18] ITU-T Recommendation G.992.1 (1999) – Asymmetrical Digital Subscriber Line (ADSL)
- 25 Transceivers
- 26 [19] ITU-T Recommendation G.992.3 (2002) - Asymmetric Digital Subscriber Line (ADSL)
- 27 transceivers -2 (ADSL2)
- 28 [20] ITU-T Recommendation G.992.5 (2003), Asymmetric Digital Subscriber Line (ADSL)
- 29 transceivers– Extended Bandwidth ADSL2 (ADSL2plus)
- 30 [21] ITU-T Recommendation G.994.1, 2004 - Handshake procedures for digital subscriber
- 31 line (DSL) transceivers
- 32 [22] ITU-T Recommendation G.993.2 (2005) - Very high speed digital subscriber line
- 33 transceivers 2 (VDSL2)
- 34 [23] ITU-T Recommendation I.361: "B-ISDN ATM Layer Specification"
- 35 [24] ITU-T Recommendation I.363.5: "B-ISDN ATM Adaptation Layer (AAL) Specification"
- 36 [25] ATM User-Network Interface (UNI) Specification Version 4.0, ATM Forum, July 1996.
- 37 [26] ITU-T Recommendation I.610 - Integrated Services Digital Network (ISDN): maintenance
- 38 principles. B-ISDN operation and maintenance principles and functions", March 1993
- 39 [27] IEEE Std 802.3ah-2004, Ethernet in the First Mile
- 40 [28] IEEE Std. 802.1Q-2003, Virtual Bridged Local Area Networks
- 41 [29]

- 1 [30] USB-IF: “Universal Serial Bus Specification: Revision 2.0”, 27/4/2000
- 2 [31] Bluetooth specification Version 2.0 + EDR
- 3 [32] IEEE 802.11b “Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications:  
4 Higher speed Physical Layer (PHY) extension in the 2.4 GHz band”
- 5 [33] IEEE 802.11g Part 11: “WLAN MAC and PHY specifications” Amendment 4: “Further  
6 Higher Data Rate Extensions in the 2.4 GHz band”
- 7 [34] ETSI EN 300 328-1/2 V1.6.1 “Electromagnetic compatibility and Radio spectrum Matters  
8 (ERM); Wideband transmission systems; Data transmission equipment operating in the  
9 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN  
10 covering essential requirements under article 3.2 of the R&TTE Directive”
- 11 [35] IEEE 802.11a Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)  
12 specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band
- 13 [36] IEEE 802.11h Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)  
14 specifications—Amendment 5: Spectrum and Transmit Power Management Extensions  
15 in the 5 GHz band in Europe
- 16 [37] DSL Forum, TR-064 “Base Requirements for an ADSL Modem with Routing”, Technical  
17 Report TR-068, May 2004
- 18 [38] Organizationally Unique Identifiers (OUIs), <http://standards.ieee.org/faqs/OUI.html>
- 19 [39] DSLForum, TR-111, “TR-069 to Remote Management of Home Networking Devices”,  
20 December 2005
- 21 [40] DSLForum, TR-106, “Data Model Template for TR-069 Enabled Devices”
- 22 [41] DSLForum, TR-098, “Gateway Device Version 1.1 Data Model for TR-069”
- 23 [42] RFC list: <http://rfc.net/rfc-index.html>
- 24 [43] IETF RFC 2663 IP Network Address Translator Terminology and Considerations
- 25 [44] IETF RFC 3022 Traditional IP Network Address Translator
- 26 [45] IETF RFC 3027 Protocol Complications with the IP Network Address Translator)
- 27 [46] ETSI TS 102 034 - Digital Video Broadcasting (DVB); Transport of MPEG-2 Based DVB  
28 Services over IP Based Networks
- 29 [47] Floyd, S., and Jacobson, V., Random Early Detection gateways for Congestion  
30 Avoidance. IEEE/ACM Transactions on Networking, Volume 1, Number 4, August 1993,  
31 pp. 397-413. )
- 32 [48] TR-106, Data Model Template for TR-069-Enabled Devices, DSL Forum Technical  
33 Report
- 34 [49] <http://www.dslforum.org/techwork/treports.shtml>
- 35 [50] CEA-2014 Web-based Protocol and Framework for Remote User Interface on UPnP  
36 Networks and the Internet (Web4CE); <http://www.ce.org>
- 37 [51] <http://www.iso.org>
- 38 [52] ITU-T Recommendation H.323 - Packet-based multimedia communications systems
- 39 [53] ITU-T Recommendation H.245 - Control protocol for multimedia communication
- 40 [54] ITU-T Recommendation H.225.0 - Call signalling protocols and media stream  
41 packetization for packet-based multimedia communication systems
- 42 [55] CISPR 22: Information technology equipment - Radio disturbance characteristics -  
43 Limits and methods of measurement

