International Telecommunication Union

ITU-T

IPTV Focus Group Proceedings



2008



ITU-T

IPTV Focus Group Proceedings

2008



Preface

By Malcolm Johnson, Director of the Telecommunication Standardization Bureau, ITU

Two years ago my predecessor Houlin Zhao convened a public meeting to discover what the market need for IPTV standards was. The answer was unequivocally: that ITU should take the lead in coordinating and developing global standards to enable rapid progress and to avoid market fragmentation. As a result, the IPTV Focus Group was established in April 2006.

The completion of 21 deliverables in 20 months is an impressive feat given the breadth of the work and the number of requirements captured. The achievement is testament to commendable hard work and perseverance of Focus Group participants and is an indication of the importance attached to IPTV standardization by industry.

The focus of much of ITU-T's ongoing standards-making activities on Next-Generation Networks is essential to meet the needs of the information driven society. In the context of NGN we see the attractive promise of IPTV to generate multiple revenue streams over the same core network. Indeed IPTV is one of the most highly visible applications to emerge as part of work on the NGN, because it is aimed at consumer entertainment markets. IPTV underlies "multiple play", whereby service providers can offer bundled voice, video on demand, TV, high-speed Internet and other entertainment and communication services over the same basic network. This creates a compelling business case that is one of the principal drivers for accelerated deployment of NGNs.

The results of the work of the IPTV Focus Group will lay the foundation for an area of ICTs that is predicted to attract up to 100 million subscribers in the next three years. It's easy to see why so many of the world's leading ICT companies have been keen to progress this work.

The next phase of ITU's IPTV work – to be called the IPTV-GSI (for global standards initiative) – will focus on speedy preparation of ITU-T Recommendations (standards) based on the output of the Focus Group as well as the detailed protocols necessary. I have every confidence that this work will progress smoothly thanks to the hard work of the Focus Group.

I should mention that the Focus Group profited enormously from collaboration with all ITU-T Study Groups and with other forums and regional standards bodies including the ATIS IPTV Interoperability Forum (IIF), the DSL Forum, the DVB project, ETSI TISPAN and the Home Gateway Initiative (HGI). We are very grateful for this level of cooperation, which can now be seen throughout much of ITU-T's work. Indeed such collaboration, rather than competition, is the key to meeting the needs of this incredibly fast-moving industry.

I am proud to present in this publication the results of the Focus Group, together with information on the future direction of IPTV work in ITU-T, in a readily accessible format. It represents an impressive accomplishment in such a short time. I am sure you will find its contents both interesting and useful.

Foreword

By Ghassem Koleyni, Chairman, ITU-T Focus Group on IPTV

When in April 2006 ITU-T proposed the formation of the focus group on IPTV (FG IPTV), many people needed convincing that it was necessary. Indeed, there was scepticism in some quarters that such a group could progress very far or ever produce anything meaningful. However, thanks to the hard work and dedication of the participants and FG IPTV leaders, we can see that there was no need to worry. FG IPTV produced a large number of high quality documents. We started enthusiastically and persevered to produce what we promised and in fact delivered even better quality documents than many expected, both in content and quality. We are not claiming FG IPTV documents are complete but they certainly carry a high level of content and accuracy. We used the ITU-T Recommendation template, in consideration of the fact that these documents may become Recommendations and thus reducing unnecessary work.

More importantly, we proved to the world that ITU-T is capable of responding to market needs very quickly and can do the job in the most efficient, transparent and professional way. We showed how we can work with other Standards Development Organizations (SDOs) to produce documents worthy of being globally acceptable specifications. As the Director of ITU's Telecommunication Standardization Bureau (TSB) has also mentioned, we opened our arms and sought cooperation and collaboration from all ITU-T and ITU-R study groups and many SDOs and fora such as ATIS IIF, ETSI TISPAN, DVB project, DSL Forum and HGI and many others. We exchanged documents and benefited from things that they have done and where appropriate used existing specifications in order that we did not duplicate existing work.

I should also emphasize the help that we received from TSB. They provided us with all the assistance we required, allowing us to have our documents universally available and also allowing all voices to contribute and participate in our meetings. This was particularly constructive, providing an excellent opportunity for many non-ITU member companies to contribute and send their representatives to FG IPTV meetings.

Last but not least, I would like to acknowledge the contributions of our regional meeting hosts. Gracious hosts from the Korea (Republic of), USA, Slovenia, Japan and Malta helped sponsor five meetings, demonstrating the international nature of our activities and promoting the focus group as a true global organization.

I am happy and proud to have been part of the team which has prepared the content of this publication, and am certain that you, as the reader, will find this publication of interest and value to you and to your work.

TABLE OF CONTENTS

Page

Part I – General 1

1 Overview of FG IPTV 3

2 Overview of working groups activities and achievements 4

2.1 Architecture and requirements (WG 1) 4

2.2 QoS and performance aspects (WG 2) 5

2.3 Service security and content protection (WG 3) 6

2.4 IPTV network control (WG 4) 6

2.5 End systems and interoperability aspects (WG 5) 7

2.6 Middleware, application and content platforms (WG 6) 7

3 IPTV Global Standards Initiative (IPTV-GSI) 9

Annex A: FG IPTV management team 10

Annex B: FG IPTV meetings 12

Annex C: List of FG IPTV deliverables and correspondance with the proceedings part number 13

Annex D: List of editors 15

Annex E: List of participating companies and organizations 17

Annex F: Introduction to ITU-T 19

Part II – Texts of the FG IPTV deliverables 25

II.1 Architecture and requirements 29

II.1.1 IPTV services requirements 29

II.1.2 IPTV architecture 89

II.1.3 IPTV service scenarios 167

II.1.4 Gap analysis 201

II.2 QoS and performance aspects 205

II.2.1 Quality of experience requirements for IPTV services 205

II.2.2 Traffic management mechanisms for the support of IPTV services 237

II.2.3 Application layer error recovery mechanisms for IPTV services 257

II.2.4 Performance monitoring for IPTV 273

II.3 Service security and content protection 311

II.3.1 IPTV security aspects 311

Page

II.4 IPTV network control 363

II.4.1 IPTV network control aspects 363

II.4.2 IPTV multicast frameworks 397

II.4.3 IPTV related protocols 445

II.5 End systems and interoperability aspects 455

II.5.1 Aspects of IPTV end system – terminal device 455

II.5.2 Aspects of home network supporting IPTV services 493

II.6 Middleware, application and content platforms 549

II.6.1 IPTV middleware, application and content platforms 549

II.6.2 Toolbox for content coding 581

II.6.3 IPTV middleware 639

II.6.4 IPTV metadata 653

II.6.5 Standards for IPTV multimedia application platforms 671

II.7 IPTV vocabulary of terms 693

Part I: General

Summary
Part I – General

1 Overview of FG IPTV

2 Overview of working groups activities and achievements

3 IPTV Global Standards Initiative (IPTV-GSI)

Annex A: FG IPTV Management team

Annex B: FG IPTV meetings

Annex C: List of FG IPTV deliverables

Annex D: List of editors

Annex E: List of participating companies and organizations

Annex F: Introduction to ITU-T

IPTV Focus Group

1 Overview of FG IPTV

The TSB Circular Letter 71 of 3 February 2006, the TSB Director's open consultation meeting on IPTV standardization took place in Geneva, 4-5 April 2006. Many experts in the field attended this consultation meeting and highlighted that some of the IPTV services have been deployed or are to be deployed in many countries but all based on ad hoc solution and lacking interoperability, thus the urgent need for creation of set of globally acceptable standards. It was also recognized that many ITU-T study groups have done work or had ongoing work on IPTV related topics; that various regional organizations have already accomplished a lot of work on IPTV; that ITU is an excellent place to initiate, coordinate and harmonize global activities for IPTV standards; that the involvement of other standards development organizations and fora working on IPTV is important; and that the relation between IPTV and NGN needs to be taken into account.

The meeting discussed what would be the most efficient and effective way for ITU-T to move forward (e.g. a focus group, a joint coordination activity, or a joint Rapporteur group). The consensus reached by the meeting was to support the TSB Director to create, according to ITU-T Recommendation A.7, a focus group, the IPTV Focus Group (FG IPTV).

To provide opportunity to small companies, universities and other interested parties, in addition to ITU Member States, Sector Members and Associates, FG IPTV meetings were open to any individual from a country which is a member of ITU who wished to contribute to the FG IPTV work. This included individuals who were members of international, regional and national organizations according to ITU-T Recommendation A.7.

According to ITU-T Recommendation A.7, a focus group should have a parent study group and SG 13 was designated to be the one.

