ETSI TS 102 685 V1.1.1 (2010-01)

Technical Specification

Digital Video Broadcasting (DVB); High-level Technical Requirements for QoS for DVB Services in the Home Network

Reference
DTS/JTC-DVB-254

Keywords
DVB, QoS

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulatory bodies, content owners and others committed to designing global standards for the delivery of digital television and data services. DVB fosters market driven solutions that meet the needs and economic circumstances of broadcast industry stakeholders and consumers. DVB standards cover all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. The consortium came together in 1993 to provide global standardisation, interoperability and future proof specifications.

Introduction

As IPTV systems are deployed, improvements in the technologies used for home networking result in users expecting to be able to distribute their incoming TV services within the home environment, while that network is also carrying a range of other traffic. There might therefore be contention for resources and variations in the ability to transfer any specific stream of data reliably and consistently. The impact of timing variations and reduced resource availability frequently has the effect of reducing the presented quality of audiovisual media. We can express end users' perspective of the Quality of Experience (QoE) as a measure of how well the combination of networks and services is satisfying their requirements.

QoE involves not only the transport behaviour but also the end-to-end connection and the applications that are currently running over that connection. For attracting and satisfying customers the service provider takes care of the Quality of Service (QoS) in order to keep the QoE as high as possible. QoS deals with the actual network operating conditions. The available tools are used to classify service components and media in terms of quality, to monitor the continuity of service levels, to evaluate aberrations, to control service and media flows as well as to provide information on quality related aspects to devices concerned.

Currently, the state of the art relies on classifying packets on a per-stream basis and prioritizing one stream type over another. This has the effect of ensuring that high-priority packets get through at the expense of lower priority stream types (although this prioritization might not match the end-user's view of relative importance of a particular service) and all streams of a particular type might be impacted if the aggregate network demand exceeds capacity. Ultimately, this could well mean that the requisite QoS is not delivered in accordance with the requirements and contractual obligations of the service provider.

The requirements collected in the present document focus on the quality aspects of home networks while taking into account the end-to-end delivery of a service from the access network through the home network gateway device up to the client device. Nevertheless, these requirements may also influence networks and devices outside the home network. Additionally, the services delivered in the home network may include both DVB and non-DVB services. As their simultaneous usage may affect the performance of each other, the QoS mechanisms to be developed should also consider delivering an appropriate service quality to DVB services in the presence of non-DVB services, and to non DVB services in the presence of DVB services.

For these reasons, in the present document we establish a new framework for a higher order of QoS management within the home network and introduce some approaches for supporting that management in an attempt to move beyond current approaches to QoS. We have covered a number of technical requirements for such a system and are issuing the document to solicit responses with technologies to meet the requirements so that a formal specification can be developed for a better Home Network QoS mechanism.

This framework should enable home networks to develop where the QoS system can attempt to maintain the QoE within the HN.

1 Scope

The present document presents the high-level QoS requirements for the Home Network (HN) for the carriage of DVB services. DVB believes that, without further action, home networks will not provide the level of QoS required to deliver IPTV services to users reliably, and therefore, there is a need for developing a QoS mechanism that will improve the reliability of delivery of (streamed) content through the HN as much as possible. In the present document an agreed set of high-level technical requirements for QoS is defined that can be used as input to the relevant technical groups and organizations for the development of such QoS mechanisms.

Although this work has been done within DVB, primarily with the DVB Home Network in mind, it is applicable to any IP-based home network.

The DVB QoS requirements will address especially the situation where the home network is bit rate constrained and may be operating close to its maximum capacity, meaning that the addition of further loading can adversely affect all the services flowing through the HN. The ability to manage the services within the HN is essential to give service providers confidence that subscription and premium content will be correctly delivered to the user through the HN.

Furthermore, since DVB expects that more advanced QoS capabilities will be required for the reliable carriage of future DVB services across home networks, it is important to determine the QoS requirements now. However, the solution developed must allow a progressive evolution with backward compatibility with current QoS methods and practices and forward compatibility to the full QoS specification derived from the requirements of the present document.

DVB assumes that other standards bodies such as DLNA, HGI and DSLF will provide the QoS solution. Therefore, DVB will contribute the present document towards DLNA and other Standards Development Organizations (SDOs) and consortia in order to contribute to the process leading to a satisfactory QoS solution for the carriage of DVB service to and within the home.

In principle the DVB QoS requirements will only take into account the HN i.e. QoS requirements for the Access Network (AN) are out of scope, because there is a diverse variety of AN types and each AN or service provider has its own (proprietary) implementation. Furthermore, the AN is currently considered as being professionally managed, while it is likely that this may not be true for the HN. In this sense the QoS requirements for the HN are considered to be more important than for the AN. Therefore, the focus of the present document will be on the development of technical QoS requirements for the HN but where necessary the AN will be taken into account, to achieve a seamless transition for DVB content services from the AN into the HN.

The foundation for the high-level QoS requirements is formed by:

- A number of use cases identified for defining the QoS requirements.
- The DVB commercial requirements for the HN.
- The work done in the DVB HN work on reference model.

In an effort to maintain alignment as far as possible with DLNA the work of the DLNA CSPR QoS "Tiger Team" has been reviewed. It is recognized that the QoS management described in the present document attempts to go further than the work currently proposed in DLNA.

From these inputs a logical reference model for the extended QoS solution is derived as a framework for the technical QoS requirements described in this present document.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

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

2.1 Normative references

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

[1] ETSI TS 102 034: "Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks".

[2] ETSI TS 102 539: "Digital Video Broadcasting (DVB); Carriage of Broadband Content Guide (BCG) information over Internet Protocol (IP)".

[3] DVB BlueBook A144 (November 2009): "DVB-HN Commercial Requirements Phase 1".

[4] DLNA-1006 (October 2006): "Networked Device Interoperability Guidelines - Expanded - Volume 1: Architectures and Protocols".

NOTE: Available at: http://www.dlna.org/industry/certification/guidelines/.

[5] ETSI TS 102 824: "Digital Video Broadcasting (DVB); Remote Management and Firmware Update System for DVB IP Services".

[6] Home Gateway Initiative (HGI) (April 2008): "Home Gateway Technical Requirements: Residential Profile, Version 1.0".

[7] UPnP Forum (March 2005): "UPnP™ QoS Architecture: 1.0".

[8] UPnP Forum (October 2006): "UPnP™ QoS Architecture: 2".

[9] IEEE 802.11 (2007): "Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area network - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".

NOTE: This document reflects the combining of the 2003 Edition of 802.11 plus the 802.11g, 802.11h, 802.11i and 802.11j Amendments) (Revision of IEEE Std 802.11-1999).

[10] IEEE 802.1d (2004): "IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] DLNA (12 March 2008): "Digital Living Network Alliance Functional Requirements for Service Assurance".

NOTE: This document is available to DLNA members and under the DVB-DLNA liaison agreement.

[i.2] UPnP Forum (June 2008): "UPnP™ QoS Architecture: 3, Proposed DCP".

3 Definitions and abbreviations

3.1 Definitions

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

admission control: mechanism that responds to application requests to set-up data flows within the HN i.e. permitting or denying requests depending on resource availability for the requested flow

***dynamic config*uration:** set of parameters for configuring the QoS-aware HN devices and setting-up the content flows through the HN

NOTE: The Flow Manager sets the parameters of Dynamic *Config*uration.

flow manager: entity within the HN that makes the admission control and resource allocation decisions based on QoS policy and QoS system metrics

importance: semantic concept indicating the relative importance of the content in relation to other content flowing over the HN

***monitor*:** metrics and mechanism used by a device through which the content flows to provide a measure of the requirements of a streamed service to the QoS system

opt-in: mode of operation whereby some of the HN QoS is managed by a service provider

NOTE 1: Additionally, the user may request/agree that the service provider manages some or all of the QoS aspects of the rest of the HN. It does not preclude some local management by the user, subject to limitations agreed with the service provider.

NOTE 2: Usually, this would include management of all segments traversed by the managed service and may necessarily include others.

opt-out: mode of QoS operation whereby the HN is locally managed entirely by the user

***packet processing*:** methods which a device through which the content flows can use to modify a streamed service to optimise the QoS within the HN

***policy*:** aggregation of rules, methods and values that determines how the decisions about admitting services and resources will be made by the Flow Manager

NOTE: This is also referred to as QoS Policy.

pre-emptability: semantic concept indicating whether the content can be pre-emptively terminated or adjusted to free resource for content with a higher importance

Quality of Service (QoS): measure of how well the delivery requirements of the content in question (in terms of timeliness, error rate, reliability, etc.) are fulfilled

static configuration: set of parameters which contains some information about the topology of the HN and QoS configuration, such as queue allocation

status: set of metrics which contains some information about the actual topology and network usage of the HN

3.2 Abbreviations

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

AN	Access Network
AV	Audiovisual
AVC	Advanced Video Coding
BE	Best Effort
CBR	Constant Bit Rate
CSPR	Content Service Provider Requirements
DLNA	Digital Living Network Alliance
DSCP	Differentiated Services Code Point
DSLF	DSL Forum
DVB	Digital Video Broadcast
DVB HN	DVB Home Network
DVB SI	DVB Service Information
DVB-C/S/T	DVB Cable/Satellite/Terrestrial

NOTE: Generally used as a term to describe broadcast DVB service delivery.

EPG	Electronic Program Guide
FTA	Free-To-Air
FUS	Firmware Update System
GUI	Graphical User Interface
HD	High Definition
HGI	Home Gateway Initiative
HN	Home Network
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPTV	Internet Protocol TV
QoE	Quality of Experience
QoS	Quality of Service
RMS	Remote Management System
SD	Standard Definition
SD&S	Service Discovery and Selection
SDO	Standards Development Organization
SVC	Scalable Video Coding
UPnP	Universal Plug and Play
VBR	Variable Bit Rate
VoD	Video on Demand

4 Input QoS Related Requirements

The QoS related requirements from the DVB commercial group CM639R2 DVB-HN [3] are included in annex C, and those relevant to DVB HN have been used as the initial inputs to the present document.

