International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.622.1

(10/2008)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Broadband, triple-play and advanced multimedia services – Advanced multimedia services and applications

Architecture and functional requirements for home networks supporting IPTV services

Recommendation ITU-T H.622.1

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	**H.620–H.629**
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.622.1

Architecture and functional requirements for home networks supporting IPTV services

Summary

Recommendation ITU-T H.622.1 describes an architecture for home networks supporting IPTV services and its functional requirements.

In this Recommendation, home networks and IPTV-related entities are defined, and interfaces between these entities are identified. Functions needed for the home network to support IPTV services are described. Requirements for these functions are also described in this Recommendation.

Source

Recommendation ITU-T H.622.1 was approved on 14 October 2008 by ITU-T Study Group 16 (2005-2008) under the Recommendation ITU-T A.8 procedure.

Keywords

Delivery network gateway, home network, interoperability, IPTV services, IPTV terminal device, QoS, remote management, residential gateway, security.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T H.622.1

Architecture and functional requirements for home networks supporting IPTV services

1 Scope

This Recommendation describes the relationship between the home network (HN) and IPTV-related entities. It also identifies rules and requirements for functions needed on the home network to support IPTV services. It further sets criteria to verify compliance of home network devices, e.g., IPTV terminal devices, to the identified rules and requirements.

The architecture and requirements described in this Recommendation are based on current delivery network technology and thus advanced IPTV services and features that are possible with emerging NGN (next generation network) architecture, e.g., multicast control, are not covered. Advanced IPTV features and services in NGN-based home networks are for further study.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.983.x] Recommendation ITU-T G.983.x-series (in force), *Broadband optical access systems*.
<http://www.itu.int/rec/T-REC-G>

[ITU-T G.984.x] Recommendation ITU-T G.984.x-series (in force), *Gigabit-capable Passive Optical Networks (GPON)*.
<http://www.itu.int/rec/T-REC-G>

[ITU-T G.992.1] Recommendation ITU-T G.992.1 (1999), *Asymmetric digital subscriber line (ADSL) transceivers*.
<http://www.itu.int/rec/T-REC-G.992.1>

[ITU-T G.992.3] Recommendation ITU-T G.992.3 (2005), *Asymmetric digital subscriber line transceivers 2 (ADSL2)*.
<http://www.itu.int/rec/T-REC-G.992.3>

[ITU-T G.992.5] Recommendation ITU-T G.992.5 (2005), *Asymmetric digital subscriber line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2plus)*.
<http://www.itu.int/rec/T-REC-G.992.5>

[ITU-T G.993.2] Recommendation ITU-T G.993.2 (2006), *Very high speed digital subscriber line transceivers 2 (VDSL2)*.
<http://www.itu.int/rec/T-REC-G.993.2>

[ITU-T H.622] Recommendation ITU-T H.622 (2008), *A generic home network architecture with support for multimedia services*.
<http://www.itu.int/rec/T-REC-H.622>

[ITU-T J.190] Recommendation ITU-T J.190 (2007), *Architecture of MediaHomeNet*.
<http://www.itu.int/rec/T-REC-J.190>

[ITU-T X.1111] Recommendation ITU-T X.1111 (2007), *Framework of security technologies for home network.*
<http://www.itu.int/rec/T-REC-X.1111>

[ATIS-0800002] ATIS standard ATIS-0800002 (2006), *IPTV Architecture Requirements*.
<https://www.atis.org/docstore/product.aspx?id=21213>

[HGI] HGI-RD001-R1-obs Home Gateway Initiative (2006), *Home Gateway Technical Requirements: Release 1.0*.
<http://www.homegatewayinitiative.org/publis/HGI_V1.0.pdf>

[IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.
<http://www.ietf.org/rfc/rfc2236.txt>

[IETF RFC 2710] IETF RFC 2710 (1999), *Multicast Listener Discovery (MLD) for IPv6.*
<http://www.ietf.org/rfc/rfc2710.txt>

[IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3*.
<http://www.ietf.org/rfc/rfc3376.txt>

[IEEE 802.1D] IEEE Std. 802.1D (2004), *IEEE standard for local and metropolitan area networks – Media Access Control (MAC) Bridges*.
<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf >

[IEEE 802.1Q] IEEE Std. 802.1Q (2005), *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks*.
<http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>

[IEEE 802.3] IEEE Std. 802.3 (2005), *IEEE standard for Information technology – Telecommunications and information exchange between systems-Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*.
<http://standards.ieee.org/getieee802/802.3.html>

[IEEE 802.11] IEEE Std. 802.11 (2007), *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[IEC 62481-1] IEC 62481-1 (2007), *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 1: Architecture and protocols*.
<http://webstore.iec.ch/webstore/webstore.nsf/artnum/038283>

[IEC 62481-2] IEC 62481-2 (2007), *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 2: DLNA media formats*.
<http://webstore.iec.ch/webstore/webstore.nsf/artnum/038284>

[ISO/IEC 8802-1] ISO/IEC 8802-1 (2001), *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 1: Overview of Local Area Network Standards*.
<http://webstore.iec.ch/webstore/webstore.nsf/artnum/040657>

[ISO/IEC 15045-1] ISO/IEC 15045-1 (2004), *Information technology – Home electronic system (HES) gateway – Part 1: A residential gateway model for HES*.
<http://webstore.iec.ch/webstore/webstore.nsf/artnum/031683>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 delivery network gateway (DNG) [ATIS-0800002]: A device implementing the delivery network gateway function (DNGF).

NOTE – Many terms such as home access (HA) [ITU-T J.190], home gateway, residential gateway, delivery network gateway and so on are used for the same device.

3.1.2 home network (HN) [**ITU-T H.622**]: A home network is the collection of elements that process, manage, transport and store information, thus enabling the connection and integration of multiple computing, control, monitoring, communication and entertainment devices in the home.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 delivery network gateway functions (DNGF): Set of functions that mediate between the network and service provider domains and the IPTV terminal function (ITF).

NOTE – A device implementing the DNGF is commonly referred to as the residential gateway (RG) or delivery network gateway (DNG).

3.2.2 home network (HN) capable IPTV TD: An IPTV TD which has HN capability. This is typically a server and/or a client to HN devices.

3.2.3 HN capable TD: A TD which has HN capability. This is typically a server and/or a client to HN devices.

3.2.4 IPTV TD: A terminal device which has IPTV terminal function (ITF) functionality, e.g., a set-top box.

3.2.5 IPTV terminal function (ITF): The end-user function(s) associated with a) receiving and responding to network control channel messages regarding session set-up, maintenance and tear-down, and b) receiving the content of an IP transport from the network and rendering.

3.2.6 terminal device (TD): A device which typically presents and/or processes content, such as a personal computer, a computer peripheral, a network appliance, a mobile device, a television set, a monitor, a voice over IP terminal or an audiovisual media player.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

ALG Application Layer Gateway

ALL Application Layer Logic

AN Access Network

BC-NW Broadcast Network

DA Destination Address

DHCP Dynamic Host Configuration Protocol

DLNA Digital Living Network Alliance

DMP Digital Media Player

DMS Digital Media Server

DMZ	Demilitarized Zone
DNG	Delivery Network Gateway
DNGF	Delivery Network Gateway Function
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DTCP	Digital Transmission Content Protection
ECG	Electronic Content Guide
EPG	Electronic Programme Guide
FEC	Forward Error Correction
GUI	Graphical User Interface
HA	Home Access
HN	Home Network
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPI	Internet Protocol Interface
IPTV	Internet Protocol Television
L2	Layer 2
LAN	Local Area Network
MAC	Media Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface Crossover
MLD	Multicast Listener Discovery
NAT	Network Address Translation
NT	Network Terminal
NW	Network
OAM	Operations, Administration and Maintenance
OLT	Optical Line Terminal
ONT	Optical Network Termination
OUI	Organizationally Unique Identifier
PLT	Power Line Transmission
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PVC	Permanent Virtual Circuit
PVR	Personal Video Recorder

QoS	Quality of Service
RG	Residential Gateway
RTSP	Real-Time Streaming Protocol
SA	Source Address
SCP	Service and Content Protection
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STUN	Simple Traversal of User Datagram Protocol (UDP) through network address translation (NAT)
TCP	Transmission Control Protocol
TD	Terminal Device
UDP	User Datagram Protocol
USB	Universal Serial Bus
VC	Virtual Channel
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VoD	Video on Demand
VoIP	Voice over IP
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WRR	Weighted Round Robin
XML	eXtensible Markup Language

5 Conventions

In this Recommendation, the following conventions apply.

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is not recommended**" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

Furthermore, [HGI_Rn] means the n-th requirement as identified in [HGI]. For example, [HGI_R100] means the R100 requirement identified in [HGI].

The items tagged by [HGI_Rn] have been included in this Recommendations with the kind permission of the Home Gateway Initiative. Readers interested in the most current publication of Home Gateway Initiative should consult the website of that body here: http://www.homegateway.org/publis/index.html.

6 Home network architecture

The home network has become a preferred environment for many users to receive multimedia services in the home. Thus, IPTV services are likely to be delivered using home networking technology. In order to provide IPTV users with good user experience and to bring down the costs, IPTV devices need to interact seamlessly with the home network and with each other on the home network. For that purpose, a standardized home network architecture supporting IPTV services is essential.

Figure 6-1 below depicts the home network architecture defined in this Recommendation.

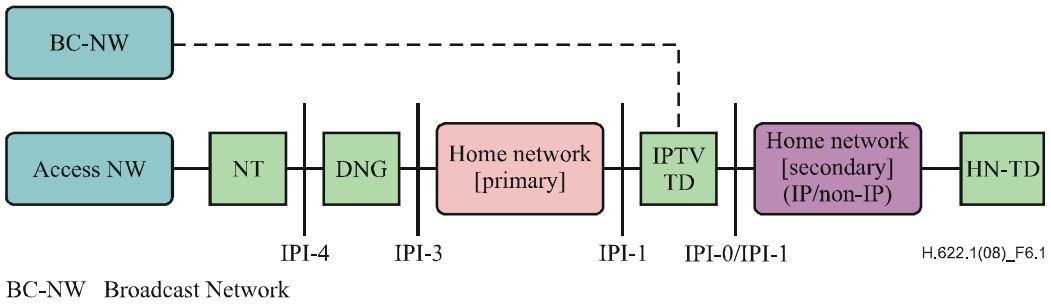

Figure 6-1 – Home network architecture

The components of the home network architecture are described as follows.

Primary domain (IP-HN-P)

The primary domain deals with IPTV-related IP traffic between the access network and the IPTV terminal device (IPTV TD) including audio and video streams. Traffic in the primary domain is associated with traffic to and from the access network. The devices and traffic related to the primary domain are required to be configured to be reachable to and from the access network, directly or indirectly (e.g., via NAT). Since this domain is expected to work as an extension of the access network, technical coordination such as QoS mapping with the access network is required.