FG IPTV mission statement was:

> *The mission of IPTV Focus Group is to coordinate and promote the development of global IPTV standards taking into account the existing work of the ITU study groups as well as Standards Developing Organizations, Fora and Consortia.*

The FG IPTV also had the following goal:

- Definition of IPTV
  - Identification of scenarios, drivers and relationships with other services and networks
  - Identify requirements and define framework architecture
- Review and gap analysis of existing standards and ongoing works
  - Identification of opportunities for ITU-T
  - Identification of activities that ITU-T would encourage other organizations to pursue
- Coordination of existing standardization activities
- Harmonization of the development of new standards
- Encourage interoperability with existing systems where possible

The FG IPTV management team with tremendous help from the TSB started its work and successfully fulfilled its mandate producing valuable set of documents which were submitted to its parent study group, SG 13.

2 Overview of working groups activities and achievements

In the following sub-clauses a brief description of the mandate and achievements of each Working Group (WG) is provided. Complete text for all deliverables is provided in part II of this document. A brief statement indicating status of each document, as of December 18 2207, is also provided.

NOTE – Complete text of all deliverables are provided in part II of this proceeding.

2.1 Architecture and requirements (WG 1)

Mandate

To define service, user and architectural requirements and framework architecture, considering existing IPTV services and solutions. WG1 considered both non-NGN and NGN environments, through a set of deployment scenarios. Study items included:

- Definition of IPTV services,
- Identification of use cases and architectural requirements from existing IPTV services and deployed solutions, including inter-working considerations from a service convergence perspective,
- Specification of an IPTV service framework architecture, further instantiated into non-NGN and NGN environments,

Accomplishments

WG1 activities concentrated on defining and describing IPTV services requirements, IPTV framework architecture (NGN and non-NGN) and IPTV service scenarios. WG1 specification was driven by a systemic, IPTV service-wise approach, based upon practical experience and global expertise. WG1 received 474 contributions and produced four documents.

Deliverables

IPTV Services Requirements

The IPTV services requirements document provides a list of requirements that have been elaborated according to an IPTV service-wise, global and systemic approach. These requirements have been organized according to a functional taxonomy (*e.g.* QoS requirements, security requirements, middleware requirements, *etc*.), and further classified into required, recommended and optional requirements.

IPTV Architecture

This document describes the IPTV functional architecture intended to support IPTV services based on the IPTV service requirements and definitions. Starting from a basic description of IPTV players, roles and services, a high level IPTV functional model is outlined. This model is then developed into a set of functional architectures which support NGN and non-NGN transport networks, as well as operation modes with or without IMS.

IPTV service scenarios

The IPTV service scenarios document provides a list of IPTV use cases that are meant to illustrate how IPTV services can be designed, deployed and operated. From this perspective, use cases have been classified according to an IPTV service taxonomy that includes (but is not limited to) on-demand services, advertising services and broadcast services.

2.2 QoS and performance aspects (WG 2)

Mandate

Develop global QoS and performance specifications necessary to ensure end-user satisfaction, and acceptance, for IPTV services. Identify and assess the suitability of existing material relating to end-to-end QoS and QoE for IPTV, including (but not limited to) the following aspects:

- End-user performance expectations, including those for users with disabilities, and associated metrics for audio/video quality and control functionality
- QoS/QoE monitoring methodologies
- Traffic management considerations (e.g. admission control, priority, etc.)
- Reliable service delivery and network operation

Accomplishments

WG2 championed and promoted the development of global QoS and performance standards necessary to ensure high end-user satisfaction, and hence high end-user acceptance, for IPTV services. WG2 received 188 contributions and produced four documents.

Deliverables

Quality of Experience Requirements for IPTV Services

This document defines user requirements for Quality of Experience for IPTV services. The QoE requirements are defined from an end user perspective and are agnostic to network deployment architectures and transport protocols. The QoE requirements are specified as end-to-end and information is provided on how they influence network transport and application layer behaviour. QoE requirements for video, audio, text, graphics, control functions and meta-data are provided.

Traffic Management Mechanisms for the Support of IPTV Services

This document describes a set of traffic management mechanisms which are aimed to facilitate the efficient support of IPTV services over the network infrastructure. Traffic management mechanisms for the home, access, and core networks are discussed. The network supporting IPTV services will span a number of network domains which may be designed, deployed and operated by different providers and which may differ in their traffic management capabilities. Therefore, it is expected that the network provider(s) will implement a subset of these mechanisms to ensure IPTV service objectives are satisfied efficiently. Furthermore the traffic management mechanisms also depend on the specific network architectures used for IPTV services as defined in the IPTV architecture specification. The document further provides mappings of IPTV service components to the IP network QoS classes defined in ITU-T Y.1541.

Application layer error recovery mechanisms for IPTV Services

This document describes specific mechanisms and the applicability of these mechanisms to IPTV services and network conditions, and provides recommendations and guidance on their use. It has been determined that with the use of these mechanisms, consumer television quality can be achieved using the standard Y.1541 QoS Classes 0 and 1.

Performance monitoring for IPTV

This document defines monitoring points, monitoring parameters and monitoring methods for IPTV services. It covers both network and service related performance monitoring parameters from the physical up to the application layers.

2.3 Service security and content protection (WG 3)

Mandate

Address the urgent needs for globally accepted IPTV security standards as the market demands. Define the security architecture, identify and if necessary initiate the development of the security mechanisms and interface specifications for IPTV.

Accomplishments

WG3 focused on addressing the urgent needs for globally acceptable IPTV security standards as the market demands. It identified security requirements, defined the security architecture and described security mechanisms to satisfy the Business & Security requirements for the IPTV system architecture. WG 3 received 122 contributions and produced one document

Deliverables

IPTV Security Aspects

This document addresses threats, requirements, architecture, and mechanisms that pertain to security and protection aspects of IPTV content, services, networks, terminal devices, and subscriber (end-users).

2.4 IPTV network control (WG 4)

Mandate

This working group focused on following areas:

- Naming, addressing, and identification aspects
- Control and signalling mechanisms
- Content distribution and data plane aspects
- Access & Home network issues

Accomplishments

WG 4 focused on specifying detailed functional requirements of network control and multicast capability. It described various aspects of IPTV network control. It also described functional requirements and frameworks for supporting multicast capabilities in terms of IPTV network control. Finally identified protocols relevant to IPTV services and categorized these protocols relative to their specific functions in relation to IPTV services. WG 4 received 178 contributions and produced three documents.

Deliverables

IPTV Network Control Aspects

This document describes various aspects of IPTV network control. It provides a list of detailed requirements to address control and signalling matters related to authentication and authorization, content delivery, consumer domain attachment and initialization, quality of service (QoS), quality of experience (QoE) and security.

IPTV Multicast Frameworks

This document on IPTV multicast frameworks describes functional requirements and frameworks for supporting multicast capabilities in terms of IPTV network control.

IPTV Related Protocols

This document identifies protocols relevant to IPTV services and categorizes these protocols relative to their specific functions in relation to IPTV services.

2.5 End systems and interoperability aspects (WG 5)

Mandate

- Identify relationship between IPTV End System & Home Network
- Investigate basic functional architecture of the IPTV terminal.
- Provide basic functional architecture of the home network

Accomplishments

WG5 scope included IPTV terminal devices and the home network which would support IPTV services. It provided Terminal Device and Home Network architectures, and identified interfaces and service/functional requirements in harmonization with other ITU-T study groups and other SDos. The home network activities were based most significantly on the HGI work. WG5 progressed particularly in the area of defining and describing the basic framework and architecture for a Home Network, as well as defining and describing the many interfaces between different devices within a home network. WG 5 received 109 contributions and produced two documents.

Deliverables

Aspects of IPTV End System – Terminal Device

This document outlines functional requirements of the terminal device, capabilities expected to be supported by the terminal device, and the terminal device architecture.

Aspects of Home Network supporting IPTV services

This document addresses the home network architecture aspects in the context of IPTV.

2.6 Middleware, application and content platforms (WG 6)

Mandate

Identify and define middleware platforms, including applications, content formats, and their uses, that facilitate effective and interoperable use of an IPTV system for presenting and interacting with IPTV services. In particular:

- to identify the use cases and requirements of these Service aspects;
- to review and analyze existing standards to find any gaps seen against the requirements of these Service aspects;
- to coordinate, harmonize and encourage interoperability among such existing systems and standards for these Service aspects.

Accomplishments

WG 6 identified and defined middleware platforms, including applications, content formats, and their uses to facilitate effective and interoperable use of an IPTV system for presenting and interacting with IPTV services. It studied aspects of services which were relevant to discovery, navigation, selection, acquisition, delivery and presentation including interaction, of content. WG 6 received 183 contributions and produced five documents.

Deliverables

IPTV Middleware, Applications and Content Platforms

This document identifies and defines middleware platforms, including applications, content formats, and their uses, that facilitate effective and interoperable use of an IPTV system for presenting and interacting with IPTV services. This document is a general document for IPTV middleware, application and content platforms. It describes content provisioning, service discovery, channel and content identification and location resolution, and profiling. This document refers to text on middleware, content coding, metadata, which can be found in other documents.