5 DVB Home Network Reference Model

5.1 Introduction

For the purpose of the present document, this clause presents the aspects of the DVB HN reference model that are relevant to the development of the QoS concepts introduced in the present document. The DVB HN reference model is an abstract framework for understanding the significant entities and relationships amongst them within a DVB HN. In this present document the model is used for the development of a consistent set of QoS technical requirements.

The DVB HN reference model is a logical one which explicitly avoids defining implementation details, as doing so would unnecessarily constrain the possible QoS solutions.

5.2 Network Topology

Audiovisual (AV) content and other data (services) can be delivered between entities within the HN or delivered and distributed into the HN from either a broadband or broadcast AN.

The HN is defined as an IP packet based network that has the characteristics that each connected entity can unicast, multicast or broadcast IP-compliant packets between connected HN entities. The DVB HN uses a single IP subnet, in which different network segments may use either wired (100Base-TX/GigabitE) Ethernet or wireless IEEE 802.11 [9]to interconnect the identified HN entities. Network segments using different physical layers may have different behaviour and requirements in terms of QoS. The DVB-QoS system should not be restricted to these network technologies.

Furthermore, the Home Network (HN) can be connected simultaneously to multiple different types of Access Networks (ANs).

The following essential DVB HN access networks and DVB devices are defined:

- Broadband Network: is an external bi-directional AN that can be used to send and receive services from remote entities such as servers. The main assumption put on a bi-directional AN is that it can carry services (content, metadata and signalling) either upstream or downstream between the AN service provider and the HN. One restriction imposed is that a maximum of one broadband AN connection may be active at any time.

- Broadcast Network: is an external unidirectional AN that delivers content to the HN via a unidirectional gateway (DVB-Unidirectional Gateway Device) only. It may be necessary to translate the services delivered from the AN into a protocol and format appropriate for the HN.

- DVB Bi-directional Gateway Device: is the AN gateway used to enable the HN devices to access streamed, VoD or downloaded content and associated metadata and signalling delivered over a bi-directional packet-based broadband network. The DVB-Bi-directional Gateway Device may provide the necessary protocol and format conversions for translating the AN packets into the IP packet structure appropriate to the HN. Although the requirements are developed for managed networks the DVB-Bi-directional Gateway Device may also allow access to the open internet if the service provider or network operator allows.

- DVB-Unidirectional Gateway Device: is the AN gateway used to enable the HN devices to receive streamed or downloaded content, associated metadata and signalling delivered over an unidirectional broadcast network e.g. DVB-C/S/T-compliant broadcast network. The DVB-Unidirectional Gateway Device provides interconnection between one or more unidirectional ANs and the HN. The DVB-Unidirectional Gateway Device is a combination of one or more tuners or other AN terminating devices and a DVB Digital Media Server.

- DVB Digital Media Renderer: used to consume content coming from a DVB Digital Media Server. Each DVB Digital Media Renderer has a single connection with the HN.

- DVB Digital Media Server: used to expose and distribute content throughout the HN. The DVB Digital Media Server has one connection with the HN. It is capable of exposing the metadata describing the content for the DVB Digital Media Controllers.

- DVB Digital Media Controller: used to set up, manage and tear down connections between HN devices. It has one or more connections with the HN.

NOTE 1: Any example of an HN may include any combination of the devices and service delivery options described above.

NOTE 2: In the case where the HN is connected to a unidirectional delivery system, an alternative, out-of-band return path may be used for remote management system access.

6 Generic Use Cases

A service may flow over several segments of the HN subnet between server and client and the characteristics of each segment may be different. Also, the content may be carried through one or more network infrastructure devices, e.g. switches, bridges and wireless access points, which might not be DVB QoS aware. This clause describes the types of triggering changes and required responses which we need to consider as part of the extended QoS solution in general terms.

6.1 Triggering Events

Several use cases have been analysed but the general conclusion is that all the use cases where any problems occur are based on the available bit rate being heavily loaded (approaching saturation), or about to become overloaded. This is commonly referred to as the "N+1 case" where the value of "N" (number of services flowing without problem through a network segment) will depend on the bitrate (fixed or variable) needed for each service and the total available bitrate on the network segments. Furthermore, with some network physical layers the total available bitrate may not be constant due to physical layer characteristics or unmanaged streams flowing through some segments. This requires a dynamic management strategy at least for those segments.

The main types of changes that may occur on any network segment across which services are to be delivered and which must be considered in terms of QoS are listed below.

All use cases are based on one of the following changes in conditions:

- A new stream with QoS requirements is requested.
- A new stream with no QoS requirements is requested.
- An existing stream with QoS requirements changes its requirements e.g. due to trick mode operation.
- A running service with QoS requirements stops.
- A running service with no QoS requirements stops.
- The network resource/capacity of a network segment changes.

NOTE: Streams with no QoS requirements will be treated in a "best effort" manner, i.e. they are forwarded without any delivery guarantees.

6.2 Importance and Pre-emptability of Services

In a congested network where there is insufficient resource available to carry newly requested flows, it may be possible to reconfigure existing services that are competing for the same resource. Furthermore, if the network performance changes dynamically in some segments or existing flows exceed their allocated resource and a segment becomes overloaded, then the same methods may be used to reduce the demand on the overloaded segments.

A method is therefore required for determining which services can and/or should be adjusted and/or terminated to make sufficient resource available in the segments that are either unable to carry the extra load or becoming overloaded.

We have defined two semantic concepts for this purpose:

- The first is an arbitrary evaluation of the relative Importance of services. In this case, the Service Provider and user provide some indication of the value of that service in relation to others - perhaps on the basis of some elements of the policy. This allows an evaluation as to which services are regarded as having less value and are therefore first candidates for pre-emption.

- The other concept is a description of whether the service can be asked to reduce its resource demand or stop altogether. We refer to this as Pre-emptability.

The QoS system will use these semantic concepts (which will be represented by parameters) to decide whether a new service can be admitted or not and will then use them for allocating, rescaling, downgrading and/or de-allocating resources accordingly. There is a balancing act to be performed - for example, it may be better to scale down some more important service rather than stop a less important one. This decision process may be driven by the policy or be a feature of a particular implementation.

6.3 Possible QoS management options

Table 1 presents an overview of the possible triggering events and related QoS decisions that can be taken. The decisions will be based on the QoS policy and the relative importance and pre-emptability of the services in question.

Table 1: Triggering Events versus Possible QoS Decisions

Triggering Event	Possible QoS Decision
• A new service is requested. • An existing service requests more resources e.g. due to trick mode operation.	1) Reject request. 2) Accept request with no changes. 3) Pre-emptively terminate one or more existing services and accept request. 4) Pre-emptively scale down one or more existing services and accept request. 5) Scale down the requested service and accept request. 6) Pre-emptively downgrade one or more existing services and accept request. 7) Downgrade the requested service and accept request e.g. accept the request as best effort traffic. 8) A combination of 3 to 7.
• A network resource stops. • A network resource decreases.	9) Stop one or more existing services. 10) Scale down one or more existing services. 11) Downgrade one or more existing services. 12) A combination of 9 to 11
• A service stops. • A service decreases its resource requirements. • A network resource is added. • A network resource increases its capacity.	13) Restore one or more previously affected services due to QoS decisions 3 to 8 or 9 to 12.
NOTE 1: The QoS system may be able to enforce the QoS decisions automatically or only after confirmation by the user. This will be implementation dependent within the controlling application. NOTE 2: The QoS system may notify the service provider (i.e. remote management system) and/or user when a change due to a QoS decision has been executed.	

The ability of the QoS system to adjust existing services in QoS decision options 9 to 11 of table 1 may not be restricted by the "pre-emptability" attribute, although the system would typically target services marked in this way first. For example, where a wireless segment reduces bandwidth such that it is unable to support all the services carried on it, the QoS system would typically terminate or reduce the demand of low importance, pre-emptable services first, then more important services, until it could accommodate the combined bandwidth demand. However, if that did not prove sufficient, it might terminate one or more non-pre-emptable services until it can accommodate the remaining bandwidth demand. This termination might have to be performed using other means than those used for terminating pre-emptable services, such as policing its traffic down to zero, breaking connections, etc.

The following clause will present a functional reference model for a QoS system that can execute the aforementioned QoS decisions and actions.

7 QoS functional reference Model

This functional reference model serves to define nomenclature, and to provide a framework within which use cases can be analysed and from which technical requirements can be derived. The model is based on a set of logical entities, repositories and interfaces generically referred to as components.

Figure 1 gives an overview of the HN QoS functional reference model. In the text throughout the remainder of the present document italicized terms refer to the components shown in figure 1. The following bullet list describes the characteristics of the components of the model.