Secondary domain

The secondary domain deals with IPTV-related traffic between the IPTV TD and the home network terminal device (HN-TD). The devices and traffic belonging to the secondary domain do not need to be configured to be reachable to and from the access network. For example, there may be cases where locally assigned IP addresses are enough for this domain. The secondary domain can be divided into two parts, IP and non-IP, depending on the network layer protocol used.

IP secondary domain (IP-HN-S)

The IP secondary domain is a part of the secondary domain based on IP.

Non-IP secondary domain (PR-HN-S)

The non-IP secondary domain is a part of the secondary domain based on non-IP protocols, such as [b-IEEE 1394].

Network termination (NT)

The network termination resides between network provider's access network and home network. The NT is the termination point of the access network. For example, in the cable broadband service environment, a cable modem is the NT. Likewise, a digital subscriber line (DSL) modem is the NT in the DSL broadband service environment. Another example for NT is an optical network termination (ONT), which is a termination device of an optical access network.

Delivery network gateway (DNG)

The DNG serves as a gateway between the access network and home network. It provides crucial functions for services on the home network. Functions of the DNG are described in detail later in this Recommendation.

IPTV terminal device (IPTV TD)

An IPTV terminal device is used by end-users to receive IPTV services. An IPTV set-top box is an example of an IPTV terminal device.

Home network terminal device (HN-TD)

Terminal devices that do not directly interact with the service or network provider may be used by the end-user to use IPTV services on the home network. These devices are classified as HN-TD. An example of such terminal devices is a traditional digital TV connected to the home network using the IEEE 1394 interface.

The above architecture contains interfaces between devices and domains. These interfaces are summarized in Table 6-1 below.

Table 6-1 – Interfaces within the home network architecture

Interface		Note
IPI-0		Interface between IPTV TD and HN-TD that has no direct connection with the DNG.
IPI-1		Upstream side interface of IPTV TD or HN-TD. In the HN-TD case, the HN-TD has a direct IP connection with the DNG.
	IPI-1a	IPI-1 interface used for power line
	IPI-1b	IPI-1 interface used for Ethernet (10/100/1000 BASE-T)
	IPI-1c	IPI-1 interface used for home PNA
	IPI-1d	IPI-1 interface used for coaxial
	IPI-1e	IPI-1 interface used for wireless
IPI-3		Downstream side interface of DNG
	IPI-3a	IPI-3 interface used for power line (see clause 10.3.1)
	IPI-3b	IPI-3 interface used for Ethernet (10/100/1000 BASE-T) (see clause 10.3.2)
	IPI-3c	IPI-3 interface used for home PNA (see clause 10.3.3)
	IPI-3d	IPI-3 interface used for coaxial (see clause 10.3.4)
	IPI-3e	IPI-3 interface used for wireless (see clause 10.3.5)

Table 6-1 – Interfaces within the home network architecture

Interface		Note
IPI-4		Upstream side interface of DNG (see clause 10.2)
	IPI-4a	IPI-4 interface used for connection with copper access network (see clause 10.2.1)
	IPI-4b	IPI-4 interface used for connection with NT through Ethernet interface (see clause 10.2.2)
	IPI-4c	IPI-4 interface used for connection with NT through coaxial interface (see clause 10.2.3)
	IPI-4d	IPI-4 interface used for connection with wireless access network (see clause 10.2.4)
	IPI-4e	IPI-4 interface used for connection with optical access network (see clause 10.2.5)
NOTE – The layer 2 technologies listed here, e.g., Ethernet and power line, are those that are currently available. This table may be expanded in the future to include new technologies as they become available.		

7 Quality of service (QoS)

In order to provide a good user experience of IPTV services in the home network environment, the QoS aspect of the home network needs to be considered, and necessary QoS mechanisms to ensure good user experiences need to be provided. This clause discusses QoS aspect of the home network in the context of IPTV services.

There are two main QoS techniques that are being used in an IP network: priority (or class) based QoS and parameterized QoS. With the priority QoS technique, intermediate routing entities between the source and the destination of an IPTV data stream determine how to handle an IP packet from the IPTV data stream according to the priority field in the header of that IP packet. The priority field has been set to a certain value (this is called QoS marking or classification) by the source. With this technique, higher priority IP packets will get better treatment during transit to reach the destination, thus their stream can achieve better QoS than others that have a lower priority.

In the parameterized QoS technique, the QoS requirements of an IPTV data stream (e.g., bandwidth, delay and jitter) are specified and requested to the network before the first IP packet is sent. The home network then uses these QoS parameters to set up the environment so that IP packets in the IPTV stream are processed in such a way to ensure that QoS requirements of the stream are met.

The parameterized QoS technique may provide guaranteed QoS as requested for IPTV services but its technology has not yet been widely agreed upon in the industry. For that reason, the QoS aspects of the home network discussed in this Recommendation concern mainly the priority based QoS technique. The application of the parameterized QoS technique to the home network for IPTV services is for further study.

7.1 Home network QoS architecture

This clause describes a QoS architecture that is based on the home gateway initiative (HGI) and its requirements.

NOTE – The QoS mechanisms in this clause are also described in [HGI] in the context of bidirectional services like VoIP. Refer to [HGI] for more details.

7.1.1 Potential congestion points in the home network

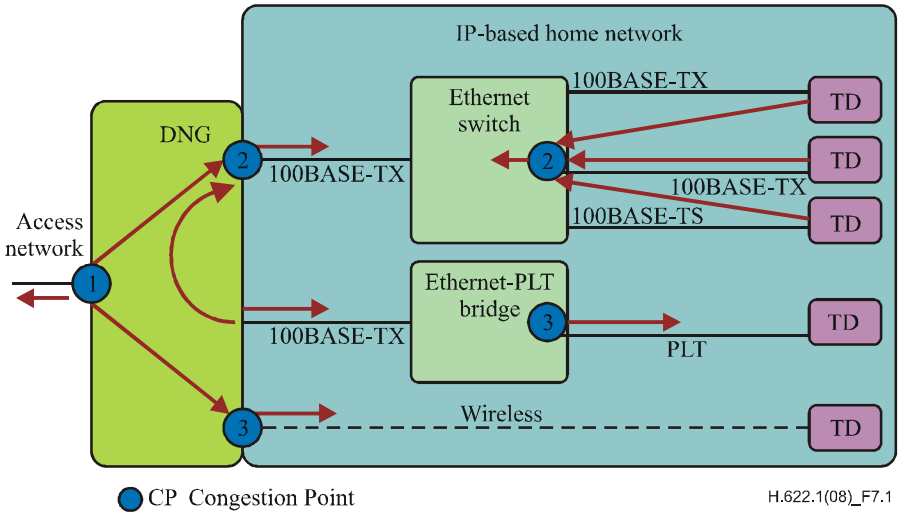

Figure 7-1 – Potential congestion points in a typical home network

The home network QoS function needs to accommodate a variety of both access and home network technologies. There are a number of potential congestion points as shown in Figure 7-1. Note that the degree to which these are actual congestion points will depend on the underlying network technologies used.

Three potential congestion points are identified in the home network.

- Congestion point CP-1

  Congestion point CP-1 is on the upstream side interface of the DNG, which is also defined as IPI-4. Because some IP-based access network technologies such as DSL and cable modem have relatively limited capacity for the upstream traffic, it is likely to see traffic congestion at this interface point.

- Congestion point CP-2

  Congestion point CP-2 is at the egress port of the device in which traffic from two or more network links is collected. A typical example is an Ethernet switch. If combined traffic from several ports or links exceeds a certain amount, the congestion at the egress port will happen. Congestion point CP-2 is also possible at the DNG, if it contains switching capability for traffic on the home network side.

- Congestion point CP-3

  Congestion point CP-3 is where congestion could be caused by transmission capacity differences. The bridge device interconnecting between different network segments with different capacity between Ethernet and power line transmission (PLT), is a typical example. Congestion point CP-3 is also possible at the DNG because of the difference of transmission capacity between the access network and home network.

7.1.2 QoS mechanisms

QoS management described in this Recommendation works on the basis of packet-by-packet service classification. The service classifiers are contained in header fields in the ingress packet and value of these service classifiers are assigned via QoS marking. QoS markings of packets coming from the HN side are generally untrusted, but can be used if a trust relationship is established by some other means, or in combination with other service classifiers.

The service classification information is used to assign the packet to the appropriate queue, and may be used to set the layer 2 markings for a particular transport technology. It is also possible to drop packets on the basis of classification when necessary. The management function can optionally provide the service classifiers' value as a static policy. Where service instance classification is used (e.g., for the overload protection mechanism described below), the additional classifiers are generated within the DNG itself. There is no session awareness, except for that associated with this overload control mechanism. Class-based queuing is used to queue packets. DSCP markings of the incoming packet at the IPI-3 interface can be overwritten to zero or to a per-service configurable value. There is a QoS mapping table for layer 2 parameters for transit traffic at the DNG. The DNG does not directly support signalled admission control, but the overload protection mechanism can provide some features of admission control by limiting the number of service instances to a pre-configured value.

NOTE – See clause 5.5.4 of [HGI].

7.1.3 QoS marking

There are several class-based QoS marking schemes such as differentiated services code point (DSCP), VLAN and Ethernet priority scheme that can be used for QoS management in the home network for IPTV services. In these schemes, all traffic of the same type would have the same QoS marking value. For QoS management to be effective, the marking values need to be trusted, but since marking values, particularly in case of upstream and transit, can be set by an end-user's terminal device, they can be spoofed. Thus, the home network is required to provide a mechanism to establish trust with end devices to prevent spoofing of QoS marking values.

VLAN IDs and priority tags could be used as a QoS marking within the home network. Adding a VLAN header or priority tags increases the Ethernet frame size; and some small, unmanaged Ethernet switches simply drop such frames. Since there are at least some infrastructure devices which will drop tagged frames, the DNG is recommended not to add VLAN headers to any frames. However, it is recognized that certain DLNA devices may send tagged frames. The DNG needs to be able to receive such frames and, in the case of bridged traffic, to forward them transparently.

NOTE – See clause 5.5.5 of [HGI].

7.1.4 Traffic classification

The key requirement for traffic classification is to be able to identify a service class. Queuing, scheduling and dropping treatments are recommended to be determined based upon the service class of the packet. Each packet is classified by inspecting one or more classifiers contained in its header fields. The combination of classifiers used to identify a service class is known as the classification rule for that service.

There are in fact rather different requirements for the classification of the three types of traffic flow through the DNG, namely upstream, downstream and transit.