Toolbox for content coding

This document addresses the use of video and audio coding in services delivered over Internet Protocols (IP). It describes the use of H.264/AVC video, VC 1 video, AVS video, HE AAC v2 audio, HE AAC v2 audio, Extended AMR WB (AMR WB+) audio, and AC-3 and Enhanced AC-3 audio. In addition, this document describes the use of speech codecs within an IPTV environment and the specified codecs for this use. This document adopts a "toolbox" approach for the general case of IPTV applications delivered directly over IP and MPEG2 -TS. This document is not a specification for the use of Audio and Video Codec's for use in IPTV Services.

IPTV Middleware

This document identifies those aspects of architecture specific to IPTV middleware and describes the various functions with explanatory definitions where appropriate.

IPTV Metadata

This document gives the overview of the metadata for IPTV services and describes its elements and delivery protocols, identifying relevant standards. The IPTV metadata, the information on services and contents processed by the service and content delivery infrastructure, provides descriptive and structural framework for managing IPTV services. Aspects of transport, representation, content provisioning, and security of metadata are covered.

Standards for IPTV Multimedia Application Platforms

This document identifies and analyzes the relevant standards for IPTV multimedia application platforms.

3 IPTV Global Standards Initiative (IPTV-GSI)

In accordance with decisions taken at the April 2007 meeting of Study Group 13 the work of the IPTV Focus Group ended and its documents were transferred to the appropriate study groups via Study Group 13 for the development of draft Recommendations based on the focus group outputs as appropriate and for the continuation of the work on the unfinished topics.

Based on proposals developed by the chairman of Study Group 13 and the chairman of the IPTV Focus Group and endorsed by TSAG the ongoing work will be carried out under the umbrella of a Global Standards Initiative (the IPTV-GSI). The ongoing work on the outputs from the IPTV Focus Group will be done by the study groups (based on allocations developed by the IPTV-JCA) with coordinated planning of the activities and through co-located meetings of the involved Rapporteur groups to progress certain areas of the work as appropriate.

As part of the establishment of the IPTV-GSI, the membership of the IPTV-JCA is being extended to include other standards organizations involved with ITU-T in the IPTV work stemming from the results of the IPTV Focus Group. Also an IPTV-GSI Technical and Strategic Review (TSR) process has been set up. This will operate at every IPTV-GSI event (Study Group meetings and co-located rapporteur meetings) and will bring to the IPTV-JCA any issues requiring guidance or recommendations for action, e.g., concerning work allocation. Mr Ghassem Koleyni (Nortel Networks, Canada) was appointed as the TSR coordinator.

Annex A: FG IPTV management team

Working group 1
Architecture and requirements


Mr Junkyun CHOI
(Korea)


Mr Christian JACQUENET
(France Telecom)


Mr Julien MAISONNEUVE
(Alcatel-Lucent)

Working group 4
IPTV Network control


Mr Shin-Gak KANG
(ETRI)


Mr Daegun KIM
(Korea Telecom)

Mr Jifei SONG
(UTStarcom)


Mr Naxin WANG
(UTStarcom)

Chairmanship


Mr Ghassem KOLEYNI
(Nortel)
Chairman


Ms Duo LIU
(CATR)
Vice-Chairman


Mr Simon JONES
(BT)
Vice-Chairman


Mr Chae-Sub LEE
(ETRI)
Vice-Chairman

Working group 2
QoS and performance aspects


Mr Paul COVERDALE
(Huawei)


Mr Juergen HEILES
(Nokia Siemens Networks)

Working group 5
End systems and interoperability aspects


Mr Yoshinori GOTO
(NTT)


Mr Gale LIGHTFOOT
(Scientific Atlanta)


Mr Jianting MENG
(China Telecom)

Working group 3
Service security and content protection


Mr Glenn ADAMS
(Samsung Electronics)


Ms Catherine PERGUE
(Dell)


Mr Dong WANG
(ZTE)

Working group 6
Middleware, application and content platforms


Mr Masahito KAWAMORI
(NTT)


Mr Charles SANDBANK
(Commstel)

Annex B: FG IPTV meetings

Table B-1: Meetings dates and locations

Meeting	Date	Location
First	10-14 July 2006	Geneva, Switzerland
Second	16-20 October 2006	Busan, Republic of Korea
Third	22-26 January, 2007	Mountain View, USA
Fourth	7-11 May 2007	Bled, Slovenia
Fifth	23-31 July 2007	Geneva, Switzerland
Sixth	15-19 October 2007	Tokyo, Japan
Seventh	11-18 December 2007	Qawra, St Paul's Bay, Malta

Table B-2: General meetings statistics

	July 2006	Oct 2006	Jan 2007	May 2007	Jul 2007	Oct 2007	Dec 2007	Total*
Attendees	150	208	192	163	158	247	125	1243
Countries	21	18	16	15	20	16	20	40
Contributions	80	148	169	184	216	183	121	1101
Incoming Liaison statements	18	25	27	20	26	17	11	144
Outgoing Liaison statements	8	18	18	18	19	16	16	113
* Except for the number of countries which is unique, all other numbers are sum total								

Annex C: List of FG IPTV deliverables and correspondance with the proceedings part number

Table C-1: List of documents produced by FG IPTV

WG	Document number	Title	Part No.
1	FG IPTV-DOC-0147Rev 1	IPTV services requirements	II.1.1
1	FG IPTV-DOC- 0181	IPTV architecture	II.1.2
1	FG IPTV-DOC- 0182	Service scenarios for IPTV	II.1.3
1	FG-IPTV-DOC-0183	Gap analysis	II.1.4
2	FG IPTV-DOC- 0184	Quality of experience requirements for IPTV	II.2.1
2	FG IPTV-DOC- 0185	Traffic management mechanism for the support of IPTV services	II.2.2
2	FG IPTV-DOC- 0186	Application layer reliability error recovery mechanisms for IPTV	II.2.3
2	FG IPTV-DOC- 0187	Performance monitoring for IPTV	II.2.4
3	FG IPTV-DOC- 0188	IPTV security aspects	II.3.1
4	FG IPTV-DOC- 0189	IPTV network control aspects	II.4.1
4	FG IPTV-DOC- 0190	IPTV multicast frameworks	II.4.2
4	FG IPTV-DOC- 0191	IPTV related protocols	II.4.3
5	FG IPTV-DOC- 0192	Aspects of IPTV end system – terminal device	II.5.1
5	FG IPTV-DOC- 0193	Aspects of home network supporting IPTV services	II.5.2
6	FG IPTV-DOC- 0194	IPTV middleware, applications, and content platforms	II.6.1
		Service navigation systems	II.6.1 Appendix IV
6	FG IPTV-DOC- 0195	Toolbox for content coding	II.6.2
6	FG IPTV-DOC- 0196	IPTV middleware	II.6.3
6	FG IPTV-DOC-0197	IPTV metadata	II.6.4
6	FG IPTV-DOC-0198	Standards for IPTV multimedia application platforms	II.6.5
PL	FG IPTV-DOC-0199	IPTV vocabulary of terms	II.7

Annex D: List of editors

Working Group 1 – Architecture and requirements

Ms Hanane BECHA, Nortel Networks

Mr Jincheng LI, Huawei

Mr Mingdong LI, ZTE

Mr Clive MILLER, Royal National Institute of Blind People, UK

Ms Hyo Jin PARK, ICU

Mr Kai WEI, CATR

Working Group 2 – QoS and performance aspects

Mr Osama ABOUL-MAGD, Nortel Networks

Mr Thomas STOCKHAMMER, Digital Fountain

Mr Akira TAKAHASHI, NTT

Mr Kenneth TONEY, Tektronix

Mr Danny WILSON, Pixelmetrix Corporation

Mr Ning ZONG, Huawei

Working Group 3 – Service security and content protection

Ms Wei XIE, CATR

Mr Weijun LEE, ZTE Corporation

Working Group 4 – IPTV Network control

Ms Linli LU, Alcatel Shanghai Bell

Mr YoungHwan KWONN, ICU

Mr Michael Chen MA, UTStarcom.