- A single flow with or without QoS requirements is shown and is identified as Content. The Content Source can be either outside or inside the HN. In the case of an internally generated flow e.g. from a network server playing back content from a local storage, the content ingress flow to Device #1 will be null.
- The first device within the HN is Device #1. The Content then flows over one or more network segments and through zero or more intermediate devices constituting the HN before reaching the final device (Device #n).
- It is assumed that a Device entity is also a physical device in practice. Therefore, the QoS functional reference model is not entirely a logical model.
- In general, a mix of flows with and without QoS requirements will stream simultaneously over the HN.
- All Device entities are modelled in the same way, with *Packet Processing* and *Monitor* entities. However, this does not mean that all devices have the same, or indeed any, QoS capabilities.
- A given packet's treatment by a given Device is determined by the packet itself and by the QoS configuration. This configuration is split into *Static Config* and *Dynamic Config* repository.
- A *Flow Manager* entity has access to the *Policy*, *Static Config*, *Dynamic Config* and *Status* repositories via which it is able to discover information about the current network topology and via which it monitors the usage of HN resources for each part of the network (devices and network segments). The *Flow Manager* uses the policy stored in the *Policy* repository to make admission control and resource allocation decisions to fulfil as far as possible the QoS requirements of services running over the HN.
- The *Flow Manager* entity can monitor the Status repository, adjusting the *Dynamic Config* repository as appropriate in response to changes in network performance and load of the HN.
- Arbitration over changes to the *Policy* and Static *Config* repositories will be carried out by the respective Polic *Arbiter* and *Config Arbiter* entities.
- If allowed, various *Applications* within the HN can change the *Policy* repository via the *Local Policy* interface and *Policy Arbiter* entity, change the *Config* repository via the *Local Config* interface and *Config Arbiter* entity, make flow requests, and monitor the *Status* repository.
- In a system where the QoS management is to be configured by an RMS (e.g. DVB RMS) those external agencies will be able to change the *Policy* and Static *Config* repositories via the *Remote Policy* and *Remote Config* interfaces respectively.

The following clauses describe the components, (repositories, entities and interfaces) which make up the QoS functional reference model and the relationship between them.

The *Packet Processing* and *Monitor* entities are shown as directly related to the physical devices through which content flows. All other components are not directly associated with any specific physical devices.

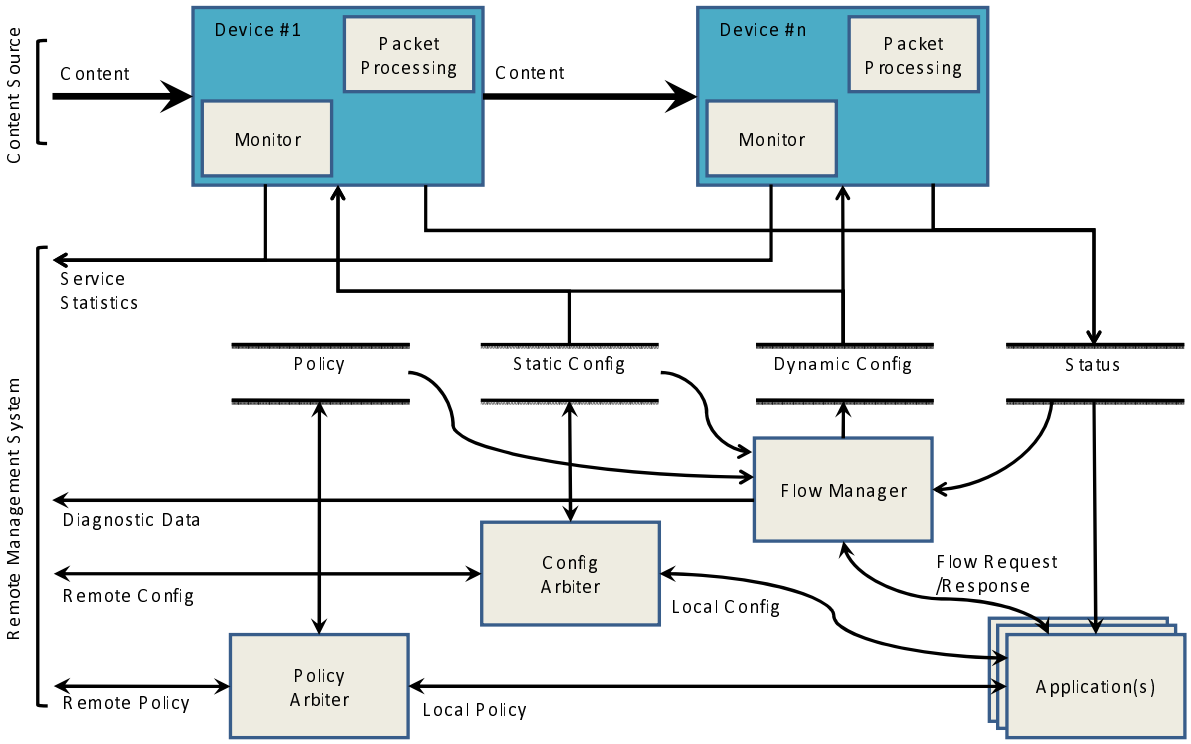


Figure 1: Home Network QoS Functional Reference Model

7.1 Repositories

The repositories are represented as data sets containing status and configuration information for devices, the HN and flows. These are logical repositories which in practice can be distributed across multiple devices in the HN. The technical requirements in clause 10 provide more detail on what type of information is stored in each repository.

7.1.1 Status Repository

The *Status* repository holds all the details of current flows, link utilization, policing statistics, queue occupancy, etc. for each single device and as an aggregation of the information from each device within the HN.

7.1.2 QoS Config and Policy Repositories

The QoS configuration is made up of settings that describe services and determine how individual packets will be treated (classification, marking, policing, queuing, etc.). The QoS configuration is split into *Static Config*, *Dynamic Config* and *Policy* repositories.

7.1.2.1 Static Config Repository

The *Static Config* repository is the QoS configuration defined by the user and the service provider. The *Static Config* repository is expected to be non-volatile.

7.1.2.2 Dynamic Config Repository

The *Dynamic Config* repository is a volatile data set which is written only by the *Flow Manager* and subsequently used by devices.

The *Dynamic Config* repository contains information that persists only for the lifetime of a flow, e.g. it may contain temporary QoS flow recognition rules set by the *Flow Manager*.

As a general rule the *Dynamic Config* will take precedence over the *Static Config* if any conflict exists.

7.1.2.3 Policy Repository

The *Policy* repository is a non-volatile data set which is written by the *Policy Arbiter*, and is read by the *Flow Manager* and, if necessary by *Applications*.

The *Policy* repository holds the set of criteria which will be used by the *Flow Manager* to interpret the characteristics of existing and requested flows in order to make admission control, flow modification and/or resource allocation decisions. There will be a single active policy for the HN.

7.2 Entities

7.2.1 Packet Processing Entity

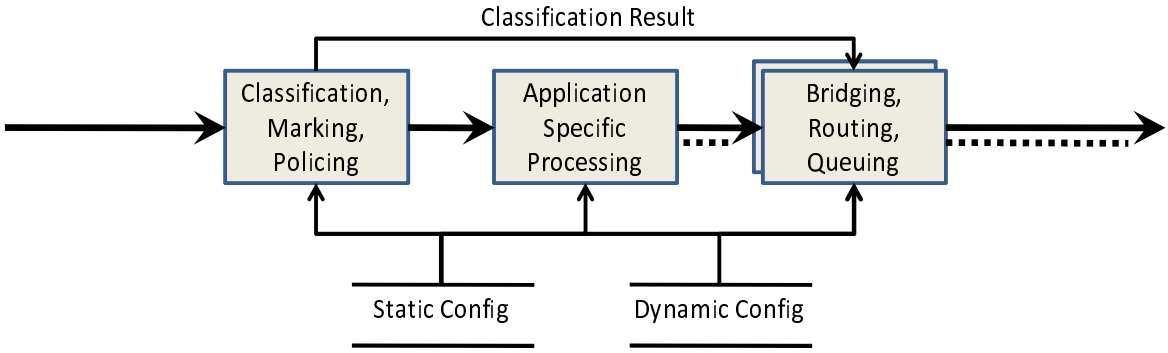
The *Packet Processing* entity is part of each device. It is assumed that the packets flowing into the *Packet Processing* entity are IP packets. If not, it is assumed that an initial processing stage (not shown) will produce IP packets.

Figure 2 shows the functions of the *Packet Processing* entity:

- Classification, Marking, Policing.
- Application Specific Processing.
- Bridging, Routing, Queuing.

Not all functions need to be implemented e.g. for a bridge the routing operation is null.

Application Specific Processing function includes such functionality as replication e.g. conversion of multicast to unicast.



NOTE: The dotted lines represent potential multiple streams resulting from multicast to unicast conversion or other forms of replication.

Figure 2: Device QoS Packet Processing

7.2.2 Monitor Entity

The *Monitor* Entity that is part of a Device collects Service Statistics information about the Content flow. This information can be fed back to the RMS for diagnostics and service monitoring.

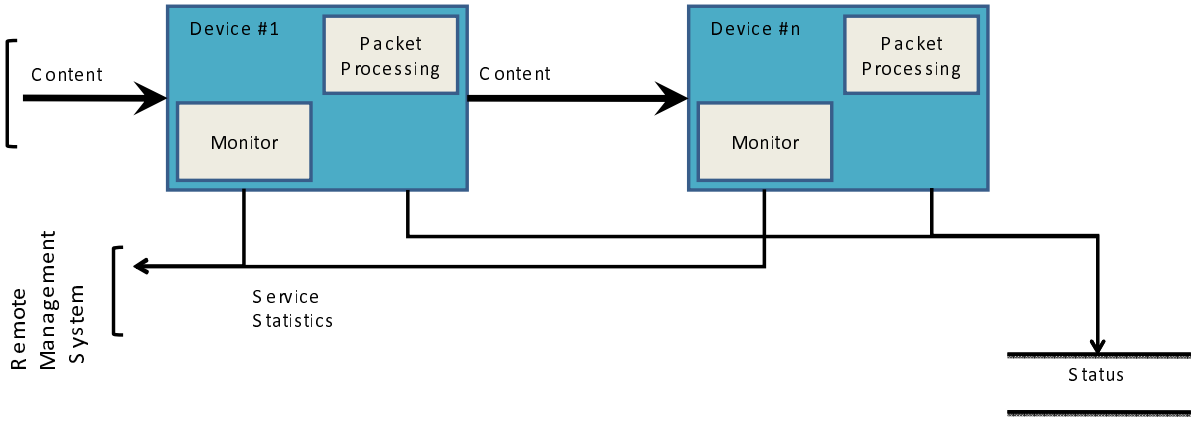


Figure 3: Context of Device Monitor Entity

7.2.3 Flow Manager Entity

The *Flow Manager* entity plays two crucial roles:

- Receiving flow requests from *Applications* and trying to manage the content flows accordingly in such a way that the QoS requirements of services are fulfilled as far as possible.
- Reacting to changes in the network and/or current content flows to maintain the QoE.