For basic IPTV services, such as linear TV QoS, downstream traffic is the most important, next transit traffic and lastly upstream traffic. In the downstream direction, the main aim is to maintain the QoS characteristic of incoming traffic and to ensure that it is not compromised by transit traffic. The classifiers are briefly described below with a rationale as to when and how they might be used.

NOTE 1 – See clause 5.5.6 of [HGI].

NOTE 2 – For interactive applications such as gaming, QoS treatment for upstream traffic is also important.

7.1.5 Downstream classifiers

The main requirement in the downstream direction is to be able to distinguish IPTV traffic from other traffic. When the DNG is connected to the access network that is managed to provide required QoS for IPTV traffic, it is likely that QoS marking, such as DSCP, is available. Because this QoS marking is set by the network provider, it is trustful and correctly reflects the QoS policy of the

network provider. Therefore, when QoS marking is set for downstream traffic, using this QoS marking as the QoS classifier is desirable. Other classifiers such as IP DA and SA, physical port, packet length, MAC SA and DA, TCP/UDP port number and protocol type fields, which are identified as upstream classifiers in [HGI] (see clause 5.5.7 of [HGI]), can also be used.

7.1.6 Transit classification

Preventing adverse impacts to IPTV services by transit traffic is a key objective of QoS control of transit traffic. This could be done by giving better priority to the downstream IPTV traffic (relative to transit traffic).

The service differentiation can be done by using QoS marking. However, as mentioned above, there is a potential problem of using QoS marking of transit traffic. The QoS marking of transit traffic is set by the end-user devices that are typically not controlled by the network provider and thus is not trustful. Also, it is difficult to ensure the consistency of QoS marking policy between end-user devices and the network provider. It is possible to have conflicting QoS policies since they are set by end-user devices and network provider separately without coordination.

Therefore it is desirable to use a simple transit priority scheme, which is essentially device-based and uses MAC address pairs (SA and DA) to identify traffic which can be given higher priority. Also, the use of other classifiers needs to be considered. Once transit traffic is classified at the DNG, the relevant value of QoS marking is recommended to be set for the packets. This will help bridging devices in the home network to prioritize the packets efficiently.

NOTE – The text above is imported from clause 5.5.9 of [HGI] with modifications.

7.1.7 Traffic classifier used in the home network

7.1.7.1 IP destination address (IP DA)

This is a particularly useful classifier in the case where the required priority is related to its destination address. The destination address in this case does not need to be limited to a unicast address since the use of multicast is likely for IPTV services. The traffic classification based on both unicast and multicast is possible and desirable in some cases. The followings are some advantages of using this approach:

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

NOTE – The text above is imported from clause 5.5.7.1 of [HGI] with modifications.

7.1.7.2 IP source address (IP SA)

The use of the SA as a traffic classifier may be appropriate when there is a large number of DAs associated with a service and the use of the DA as a classifier may cause difficulty. In case of IPTV, the IP SA represents the corresponding video server. If the IP address of such a device is managed in a reliable way and the number of IP SAs is sufficiently small, the use of the IP SA as a traffic classifier might be considered.

NOTE – The text above is imported from clause 5.5.7.2 of [HGI] with modifications.

7.1.7.3 MAC source address (MAC SA) and destination address (MAC DA)

These can be used to distinguish different physical devices, and therefore different instances of the same service as per clause 5.5.7.5 of [HGI].

7.1.7.4 TCP/UDP port number

The TCP/UDP port number can be used to identify certain applications as per clause 5.5.7.6 of [HGI].

7.1.7.5 Protocol type

Distinguishing between TCP and UDP protocols can allow a more general distinction between different types of service as per clause 5.5.7.7 of [HGI].

7.1.7.6 QoS mapping between different HN technologies

As in the case of bridging the HN with the access network function, the DNG bridging between different HN technologies needs consideration in order to provide well-harmonized QoS within the home network. Consideration includes mapping between the layer 2 and layer 3 marker (or classifier) and use of marking in the different HN segments.

NOTE – The details of QoS mapping require further study.

7.1.8 Downstream and transit queue structure

The main functional requirements of QoS architecture are to avoid excessive delay and jitter as well as packet loss for multimedia services such as IPTV, to provide sufficient bandwidth for IPTV services, and to prevent best-effort traffic from being completely starved by higher priority queues.

In the downstream direction, there are two major concerns: 1) ensuring that traffic from the AN is not blocked by transit traffic, and 2) if there is downstream congestion due to a rate mismatch caused by a slow HN technology (congestion point CP-3), ensuring that the value-added traffic gets higher priority. There may be two different types of transit traffic: simple data traffic and streaming traffic, e.g., from a media player. For a better user experience, streaming traffic is recommended to get higher priority than simple data traffic. From a QoS perspective, simple data traffic is considered best effort traffic and streaming traffic is considered managed service traffic.

Based on these considerations, the downstream would need four queues per IPI-3 interface to manage traffic: 1) managed services from the AN, 2) best effort from the AN, 3) managed services within IP-HN-S/P, and 4) best effort within IP-HN-P/S.

NOTE – There are three fundamentally different types of traffic within a managed services class with regard to QoS: voice, video and data. Each of these traffic types may require its own queues. Also, there may be a need to further distinguish between two different types of data traffic (e.g., for higher priority control data or to support a premium data service). Further, the overload protection mechanism may require an additional queue. However, it should be noted that the larger number of queues may increase the implementation difficulty of HN devices such as the DNG, and it is technically possible to have a smaller number of queues by merging some of these queues. Further study is needed for queues implementation.

7.1.9 Class based QoS, sessions and policy

The QoS approach used here is essentially traffic-class based, i.e., the QoS treatment is the same for all flows belonging to the same class. This approach was chosen for simplicity and scalability. Consequently, there is limited flow awareness to support overload protection mechanisms. Flows are closely related to sessions, which have two possible uses in a QoS scheme: 1) allowing QoS policy to be applied per session, and 2) preventing the establishment of new sessions if they would adversely impact existing ones.

However, the basic requirement here is to provide the appropriate QoS for a service type; there is no reason to suppose that this should be different on a session by session basis (see Note 1). Therefore, a static policy approach has been adopted. The potential downside of this approach is that there is no mechanism to prevent a new session overloading the class and, as a result, the entire class suffers.

NOTE 1 – It is possible for different kinds of IPTV services to be given different QoS treatment. For example, the required QoS treatment for a VoD service would be different from a linear TV service. Also, a video coding scheme chosen by the service provider may have an impact on the required bandwidth as well as other QoS parameters. But from a QoS perspective, all sessions that belong to the same service type (e.g., VoD service) are treated in the same manner.

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

The DNG can support a basic overload protection mechanism which allows a new service instance to be allowed on a trial basis to see whether or not it can be supported without impacting existing traffic. This mechanism works in the following fashion. Within a service class, there is the concept of a recognized and an unrecognized service instance. The simplest way of doing this would be to classify the instance on the basis of the associated IP or MAC address of the IPTV TD. Any packet with the known service class, but unknown instance, would be put into a queue that is different from the recognized instances queue. Each classification rule has an optional pointer to an application layer logic (ALL). For overload protection, the ALL would check if this was a known service instance. If not, it would initiate a procedure which would check (over a relatively short period of time) if this new instance could be accommodated without causing overload as measured by excessive queue length. Further details of this mechanism are given along with the requirements in clause 7.2.3.

NOTE 2 – The text above is imported from clause 5.5.12 of [HGI] with modifications.

7.2 Quality of service requirements

This clause specifies the QoS data path functions which are required to be supported by the DNG, and the QoS management objects which are used to configure QoS policy within the DNG. Core QoS traffic management functions include classification, marking, congestion management, queuing, shaping and egress scheduling.

Figure 7-2 shows a conceptual view of the core QoS traffic management functions as packets are received from the IPI-3 interfaces or from internal DNG sources. Note that this diagram is not meant to determine the implementation structure of the QoS functions nor those of the related data path functions.

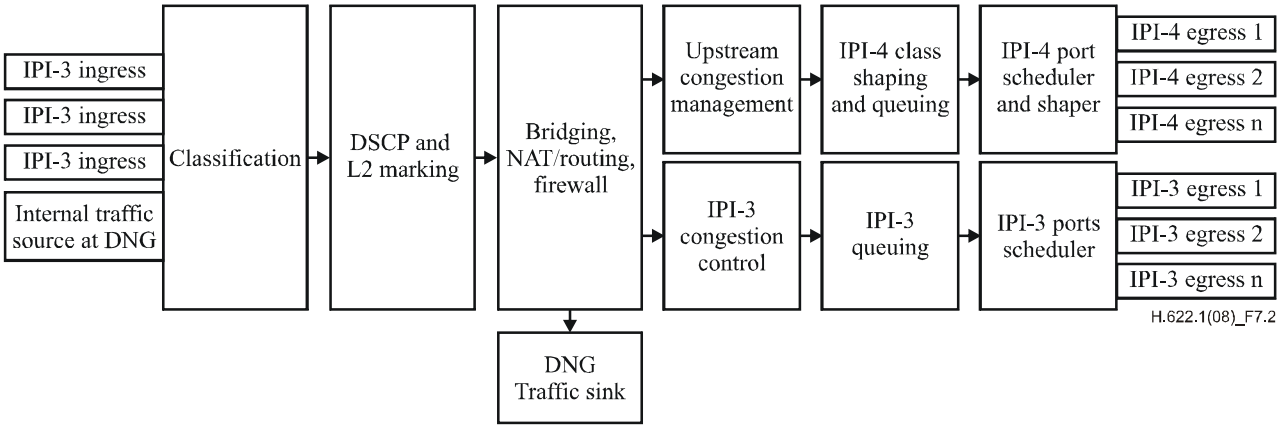

Figure 7-2 – QoS functions from IPI-3 interfaces

Figure 7-3 shows a conceptual view of the core QoS traffic management functions as packets are received from the IPI-4 interfaces. Note that while these are logical IPI-4 interfaces, there is only one physical IPI-4 interface. This diagram is not meant to determine the implementation structure of the QoS functions nor those of the related data path functions.

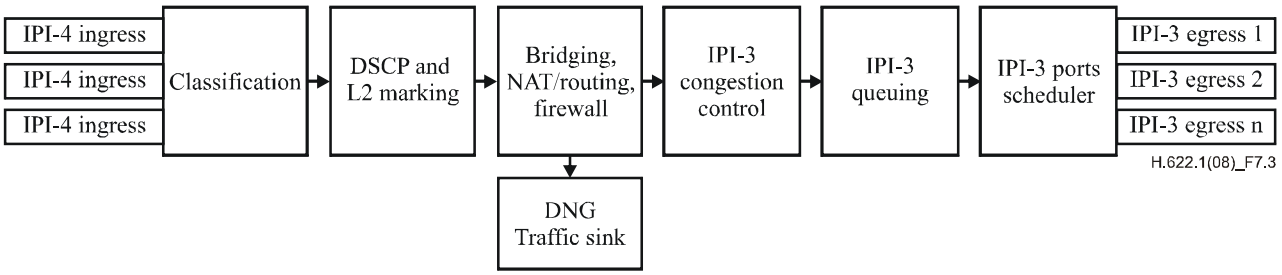

Figure 7-3 – QoS functions from IPI-4 interface

These QoS functions are described below.