Mr Juyoung PARK, ETRI

MrYeong-il SEO, KT

Mr Michael R. SHANNON, Scientific Atlanta

Mr Peilin YANG, Huawei

Mr Ning ZONG, Huawei

Working Group 5 – End systems and interoperability aspects

Mr Yoshinori GOTO, NTT

Mr Gale N. LIGHTFOOT, Jr., Scientific Atlanta

Mr Jianting MENG, China Telecom

Mr Nhut NGUYEN, Samsung Electronics

Mr Michael SHANNON, Scientific Atlanta

Working Group 6 – Middleware, application and content platforms

Mr Damien ALLIEZ, NDS France

Mr Mathias BENDULL, Coding Technologies

Mr Christian BERTIN, France Telecom

Ms Kyunghee JI, TVSTORM

Mr Richard NICHOLLS, Dolby Laboratories

Mr Menghua TAO, China Netcom Group

Mr Quan WANG, UTStarcom

Mr Yasuaki YAMAGISHI, Sony

IPTV Vocabulary of terms

Mr Ghassem KOLEYNI, Nortel Networks

Annex E: List of participating companies and organizations

Abtin Technologies, Iran
Aethra, Itay
Agere Systems
Alcatel-Lucent
Alcatel Shanghai Bell
Alticast, Korea
AT&T
ATIS
AVS
Bangladesh National Press News
BellSouth
BT
C&M Communication
Cable Labs, USA
Calix
CATR
China Mobile Communications
China Network
China Netcom Group
China Telecom
Cinea
Cisco
Coding Technologies GmbH
Comverse Network Systems
ContentGuard, USA
Dell
Deutsche Telekom
Digital Fountain
Dolby Laboratories
Dongeui University
DRM Inside
EBU/UER
ECI Telecom Ltd.
Egypt Telecoms Regulatory Authority
Envivio
Espial Group
ETRI
Expway
Federal Network Agency, Germany
Fondazione Ugo Bordoni
France Telecom
Freescale Semiconductor
Fucapi
Fujitsu
Hanaro Telecom
Hankuk University of Foreign Studies, Korea
Hanoratelecom
Harris Corporation
Hitachi
Huawei Technologies
HUFS, Korea
ICL/ITRI
Information and Communication University, Korea
IEEE BTS/CRC
Ima-Norway/Telenor
Intel, Japan
Intelsat LLC
Iskratel, Slovenia
ITRI International
ITU Association of Japan
Japan Broadcasting Corporation
Japan Cable Laboratories
Japan Cable & Telecom Association
Juniper Networks
JCU
Kangwon National University, Korea
KDDI Corporation
KNK-MPEG.COM
Korea University
KT
LG Electronics
LG-Nortel
LM Ericsson
Matsushita Electric Industrial/Panasonic, Japan
MIC, Japan
Microsoft

MII, China
Ministry of Information and Communication, Korea
Ministry of Competitiveness & Communications, Malta
Mitsubishi Electric
Motorola
Myongi University, Korea
NDS Technologies France
NEC
Netopia
Net one Systems, Japan
Net & TTV, Korea
Nikkei Business Publications, Japan
Nikkei Communications
Nippon Television Network Corporation
Nissho Electronics Corp.
NICT
Nihon Minkan Hoso Renmei
Nippon Television Network Corporation
Nokia Siemens Networks
Nortel Networks
NSU, Korea
NTT
NYK Line, Japan
Oki Electric Industry
Oman TRA
Orca Interactive
Peking University
Pixelmetrix Corporation
Plala Networks
Pluton House/RNIB
QoSmetrics
Quality Broadband, Japan
Quantum Leaps, Japan
Radvision
Republic Telecommunication Agency, Serbia
Rohde & Schwarz
Royal National Institute of Blind People, UK
Samsung Electronics
SCAT (Support Centre for Advanced Telecommunications), Japan
Scientific Atlanta
SHARP
Softbank BB, Japan
Sony
Sumitomo Electric
Sun Microsystems
Symmetricom
Tanzanian Communication Regulatory Authority
Tektronix
Telchemy
Telecom Italia
Telekom Austria
Telekomunikacja Polska
Texas Instruments
Think and Tech
Thomson
Tokyo Broadcasting System
Toshiba
Tsinghua University
TTA
TTC
Turk Telekom
TV Storm
University of Applied Sciences, Switzerland
University of Ljubljana
UTStarcom
Verivue
Verizon Technology
Waseda University, Japan
Widevine Technologies
XFSI
Yonsei University
ZTE Corporation

Annex F: Introduction to ITU-T

ITU: A Short History

On 17 May 1865, after the first International Telegraph Convention was signed in Paris by 20 founding members, the International Telegraph Union (ITU) was established.

In 1947, after the Second World War, ITU held a conference in Atlantic City with the aim of developing and modernizing the organization. The newly created United Nations recognized ITU's specific competencies and the organization became a UN specialized agency.

- 1837 Invention of the first electric telegraph
- 1844 Samuel Morse sent his first public message over a telegraph line between Washington and Baltimore
- 1865 17 May Foundation of the International Telegraph Union by twenty States with the adoption of the first Convention. First Telegraph Regulations.
- 1876 Alexander Graham Bell patents his invention of the telephone
- 1924 Paris – Creation of CCIF (International Telephone Consultative Committee)
- 1925 Paris – Creation of CCIT (International Telegraph Consultative Committee)
- 1927 Washington – Creation of the CCIR (Intl. Radio Consultative Committee)
- 1932 Madrid – Plenipotentiary Conference. Telegraph Union changes name to International Telecommunication Union
- 1947 ITU became a Specialized Agency of the United Nations
- 1956 Geneva – CCIF and CCIT merged into CCITT (International Telegraph and Telephone Consultative Committee)
- 1992 Geneva – Plenipotentiary Conference. Creation of 3 Sectors: ITU-T replaces CCITT, ITU-R replaces IFRB, CCIR, and ITU-D replaces TCD

Figure F-1 – History

In 2004 ITU was named as one of the world's top ten most enduring institutions by a panel of distinguished scholars from universities across the United States. The awards were announced by Booz Allen Hamilton, a global strategy consulting firm, in order to celebrate institutions that "have reinvented themselves time and again – and remained market leaders – as the unique circumstances of their founding have given way to changing conditions."

ITU provides an essential forum without which the global telecommunications network (including the Internet) of today could not have been realised and the next generation network (NGN) would remain an unfulfilled dream.

ITU Today

The main work of ITU is divided between three Sectors, namely:

- the Radiocommunication Sector (ITU-R);
- the Telecommunication Development Sector (ITU-D);
- the Telecommunication Standardization Sector (ITU-T).

ITU-R plays a vital role in the management of the radio-frequency spectrum and satellite orbits, finite natural resources which are increasingly in demand from a large number of services such as fixed, mobile, broadcasting, amateur, space research, meteorology, global positioning systems, environmental monitoring and, last but not least, those communication services that ensure safety of life at sea and in the skies.

ITU's Telecommunication Development Bureau has well-established programmes of activities to facilitate connectivity and access, foster policy, regulatory and network readiness, expand human capacity through training programmes, formulate financing strategies and e-enable enterprises in developing countries.

ITU-T ensures the efficient and on-time production of high quality standards covering all fields of telecommunications on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services.

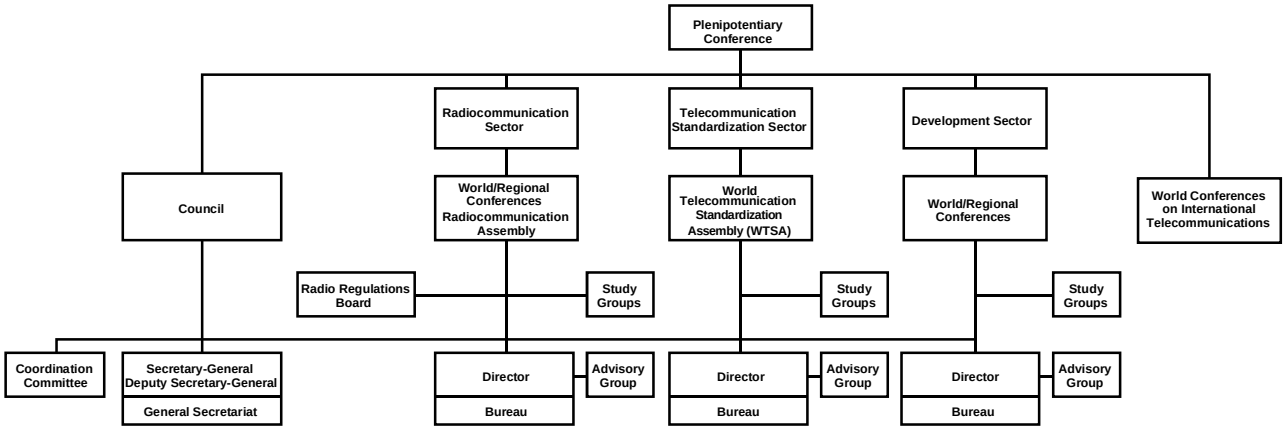


Figure F-2 – The Structure of ITU

What does ITU-T do?

The Telecommunication Standardization Sector (ITU-T) of ITU is the premier **International Platform for the Creation of Standards for Information and Communication Technologies (ICT)**. Nearly 3000 ITU standards (in ITU parlance, ITU-T Recommendations), are in place and **form the backbone of the world's communications systems, ranging from fixed-telephony through mobile telephony to the Internet.**

ITU-T provides a unique environment open to all – private and public sector – in which standards are built to meet the demands of the fast moving ICT industry. Currently, besides the 191 Member States, ITU-T comprises some 450 Sector Members from the private sector including service/network providers, manufacturers, regulators, research and development institutions, universities, regional/international telecommunication organizations, forums, consortia etc. ITU-T produces standards that are a fair representation of its members' concerns using a consensus based voting system.