In order to do this:

- The *Flow Manager* uses information about current network performance, resource usage and content flows through the DVB HN from the *Status* repository and reacts to correct problems when necessary.
- The *Flow Manager* is able to discover information about the current network topology from the *Static Config* repository and *Status* repository (using such methods as automatic topology discovery) as one of the decision criteria for the changes to the flows and network configuration.
- The *Flow Manager* applies the rules in the *Policy* repository for content flow resource management and admission control.
- The *Flow Manager* responds to an application issuing a request for a new flow indicating whether the request is admitted, denied or admitted in a modified form.
- The information in the *Dynamic Status* repository will be updated as a result of the logical decisions made about content flow management.
- Any changes to content flows required by the *Flow Manager* are communicated back to the Application controlling that flow.
- The *Flow Manager* is able to supply diagnostic information to the remote management service over the Diagnostic Data interface.

Figure 4 shows the context of the *Flow Manager* entity.

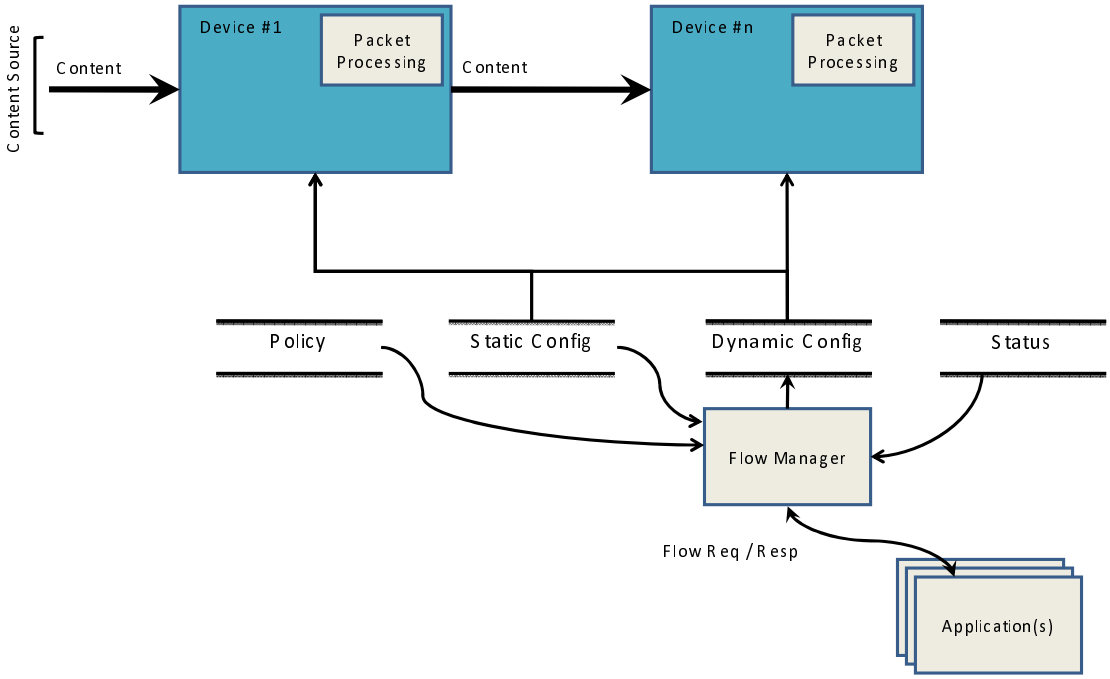


Figure 4: Context of Flow Manager Entity

Figure 5 illustrates the operation of the *Flow Manager* entity in terms of the inputs and outputs. The input data to the *Flow Manager* entity is made up of a combination of:

- In the case of an *Application* requesting a change in the overall flows a Flow Request carries the request for change (new or modified flow) and metadata from an *Application*.
- *Static Config* repository may hold some or all topology information about HN Devices and connectivity for devices which cannot provide the information dynamically (e.g. on connection to the network or a boot time), and QoS system defaults. This effectively "bounds" the decision process.
- *Status* repository holds information about current network usage and HN device topology from the devices which can provide it dynamically, queue occupancy, etc.
- *Policy* repository holds information about how ordering should be done based on metadata and properties of existing flows.

Using these input data sets the *Flow Manager* entity can make the admission control decisions and set the system parameter values for the *Packet Processing* entity.

Output from the flow management process:

- *Dynamic Config* repository will be populated with parameters to set and control *Packet Processing* in each Device.
- Several flows and devices may need to change configuration if common network segments are involved where contention has been introduced by increased flow requirements.
- Flow Response carries update information to the *Application*, e.g. success, failure, message to be displayed for user.

Using these parameter values the *Packet Processing* in each Device can be reconfigured accordingly.

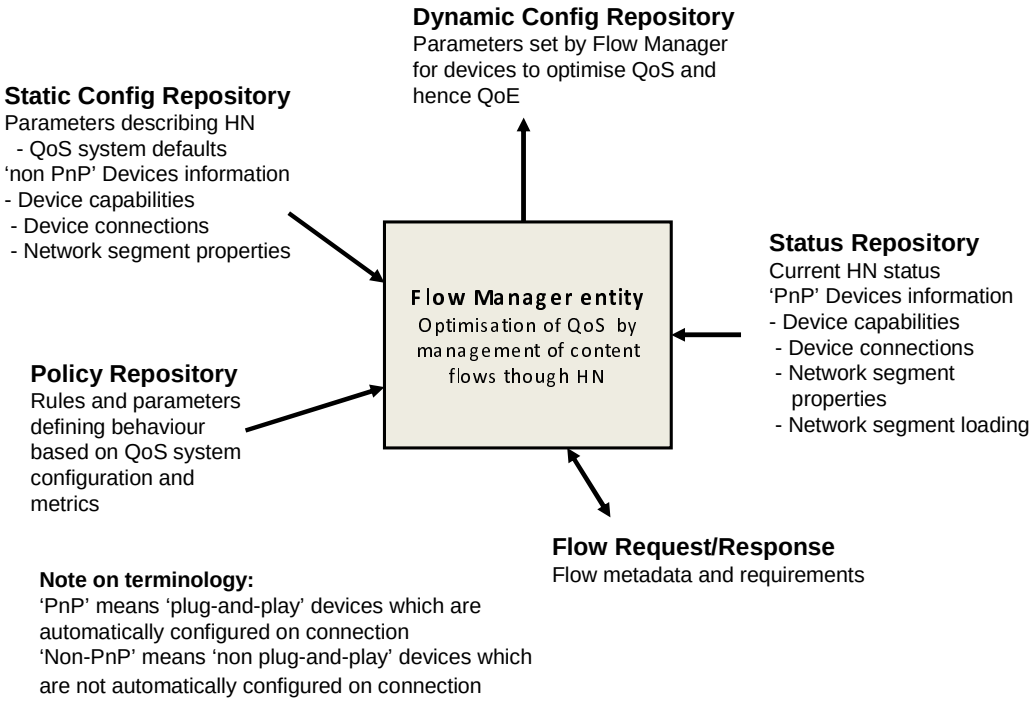


Figure 5: Operation of Flow Manager Entity

7.2.4 Policy Arbiter Entity

The *Policy Arbiter* entity is the logical process by which the criteria of the *Policy* are set.

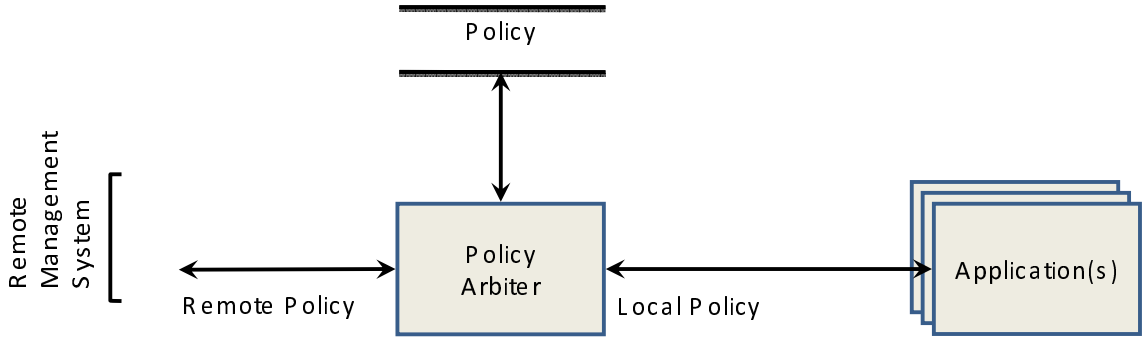


Figure 6: Context of *Policy Arbiter* Entity

The QoS policy can either be based on "Opt-in" where the service provider will take precedence in setting the policy or "Opt-out" where the user will set the policy using an Application. Where the DVB HN uses an "Opt-in" policy there may be some policy parameters which the user is allowed to control.

The user and service provider supply policy via the *Local Policy* and *Remote Policy* interfaces respectively. Figure 6 shows the context of the *Policy Arbiter* entity.