NOTE – The text above is imported from clause 6.4 of [HGI].

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

NOTE – The text above is imported from clause 6.4.1 of [HGI].

7.2.1.1 Requirements for classification of packets received upon the IPI-4 interface

The requirements in this clause pertain to packets received upon the IPI-4 interface:

- The DNG is required to classify all packets received on the IPI-4 interface [HGI_R100].
- The DNG is required to be able to set the home network priority level for each packet by setting the DSCP bits on the basis of the classification result [HGI_R101].
- The DNG is required to 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 [HGI_R102].

NOTE 1 – The packet drop in this context refers to an ingress function where packets may be dropped as a direct result of classification:

- The DNG is required to be able to classify packets based upon the relevant classifiers [HGI_R103r1].
- The DNG is recommended to be able to classify packets based upon IP packet size [HGI_R111].
- The DNG is recommended to be able to classify packets on a combination of the IPI-4 interface classification parameters [HGI_R113].

Where Ethernet is present on the IPI-4 interface to connect NT, the following requirements are applied:

- The DNG is required to be able to classify packets based upon Ethernet priority, as defined in [IEEE 802.1D] [HGI_R115].
- The DNG is required to be able to classify packets based upon VLAN ID, as defined in [IEEE 802.1Q] [HGI_R116].
- The DNG is required to be able to classify packets based upon MAC source address [HGI_R117].

- The DNG is required to 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 [HGI_R118].
- The DNG is required to be able to classify packets based upon MAC destination address [HGI_R119].
- The DNG is required to 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 [HGI_R120].
- The DNG is required to be able to classify based upon the Ethernet length/type field [HGI_R121].

NOTE 2 – The text above is imported from clause 6.4.1.1 of [HGI].

7.2.1.2 Requirements for classification of packets received on the IPI-3 interfaces

The following requirements pertain to the classification of packets received on the IPI-3 interfaces which are destined for the AN or are bridged to the HN after multi-field classification. There is an alternative, simpler classification set for locally bridged, transit traffic:

- The DNG is required to classify all packets received on the IPI-3 interfaces [HGI_R124].
- For packets bridged to the HN, the DNG is required to be able to set the home network priority level for each packet by setting the DSCP bits on the basis of the classification result [HGI_R125].
- For packets sent to the WAN, the DNG is required to 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 [HGI_R126].
- The DNG is required to 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 [HGI_R127].
- The DNG is required to be able to classify packets based upon the relevant classifiers (e.g., LAN type, physical port, MAC address, Wi-Fi SSID, IP source/destination address, DSCP, the protocol field in the IP header and TCP/UDP port number) [HGI_R128r1].
- The DNG is recommended to be able to classify packets based upon IP packet size [HGI_R143].
- The DNG is recommended to be able to classify packets received at the IPI-3 interface on a combination of the classification parameters [HGI_R145].

NOTE – The text above is imported from clause 6.4.1.3 of [HGI].

7.2.2 VLAN support at IPI-3 interfaces

The following requirements pertain to VLAN support on an IPI-3 interface:

- The DNG is required not to add VLAN headers to any frames which are transmitted on an IPI-3 interface [HGI_R157].

  The DNG is required to be able to receive VLAN tagged or priority tagged frames on any of its IPI-3 interfaces. Where these frames are locally bridged to the HN, the VLAN ID and priority tag is required to be forwarded unchanged [HGI_R158].

  Where VLAN or priority tagged frames received on the WAN are bridged to the LAN, the VLAN ID and priority tag is recommended to either be forwarded unchanged or removed. This is required to be remotely configurable [HGI_R159].

NOTE – The text above is imported from clause 6.4.2 of [HGI] with modifications.

7.2.3 Overload protection mechanism

The following requirements relate to the overload protection mechanism described in clause 7.1.9. This mechanism serves as an example of overload protection; alternative protection mechanisms may be employed.

The overload protection mechanism utilizes an instance table within the DNG. The instance table is used by the DNG to record instances of services which have been recognized by the relevant classification. The formulation of the instance table is out of the scope of this Recommendation.

- The DNG is recommended to support a mechanism which:
  - i) Differentiates instances of a service on the basis of one or more configured parameters (e.g., IP SA).
  - ii) Creates a service instance table entry for each newly recognized 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 an instance table for each service for which this technique is used.
  - iii) Increments a packet count every time a recognized service instance packet is classified.
  - iv) Performs a real-time check of each service instance packet count against a configurable upper and lower limit (i.e., < InactivePackets per SampleInterval >, < ActivePackets per SampleInterval >).
  - v) Checks whether a configurable queue length threshold (QueueThreshold) has been exceeded during the same SampleInterval time period.
  - vi) When the upper limit is exceeded without the queue length threshold being exceeded, adds a new classification rule 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.
  - vii) When the lower limit is not met, deletes the instance-specific rule from the rules table.
  - 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. [HGI_R177]

NOTE – The text above is imported from clause 6.4.4 of [HGI].

7.2.4 QoS mappings

In case of using class based QoS in which a marker such as DSCP is used for traffic prioritization, each service requiring better QoS treatment needs to be associated with the relevant marking. This requires various considerations including, but not limited to, technical requirements and social importance or recognition. [b-ITU-T Y.1541] gives good guidance for these considerations.

Also, the marking scheme needs to be well aligned with other marking schemes, particularly in case of using different marking techniques in parallel or connecting different network segments using different marking techniques. In this sense, it is important to consider constructing a mapping table giving the association between different mapping schemes. Several documents, for example clause 6.4.5 of [HGI], provide examples and practice of QoS mappings.

QoS mapping is not described in this Recommendation and is for further study.

7.2.5 Class queue structure and scheduling

7.2.5.1 Queuing into the IPI-3 interfaces

The following requirements pertain to DNG's IPI-3 output interface class queue structures and scheduling from those queues into the port level:

- The DNG is recommended to support queuing of data from any source into the IPI-3 output interface (as a result of the classifier) [HGI_R200].
- The DNG is required to implement at least four class queues for each IPI-3 output interface [HGI R201].
- When all strict priority queues are empty, the weighted round robin (WRR) queues (Note 1) are required to be serviced according to their weighting priority [HGI_R207].

NOTE 1 – One of the WRR queues would typically be used for WAN ingress best effort traffic, and the other for transit best effort traffic.

NOTE 2 – The text above is imported from clause 6.4.7.2 of [HGI].

7.2.6 Bridging devices within IP-HN-S and IP-HN-P

The following requirements pertain to the use of priority markings for non-integrated wireless or power line access devices that are connected via Ethernet:

- The wireless or power line device within IP-HN-P or IP-HN-S is recommended to 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 [HGI_R211].
- For packets it sends to the Ethernet, the wireless or power line device within IP-HN-P or IP-HN-S is recommended to translate its native layer 2 marking to DSCP using the correspondence between DSCP and native layer 2 markings [HGI_R212].

NOTE 1 – The text above is imported from clause 6.4.9.1 of [HGI].

The following requirements pertain to the interpretation of priority markings for bridging devices within IP-HN-S and IP-HN-P that are typically bridges and switches:

- Bridging devices within IP-HN-S and IP-HN-P are recommended to determine the QoS treatment by internally translating the received DSCP value to user priority.

NOTE 2 – The text above is imported from clause 6.4.9.2 of [HGI].

8 Security

As home networks are connected to a network function, the home network itself as well as devices connected to it are subject to security attacks that may lead to undesired effects such as loss of IPTV services. Examples of security threats on home networks include denial-of-service (DoS) attacks, malicious software on home network devices and attacks on information that flows or that is stored on the home network device. A DoS attack may make the home network unusable to deliver any services, including IPTV, while malicious software attacks, e.g., viruses on a home network device (e.g., a PC) on the home network may make the device unusable. Attacks on information that is exchanged on a home network or stored in a device on the home network also need to be addressed. If not protected, the information may be compromised, may lead to identity theft and may allow other unauthorized use.

Thus, it is important that security issues in the home network be addressed to ensure a good quality of experience for IPTV end-users.

Refer to the document "IPTV security aspects" [b-ITU-T X.1191] for more details on security issues and requirements in home networks.

8.1 Home network security threats

Home networks that are used to deliver IPTV services have the same characteristics as defined in [ITU-T X.1111]. Thus, security threats identified in [ITU-T X.1111] also apply to home networks supporting IPTV services. For example, if wireless transmission technologies are used, it may lead to eavesdropping, disclosure, modification and interception attacks.

Refer to [ITU-T X.1111] for more details on home network security threats.

8.2 Home network security requirements

The security function for the home network is required to support the following requirements:

- the DNG is required to be authenticated by the management system;
- the DNG authentication is required to be service independent;
- the DNG is required to support a specified list of ALGs, and the list can be upgraded;
- the DNG is required to provide a firewall function which is remotely configurable;
- the DNG is required to provide a unique hardware identifier which can be read remotely;
- pairing is required for wireless devices.

Also, [ITU-T X.1111] identifies requirements for security on the home network based on threats analysis. These requirements also apply to home networks supporting IPTV services.

For detailed information on these security requirements, refer to [ITU-T X.1111].

8.3 Link protection requirements

Some IPTV content is required to be protected on the communication links in the home network. For this purpose, the IPTV TD and HN-TD are required to implement relevant security mechanisms such as encryption and copy protection to protect IPTV contents during transmission between home network devices. Security mechanisms for link protection are recommended to be optionally activated or deactivated for other contents, e.g., user-generated content, when needed.

There are many existing technologies that can be used to protect IPTV content during transmission in the home network. Considering the differences of the home network recognized as the primary and secondary domains, the use of a security mechanism in the home network is heterogeneous. Between the DNG and IPTV TD, the content is protected by the SCP function applied by the service provider as it is applied in the other parts of the public network. Once the content is received at the IPTV TD, another security mechanism (e.g., DTCP [b-DTCP]) is applied for the protection between the IPTV TD and HN-TD. Selecting or recommending a technology for link protection purposes is for further study.

9 Interoperability

9.1 Interoperability between the IPTV access network and home network

9.1.1 Interfaces

Refer to clause 6 for the interface definition.

9.1.2 Protocols

The DNG is connected to the access network and functional entities beyond it by the protocols specified for the IPTV service.