- 1 [56] CISPR 24: Information technology equipment - Immunity characteristics - Limits and  
2 methods of measurement
- 3 [57] IEC 60950-1: Information technology equipment – Safety – Part 1: General requirements
- 4 [58] IEC 60950-21: Information Technology equipment – Safety – Part 21: Remote  
5 feeding.
- 6 [59] IEC 61000-3-2: Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limits for  
7 harmonic current emissions (equipment input current <16 A per phase)
- 8 [60] IEC 61000-3-3: Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limitation  
9 of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems,  
10 for equipment with rated current < 16 A per phase and not subject to conditional  
11 connection
- 12 [61] IEC 61000-4-2: Electromagnetic compatibility (EMC) – Part 4: Testing and  
13 measurement techniques – section 2 - Electrostatic Discharge immunity test
- 14 [62] IEC 61000-4-3: Electromagnetic compatibility (EMC) – Part 4: Testing and  
15 measurement techniques – section 3 - Radiated EM field immunity test
- 16 [63] IEC 61000-4-4: Electromagnetic compatibility (EMC) – Part 4: Testing and  
17 measurement techniques – section 4 - Fast Transient/Burst immunity test
- 18 [64] IEC 61000-4-5: Electromagnetic compatibility (EMC) – Part 4: Testing and  
19 measurement techniques – section 5 - Surge immunity test
- 20 [65] IEC 61000-4-6: Electromagnetic compatibility (EMC) – Part 4: Testing and  
21 measurement techniques – section 6 - Conducted RF Disturbances immunity test
- 22 [66] IEC 61000-4-8: Electromagnetic compatibility (EMC) – Part 4: Testing and  
23 measurement techniques – section 8 - Power Frequency Magnetic Field immunity test
- 24 [67] IEC 61000-4-11: Electromagnetic compatibility (EMC) – Part 4: Testing and  
25 measurement techniques – section 11 - Voltage fluctuations immunity test
- 26 [68] IEC 60320-1 Appliance couplers for household and similar general purposes - Part 1:  
27 General requirements
- 28 [69] IEC 60083 Plugs and socket-outlets for domestic and similar general use standardized  
29 in member countries of IEC
- 30 [70] EN 50371: Generic standard to demonstrate the compliance of low power electronic  
31 and electrical apparatus with the basic restrictions related to human exposure to  
32 electromagnetic fields (10 MHz - 300 GHz) - General public
- 33 [71] EN 300 328: Electromagnetic compatibility and Radio spectrum Matters (ERM);  
34 Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz  
35 ISM band and using wide band modulation techniques; Harmonized EN covering  
36 essential requirements under article 3.2 of the R&TTE Directive
- 37 [72] EN 301 489-1: Electromagnetic compatibility and Radio spectrum Matters (ERM);  
38 ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1:  
39 Common technical requirements
- 40 [73] EN301 489-17: Electromagnetic compatibility and Radio spectrum Matters (ERM);  
41 ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17:  
42 Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high  
43 performance RLAN equipment
- 44 [74] EN 301 893 Broadband Radio Access Networks (BRAN); 5 GHz high performance  
45 RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE  
46 Directive

## 1 10 Acronyms

2	AAL	ATM Adaptation Layer
3	ACL	Access Control List
4	ACS	Auto-Configuration Server
5	ADSL	Asymmetric Digital Subscriber Line
6	ALG	Application Layer Gateway
7	ALL	Application Layer Logic
8	AP	Access Point
9	AN	Access Network
10	ATF	Architecture Task Force of HGI
11	ATM	Asynchronous Transfer Mode
12	ATA	Analogue Terminal Adapter
13	BG	Business Group of HGI
14	BRAS	Broadband Remote Access Server
15	BSP	Broadband Service Provider
16	BSS	Billing Support System
17	CAC	Call Admission Control
18	CBR	Constant Bit Rate
19	CFB	Call Forwarding on mobile customer Busy
20	CFU	Call Forwarding Unconditional
21	CFNR	Call Forwarding on No Reply
22	CLIP	Calling Line Identification Presentation
23	CoS	Class of Service
24	CPE	Customer Premises Equipment
25	CWMP	CPE WAN Management Protocol
26	DA	Destination Address
27	DECT	Digital Enhanced Cordless Telecommunications
28	DHCP	Dynamic Host Configuration Protocol
29	DMZ	De-Militarised Zone
30	DNS	Domain Name System
31	DS	Downstream
32	DSCP	Differentiated Services Code Point
33	DSL	Digital Subscriber Line
34	DVB	Digital Video Broadcasting
35	EAP	Extensible Authentication Protocol
36	ED	End Device
37	EDR	(Bluetooth) Extended Data Rate