"The functions of the Telecommunication Standardization Sector shall be, bearing in mind the particular concerns of the developing countries, to fulfil the purposes of the Union relating to telecommunication standardization,… by studying technical, operating and tariff Questions and adopting Recommendations on them with a view to standardizing telecommunications on a worldwide basis."

Chapter III, Article 17, the ITU Constitution.

The work of ITU-T fosters seamless interconnection of the world's communication network and systems. And moving forward, ITU-T is already playing a leading role in shaping the next generation of ICT.

International standards for ICT are growing in importance not only because of globalization but also because the ICT sector is one of the pillars in today's economy. Whether we exchange voice, data or video messages, communication cannot take place without standards linking the sender and the receiver such as Q.708, E.164, E.212, H.262, H.264, X.509, X.805, J.112, G.711, H.323, T.30, T.80, T.800, etc. The telephone network, arguably one of the most complex projects ever undertaken, is based on a myriad of standards, and ITU's work was instrumental in its creation. ITU's work has also been one of the key enablers of the rapid growth of the two most recent telecommunication technologies: mobile telephony and Internet.

ITU-T Recommendations aim to create a world of ICTs that work together, where innovation is encouraged, and not stifled by restrictive proprietary environments. Network interoperability is a key concern for service providers who don't want to be locked into the equipment of one manufacturer and need the reassurance that as they move to more converged services all network elements will work together. Consumers want the reassurance that products that they buy will work with other products – reassurance that only products produced using standards can offer.

ITU-T aims to continue to be recognized as the pre-eminent worldwide telecommunication standards body. In recognition of the rapidly changing ICT environment, ITU-T has been changing its procedures and practices to ensure that it can respond quickly to the demands of the industry. The Alternative Approval Process (AAP) introduced in 2000 has been a tremendous success, with the majority of new Recommendations being approved within six weeks of completion.

	Before 1988	**1989-1993**	**1993-1996**	**1997-2000**	**2001-2004**
Approval time	4 years	2 years	18 months	9 months (exceptional case: 5 months)	2-9 months
Publication time	2-4 years	2 years	1-1.5 year	6-12 months	3-9 months

Figure F-3 – ITU-T's refined processes have contributed to a much improved time to market for its standards

Activities

ITU-T Study Groups do the technical work of ITU-T developing Recommendations and other publications. The people involved in these groups are experts in telecommunications from all over the world.

ITU-T workshops and seminars are held to promote existing work areas or explore new ones. The events cover a wide array of topics in ICT and attract high-ranking experts as speakers, attendees from engineers to high-level management from all industry sectors. Recent topics covered have been next generation networks, ICT in vehicles, IPv6, home networking, cybersecurity and video coding.

Current work areas

ITU-T is now addressing standards needs for the 21st century in areas such as:

- Next-generation networks (NGN);
- Broadband access;
- Multimedia services;
- Emergency telecommunications;
- Home Networking;
- IP issues;
- Optical networking;
- Network management;
- ICT security issues;
- Fixed/mobile convergence.

ITU-T Structure

The technical work of ITU-T is managed by the study groups (SGs) that develop Recommendations and other publications. The people involved in these SGs are experts in telecommunications from all over the world.

There are 13 SGs:

SG 2 – Operational aspects of service provision, networks and performance

SG 3 – Tariff and accounting principles including related telecommunication economic and policy issues

SG 4 – Telecommunication management

SG 5 – Protection against electromagnetic environment effects

SG 6 – Outside plant and related indoor installations

SG 9 – Integrated broadband cable networks and television and sound transmission

SG 11 – Signalling requirements and protocols

SG 12 – Performance and quality of service

SG 13 – Next-Generation Networks (NGN)

SG 15 – Optical and other transport networks infrastructures

SG 16 – Multimedia terminals, systems and applications

SG 17 – Security, languages and telecommunication software

SG 19 – Mobile telecommunication networks

In addition, TSAG (Telecommunication Standardization Advisory Group) meets regularly to review the priorities, programmes, operations, financial matters and strategies of the Sector.

WTSA (World Telecommunication Standardization Assembly) meets every four years, to adopt working methods and procedures for the management of ITU-T's activities. The last WTSA, WTSA-04 was held in October 2004. Specific matters within the competence of WTSA can be assigned to TSAG. The four-year cycle between two WTSAs is called a Study Period. The current Study Period is 2004-2008.

Focus groups

Focus groups are an instrument created by ITU-T to provide an additional working environment for the quick development of standards in specific areas. The procedure in ITU-T Rec. A.7 defines how an "arms-length" entity (called a "focus group" in ITU-T parlance) can be created to work with an ITU-T study group as a parent body while at the same time maintaining a high degree of independence, in particular concerning working methods, types of outputs, membership, financing and administration.

Focus groups generate outputs in well-defined areas within a short-term charter; these products can remain stand-alone focus group deliverables (e.g. technical specifications or technical reports), or may be progressed into the study groups in order to become traditional ITU-T products (e.g. Recommendations and supplements).

Focus groups can originate within ITU-T or from an external group.

Products

The main products of ITU-T are non-binding Recommendations. These are divided into themed series, i.e. the G-series covers Recommendations on "Transmission systems and media, digital systems and networks"; and the H-series covers "Audiovisual and multimedia systems". Recommendations can be amended with additions or corrections that could become Annexes, Amendments or Corrigenda, depending on the nature and content of the changes. Additionally ITU-T develops other products including supplements to Recommendations, implementer's guides, handbooks and manuals.

Catalogues of publications as well as a complete list of ITU-T Recommendations are available at: itu.int/ITU-T/publications

ITU-T also publishes the Operational Bulletin, which is a fortnightly detailed update containing information that is required to maintain the global interconnection of the world's telecommunication networks. In particular, it contains information on changes to numbering and routing plans, whether at the national or international level.

Cooperation with other organizations

ITU-T cooperates with many other organizations which also develop international standards such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC). In addition ITU-T has established partnerships with many others including the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the third generation partnership projects (3GPP/3GPP2) etc. There is also active cooperation with other standards development organizations (SDOs) and forums and consortia. The procedures for communicating with forums and consortia are defined in ITU-T Recommendation A.4.

Recommendation A.5 deals with situations where ITU-T wishes to make reference in its own Recommendations to documents from forums and consortia or other SDOs.

Recommendation A.6 addresses cooperation and exchange of information between ITU-T and national and regional standards development organizations.

The list of qualified organizations according to ITU-T Recs. A.4, A.5 and A.6 is available at: itu.int/ITU-T/tsb-director/sdo/qualified.html.

For more detail on working methods, ITU-T structure and meeting logistics please request a copy of the ITU-T Guide for Beginners from standards@itu.int.

The Telecommunication Standardization Bureau (TSB)

Friendly and Educated to the highest level, ITU-T's **Secretariat** – the **Telecommunication Standardization Bureau (TSB)** – offers a range of services to create the best environment for the creation of world-class standards, from **Electronic Working Facilities** to **Meeting Management**. ITU's headquarters in Geneva has many **Meeting Rooms** equipped with **State-of-the-Art Meeting Facilities** and **over 60 Multilingual Staff** to provide meeting support, backed by the ITU General Secretariat.

Meeting facilities include **Wireless LAN coverage** throughout, **LAN** and **Power Points** at every delegate position, **Multiple PCs** for delegate use, and an option for **Paper or Electronic Documents**.

Essentially, TSB provides logistical support to the Study Groups in which standards are made. It also manages telecommunication numbering resources, ICT Intellectual Property Rights (IPR) issues, promotion, workshops, membership, documents, finance, the website etc. Headed by an elected representative, it's the body responsible for providing cohesion to ITU-T's standards making process. In addition TSB acts as an **Umbrella Organization** for forums wishing to give their work the added value and **International Status** that comes with the ITU-T brand.

Membership

Membership of ITU-T offers the chance for the private sector to join with international administrations to shape the future of ICTs, in a **Open, Fair and Transparent Environment**. As well as **Networking Opportunities** and the chance to **Influence the Creation of Worldwide Standards**, members have a unique opportunity to get **Return on Investment** (ROI) by being able to **Implement Ahead of the Pack**, and **Get Products and Services to Market Quicker than their Competitors**. **Exposure on an International Platform** allows access to a wealth of information and offers unbeatable marketing opportunities.

Members that participate in the ITU-T standards making process have an unparalleled opportunity to shape standards, ensuring that their concerns are heard and that they are able to implement standards before they are officially released as Recommendations.

ITU-T meetings attract the cream of the ICT world, and offer an unparalleled opportunity for networking for all concerned with the refinement and development of ICTs. Visibility at ITU-T's meetings is to mix with and become a player in global ICTs.

ITU-T's membership fee is currently very low, at 23,500 USD a year.