NOTE – The protocols specifically needed for the DNG still need to be identified.

9.2 Interoperability among home network devices

9.2.1 IEC 62481 (DLNA) based devices

The IPTV TD is recommended to support [IEC 62481-1] and [IEC 62481-2] for interconnection with HN-TD devices, such as display devices. The home network area associated with [IEC 62481-1] and [IEC 62481-2] is IP-HN-S (see Note 1).

In this model, the IPTV TD and HN-TD are recommended to work as the DMS and DMP, respectively (see Note 2). It should be noted that there might be a possibility for the IPTV TD to act as a DMP, but this depends upon the implementation.

NOTE 1 – The applicability of IEC 62481 to IP-HN-P and beyond the DNG is for further study. It should be noted that there might be a controversial case where content is distributed beyond the access network.

NOTE 2 – Some types of HN-TD, such as external PVR may act as a DMS.

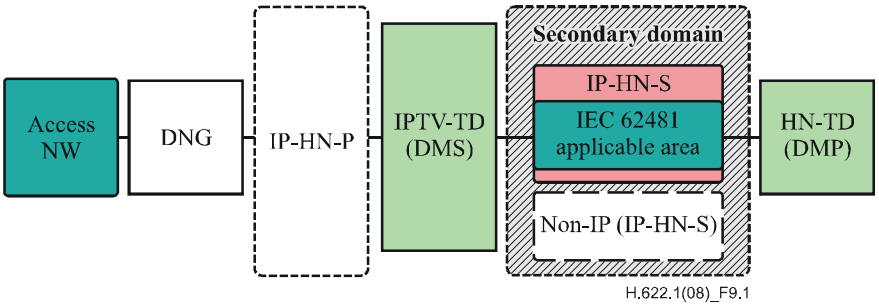

Figure 9-1 – IEC 62481 in the IPTV home network context

The HN-TD connected to the IPTV TD is recommended to be allowed to control the IPTV TD remotely. The control capability includes changing channel of broadcast TV, requesting content provided by VoD, presenting EPG/ECG and managing internal a PVR residing in the IPTV TD (Notes 3, 4, 5).

NOTE 3 – There may be other service cases that are enabled by IEC 62481 or technologies based on it. Further study is needed.

NOTE 4 – There is a possibility that IEC 62481 cannot provide a complete set of functions required for these services. Further analysis on this technology is needed and, if identified, the gap should be filled by the appropriate group/organization.

NOTE 5 – There are some system use cases defined in IEC 62481 such as 2-box pull system usage, 2-box push system usage and so on. The applicable usage cases should be identified in the IPTV context.

9.2.2 UPnP based devices

NOTE – Refer to Appendix II.

10 Delivery network gateway (DNG)

This clause describes the delivery network gateway which may be used in the home network to support IPTV services.

10.1 DNG functional overview

The DNG is an always-on, always-connected device, which acts as the central point for distributing IPTV content in the home network environment. It is supposed that there is only one DNG per household which is connected to a single access network (AN). The use of multiple DNGs and ANs, except the case of using with RF-based broadcasting/cable access network, is for further study.

The DNG is able to monitor and perform actions on IPTV data flows within the home network, as well as on bidirectional communication flows between the home network and the access network. Given the variety of access network technologies, the DNG architecture has to be flexible in terms of providing the support for different IPI-4 interface types, although there will only be one AN connection at a time.

The home network can support a number of home network technologies, but only one DNG manages the whole network.

The DNG is typically not an IPTV service end point. IPTV services terminate on the IPTV TD connected to the DNG through the home network. However, service-specific parameters and functionalities are needed in the DNG to improve efficiency and to enable important features related to provisioning and operations, administration and maintenance (OAM), remote management of the DNG, home network device management, QoS control and security. In addition, the DNG may include built-in features in order to offer local services on the home network or to support terminals not having the necessary functionalities to deliver the service (i.e., legacy TV display used for an IPTV service).

The DNG can be regarded as an expandable system, both from the software and hardware points of view. However, any additional hardware modules will be external, and will be connected to the DNG via one of the integrated IPI-3 interfaces.

NOTE 1 – The text above is imported from clause 5.3.1 of [HGI] with modifications.

NOTE 2 – There are several possible implementations of the DNG device. The clauses above are based on [HGI] with some modifications that are specific to IPTV.

NOTE 3 – [ISO/IEC 15045-1] also provides a generic framework of a DNG device. Annex A describes [ISO/IEC 15045-1] and necessary considerations for IPTV services.

10.1.1 DNG functionalities

The DNG architecture is defined as a set of functionalities, each of which is a task or a set of tasks to be performed through a software program and/or a hardware device/interface/component. The actual detailed requirements for the interfaces and tasks are given in clauses 10.2, 10.3, 10.4, 10.5 and 10.6.

The information flows that need to be handled by the DNG are defined as follows:

- Data flows provide information to the end-user.
- Control flows 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 are related to actions setting up parameters of a more permanent nature than just a communication session and can be related to DNG as a whole and to resources and parameters related to the protocols handled by the DNG itself. OAM information flows are included here.

The interfaces and functionalities of a DNG are described as follows.

IPI-4 interface: The physical interface towards the access network and the functionalities related to the IPI-4 interface at layers 1 and 2. Different types of IPI-4 interface are possible, but only one interface is supported at a time.

IPI-3 interfaces: The physical interfaces towards the home network and the related functionalities at layer 1 and 2. A number of different interfaces $I_1 \ldots I_n$, are included. A distinction needs to be made between the interfaces corresponding to different home network technologies (Ethernet, Wi-Fi, USB, etc.) and service-specific interfaces. The LAN technologies are handled at the lower layers, while any service-specific functions are described in the service support block. For example, Wi-Fi security (WEP/WPA keys and ACL management) function is included here.

Packet processing: This function provides the interconnection functions at layer 2 and/or layer 3 for upstream, downstream and transit traffic. This means it provides relaying, forwarding, bridging, and also NA(P)T functions where appropriate. The internal connection functions also include the routing of IP traffic which is going to, or coming from, the DNG itself (local traffic). This function 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 function does not perform any functions involving an analysis of the packet payload.

Control functions: This function 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 or PPP and signalling protocols) and device discovery inside the home (using DHCP). For credentials acquisition, it has a relationship with the security function.

Security: All functionalities defining policies related to network security are contained in this function. It covers protection for the user from security attacks and intrusions and for the operators from malicious use of the broadband link. Thus, security mechanisms and policies such as firewall rules and authentication handling functions are all defined here.

QoS: This function implements the policies for QoS management in the DNG and the home network, as well as any mapping between the IPI-3 side and IPI-4 side. It contains the rules to perform classification and queuing, and priority field mappings.

Service support: This function contains a limited set of functions to support IPTV services, e.g. multicast.

Management: This function consists of the management communication stacks and the management handling. It contains all the functionality needed to manage DNG itself (configuration, firmware upgrade, QoS and security management, etc.), DNG services (provisioning, troubleshooting) and also devices (device configuration) and services (service configuration) reachable through the DNG.

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

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

NOTE – The text above is imported from clause 5.3.2 of [HGI] with modifications.

10.2 IPI-4 interfaces

A number of possible IPI-4 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 requirements:

- DNG's IPI-4 interface is required to be easily identifiable and separated from the IPI-3 interface(s) [HGI_R1].
- DNG is recommended to support at least one IPI-4 interface [HGI_R2].

In addition to the above requirements identified by HGI, the following requirements are applied for IPI-4 interface for IPTV services:

- IPI-4 interface is required to provide sufficient bandwidth for IPTV services.

The sufficient bandwidth for each channel includes both the required bandwidth for one video stream, which is derived from its resolution and codec, and a sufficiently engineered margin which is supposed to be from 10% to 50% as a provisional value. This margin is used to take into account additional information for IPTV services, such as overhead of packetization, forward error correction (FEC), audio and data services. Further study is needed to establish a better model for the estimation of sufficient bandwidth.

NOTE – It is desirable to provide two or more channels simultaneously over a single link in an access or home network. A required or recommended number of channels is for further study.

10.2.1 IPI-4a interface

The following requirement applies to the IPI-4a interface:

- The DNG, if IPI-4a interface equipped, is recommended to support one of the relevant IPI-4a interfaces as listed below:
  - [ITU-T G.992.5] (Note 1).
  - [ITU-T G.992.1] (Note 2).
  - [ITU-T G.992.3] (Note 3).
  - [ITU-T G.993.2] (Note 4).

NOTE 1 – This Recommendation supports a net data rate ranging up to 16 Mbit/s downstream and 800 kbit/s upstream. Support of net data rates above 16 Mbit/s downstream and support of net data rates above 800 kbit/s upstream are optional.

NOTE 2 – This Recommendation supports a net data rate ranging up to 6.1448 Mbit/s downstream and 640 kbit/s upstream.

NOTE 3 – This Recommendation supports a net data rate ranging up to 8 Mbit/s downstream and 800 kbit/s upstream. Support of net data rates above 8 Mbit/s downstream and support of net data rates above 800 kbit/s upstream are optional.

NOTE 4 – This Recommendation supports a bidirectional net data rate up to 200 Mbit/s.

It is well recognized that the performance of DSL depends on the distance of the DSL modem from the local exchange as well as the physical condition of metallic cable. Also, it should be noted that transmission performance, such as packet loss, is affected by electronic and magnetic noise. Applying the nominal performance metrics mentioned in these Recommendations may be problematic in the consideration of service quality. Further study is needed on the operational condition of DSL as well as operational guidelines for it.

Functional requirements of a non-IPTV nature are defined for each DSL Recommendation. Refer to [HGI] for details.

10.2.2 IPI-4b interface

The following requirements apply to the IPI-4b interface:

- The DNG, if IPI-4b interface equipped, is required to support Ethernet 10BASE-T or 100BASE-TX technology for twisted pair (Cat-5 or Cat-6) [HGI_R32].
- The DNG, if IPI-4b interface equipped, is required to support the related Ethernet protocols at layer 2, with VLAN management (support for untagged frames and IEEE 802.1 Q-tagged frames containing priority-tagged information (IEEE 802.1p) and VLAN-ID information) on the IPI-4 interface [HGI_R33].

NOTE – The above requirements are from [HGI].

10.2.3 IPI-4c for coaxial interface

The following requirement applies to the IPI-4c interface:

- The DNG is recommended to support the relevant interface for coaxial connection with the NT.

10.2.4 IPI-4d for wireless interface

The following requirement applies to the IPI-4d interface:

- The DNG is recommended to support the relevant interface for wireless connection with the NT.