1	ETH	Ethernet
2	FTTB	Fibre To The Building/Business
3	FTTCab	Fibre To The Cabinet
4	FTTH	Fibre to the Home
5	FXO	Foreign eXchange Office
6	FXS	Foreign eXchange Subscriber
7	HG	Home Gateway
8	HGI	Home Gateway Initiative
9	HGW	Home gateway Architecture and Security Group of HGI
10	HN	Home Network
11	HNA	Home Network Architecture Group of HGI
12	HomePNA	Home Phonenumber Networking Alliance
13	HTTP	Hypertext Transfer Protocol
14	ICSA	International Computer Security Association
15	IDS	Intrusion Detection System
16	IEEE	Institute of Electrical and Electronics Engineers
17	IGMP	Internet Group Management Protocol
18	ILMI	Interim Local Management Interface
19	IP	Internet Protocol
20	IPv4	Internet Protocol version 4
21	IPv6	Internet Protocol version 6
22	ISP	Internet Service Provider
23	ITU-T	International Telecommunication Union – Telecommunication
24		standardisation sector
25	LAN	Local Area Network
26	MAC	Media Access Control
27	MoCA	Multimedia over Coax Alliance
28	MPEG	Moving Picture Expert Group
29	NAPT	Network Address and Port Translator
30	NAT	Network Address Translator
31	NTP	Network Time Protocol
32	OSGi	Open Services Gateway Initiative
33	OAM	Operations, Administration & Maintenance
34	OSS	Operations Support System
35	PIN	Personal Identification Number
36	PLT	Power Line Transmission
37	POTS	Plain Old Telephone Service
38	PPP	Point-to-Point Protocol

1	PPPoA	PPP over ATM
2	PPPoE	PPP over Ethernet
3	PSTN	Public Switched Telephone Network
4	PVC	Permanent Virtual Connection
5	QoS	Quality of Service
6	RMS	Remote management System
7	RODM	Remote Operations and device management Group of HGI
8	SA	Source Address
9	SDO	Standard Development Organization
10	SOHO	Small Office Home Office
11	SNMP	Simple Network Management Protocol
12	SP	Service Provider
13	SSID	Service Set Identifier
14	STB	Set Top Box
15	UPnP	Universal Plug&Play
16	VAS	Value Added Service (in this context considered equivalent to Managed
17		Service, see section 11)
18	VCI	Virtual Channel Identifier
19	VDSL	Very high speed Digital Subscriber Line
20	VLAN	Virtual Local Area Network
21	VoD	Video on Demand
22	VoDSL	Voice-over Digital Subscriber Line
23	VoIP	Voice over IP
24	VP	Virtual Path
25	VPI	Virtual Path Identifier
26	VPN	Virtual Private Network
27	WAN	Wide Area Network
28	WEP	Wired Equivalent Privacy
29	WPA	Wireless Protected Access
30	WRR	Weighted Round Robin

## 11 Definitions

- **Access Point:** connection point where devices using the same link layer technology could be connected to the home network. It can be part of the Home Gateway or a separate box providing an integration point for non-common technologies.
- **Bridge:** link layer function connecting two or more HN segments sharing the same data link layer. For management purposes it may also have an IP address
- **Global usage scenario:** As the Home Gateway needs to support several usage scenarios at the same time, the “global usage scenario” describes a scenario where several “single” usage scenarios are happening at the same time.
  - Example Dual play: Television over broadband + Voice communication using an analogue phone.
- **Home Gateway:** device connecting the HN to the Internet and Service Platforms on the basis of one of the possible models described in Section 5.2
- **Hub:** physical layer function that repeats signals coming from one of its ports to all the other ports. Hubs have all the disadvantages expected from a shared medium.
- **LM Remote UI** (Local Management User Interface): UI to let a user manage the RM client on the gateway from a device on the HN
- **Managed Device:** device that has a remote management client that communicates directly or indirectly (via the Home Gateway) with a remote management server.
- **Managed service:** A managed service is a service for which the BSP provides preferential treatment (that can include QoS...) for the customer. The service can be a service offered by the BSP or operated by the BSP on behalf of a third party. A managed service can also be local: watching a video on a PC recorded on the IPTV STB; as explained in the IPTV PVR use case. Managed services does not necessarily involve use of the remote management system; management only means that the operator has taken some responsibility for the service (e.g. its QoS treatment) in order to provide the appropriate quality of experience.
- **Per class QoS management:** QoS treatment based on a service classes rather than individual flows.
- **Relative QoS:** This term is used to refer to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It is used to handle certain classes of traffic differently from other classes.
- **Router:** network layer function that connects two or more IP segments and re-distributes IP packets of one segment to another.
- **Unmanaged Device:** device that does not have a remote management client or that does not communicate directly or indirectly (via the Home Gateway) with a remote management server.
- **Use case:** Description of a general user need. It contains the context of usage behaviour that meets the need and serves as an umbrella scenario.
  - Example: Voice communication
- **Usage scenario:** The usage scenario is a real scenario demonstrating the use case.
  - Each scenario provides details about the user (attitude, knowledge, habits, etc.), the use context (social factors, environment, information requirements, etc.), and a solution that supports or enables the particular use.
  - Example: Voice communication using an analogue phone.

- 1
- 2
- **Unmanaged Service:** An unmanaged service is a service for which the BSP has no commitment to the customer (especially in terms of QoS).