Members are entitled to **Unlimited Participation** in any or all of ITU-T's Study Groups. Associates can participate in meetings of their chosen Study Group.

Resources

ITU-T has a wealth of **Freely Available Resources** through its **Website**. These include **Databases** of **Numbering Resources**, **ASN.1 Modules**, **Terms and Definitions**, **Implementation Guides for Recommendations**, **Guides and Tutorials** for systems designers. **All new** Recommendations and related texts are available in **Six Different Languages**, online and on **Fully Searchable CD-ROMs**. Members enjoy free web-access to ITU-T Recommendations with one user account per membership.

An ITU-T specific **Communications Centre**, *the Lighthouse*, offers a web-based user-friendly and alternative view of ITU-T. With dynamic content, news, features and FAQs, *the Lighthouse* sheds light on ITU-T's activities, past, present and future.

Part II: Texts of FG IPTV deliverables

Summary

Part II – Texts of FG IPTV deliverables

II.1 Architecture and requirements

II.1.1 IPTV services requirements

II.1.2 IPTV architecture

II.1.3 Service scenarios for IPTV

II.1.4 Gap analysis

II.2 QoS and performance aspects

II.2.1 Quality of experience requirements for IPTV

II.2.2 Traffic management mechanisms for the support of IPTV services

II.2.3 Application layer reliability error recovery mechanisms for IPTV

II.2.4 Performance monitoring for IPTV

II.3 Service security and content protection

II.3.1 IPTV security aspects

II 4 IPTV network control

II.4.1 IPTV network control aspects

II.4.2 IPTV multicast frameworks

II.4.3 IPTV related protocols

II 5 End systems and interoperability aspects

II.5.1 Aspects of IPTV end system – terminal device

II.5.2 Aspects of home network supporting IPTV services

II 6 Middleware, application and content platforms

II.6.1 IPTV middleware, application and content platforms

II.6.2 Toolbox for content coding

II.6.3 IPTV middleware

II.6.4 IPTV metadata

II.6.5 Standards for IPTV multimedia application platforms

II.7 IPTV vocabulary of terms

II.1 ARCHITECTURE AND REQUIREMENTS

II.1.1 IPTV services requirements

This document includes input provided by all the different Working Groups of the IPTV FG.

CONTENTS

Page

1 Scope 32
1.1 Organization of the Document 32
1.2 IPTV functional Domains 32
2 References 33
3 Definitions 33
3.1 Terms defined elsewhere 33
3.2 Terms defined in this document 34
4 Abbreviations and acronyms 38
5 Conventions 39
6 IPTV Services 40
6.1 Architecture and Services 40
6.1.1 Scenarios and drivers 42
6.1.2 Accounting and charging 42
6.1.3 Revenue Collection Architecture 42
6.1.4 Relationship with other services and networks 46
6.2 QoS and Performance Aspects 47
6.2.1 Quality of Experience 47
6.2.2 Performance 47
6.2.3 Traffic Management 48
6.2.4 Bandwidth and constraints 48
6.2.5 Application error recovery 48
6.3 Service Security and Contents Protection Aspects 48
6.3.1 General IPTV security 48
6.3.2 Content protection 49
6.3.3 Service Security 51
6.3.4 Network Security 52
6.3.5 Terminal Security 53
6.3.6 Subscriber Security 53
6.4 Network and Control Aspects 54
6.4.1 Network 55
6.4.2 Control protocol and signalling 56
6.4.3 Content distribution 57
6.5 End Systems and Interoperability aspects 60
6.5.1 End-user 61
6.5.2 IPTV terminal devices 67
6.5.3 Content Provision 71

Page

6.5.4 End-user domain (home and extensions) 72
6.5.5 Remote management 72
6.6 Middleware, Application and Content Platforms 73
6.6.1 General 73
6.6.2 Middleware 73
6.6.3 Metadata 75
6.6.4 Content 78
6.6.5 Service navigation 80
6.6.6 Service/Content Discovery and Selection 81
6.6.7 Returned data 82
6.7 Public interest 82
6.7.1 Accessibility 82
6.7.2 Emergency telecommunications 83
6.7.3 Provider Selection and Portability 83
Bibliography 84
Appendix I – Public Services cross-reference 84
Appendix II – Home Network (Consumer domain) Architecture 85

IPTV services requirements

1 Scope

This document describes requirements for the design, deployment and operations of IPTV services.

1.1 Organization of the document

The taxonomy that articulates the IPTV Services Requirements document is therefore twofold:

- A functional taxonomy, which aims at reflecting the fact that IPTV services are deployed and operated according to the combined activation of a set of elementary capabilities – IPTV traffic forwarding and routing, IPTV Quality of Service and Quality of Experience, IPTV Security, IPTV Middleware, etc.,
- Within each of the aforementioned functional areas, a further classification organizes the requirements into mandatory requirements, recommended requirements and optional requirements.

1.2 IPTV functional Domains

The following figure shows the main functional domains that are involved in the provision of an IPTV service. It is provided in this document to help understanding of requirements which in some way relates to these domains. Full description of all domains is provided in other document addressing IPTV functional architecture. These functional domains do not define a business model. Also, one provider may play several functional domains in an actual service.

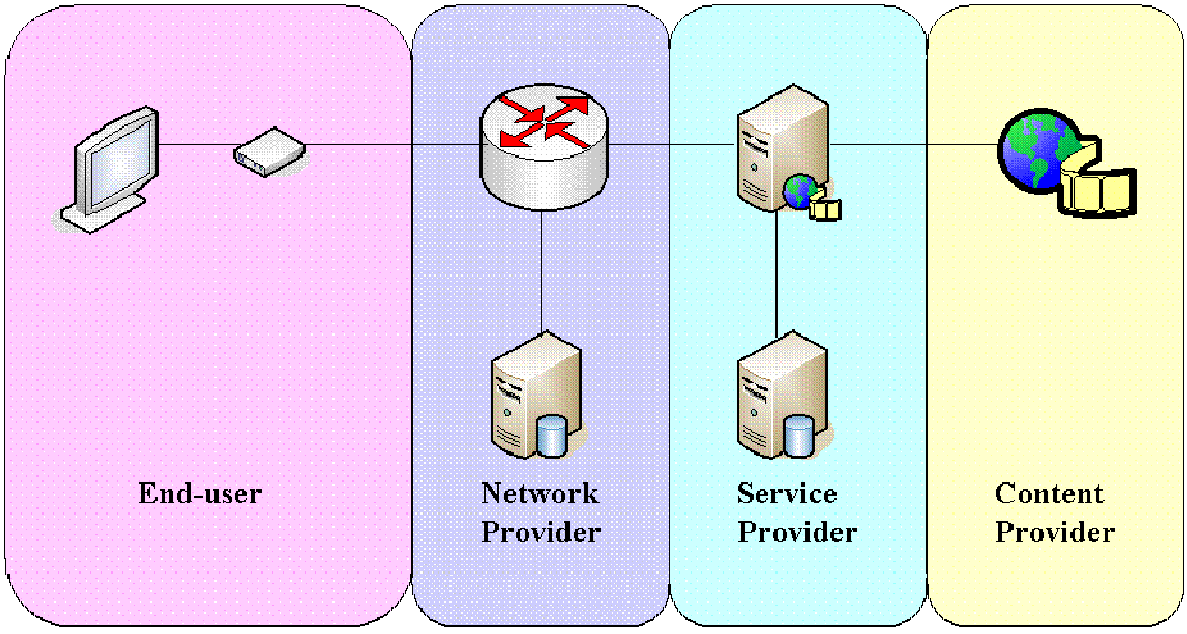


Figure 1-1: IPTV Domains

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[IETF RFC 1772] IETF RFC 1772 (1995), *Application of the Border Gateway Protocol*

[ITU-T H.Sup.1] ITU-T Recommendation H.Sup.1 (1999), *Application profile – Sign language and lip-reading real-time conversation using low bit-rate video communication*

[ITU-T J.112] ITU-T Recommendation J.112 (1998), *Transmission systems for interactive cable television services*

[ITU-T M.60] ITU-T Recommendation M.60 (1993), *Maintenance terminology and definitions*

[ITU-T M.1400] ITU-T Recommendation M.1400 (2006), *Designations for interconnections among operators' networks*

[ITU-T Q.1290] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*

[ITU-T Q.1702] ITU-T Recommendation Q.1702 (2002), *Long-term vision of network aspects for systems beyond IMT-2000*

[ITU-T Q.1741.3] ITU-T Recommendation Q.1741.3 (2003), *IMT-2000 references to release 5 of GSM evolved UMTS core network*

[ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*

[Accessibility Checklist] ITU-T FSTP-TACL (2006), *Telecommunications Accessibility Checklist*

[ATIS-0800002] ATIS standard ATIS-0800002(2006), *IPTV Architecture Requirements*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Aspect ratio [ITU-T T.101]: The ratio of the width to the height of the image rectangular area.