10.2.5 IPI-4e for optical access network

The following requirement applies to the IPI-4e interface:

- The DNG, if it contains an NT function, is required to comply with one of the following optical access networks.
  - [ITU-T G.983.x] (Note 1).
  - [ITU-T G.984.x] (Note 2)
  - [IEEE 802.3] (Note 3).

NOTE 1 – A typical configuration of [ITU-T G.983.x] considered in this list is to provide 622 Mbit/s downstream for up to 32 ONTs. There are other configurations allowed by this series of Recommendations.

NOTE 2 – A typical configuration of [ITU-T G.984.x] considered in this list is to provide 2.48 Gbit/s downstream for up to 32 ONTs. There are other configurations allowed by this series of Recommendations.

NOTE 3 – A typical configuration of [IEEE 802.3] considered in this list is to provide 1.25 Gbit/s downstream, which is decreased to 1 Gbit/s after 8B/10B demodulation, for up to 32 ONTs. There are other configurations allowed by this standard.

In the PON architecture, a maximum number of ONTs connected to a single OLT depends on the operational condition such as distance between OLT and ONT. For example, a longer optical access fibre may require a restriction on branching of optical fibre in order to provide sufficient optical signal to the ONT. This results in a reduced number of ONTs and thus increased bandwidth for each ONT. In such cases, the available service may be different from the table.

As with other point-to-multipoint access networks, reduction of the required total bandwidth for an OLT is possible if the access network entity supports multicast packets. This effect depends on the proportion of multicast traffic to the whole IPTV traffic. Service availability taking into account this effect is for further study.

10.3 IPI-3 interfaces

10.3.1 IPI-3a interface

The following requirement applies to the IPI-3a interface:

- The DNG is recommended to support the relevant IPI-3a interface for a power line home network.

10.3.2 IPI-3b interface

The following requirement applies to the IPI-3b interface:

- The DNG is required to contain an Ethernet [IEEE 802.3] and [ISO/IEC 8802-1] switch for IPI-3b with sufficient bandwidth for IPTV services, with at least two ports. These ports are required to support auto-sensing between full or half duplex, auto-sensing between 10 and 100 Mbit/s, and auto-sensing between MDI and MDI-X [HGI_R39].

10.3.3 IPI-3c interface

The following requirement applies to the IPI-3c interface:

- The DNG is recommended to support the relevant IPI-3c interface for a home PNA.

10.3.4 IPI-3d interface

The following requirement applies to the IPI-3d interface:

- The DNG is recommended to support the relevant IPI-3d interface for a coaxial home network.

10.3.5 IPI-3e interface requirements

If wireless interface is used for IPI-3, the following requirements apply:

- The DNG, when equipped with an IPI-3e interface, is recommended to support one of the IPI-3e specifications listed below.
  - IEEE 802.11a [IEEE 802.11].
  - IEEE 802.11b [IEEE 802.11].
  - IEEE 802.11g [IEEE 802.11].

It is well recognized that the performance of a wireless LAN depends on the operational environment such as the distance between transmitter and receivers and may be unstable for IPTV services. Applying the nominal bandwidth mentioned in these specifications for the consideration of relevancy may be on problematic. Further study is needed for requirements and guidelines on operational conditions of wireless LANs for IPTV services.

Functional requirements of a non-IPTV nature are defined for each wireless LAN specification. Refer to [HGI] for details.

In the following clauses, additional requirements that are needed to support IPTV services are described. Requirements that are not specific to IPTV services can be found in [HGI]

10.4 Packet processing

10.4.1 Support of routed model and extensions – IPI-3 side

10.4.1.1 NAT function

The following requirements apply to the NAT function of the DNG:

- NAT function is required not to interfere with the interaction between the DNG and functions of the service provider network.
- NAT function is required not to prevent interaction between functions of the server provider network and IPTV terminal devices on the home network.

Protocols that are used on interfaces between a service provider network and home network are out of scope of this Recommendation.

10.4.1.2 IPI-3-side DHCP requirements

The following requirements apply to the DHCP server function of the DNG:

- If IPv4 is used in a home network, an IPI-3-side DHCP server is recommended to be available on DNG [HGI_R81].
- If IPv4 is used in a home network, the DNG is recommended to support a means to remotely configure the DHCP server [HGI_R82].

- The DHCP server is required to support fixed IP address allocation to specific device names or MAC addresses to be used in combination with port forwarding or DMZ host [HGI_R85].
- The DHCP server can optionally provide the same IP address to each device [HGI_R86].
- The DNG is required to support the use of public IP addresses (that are within the proper subnet mask defined for the IP connection to the AN) on the HN, and properly route the device traffic [HGI_R88] (Note 1).

NOTE 1 – It is assumed that devices with public IP addresses will be manually configured.

NOTE 2 – The text above is imported from clause 6.3.2.3 of [HGI].

10.4.2 Support of hybrid model and extensions

The following requirements apply to operation of the DNG:

- The DNG is required to support configuring and enabling multiple instances of bridging between WAN side logical interfaces (PVC, VLAN, etc.) and LAN side physical interfaces (Ethernet port, SSID, etc.) [HGI_R90].
- The DNG is required to support configuring and enabling one or more IPI-4 logical interfaces and one or more physical IPI-3 interfaces [HGI_R91].
- The DNG is required to run both bridging and routing simultaneously [HGI_R92].
- The DNG is required to be able to forward traffic to the correct connection in the case of having multiple connections such as multiple PVCs, multiple PPPoE sessions, multiple VLANs, etc. [HGI_R93].

NOTE – The text above is imported from clause 6.3.3 of [HGI].

10.4.3 Session initiation and support

The following requirement applies to operation of the DNG:

- The DNG is required to operate in an "always-on" mode for connections. If a DSL access network is used, the DNG is required not to time out DSL sessions (IP and PPP) and is required to automatically re-establish any sessions after disconnection, lease expiration or loss and restoration of power [HGI_R96].

NOTE – The text above is imported from clause 6.3.4 of [HGI].

10.5 Network services support

The following requirements apply to network services on the DNG:

- A dynamic DNS client is recommended to be provided on the DNG to associate DNG IP address to a user-chosen domain in the DNS system [HGI_R348].
- As an alternative to the above requirement, the dynamic DNS client can optionally be implemented in the management functions [HGI_R349].
- The DNG is required to have a unique hardware ID for authentication and remote management purposes, composed of an organizationally unique identifier (OUI) and serial number [HGI_R350].
- The DNG is required to support a time server client to obtain the time and date [HGI_R351].
- The DNG is required not to implement any explicit function to reset time and date [HGI_R355].

NOTE – The text above is imported from clause 6.6 of [HGI].

10.5.1 Application layer gateway (ALG) functions

The following requirements apply to ALG functions on the DNG:

- The DNG is recommended to support an ALG function to support interoperability with NAT mechanisms; however, the protocols to be used are out of the scope of this Recommendation.
- DNG ALGs are required to be able to be switched off in case of conflicts with external devices using STUN for NAT traversal [HGI_R358].

NOTE – The text above is imported from clause 6.6.1 of [HGI].

10.5.2 Multicast support

The following requirements apply to multicast support on the DNG:

- The DNG is recommended to support IGMP v1/v2 in the IPv4 environment [IETF RFC 2236] or multicast listener discovery (MLD) in the IPv6 environment [IETF RFC 2710].
- The DNG is recommended to support v3 queries function according to [IETF RFC 3376] [HGI_R385].
- If a multicast stream data flow coming from the AN is NOT terminated in the DNG, the DNG is recommended to keep a record of which IPTV-TDs are subscribed to which multicast group [HGI_R386].
- If a multicast stream data flow coming from the AN is NOT terminated in the DNG, the DNG is required to forward inbound multicast packets only to those physical interfaces which are connected to devices that have joined the specific multicast group [HGI_R387].
- If a multicast stream data flow coming from the AN is terminated in the DNG, the DNG is required to 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 [HGI_R388].
- Where there is a multicast stream in the home network, the DNG is required to support a capability to perform a link layer multicast to unicast translation [HGI_R389].

NOTE – The text above is imported from clause 6.6.3 of [HGI].

10.6 IGMP functionality

10.6.1 IGMP proxy

An IPTV TD is recommended to support IGMP proxy for IGMP v2 and IGMP v3. If more than one upstream interface is available (e.g., different VLANs) the following rules apply.

"Simple mode", only one upstream interface for IGMP/multicast: If only one upstream interface needs to support multicast/IGMP, it is recommended, if possible, to select the proxy interface by static configuration or a dynamic mechanism such as a multicast default route using the DHCP option 121 (classless static route option).

"Extended mode", different upstream interfaces for IGMP/multicast: More than one upstream interface needs to support multicast/IGMP (e.g., different service VLANs). In this scenario, the multicast groups/multicast channels need to be configured on the corresponding interfaces; e.g., 239/8 on interface #1 and 232/8 on interface #2. The proxy needs to separate the address spaces, e.g., an IGMP report on interface #1 must not include information about multicast groups/channels on interface #2. The device is required to support a mechanism to configure (assign) the multicast groups/channels to the corresponding upstream interfaces. This can be done by using static configuration (pre-configured device, using a GUI, etc.) or a dynamic mechanism.

"Forking mode": In this mode, IGMP reports are sent to more than one upstream interface. Queries will be answered on all upstream interfaces which are configured for "forking mode"; reports include information about all multicast groups/channels the CPE is subscribed to. It is within the responsibility of the receivers of the membership reports to take action on the received reports. In a standard scenario, only one of the receivers will forward multicast traffic to avoid duplicate traffic. Other network components can act on the membership reports (e.g., change filters or QoS settings) without forwarding the traffic (see Figure 10-1).

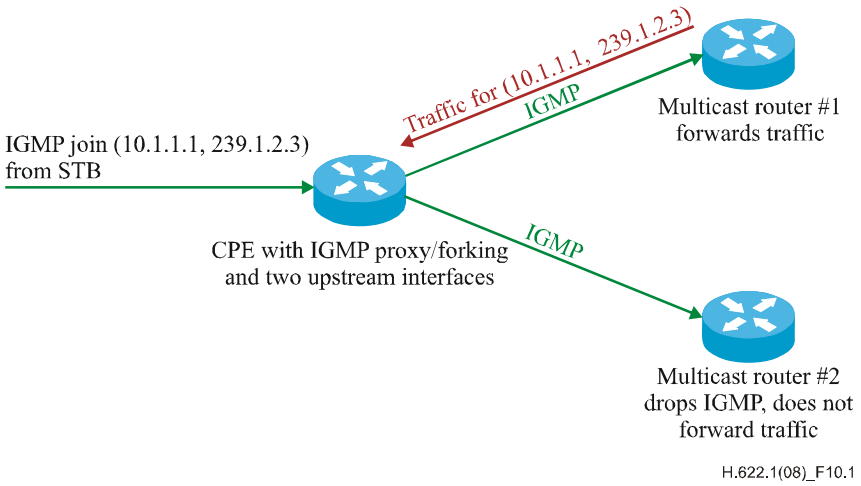

Figure 10-1 – IGMP proxy in forking mode

10.6.2 Source-specific multicast

The proxy is required to support source-specific multicast (SSM) in the standard SSM address range 232/8. SSM is recommended to be supported in other address ranges as well. All IGMP v3 filter modes are recommended to be supported.