7.2.5 *Config* Arbiter Entity

The *Config Arbiter* entity is a logical process which merges the *Local Config* information that is provided using an Application, and that provided by a remote management service over the interface. The *Remote Config* will take precedence if the QoS system is operating in the "Opt-in" mode. Figure 7 shows the context of the *Config Arbiter*.

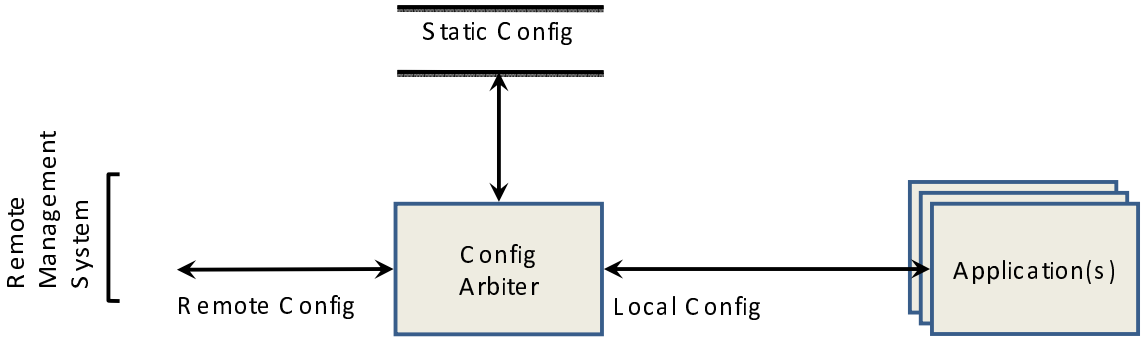


Figure 7: Context of *Config Arbiter* Entity

7.2.6 Applications

The *Applications* are generally out of scope of the specification, although a standardized interface to the other entities and repositories is needed to allow the *Applications* to be interoperable with the other parts of the QoS system.

Applications will communicate primarily with the *Flow Manager*, but may also read the *Status* repository to get information about the current HN usage directly. It is assumed that an Application will remain active during the lifetime of the service(s) initiated by that Application.

Applications interact with the QoS system to:

- Request the *Flow Manager* to allow another content flow through the HN.
- Request the *Flow Manager* to adjust the HN to accommodate changes in the existing content flows, e.g. for trick mode operation.
- Receive requests from the *Flow Manager* to terminate or change the characteristics of a content flow. Subsequently, the Application should instruct the content source accordingly.
- *Monitor* and report HN functions using the data in the *Status* repository for diagnostics.
- Act as a method of providing information or feedback to the user when changes are taking place, either triggered by a request or by a change in HN delivery capability.
- Provide a mechanism allowing the user to manage the behaviour of the QoS system through the *Policy* and *Static Config* using the "*Local Policy*" and "*Local Config*".

Figure 8 shows the context of Application(s).

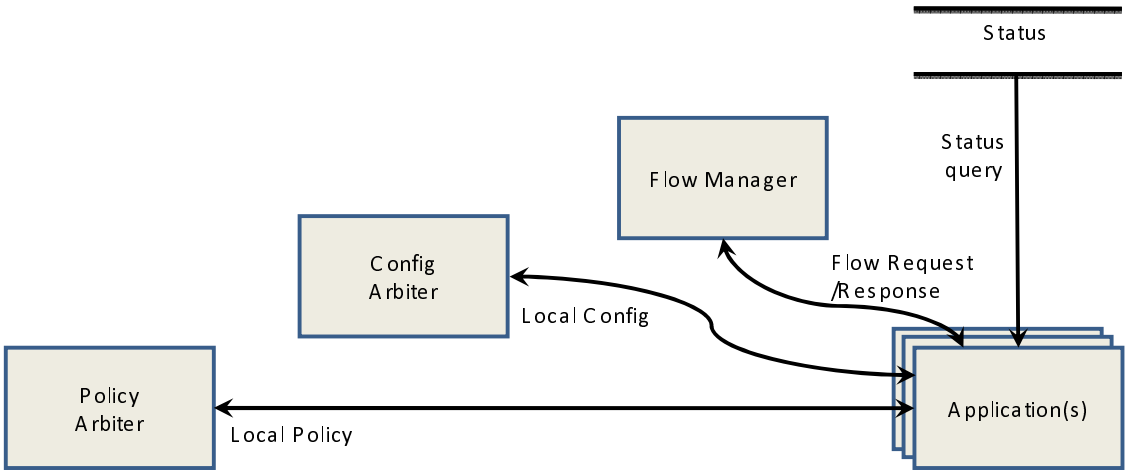


Figure 8: Context of Application Entities

7.3 Interfaces

The term "Interface" is used here to describe a demarcation within the QoS functional reference model across which information is transferred, into or out of the model or between logical entities within model.

7.3.1 Access Network Interfaces

7.3.1.1 Content Interface

The Content Interface is the interface over which Content from an AN enters the HN. In the case of a locally sourced flow, this interface is not present.

7.3.1.2 Service Statistics Interface

The Service Statistics interface is the interface over which service statistics are communicated to a RMS. It is assumed that this interface will be compatible with existing RMS standards. This may require some extensions to those standards.

7.3.1.3 Diagnostic Data Interface

The Diagnostic Data interface is the interface over which the *Flow Manager* communicates diagnostic information to a RMS. It is assumed that this interface will be compatible with existing RMS standards. This may require some extensions to those standards. The data model for the diagnostic data is not defined in the present document.

7.3.1.4 Remote Policy Interface

The *Remote Policy* interface is the interface via which a RMS can populate the *Policy* repository. It is assumed that this interface will be compatible with existing RMS standards. This may require some extensions to those standards.

7.3.1.5 Remote *Config* Interface

The *Remote Config* interface is the interface via which a RMS can populate the *Static Config* repository e.g. to accommodate new devices, installed remotely, on the HN which may not be fully "plug and play", i.e. those where the QoS capabilities, network connection capabilities, etc. are not advertised using any standardized device discovery methods. It is assumed that this interface will be compatible with existing RMS standards. This may require some extensions to those standards.

7.3.2 Internal Interfaces

7.3.2.1 Flow Request/Response Interface

The Flow Request/Response interface is the interface via which the *Applications* and the *Flow Manager* communicate with each other.

A flow request either for change to an existing flow or a request for a new flow will include a set of QoS requirements for that flow. An *Application* might also use the interface to query the *Flow Manager* for some aspects of the operational status possibly to display to the user.

The *Flow Manager* will also use this interface to direct *Applications* to terminate or change existing flows in accordance with decisions made by the *Flow Manager* when accommodating other flow requirements or dynamic network changes.

7.3.2.2 Flow Manager Policy Interface

The *Flow Manager Policy* interface is the interface via which the *Flow Manager* accesses the *Policy* repository.

7.3.2.3 Flow Manager Static *Config* Interface

The *Flow Manager Static Config* interface is the interface via which the *Flow Manager* accesses the Static *Config* repository.

7.3.2.4 Flow Manager Dynamic *Config* Interface

The *Flow Manager Dynamic Config* interface is the interface via which the *Flow Manager* accesses the *Dynamic Config* repository.

7.3.2.5 Flow Manager Status Interface

The *Flow Manager Status* interface is the interface via which the *Flow Manager* accesses the *Status* repository.

7.3.2.6 Application Status Interface

The *Application Status* interface is the interface via which the Application(s) can read the *Status* repository.

7.3.2.7 Local Policy Interface

The *Local Policy* interface is the interface via which the Application(s) can access the *Policy* repository.

7.3.2.8 Local *Config* Interface

The *Local Config* interface is the interface via which the Application(s) can access the *Config* repository. For example, this would permit users to adjust the configuration of devices in the HN through a local GUI Application.

8 QoS Functionality Levels

QoS systems can be categorized into levels dependent on their QoS functionality. Each level may use the functionality of the lower levels. It is possible that within a level multiple options may exist for making more or less complex implementations of the QoS functionality of that level.

Table 2 also provides an indication of the correspondence of the QoS levels to legacy home networks which may be found.

Five levels with their options are identified in table 2.