3.1.2 Broadcast [ITU-T M.60]: One-way transmission from one point to two or more other points.

3.1.3 Converged services [ITU-T Q.1702]: The integration of Internet, multimedia, e-mail, presence, instant messaging, m-commerce, etc., services with voice service.

3.1.4 Delivery network gateway (DNG) [ATIS-0800002]: A device implementing the DNGF.

NOTE – DNG also is commonly referred to as the Residential Gateway (RG).

3.1.5 End-user [ITU-T J.112]: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

3.1.6 Network provider [ITU-T Q.1290]: The organization that maintains and operates the network components required for IPTV functionality. A network provider can optionally also act as service provider.

3.1.7 Service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider can optionally or can optionally not be a customer of another service provider.

3.1.8 Subscriber [ITU-T Q.3050.1]: The subscriber is responsible for concluding contracts for the services subscribed to and for paying for these services.

3.1.9 Subscription [ITU-T Q.1741.3]: A subscription describes the commercial relationship between the subscriber and the service provider.

3.2 Terms defined in this document

This document defines the following terms:

3.2.1 Accessibility feature: An additional content component that is intended to assist people hindered in their ability to perceive an aspect of the main content. Examples**:** captions for the hard of hearing, subtitles in various languages, sign-language interpretation video and descriptive audio.

3.2.2 Acquisition: The process of obtaining content by the end-user.

NOTE – For content with accessibility features this means that the content will be available in a form that can be used by the end-user.

3.2.3 Audio description: This service provides a commentary describing the visual events pertinent to the content and augments the dialog in the content.

NOTE – Audio description is primarily intended to assist users who are unable to see the video content clearly. The narrative passages fit between the dialogue and other significant audio content so as not to interfere with it. Ideally the user can control the volume and spatial positioning of the audio or derive it from a separate output.

3.2.4 Bitstream: Coded representation of a video or audio signal.

3.2.5 Broadcast TV: One-way transmission of TV signals from one point to two or more other points.

3.2.6 Captions: Captions provide a real-time on-screen transcript of the dialogue as well as any sound effects.

NOTE – This service can be provided by means of either textual or graphical supplementary content. The captions and the dialogue are usually in the same language. The service is primarily to assist users having difficulty hearing the sound. Ideally, users may have some control over the position and size of the presentation. Different speakers are distinguished, usually by different colours.

3.2.7 Channel: Content formatted as a selectable set of data and transported as part of a data stream

3.2.8 Channel changing: The act of changing from one channel to another.

3.2.9 Channel zapping: The act of fast changing from one channel to another

3.2.10 Closed Captions: captions that can be switched on or off by the viewer.

3.2.11 Conditional Access: A component of a Service and Content Protection system the purpose of which is to prevent unauthorized (unentitled) access to a service or to content.

3.2.12 Content protection: Ensuring that an end-user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder.

3.2.13 **Content tracing:** A process to enable the identification of the (arbitrary) origin of content, and/or the responsible party (e.g. the end-user), to facilitate subsequent investigation in the event of unauthorized content copying or distribution.

NOTE – Content tracing information may be attached to content either as metadata, or as a forensic watermark.

3.2.14 **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).

3.2.15 **Electronic program guide (EPG):** A structured set of data, intended to provide information on available content that may be accessed by end-users.

3.2.16 **Home network (HN):** A communication system designed for the residential environment, in which two or more devices exchange information.

3.2.17 **Hybrid terminal device:** An IPTV terminal device that can also receive content from different types of transmission systems (e.g. satellite, cable).

3.2.18 **Interstitial program:** A short program which is shown between events (e.g. between two movies) or embedded during presentation of an event (e.g. advertisement).

3.2.19 **IPTV:** IPTV is defined as multimedia services such as television/video/ audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

3.2.20 **IPTV terminal function (ITF):** The functionality that is responsible for processing the content conveyed by the IP transport.

3.2.21 **IPTV TD:** A terminal device which has ITF functionality, e.g. a STB.

3.2.22 **Linear TV:** A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed.

3.2.23 **Mobility:** The ability for the end-user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.2.24 **Multicrypt:** A mechanism that enables the reception of programmes encrypted according to various encryption systems by means of a Common Interface (CI).

3.2.25 **Multi-channel audio:** Audio signal with more than two channels

3.2.26 **Network personal video recorder (nPVR):** Same as PVR except that the recording device is located at the service provider premises.

3.2.27 **Open Captions:** captions that are displayed and cannot be switched off by the viewer.

3.2.28 **Package:** A collection of content components that in some combination (either all or a subset) together provide an end-user experience and are intended to be used together.

NOTE – A package can be instantiated with or without audio visual content depending on scenarios, in which audio visual content and package can be tightly associated or can be loosely coupled enough to be handled (generation, delivery, consumption) independently.

3.2.29 **Pay per view (PPV):** A TV service where a particular program event (e.g. a hockey match) can be bought separately from any package or subscription. The transmission of the program event is made at the same time to everyone who has ordered it.

3.2.30 Personal digital recorder (PDR): See PVR.

3.2.31 Personal mobility: This is the mobility for those scenarios where the end-user changes the terminal device used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

3.2.32 Personal video recorder (PVR): An end-user controlled device that records, stores and plays back multimedia content. PVR is also known as personal digital recorder (PDR).

3.2.33 Public Information Services: are specific un-associated Information Services. Examples of un-associated information services**:** news highlights, stock exchange, traffic conditions, sport results.

3.2.34 Push VoD: A TV service where multimedia content is packaged and delivered at the discretion of the service provider to the end-user's storage system.

3.2.35 Random access point: A point in the content from which playback can begin. NOTE – For example, in MPEG encoding, this would be an I-frame, as opposed to a P-frame or B-frame.

3.2.36 Rights: One or more legal or business entitlements to Use or employ Content, e.g., to view, record, redistribute Content.

3.2.37 Rights Expression: The syntactic embodiment of Rights in a concrete form.

3.2.38 Re-transmission Broadcast Service: A service in which content is provided from various broadcasting environments including, but not limited to, terrestrial, satellite and cable, and re-transmitted into IP network simultaneously or otherwise.

3.2.39 SCP: A combination of service protection and content protection.

3.2.40 Service: A set of functionality enabled by a provider for end users; for example, providing IP connectivity with managed quality of service, providing an IPTV Service, providing a content on demand service, etc.

3.2.41 Service Protection: Ensuring that an end-user can only acquire a service, and, by extension, the content contained therein, that they are entitled to receive.

3.2.42 Sign language interpretation: A video service showing an interpreter who uses hand gestures and facial expression to convey the main audio content and dialogue to sign language and lip readers.

NOTE – This service comes in the form of supplementary video content, usually smaller in image size to that the main video content. Ideally the user can control the position, size and background properties (solid or transparent and the colour, if solid). It is of sufficient temporal and spatial quality to enable sign reading and lip reading.

3.2.43 SimulCrypt: A mechanism that facilitates using several service protection systems.

3.2.44 Skin: A customized graphical appearance (the visual aspect of a graphical user interface (GUI)) applied to certain software and websites for aesthetic reasons or ease of use.

3.2.45 Subtitles: Subtitles provide a real-time on-screen transcript of dialogue for the purpose of language translation or to clarify speech that is unclear.

NOTE – This service can be provided by means of either textual or graphical supplementary content. The subtitles and the dialogue are usually in different languages. The assumed audience for subtitling is hearing people who do not understand the language of the dialogue.

3.2.46 **Supplementary content:** This is defined as video, audio, textual, graphical or other forms of content that can be optionally accessed by the end-user and rendered by the terminal. It has the following features:

- It only works in conjunction with the main content.
- It is synchronous with the main content.

3.2.47 **Terminal device (TD):** A device which typically presents and/or processes the content, such as a personal computer, a computer peripheral, a network appliance, a mobile device, a TV set, a monitor, a VoIP Terminal or an audio-visual media player.

3.2.48 **Terminal device protection:** Ensuring that a terminal device employed by an end-user in the reception of a Service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters not otherwise protected by encryption or watermarking.

3.2.49 **Terminal mobility:** This is the mobility for those scenarios where the same terminal equipment is oving or is used at different locations. The ability of a terminal to access IPTV services from ifferent locations and while in motion, and the capability of the network to identify and locate that terminal.

3.2.50 **Time shifting:** A function which allows playback of content after its initial transmission.

3.2.51 **Time-shift TV:** A TV program that has been time shifted.

3.2.52 **Trick mode functionality:** The ability to pause, rewind or forward stored content

3.2.53 **TV with trick mode:** TV service with trick mode functionality.

3.2.54 **Universal Design:** It is the design of the products and environments to be useable by all people, to the greatest extent possible by including accessibility features in the original design to prevent the need for adaptation after deployment.

NOTE – The intent of universal design is to simplify life for everyone by making products, communications, and the built environment more usable by as many people as possible at little or no extra cost. Universal design benefits people of all ages and abilities.