10.6.3 Filter

L3 filters for IGMP are recommended to be supported. It is also recommended to allow the exclusion of certain multicast addresses or address ranges from the proxy functionality (e.g., UPnP). Such membership reports are not forwarded to the upstream interface(s) and not reported as answer on an IGMP query from the network. This avoids unnecessary states for multicast groups which have only local relevance. It is also recommended to provide a mechanism to configure the filters (e.g., analogue-to-port forwarding rules or firewall rules).

11 Network management

11.1 Remote management

When IPTV services are deployed, a large number of IPTV terminal devices (IPTV-TDs) will be managed by the service or network provider, and these devices may need to be managed remotely. IPTV services also need to be managed remotely. Thus, it is very important for service or network providers to have a standardized way to remotely manage numerous IPTV terminal devices and IPTV services in an efficient and economical way.

Remote management architecture and functional requirements necessary to build standardized systems for remote management of IPTV terminal devices and IPTV services in the home network are for further study.

11.2 QoS management functions on the DNG

QoS management is a critical network management aspect for ensuring the correct delivery of the services. Definition and mechanisms of QoS management are covered in QoS clauses 7.1 and 7.2.

NOTE – The text above is imported from clause 5.4.2 of [HGI].

11.3 Security management functions on the DNG

Security and privacy are critical issues in home environment management. Most end-users are very concerned about unauthorized access 'into' their home and about the privacy of their data. Therefore, the DNG includes manageable security elements to enhance the confidence of the end-user about these concerns. This mainly concerns the remote management of the firewall and NAT capabilities of the DNG. The user may also wish to have the ability to 'hide' some end devices from the service provider, so that the service provider does not have full visibility of the HN.

NOTE – The text above is imported from clause 5.4.3 of [HGI].

11.4 Performance monitoring and diagnostics, and troubleshooting functions on the DNG

Any DNG system-level fault (e.g., hardware, operating system or software related) can optionally be detected and communicated to the service or network provider. Three scenarios are possible and all are supported:

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

Some examples of faults which need to be detected are:

- Malfunction of hardware modules.
- Malfunction of the main software components of the DNG (to detect failures, partial crashes, etc., that affect the normal operation of the DNG).

NOTE – The text above is imported from clause 5.4.5 of [HGI].

11.5 Local management application for the DNG

In order to provide better support for the DNG, a local management interface may be needed to complement the remote management.

The local management interface is the access method the end-user uses to view or make changes to DNG configuration, end-user managed services, end-user managed devices and other 'safe' settings.

Three levels of management are present in the DNG, with the following precedence (high to low):

- End-user device management functional block can manipulate all managed objects in the DNG, including lower order user rights.
- Administrator management can manipulate objects that do not interfere with end-user device management functional block or managed service operation. It can manage local user access rights (e.g., additional firewall rules, specific NAT for unmanaged devices).
- Users can only manipulate objects when allowed by the administrator (e.g., URL access).

The local user interface access is completely controlled by DNG's firmware itself. This will require access control in order to limit this to a local administrator. The administrator will have the ability to change settings for certain managed services or devices, but general users will only have the ability to view (some of) these managed areas. In Figure 11-1, an overview of the local management interface is provided. On the access network side, the end-user device management functional block

will configure parameters of this interface through the CPE WAN management protocol management interface.

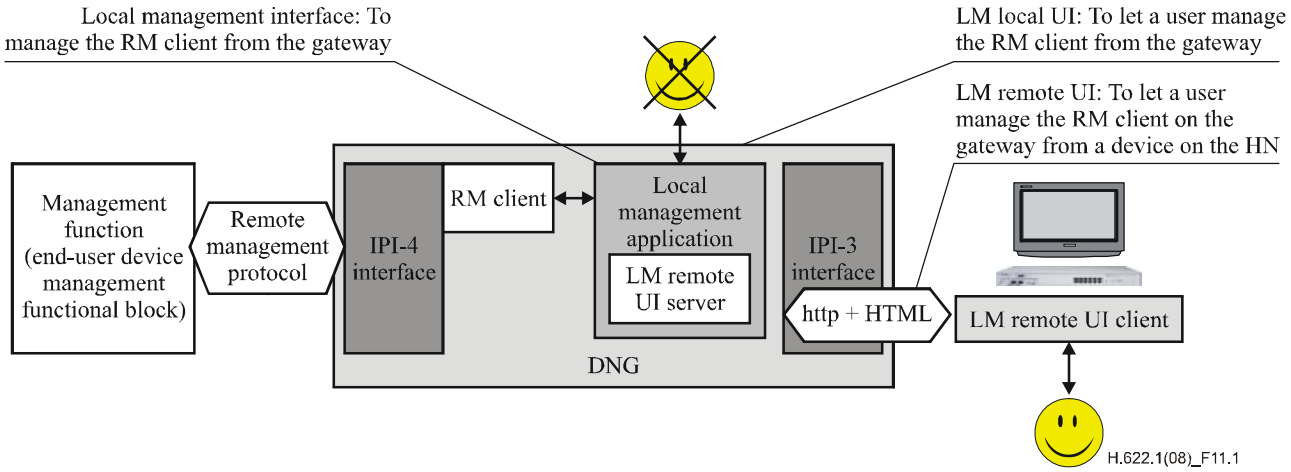

Figure 11-1 – Local management interface overview

In the DNG, a local management remote user interface server (LM remote UI server) will host a web-based local management remote user interface, which can be accessed from any end devices equipped with a browser and located in the HN.

The other possible user interface, the local management local user interface (LM local UI), implies that a user interface is directly accessed on the DNG and therefore the DNG must be able to connect to a display device and some input device (such as an infrared remote control). This is not supported in this Recommendation.

NOTE – The text above is imported from clause 5.4.6 of [HGI].

11.6 IPTV service information report

For operational purposes network management function is recommended to generate and report information regarding IPTV services.

NOTE – Privacy and security of subscribers/consumers should be considered when implementing IPTV service information reporting functionalities.

Annex A

Considerations on ISO/IEC 15045-1 for IPTV services

(This annex forms an integral part of this Recommendation)

A.1 Introduction

[ISO/IEC 15045-1] describes the model and key functions of the DNG. Since the key subject of [ISO/IEC 15045-1] is a generic model applicable to various implementation scenarios, regardless of IP or non-IP environment, some specific considerations are needed for the IPTV service. This annex provides considerations for IPTV-specific issues.

A.2 Comparison of terminology

Since [ISO/IEC 15045-1] is developed by a different standards body, it uses different terminology than that used in this Recommendation. For the convenience of the reader, the following table is provided for comparison of terminology used in both documents.

Table A.1 – Comparison of terminology with [ISO/IEC 15045-1]

[ISO/IEC 15045-1]	Corresponding term	Note
HAN	Home network (HN)	If it means all the networks and entities placed beyond the DNG.
	IP-HN-P	If it means only the network and entities directly connected with the DNG.
	IPI-3 interface	If it specifically means the HN-side interface.
HGI (HAN to gateway interface)	IPI-3 interface	The same term is used for a different meaning (HGI, home gateway initiative).
LAN	Home network	
PAN	Home network	
RG	DNG	
WAN	Access NW	If it means the network and related entities connected to the DNG.
	IPI-4 interface	If it specifically means the AN-side interface.
WGI (WAN to gateway interface)	IPI-4 interface	

A.3 Packet processing and interfaces of the DNG

[ISO/IEC 15045-1] allows the use of both IP and non-IP at the interface, IPI-4 or IPI-3, of the DNG. In the case of IPTV, the network protocol used by the IPTV TD is limited to IP by its definition. Although it is possible to use a non-IP protocol, for example [b-IEEE 1394], beyond the IPTV TD as a part of the secondary domain, as depicted in the architecture, the access and home network around the DNG need to be an IP-based network except in cases where the DNG is incorporated in the IPTV TD. A DNG without IPI-3 and IPI-4, specified in this Recommendation, is not relevant for IPTV services.

The interface and traffic across the DNG is described in clause 5 of [ISO/IEC 15045-1]. The packet processing in the sense of QoS and multicast at the gateway device, which are important aspects for IPTV, is not mentioned in the standard. The technical information relevant for the home network supporting IPTV services is described in clauses 7 and 10. A [ISO/IEC 15045-1] compliant device is also required to meet these requirements.

A.4 Security consideration

In clauses 6 and 7 of [ISO/IEC 15045-1] security issues necessary for the DNG are described. Some considerations are described in the context of remote control of consumer electronic devices from an outside controller. Different from an IPTV TD, some kinds of consumer electronic devices potentially carry a risk caused by physical action that may result in the loss of physical property and, in the worst case, serious damage to the human body. While a security mechanism addressing such risk is important, IPTV requires some additional considerations of, for example, content protection. The risks to which IPTV content and associated information are exposed and the methods addressing them are described in [b-ITU-T X.1191].

In addition to the protection of devices and information, designing a DNG product requires the operational aspects of IPTV services. Limiting types of traffic across the DNG is a way of enhancing the security. However, there is a potential risk of intercepting a necessary packet by such a mechanism. Designing the filtering mechanism requires detailed analysis of IPTV traffic and associated protocols.

Appendix I

An explanation of the layered model for the IPTV home network

(This appendix does not form an integral part of this Recommendation)

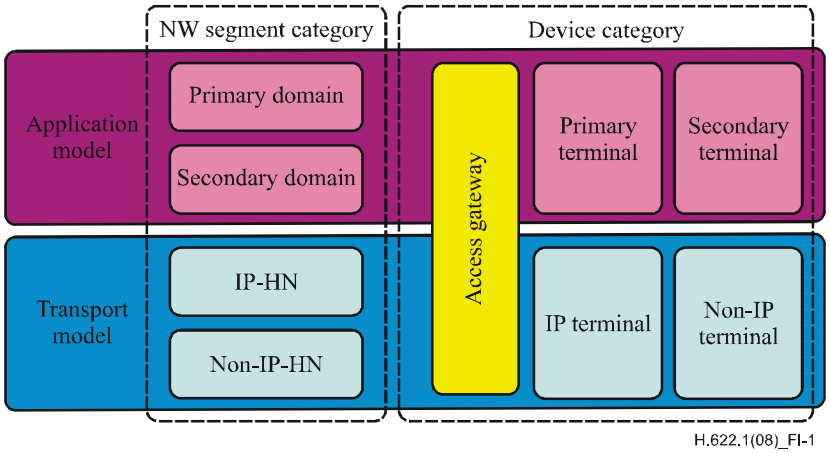

Figure I.1 – Conceptual diagram of the layered model

The layered functional architecture includes two layers represented as models. Those are transport and application models. The detailed descriptions are presented as follows:

a) The **transport model** is responsible for linking the network clients together and transferring the data packets across the network. The transport model described in this appendix corresponds to lower layers of the OSI reference model (basically, the bottom three layers). Thus, it includes the function of the physical layer, data link layer and network layer. The transport model is for further study.

b) The **application model** is responsible for allowing users to interact with the networks, including defining the format of data, designing the service and designing the interface. There are many services at present, such as TV gaming, TV education, linear TV, etc. Providing more IPTV services may help drive users toward widespread use of IPTV, so it is necessary to create more new types of service. The format of data in different services can vary widely, so the design of the data format is an important component of the application functional model. The application model is the main subject of [ITU-T H.622].