Table 2: Definition of QoS Levels

#	QoS Level	Description
0	No QoS support	The network forwards all flows equally i.e. there is only one class of traffic and that is best effort.
1A	Service based Traffic Classification	Flows are put in specific classes based on service type e.g. all video flows are put in one video class. All flows in one specific class are treated equally. Flows of one class are tagged with a specific priority tag. Subsequently the flows are treated according to their priority tag.
1B	Policy based Traffic Classification	Flows are put in specific classes based on rules (policy) e.g. all video flows of a particular service provider are put in one class and the ones originating from the HN are put in another. Flows within one class are tagged with a specific priority tagging. Subsequently the flows are treated according to their priority tag.
2A	User-based admission control	When a flow is set-up, the system checks whether it can fit the flow with the ones that are already admitted. If this is the case the flow is admitted. If the flow cannot be accommodated, the user is asked what action should be taken. Subsequently, the traffic classification of the admitted flow is service based i.e. level 1A. Furthermore, it does not take into account: • Dynamic changes in flows. • Dynamic changes in network performance.
2B	Policy-based admission control	When a flow is set-up, the system checks whether it can accommodate the flow with the ones that are already admitted according to the policy. If this is the case the flow is admitted. If the flow cannot be accommodated, the user may be asked what action should be taken. Subsequently, the traffic classification of the admitted flow is either service or policy based i.e. level 1A or 1B respectively. It does not take into account • Dynamic changes in flows. • Dynamic changes in network performance.
3A	Policy-based admission control with pre-emption	When a flow is set-up, the system checks whether it can guarantee the appropriate delivery of the flow. If there are not enough resources, the QoS system can decide on basis of a set of rules (policy) to stop or adjust one or more existing flows. The resources of stopped or adjusted flows are made available for the requested flow. Subsequently, the traffic classification of the admitted flow is either service or policy based, i.e. level 1A or 1B respectively. (See notes 3 and 4).
3B	Policy-based admission control with dynamic network tracking	The QoS system dynamically tracks the status of the network continuously. When a flow is set-up, the system checks whether it can accommodate that flow. If this is the case the flow is admitted. If the flow cannot be accommodated, the user is asked what action should be taken. Subsequently, if resource availably problems occur for a flow the user is asked what action should be taken. The traffic classification of the admitted flow is either service or policy based i.e. level 1A or 1B respectively.
4	Policy-based admission control with pre-emption and dynamic network tracking	The QoS system dynamically tracks the status of the network continuously. When a flow is set-up, the system checks whether it can accommodate the flow. If there are not enough resources, the QoS system can decide to stop or adjust one or more existing flows on the basis of a set of rules (policy). The resources of stopped or adjusted flows are made available for the requested flow. Subsequently, the QoS system can dynamically react to changes in the network characteristics by stopping and/or adjusting existing flows on the basis of the policy. The traffic classification of the admitted flow is either service or policy based i.e. level 1A or 1B respectively.
NOTE 1: In all levels it may be necessary to inform the user when some changes in flow delivery are necessary. NOTE 2: Each level requires an appropriate subset of the requirements listed in clause 10. NOTE 3: If the request cannot be fulfilled it can be part of the policy to warn the user or ask how to solve any contention. NOTE 4: The QoS system may not actually know what the current resource availability is, but only what it is told by *Applications*, e.g. one of the flows may have changed or stopped (this is an error condition for which there is no defined solution).		

Clause 9 contains the detailed QoS requirements of each component of the QoS functional reference model given in figure 1. Subsequently table 3 shows which of the functional QoS components are required for each QoS level.

9 Technical requirements

The technical requirements derived from the study of the use cases and appropriate to the QoS functional reference model are described in this clause. The technical requirements are grouped according to the component they are associated with, and some requirements may be duplicated for more than one component if they are appropriate to multiple components.

9.1 Entities

The entities refer to those shown in figure 1, and the requirements appropriate to each entity are given below.

The functionality of the entities may be distributed among the HN devices except for the *Packet Processing* and *Monitor* entities which in practice are assumed to be included in physical devices through which content flows.

9.1.1 Flow Manager Entity

ReqID	Requirement
QR-1000	The *Flow Manager* should minimize service disruption to the user when the service provider makes changes in *Policy* and Static *Config*.
QR-1010	The *Flow Manager* shall support interaction with multiple active *Applications* at the same time.
QR-1020	The *Flow Manager* shall respond to requests from *Applications* to allocate resources for new flows in the HN.
QR-1030	The *Flow Manager* shall respond to requests from *Applications* to adjust the allocation of resources for existing flows in the HN.
QR-1040	The *Flow Manager* shall respond to changes in resource availability and dynamic demands on the HN by adjusting the network behaviour on a per-flow basis, both via the *Dynamic Config* and the *Applications* controlling each flow.
QR-1050	The *Flow Manager* should minimize service disruption to the user due to changes to the network flows.
QR-1060	The *Flow Manager* shall use the information available from a combination of *Policy*, *Static Config* and *Status* to determine the appropriate actions for managing the flows, and set the parameters of the *Dynamic Config* accordingly.
QR-1070	The *Flow Manager* may be implemented as a distributed or duplicated function in the HN.
QR-1080	There may be multiple *Flow Manager*s in the network but only one shall be active at any time.
QR-1090	It shall be possible to identify the *Flow Manager* which is active in the HN.
QR-1100	An Application requesting a change in the network flows shall provide the necessary metadata describing the flow or flows involved to the *Flow Manager.*
QR-1110	The simple systems shall be able to tolerate (ignore) parameters or elements of information they do not understand.
QR-1120	It should be possible for the *Flow Manager* to report diagnostic information across the Diagnostic Data interface to the remote management system.

9.1.2 Policy Arbiter Entity

ReqID	Requirement
QR-1200	The *Policy Arbiter* entity shall be the logical mechanism by which the remote management service and/or a local Application populates the *Policy* repository.
QR-1210	It shall be possible to switch between policies which may be based on Opt-in/Opt-out and between several service provider policies.
QR-1220	In the case of Opt-out the user shall be able to populate all of the *Policy* repository parameter values via an Application.
QR-1230	In the case of Opt-in the remote manager shall be able to populate some or all of the *Policy* repository parameter values as agreed between the service provider and the user, taking precedence over the ability of the user to set those parameter values. The remote manager may allow the user to set some of the *Policy* repository parameter values.
QR-1240	It shall be possible for the *Policy Arbiter* entity to inform the user through an Application when policy changes are made.

9.1.3 Config arbiter Entity

ReqID	Requirement
QR-1400	The *Config Arbiter* entity shall be the logical mechanism by which the remote management service and/or a local Application populates the Static *Config* repository.
QR-1410	It shall be possible to switch between versions of *Static Config* which may be based on Opt-in/Opt-out and between several service provider policies.
QR-1420	It shall be possible for the user to elect to manage the *Static Config* (Opt-out mode) at any time.
QR-1430	In the case of Opt-out the user shall be able to populate all of the *Static Config* repository parameter values via an Application.
QR-1440	In the case of Opt-in the remote manager shall be able to populate some or all of the Static *Config* repository parameter values as agreed between the service provider and the user, taking precedence over the ability of the user to set those parameter values. The remote manager may allow the user to set some of the *Static Config* repository parameter values.
QR-1450	It shall be possible for the *Config Arbiter* entity to inform the user through an *Application* when configuration changes are made.

9.1.4 Packet Processing Entity

ReqID	Requirement
QR-1500	A *Packet Processing* entity shall be associated with each device within the DVB HN, although unnecessary functions may be null.
QR-1510	A *Packet Processing* entity may optionally contain the following functions which shall be configured according to the *Static Config* and *Dynamic Config*: • Classification, Marking and Policing. • Application Specific Processing. • Change of encoding. • Change of transport protocol. • Bridging, Routing and Queuing. • Queue mapping.

9.1.5 Monitor Entity

ReqID	Requirement
QR-1600	A *Monitor* entity shall be associated with each device within the HN.
QR-1610	Each *Monitor* entity shall provide information about the ingress and egress packet flows across each of its network interfaces, to be made available to the *Status* repository and over the Service Statistics interface to the remote management service.

9.1.6 Applications

The functionality of *Applications* is out of scope of the present document.

ReqID	Requirement
QR-1700	An Application requesting a change in the flows shall provide the necessary metadata describing the flows involved to the *Flow Manager*.
QR-1710	*Applications* shall use an open interface specification as far as possible so that *Applications* may communicate with entities and repositories in the HN in an interoperable way.
QR-1720	The Application shall have a means to inform the user if any changes carried out by the *Flow Manager* may produce change of quality for service flows associated with that Application.
QR-1730	An extensible open specification shall be defined for exchange of information with the user.
QR-1740	The QoS system shall allow multiple *Applications* to be active at the same time.
QR-1750	*Applications* shall be able to communicate with the *Status* repository, the *Flow Manager*, and the *Policy* and *Config Arbiter* entities.
QR-1760	*Applications* shall be able to: • Request the *Flow Manager* to allocate resources for a new service. • Request the *Flow Manager* to change the resource allocation for an existing service. • Accept QoS related information to be presented to the user, e.g. diagnostics, service statistics, user information. • Accept requests from the *Flow Manager* to alter or stop a service which it controls.
QR-1770	*Applications* shall be able to tolerate (ignore) parameters or elements of information they do not understand.

9.2 Repositories

The repositories refer to those shown in figure 1, and the specific requirements appropriate to each are given in those clauses following. However, the following general requirements are applicable to all repositories.

9.2.1 General Repository requirements

ReqID	Requirement
QR-2000	Repositories may be duplicated (redundancy) or distributed between devices.
QR2010	There shall be means to maintain the consistency of the information held by the repositories in such circumstances as multiple applications/entities reading and writing the repositories simultaneously, where it takes time for changes to propagate through the system, etc.

9.2.2 Policy Repository

ReqID	Requirement
QR-2100	There shall be a mechanism to determine the *Policy* in use.
QR-2110	There shall be a mechanism to select the *Policy* to be used.
QR-2120	It shall be possible for the *Flow Manager* and any active QoS *Applications* to read the *Policy* repository.
QR-2130	There shall be a default policy defined in the QoS system which can be used by the *Flow Manager* in the absence of either a user-defined or remote policy.
QR-2140	There may be multiple policies stored within the HN but there shall be only one active *Policy* at any time.
QR-2150	It shall be possible to define each element of the policy remotely or locally depending on the Opt-in/Opt-out state. This represents the functionality of the *Policy Arbiter*.
QR-2160	It shall always be possible for the HN user to revert to Opt-out mode. Also see clause C.9, Req 4.7.1.7.
QR-2170	The representation of policy shall be extensible to accommodate new policy rules and methods as they arise and shall address at least the following: • Relative importance of the different content and services based on specific criteria, e.g. service origin, premium services, etc., refer to clause B.9, Req 4.7.1.7. • Pre-emption of services. • An option to delegate policy configuration to a 3rd party (Opt-in/Opt-out). • Various user preferences (e.g. HD only). • Contention management and conflict resolution policies. • Admission control rules.
QR-2170	The *Policy* repository shall be extensible in a standardized way.

9.2.3 Static Config Repository

The *Static Config* contains some of the information about the HN devices which may be required by the *Flow Manager* to manage the HN QoS.