Functional components are relevantly defined for each model. These components can be associated with the home network architecture in this Recommendation as shown in Table I.1 below.

Table I.1 – Explanation of components

Architecture of IPTV home network	Application model	Transport model	Note
DNG	DNG	DNG	
Primary domain (IP-HN-P)	Primary domain	IP home network	For IPTV, the primary domain is limited to the IP home network.
Secondary domain	Secondary domain	IP home network or proprietary home network	
IP secondary domain (IP-HN-S)	Secondary domain	IP home network	A part of secondary domain.
Non-IP secondary domain (PR-HN-S)	Secondary domain	Proprietary home network	A part of secondary domain.
IPTV TD	Primary terminal	IP terminal	
HN-TD	Secondary terminal	IP terminal or proprietary terminal	

Appendix II

UPnP-based home network for IPTV services

(This appendix does not form an integral part of this Recommendation)

The UPnP audio/video architecture consists of a media renderer, media server and control point (refer to UPnP A/V architecture document, [b-UPnP DA]).

The media renderer obtains content from the media server and renders it (e.g., displays, decodes). For example, the role of media renderer is playback through a TV set, MP3 player, etc.

The media server is used to make content available on the home network and transfer it to the terminal devices. It supports multiple transfer protocols and data formats and has the functionality to convert from one format to another one in the real time.

The main tasks of the control point are synchronization and management of A/V devices in a home network. It allows an end-user to select, play, pause and stop content from a media server and display it on a media renderer. The control point is able to control the media renderer characteristics, e.g., brightness, contrast, volume, etc. An example of a control point is a TV set with remote control.

All devices that support UPnP should have implemented a basic UPnP terminal device profile.

Additionally, IPTV TD may be compatible with the UPnP specification for the media server in order to locate and transmit content, for instance, to the HN device and other devices in the home network. Content could be selected remotely from the IPTV NW or locally from a hard disk. The end-user has the possibility of recording A/V files by using the UPnP scheduled recording functionality. IPTV TD also works as a control point in order to allow an end-user to select and control content. When the HN IPTV TD works as a standalone device, it should also have media renderer functionality as an option.

An HN device should play the role of media renderer and control point. In that case, the HN device uses content delivered from a media server. The connection between the IPTV TD and HN device is established automatically by using UPnP protocols (e.g., SOAP, HTTP) and based on an XML discovery mechanism. Control point functionality allows the end-user to locate, choose and control content flows from the media server. The transport protocol and data format are chosen automatically depending on which of them are supported by the media renderer. The IPTV end system architecture which uses UPnP is shown in Figure II.1.

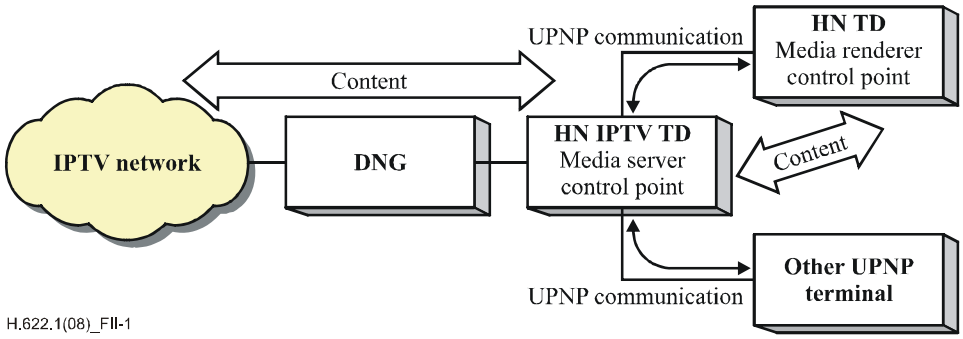

Figure II.1 – UPnP home network architecture for IPTV end system

NOTE – Since UPnP is not qualified under A.5, this issue is described as an appendix. Considering the importance of UPnP, the content of this appendix will be moved into a relevant part of the main body of this Recommendation when the UPnP specification is approved by another organization such as ISO/IEC.

Appendix III

Consideration of retransmission of free-to-air broadcast content

(This appendix does not form an integral part of this Recommendation)

III.1 Middleware aspect

IPTV services can comprise interactive TV applications. [b-ITU-R BT.1699] and [b-ITU-R BT.1722] are Recommendations of harmonization of declarative and procedural content format, respectively, for broadcast content. These Recommendations would enable proper presentation and interactivity for broadcast programme content over IPTV.

III.2 Content protection issue

The following is the consideration for retransmission of free-to-air broadcast content, from the viewpoint of [b-ITU-R BT.1736]:

- Retransmitted free-to-air broadcast content should be handled such as to conform to the content protection assigned by the content provider.

III.3 Privacy protection issue

[b-ITU-R BT.2052] describes overall analysis of an end-user's privacy protection in an interactive broadcast chain. In the case of retransmission of free-to-air broadcast content, clauses 4 through 6 of this report provide useful information on this issue.

III.4 Delivery control of retransmission

In a case where delivery control for retransmission of free-to-air broadcast content is needed, the IPTV system is required to provide such functionality. [b-ITU-T J.281] describes the requirements for similar control.

III.5 Provision of emergency broadcast

Recognizing the need and the importance of emergency broadcasting, ITU-R has developed the Recommendations [b-ITU-R BT.1774] and [b-ITU-R BO.1774]. Support of this function by IPTV systems may be required depending on national regulations.

Appendix IV

Example configurations for an IP-based home network

(This appendix does not form an integral part of this Recommendation)

Figure IV.1 shows an example of a physical configuration of an IP-based home network. Two home network areas, IP-HN-P and IP-HN-S, can overlap physically as shown in the bottom diagram of Figure IV.1. IPTV-TD deals with IPTV-related traffic only. Devices which do not handle IPTV traffic are required to be connected to IP-HN-S.

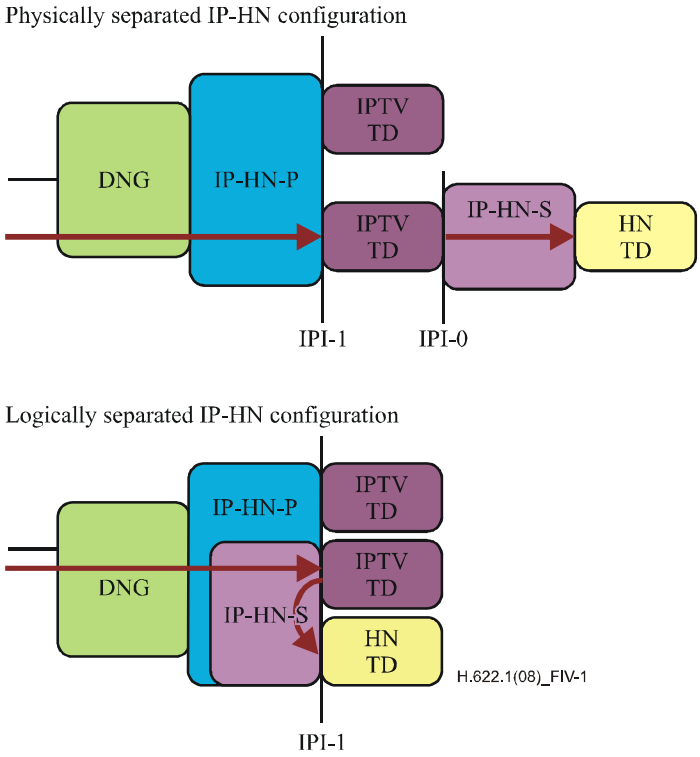

Figure IV.1 – Example configurations for an IP-based home network

Bibliography

[b-ITU-T J.281] Recommendation ITU-T J.281 (2006), *Requirements for multichannel video signal transmission over IP-based fibre network.*
<http://www.itu.int/rec/T-REC-J.281>

[b-ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services.*
<http://www.itu.int/rec/T-REC-Y.1541>

[b-ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects.*
<http://www.itu.int/rec/T-REC-X.1191>

[b-ITU-R BO.1774] Recommendation ITU-R BO.1774 (2007), *Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief.*
<http://www.itu.int/rec/R-REC-BO.1774>

[b-ITU-R BT.1699] Recommendation ITU-R BT.1699 (2005), *Harmonization of declarative content format for interactive TV applications.*
<http://www.itu.int/rec/R-REC-BT.1699>

[b-ITU-R BT.1722] Recommendation ITU-R BT.1722 (2007), *Harmonization of the instruction set for the execution engine for interactive TV applications.*
<http://www.itu.int/rec/R-REC-BT.1722>

[b-ITU-R BT.1736] Recommendation ITU-T BT.1736 (2006), *Broadcasting of redistribution signalling for television.*
<http://www.itu.int/rec/R-REC-BT.1736>

[b-ITU-R BT.1774] Recommendation ITU-R BT.1774 (2007), *Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief.*
<http://www.itu.int/rec/R-REC-BT.1774>

[b-ITU-R BT.2052] Report ITU-R BT.2052 (2005), *Protection of end-users' privacy in interactive broadcasting systems.*
<http://www.itu.int/publ/R-REP-BT.2052>

[b-IEEE 1394] IEEE 1394 (1995), *IEEE standard for a high performance serial bus.*
<http://ieeexplore.ieee.org/xpls/abs_all.jsp?tp=&isnumber=11289&arnumber=526693&punumber=3871>

[b-UPnP DA] UPnP Forum (1999), *Device Architecture 1.0.*
<http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf >

[b-DTCP] Digital Transmission Licensing Administrator (2007), *DTCP Volume 1 Supplement E Mapping DTCP to IP.*
<http://www.dtcp.com/data/info%2020070615%20DTCP%20V1SE%201p2.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009