ReqID	Requirement
QR-2300	In order for the QoS system to manage the content streams it shall be possible to populate the *Static Config* with information describing the capabilities and expected behaviour of devices for which the topology cannot be discovered dynamically, i.e. "non-plug-and play" devices.
QR-2310	The format of the *Static Config* repository shall be defined to allow at least the following information to be contained. • Capabilities and expected behaviour for "non-plug-and play" devices: - Device ID - Re-encoding capability - For each network interface: ▪ Network interface ID ▪ Bitrate capability ▪ QoS capability (levels of QoS support) ▪ Supported technologies, e.g. wired Ethernet, 802.11a/g [9], PowerLine ▪ Device ID of HN device connected on this interface • For the *Flow Manager* operational settings: - Default queue mapping, i.e. mapping of service types to queues - Default queue sizes - Default classification rules - Mapping QoS from AN to HN and vice versa - Parameters to be monitored for diagnostic and statistical feedback including, e.g.: ▪ Per flow parameters ▪ Per flow class ▪ Per queue class ▪ Queue occupancy ▪ Network segment utilization
QR-2320	The *Static Config* repository shall be extensible in a standardized way.

9.2.4 Dynamic Config Repository

ReqID	Requirement
QR-2400	The *Dynamic Config* shall maintain an on-going set of QoS operating parameters programmed by the *Flow Manager* to maintain the desired content flows through the devices within the HN.
QR-2410	The format of the *Dynamic Config* repository shall be defined to allow the following information to be set by the *Flow Manager*: • For each existing content flow: - Flow ID - Source IP address - Destination IP address - Source port - Destination port - QoS marking parameters - Protocol - Flow management parameters: ▪ Queue allocation ▪ Policing/shaping - Re-encoding parameters
QR-2420	The *Dynamic Config* repository shall be extensible in a standardized way.

9.2.5 Status Repository

ReqID	Requirement
QR-2500	Shall be possible for the *Flow Manager* and any active QoS *Applications* to read the *Status* repository.
QR-2510	A mechanism shall be specified that allows the *Flow Manager* to discover the current topology of the HN from devices that are able to report on their interconnections. This information makes up part of the representation of the *Status* repository.
QR-2520	A mechanism shall be specified that allows the *Flow Manager* to monitor the current usage and performance metrics of the HN and the service flows from devices that are able to report this information. This information makes up part of the representation of the *Status* repository.
QR-2530	The format of the *Status* repository shall be defined to allow the following information to be contained about the device capabilities and current network connection usage: • The system capabilities: • Device ID • Re-encoding capability • For each network interface: - Network interface ID - Bitrate capability - QoS capability (levels of QoS support) - Supported technologies, e.g. wired Ethernet, 802.11a/g [9], PowerLine - Device ID of HN device connected on this interface • The current usage: - For each network interfaces: ▪ Network interfaces ID ▪ Per flow • Flow ID • Flow statistics
QR-2540	The HN shall have a mechanism to locate the information making up the *Status* repository.
QR-2550	The repository shall be extensible in a standardized way.

9.3 Interfaces

The interfaces refer to those shown in figure 1, and the requirements appropriate to each are given below.

ReqID	Requirement
QR-3000	In order for the logical functions linked by the interfaces to be interoperable the data formats and protocols shall be defined.
QR-3010	A mechanism for extending the interfaces shall be specified.
QR-3020	All interfaces shall use standards where they exist.
QR-3030	It shall be possible to authenticate the RMS.
QR-3040	It shall be possible to secure data exchanged with the RMS.

9.3.1 Network Interface

9.3.1.1 Remote Management Service Interface

ReqID	Requirement
QR-3100	This set of logical interfaces shall be compatible with existing remote management standards, e.g. those defined by the DVB RMS-FUS Specification [5]. Any necessary extensions needed to those specifications enable remote updates to service provider elements of *Config* and *Policy* should be identified to the organizations responsible for those specifications.

9.3.1.2 Service Statistics Interface

ReqID	Requirement
QR-3200	A protocol shall be defined for the Service Statistics interface to allow the QoS *Monitor* entities in each managed device to exchange information with the remote management service.
QR-3210	The data that may be exchanged (per service) should include at least: • Received packet count. • Transmitted packet count. • Retransmitted packet count. • Errored packet count. • Corrected packet count.
QR-3220	The data exchanged across the Service Statistics interface shall only be conveyed to the appropriate RMS. i.e. the RMS associated with that particular service.

9.3.1.3 Diagnostic Data Interface

ReqID	Requirement
QR-3300	A means shall be specified for *Flow Manager* to make diagnostic information available to the RMS.
QR-3310	The diagnostic information should include information from the repositories and a history log of resource allocation requests and responses.

9.3.1.4 Remote Config Interface

ReqID	Requirement
QR-3400	A protocol shall be defined for this interface to allow the RMS to populate the Static *Config* repository via the *Config Arbiter* entity.

9.3.1.5 Remote Policy Interface

ReqID	Requirement
QR-3500	A protocol shall be defined for this interface to allow the RMS to populate the *Policy* repository via the *Policy Arbiter* entity.

9.3.2 Internal Interfaces

9.3.2.1 Content Interface

ReqID	Requirement
QR-4000	The Content Interface shall not impact on the exchange of RTCP reports and similar control traffic.

9.3.2.2 Flow Request and Response Interface

ReqID	Requirement
QR-4100	The interface between the *Flow Manager* and the *Applications* should contain some or all of the following information: • Source and sink of the flow. • Criticality of the flow e.g. emergency alert. • User of the flow to distinguish between different users in the home. • User preference, e.g. HD only. • Pre-emptability: indicates that a flow can be terminated if necessary in order to give its resources to another flow. • Scalability: an indication that a flow can adjust its resource demands in some way that allows it to accommodate a reduction in the availability of resources allocated to it. Scalability may have one of two forms: - The selection between the same item in different qualities, e.g. SD and HD, depending on available network segment resource. - Scalability in terms of variable encoding (SVC). • Availability of multiple bitrate and encoding options. • Type of service. • Bandwidth and resource usage (actual for existing flow and potential for new flow). • Required delivery bitrate: depending on whether the flow is delivered using CBR or VBR, the actual figure required may be both average and maximum. • Latency: some types of traffic require tighter tolerances on latency than others, e.g. interactive gaming. • Amount of jitter which can be tolerated: similarly some types of traffic require tighter tolerances than others, e.g. audio/video. • Dependencies between flows.

9.3.2.3 Flow Manager Policy Interface

ReqID	Requirement
QR-4200	An interface shall be specified for the *Flow Manager* entity to read the *Policy* repository.

9.3.2.4 Flow Manager Static Config Interface

ReqID	Requirement
QR-4300	An interface shall be specified for the *Flow Manager* entity to read the Static *Config* repository.

9.3.2.5 Flow Manager Dynamic Config Interface

ReqID	Requirement
QR-4400	An interface shall be specified for the *Flow Manager* entity to be able to populate the *Dynamic Config* repository.

9.3.2.6 Flow Manager Status Interface

ReqID	Requirement
QR-4500	An interface shall be specified for the *Flow Manager* entity to read the *Status* repository.

9.3.2.7 Applications Status Interface

ReqID	Requirement
QR-4600	An interface shall be specified for the *Applications* to read the *Status* repository.

9.3.2.8 Local Policy Interface

ReqID	Requirement
QR-4700	A protocol shall be defined for this interface to allow the Application to populate the *Policy* repository via the *Policy Arbiter* entity.

9.3.2.9 Local Config Interface

ReqID	Requirement
QR-4800	A protocol shall be defined for this interface to allow the Application to populate the Static *Config* repository via the *Config Arbiter* entity.

10 Mapping of QoS Components to QoS Levels

Table 3 shows which entities, repositories and interfaces of the QoS functional reference model are required for the QoS levels as described in clause 9, table 2.

Table 3: Mapping of QoS Functional Components to QoS Levels

	Levels							
	0	**1A**	**1B**	**2A**	**2B**	**3A**	**3B**	**4**
Entities								
Packet Processing			●	●	●	●	●	●
Monitor					●	●	●	●
Flow Manager			●	●	●	●	●	●
Config Arbiter			●	●	●	●	●	●
Policy Arbiter			●	●	●	●	●	●
Applications			●	●	●	●	●	●
Repositories								
Policy			●	●	●	●	●	●
Static Config			●	●	●	●	●	●
Dynamic Config				●	●	●	●	●
Status							●	●
Interfaces								
Content	●	●	●	●	●	●	●	●
Service Statistics			○		○	○	○	○
Diagnostic Data			○	○	○	○	○	○
Remote Config			●	●	●	●	●	●
Remote Policy			●	●	●	●	●	●
Legend: ● = required; ○ = optional.								

Annex A (informative): QoS in other SDOs

This annex contains an overview of what we currently understand to be the QoS level assumed in the specifications listed below developed in the various SDO and consortia as referred to the QoS levels described in table 2.

Table A.1: QoS Functional Levels as specified in current Home Networking Specifications

SDO or Consortium	Specification Title	QoS Level	Comment
DVB	"Digital Video Broadcasting (DVB);Transport of MPEG-2 TS Based DVB Services over IP Based Networks" [1]	1A	Priority based QoS. DVB specifies a table for the DSCP values to be used for the specific services
DLNA	"DLNA Networked Device Interoperability Guidelines" [4].	1A	Priority based QoS. DLNA specifies a table for DSCP values to be used for the specific services.
HGI	Gateway Technical Requirements: Residential Profile" [6]	1B	Priority based QoS. HGI specifies a table for the DSCP values to be used for the specific services. Includes some elements of 2B for SIP based voice services
DLNA CSPR TT	"Digital Living Network Alliance Functional Requirements for Service Assurance" [i.1]. This commercial requirements document targets QoS level 2.		V2 1B It is possible that when a user selects another policy, the service provider cannot perform management anymore (Opt-out).
UPnP v1	"UPnP QoS Architecture:1.0" [7]	1B	
UPnP v2	"UPnP QoS Architecture:2" [8]	1B	It is possible that when a user selects another policy, the service provider cannot perform management anymore (Opt-out).
UPnP v3	"UPnP QoS Architecture:3" [i.2]	2B/partial 3A	Not yet released. Currently under review by UPnP members. UPnP V3 can only pre-empt services by stopping them. UPnP V3 specifies an optional feature to perform pre-emption automatically, if requested by the user.

Annex B (informative): Relationship with other DVB Specifications

The following DVB specifications have been taken into account for the present document.

B.1 DVB IPTV Handbook

The DVB IPTV Handbook for the transport of MPEG-2 transport stream based DVB services over IP-based networks [1] describes how DVB services can be delivered to the home over an IP-based network. It covers both "live media broadcast" services à la "classical" TV and radio broadcasts, "media broadcast" with trick modes and Content on Demand (CoD) services i.e. IPTV services. The DVB IPTV Handbook defines the mechanisms required for a consumer to be able to buy a standard DVB Home Network End Device (HNED), take it home, plug it into an IP network, subsequently choose and consume DVB services available over the IP network.

The DVB IPTV Handbook describes the DVB services that are to be managed by the QoS system.

B.2 Broadband Content Guide

The Broadband Content Guide (BCG) specification [2] is an addendum to the DVB IPTV Handbook [1] specifying the signalling and the transport of TV-Anytime information over a broadband network. The specification allows for metadata describing both CoD and live broadcast services delivered over any type of network using DVB specifications.

The BCG is a candidate for delivering some of the more content specific metadata needed for the QoS system.

B.3 Remote Management and Firmware Update System

The Remote Management System and Firmware Update System for DVB IP-based services, TS 102 824 [5], specification specifies the remote management and firmware update system for DVB services and forms an addendum to the DVB IPTV Handbook [1]. All aspects of the RMS and FUS functionality, which are standardized by DVB are described within TS 102 824 [5].

The DVB RMS and FUS specification is a candidate for the identified remote management system for the QoS system.

Annex C (normative): QoS related commercial requirements from DVB

The requirements documented in this annex are selected from the DVB BlueBook A144 [3] as those with some relevance in terms of QoS. Direct reference is made to the numbering used for the requirements in [3] throughout this clause.

C.1 Technology Requirements

Req 4.1.2.2	**Technology.Independence**
DVB-HN shall be able to include wired and wireless network segments	
Notes	
Req 4.1.2.5	**Technology.Interfacing**
DVB-HN device shall be able to interface with a wired and/or a wireless network segment. It is recommended that DVB-HN compliant devices include an Ethernet 100 Base-T interface to achieve maximum interoperability and QoS.	
Notes	
Req 4.1.2.7	**Technology.DLNA.Compatibility**
The standard shall guarantee the following level of compatibility between a DVB-HN compliant device and a DLNA compliant device: A DVB-HN compliant server shall offer DVB content in an optional or mandatory DLNA compliant manner and format. A DVB-HN compliant player shall be able to discover all contents on a DLNA compliant server. Transcoding between content formats, such as AVC to MPEG-2 is not required.	
Notes	If content is streamed between a DVB-HN and a DLNA compliant device the quality and/or user experience may be lower than when the same content is streamed between two DVB-HN devices. In all cases DVB-HN solutions should be identical or based on DLNA protocols when available.

C.2 Content Formats

Req 4.2.2.2	**Content.Other**
DVB-HN shall not preclude non-DVB services like PC networking, DVD, gaming, IP telephony (including hand-over from mobile), video-telephony, surveillance cameras, data services, general internet inc. web browsing and file transfers, VPN, e-mail, video, audio and text messaging, (multi-media) chat. These non-DVB services may occur simultaneously with DVB services.	
Notes	

C.3 Network Topology

Req 4.3.1.4	**Topology.Dynamics**
The HN shall support the dynamic addition and removal of DVB-HN devices.	
Notes	
Req 4.3.1.7	**Topology.Monitor**
It shall be possible to monitor the ongoing network state, including existing connections and their respective end-points.	
Notes	

C.4 Third Party Management

Req 4.3.4.1	**Management.ThirdParty**
The HN technology shall not prohibit nor shall it mandate remote network management by a third party from outside the home. If a remote management technology exists, it shall be a standardized mechanism.	
Notes	It does not mandate remote management by a 3rd party but it does allow it.
Req 4.3.4.2	**Management.Authorization**
Remote management and configuration by a 3rd party outside the home shall only take place after explicit authorization by the home owner.	
Notes	The home owner is the end-customer.

C.5 Application Resource Management

Req 4.3.6.1	**Management.Authorization**
A means of signalling or identifying the different types of applications and their bandwidth requirements should be specified to enable appropriate network management.	
Notes	

C.6 General Home Network Functionality

Req 4.4.1.4	**Functionality.Multicast**
Multicast support of AV content within the HN is not required in phase 1. Multicast services from the access network shall be supported.	
Notes	Note that the delivery of DVB service to DLNA devices cannot be done via multicast (see "Technology.DLNA.Compatibility "- Req 4.1.2.7).

C.7 Content Discovery and Selection

Req 4.5.4	**ContentDiscovery.Beforehand**
A DVB-HN compliant server should advertise the following information in a standardized manner as available over the access network: mandatory DVB SI information, encoding format, peak bit rate, service/content name, FTA/scrambled, pricing information, parental control information, TV guide information, SD&S, TVA metadata, trick mode availability (note that there might be multiple peak bit rates for every trick mode). This includes streamed and broadcast content for which the user currently does not have a subscription and content that may have been pushed into his DVB-HN, for which he has yet to complete a financial transaction.	
Notes	

C.8 Content Presentation Control

Req 4.6.2.5	**ContentPresentation.Bitrate**
Trick modes shall not exceed the earlier signalled peak bitrate. (see "Discovery.Beforehand",Req 4.5.4)	
Notes	

C.9 Quality of Service mechanisms

Req 4.3.4.1	**Management.ThirdParty**
The HN technology shall not prohibit nor shall it mandate remote network management by a third party from outside the home. If a remote management technology exists, it shall be a standardized mechanism.	
Notes	Does not mandate remote management by a 3rd party but it does allow it.
Req 4.3.4.2	**Management.Authorization**
Remote management and configuration by a 3rd party outside the home shall only take place after explicit authorization by the home owner.	
Notes	The home owner is the end-customer.
Req 4.7.1.1	**Quality.QoS**
The HN technical solution shall include mechanisms that aim to enable the support of high quality user experience similar to DVB1.0 implementations. This is referred to as QoS mechanisms. (QoS includes bandwidth, latency and jitter: glossary). Note that 100 % QoS cannot be guaranteed, especially in wireless networks.	
Notes	
Req 4.7.1.2	**Quality.ProblemDetection**
The HN shall provide means to detect network QoS problems. Ideally, it should provide information about individual links and devices.	
Notes	
Req 4.7.1.3	**Quality.ExposeInfo**
A DVB-HN device that is connected to an access network shall expose available QoS information about this access network.	
Notes	In order to distinguish between QoS problems within the HN and QoS problems on the access network.
Req 4.7.1.4	**Quality.Priority**
No device on the DVB-HN shall be able to allocate a higher priority to its data without prior authority from the user (network manager).	
Notes	
Req 4.7.1.5	**Quality.Management**
A means of signalling or identifying the different types of applications and their bandwidth requirements should be specified to enable appropriate network management.	
Notes	
Req 4.7.1.6	**Quality.Latency**
The increase in latency due to one wireless network segment compared to one wired network segment shall be less than 20 ms to ensure that interactive TV and games applications can be supported.	
Notes	
Req 4.7.1.7	**Quality.DifferentiatedServices**
The DVB-HN shall support a configurable mechanism such that the user can indicate the relative importance of the different content and services. The user shall always be able to determine this configuration, which could be delegated to a 3rd party. It shall always be possible for the HN user to regain delegated configuration.	
Notes	In order to distinguish between QoS problems within the HN and QoS problems on the access network.
Req 4.7.1.8	**Quality. Roaming**
When a DVB HN device moves from one network segment to another network segment, there should be minimum disruption of the DVB service.	
Notes	

C.10 Contention Management

Req 4.7.2.1	**Contention.Policy**
The HN shall include policy management functionality, providing mechanisms for contention management (e.g. sharing the tuner resource). The user shall always be able determine the policy, which could be delegated to a 3rd party. It shall always be possible for the HN user to regain delegated control.	
Notes	
Req 4.7.2.2	**Contention.ResourceAvailability**
It shall be possible to discover the current availability of resources on the HN.	
Notes	It shall be possible to discover the current availability of resources on the HN.
Req 4.7.2.3	**Contention.ConflictHandling**
An established connection between DVB-HN devices shall never be interrupted without explicit user confirmation.	
Notes	
Req 4.7.2.4	**Contention.GracefulDegradation**
The HN should adapt gracefully under conditions of network degradation (e.g. by filtering out components of a service or filtering out complete services).	
Notes	In order to distinguish between QoS problems within the HN and QoS problems on the access network.

Req 4.7.2.5	Contention.Admission
The HN shall provide mechanisms for admission control of streams on the network. Notes: In order to preclude streams when network capacity is insufficient. This situation may occur when multiple users watch different live streams with time-shifting feature.	
Notes	

C.11 User Specific Functionality

Req 4.9.1.4	User.Profiles
It shall be possible to generate and retrieve network-wide user profiles.	
Notes	For example to assemble/store a personalized EPG.

History

Document history		
V1.1.1	January 2010	Publication