3.2.55 **Usage environment description:** The usage environment description includes the description of end-user characteristics, terminal capabilities, network characteristics and natural environment characteristics.

NOTE – These various dimensions of the usage environment description, which originate from end-users, can be used for accommodating, for example, the adaptation of contents for transmission, storage and consumption.

3.2.56 **Use:** The purpose(s) for which acquired content is employed.

3.2.57 **User Privacy Protection:** Ensuring that information considered to be private (or confidential) by an end-user be maintained in confidence, while remaining subject to mandatory disclosure due to legal processes.

3.2.58 **Web-based EPG:** An EPG that can be accessed on a web server by means of a URL.

3.2.59 **Wireless network characteristics:** The characteristics of a wireless network expressed in terms of current available bandwidth, packet loss and possibly other to-be-defined wireless network information parameters for a specific wireless link type e.g. WLAN, Cellular, WPAN or WMAN.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

API	Application Program Interface
ATIS	Alliance for Telecommunications Industry Solutions
CAS	Conditional Access System
CAT5	unshielded twisted pair type cable Category 5 (frequencies of up to 100 MHz)
CDR	Call Detail Records
CI	Common Interface
CoS	Class of Service
DHCP	Dynamic Host Configuration Protocol
DN	Delivery Network
DNG	Delivery Network Gateway
DNGF	Delivery Network Gateway Function
DNS	Domain Name System
DoS	Denial of Service
DRM	Digital Rights Management
DTT	Digital Terrestrial Television
EAN	Emergency Alert Notification
ECG	Electronic Content Guide
EMM	Entitlement Management Message
EPG	Electronic Program Guide
ETS	Emergency Telecommunication Service
FTA	Free To Air
FW	Firewall
GUI	Graphical User Interface
HD	High Definition
HN	Home Network
HNS	Home Network Subsystem
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPG	Interactive Program Guide
IPTV	Internet Protocol Television
ITF	IPTV Terminal Function
MoCA	Multimedia over Coax Alliance
MP3	MPEG-1 Audio Layer 3
MPEG	Moving Picture Experts Group

NACF	Network Attachment Control Function
NAPT	Network Address Port Translation
NAT	Network Address Translation
NGN	Next Generation Network
nPVR	Network PVR
OAMP	Operate, Administer, Maintain, and Provision
PC	Personal Computer
PDA	Personal Digital Assistant
PDR	Personal Digital Recorder
POTS	Plain Old Telephone Service
PPV	Pay Per View
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
QoSM	Quality of Service Measurement
RACF	Resource and Admission Control Function
RG	Residential Gateway
RTSP	Real Time Streaming Protocol
SCP	Service and Content Protection
SD	Standard Definition
SLR	Service Level Requirement
TD	Terminal Device
TDR	Telecommunications for Disaster Relief
TV	Television
UI	User Interface
UMF	Uniform Media Formats
USB	Universal Serial Bus
VoD	Video on Demand
WAN	Wide Area Network
WiFi	Wireless Fidelity (IEEE 802.11b wireless networking)
WWW	World Wide Web
xDSL	Any of the various types of Digital Subscriber Lines (DSL)
XML	eXtensible Mark-up Language

5 Conventions

In this document:

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

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document 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/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

IPI-n indicates an interface in home network as explained in Appendix II.

6 IPTV Services

6.1 Architecture and Services

Architecture requirements

- The IPTV architecture is required to support various content resolutions including High Definition (HD) and Standard Definition (SD) for the delivery of Linear TV content.
- The IPTV architecture is required to support various content aspect ratios, e.g. 4:3, 16:9.
- The IPTV architecture is required to support a means to avoid sending to an ITF content that is unable to be rendered [ATIS-0800002].
- The IPTV architecture is required to support a framework that identifies the key components and measurement points for Quality of Service Measurement (QoSM) [ATIS-0800002].
- The IPTV architecture is required to define the key service delivery components of IPTV services and their interfaces into the other domains [ATIS-0800002].
- The IPTV architecture is required to allow for two-ways communication between End-user Network and the Service Provider [ATIS-0800002].
- The IPTV architecture is required to support the addressability of particular device such as ITFs within the end-user Network [ATIS-0800002].
- The IPTV architecture is required to allow for the utilization of Internet protocols and standards [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support content segmentation [ATIS-0800002].
- The IPTV architecture is recommended to support a mechanism for obtaining information pertaining to terminal device capabilities.
- The IPTV architecture is recommended to support a functional component that presents an open interface for the third party applications to use the capabilities and resources of the IPTV network.
- The IPTV architecture is recommended to ensure content and segment data integrity.
- The IPTV architecture is recommended to support networked personal video recorder (nPVR).

- The IPTV architecture is recommended to support the display of multiple supplementary video streams and layouts.
- The IPTV architecture is recommended to allow the delivery of IPTV services over different access networks (e.g. cable, optical, xDSL, wireless)
- The IPTV architecture is recommended to allow the delivery of IPTV services to any IPTV terminal device (e.g. mobile phone, PDA, set-top-box).
- The IPTV architecture is recommended to adapt dynamically to change in wireless networks characteristics when the service is delivered over a mobile network (e.g. bandwidth, packet loss rate, etc.
- The IPTV architecture is recommended to support viewership data tracking.

  NOTE – For example this tracking may allow content provider and service provider to provide audience rating service, track popular programs, craft and target specific advertisements to particular groups of users demonstrating certain surfing patterns.
- The IPTV architecture is recommended to support software version upgrade and configuration data download by connecting to download server.
- The IPTV architecture is recommended to support XML encoding for application signalling in addition to the already existing MPEG-2 table and section based encoding.
- The IPTV architecture is recommended to have a means to allow content to be seen only by the appropriate audience. This means it may be triggered by the service provider and/or the user).
- The IPTV architecture is recommended to support presentation adaptive to usage environment.

Terminal device recommendations

- The IPTV terminal device is recommended to be able to declare Media-providing entities their usage environments description - e.g. Type of service, Type of Terminal, Type of transmission medium, User Preferences, Available QoS Level [ATIS-0800002].

Architecture options

- The IPTV architecture can optionally support separate segment and content metadata storage and distribution [ATIS-0800002].
- The IPTV architecture can optionally support a replacement algorithm for content caching and distribution.
- The IPTV architecture can optionally support advertisement insertion.
- The IPTV architecture can optionally support the time-shift TV functionality (the ability to play a content that has been broadcast in the past).
- The IPTV architecture can optionally support usage environments description.

Terminal device options

- The IPTV terminal device can optionally support the modification of display duration.
- The IPTV terminal device is required to support the decoding of at least one video and one audio format.
- The IPTV architecture is required to support maintaining accurate time based control for synchronisation e.g. lip-sync with video as judged by the general viewer at all times, pause and resume, random access.
- The IPTV architecture is recommended to support recording of files and playback of video and audio content either in the network or at the IPTV terminal device.

- The IPTV architecture is recommended to support seamless transition from one to another codec in the same channel within the limits of Digital Broadcasting networks, e.g. scheduled daily transitions between SD and HD).

6.1.1 Scenarios and drivers

Architecture recommendations

- The IPTV architecture is recommended to support various encapsulation types such as MPEG-2 TS.

6.1.2 Accounting and charging

Architecture requirements

- The IPTV architecture is required to support IPTV services charging through various payment methods (such as prepay, post pay, advice of charge, and third party charging)[ATIS-0800002].
- The IPTV architecture is required to not preclude the use of NGN charging architectures for all IPTV services Accounting and Billing functions [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for the collection of data for accounting and reporting purposes, partner settlements, and reconciliation of end-user usage – such as service subscriptions, purchases, and transactions [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for accounting and charging purposes related to IPTV services usage [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to allow service providers to integrate IPTV services Accounting and Billing functions with a system that can be used across multiple NGN services and applications [ATIS-0800002].
- The IPTV architecture is required to include capabilities for transferring settlement information between service providers [ATIS-0800002].

6.1.2.1 Subscription

Architecture requirements

- The IPTV architecture is required to support user registration.

6.1.2.2 Pay per View

Architecture requirements

- The IPTV architecture is required to support the acquisition of appropriate VOD accounting data, to fulfil licensing agreements [ATIS-0800002].

6.1.3 Revenue Collection Architecture

Architecture requirements

- The IPTV architecture is required to support mechanisms to support PPV services [ATIS-0800002].
- The IPTV architecture is required to support mechanisms to support On Demand services [ATIS-0800002].
- The IPTV architecture is required to allow for the insertion of content into VOD content [ATIS-0800002].

- The IPTV architecture is required to support interactive services such as educational and entertainment applications (e.g. games), communications services (such as mail, chat, and messaging), and information services (such as stock and weather services) [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for the delivery of interactive and downloadable games [ATIS-0800002].
- The IPTV architecture is required to support the search, download, storage, and presentation of digital photographs [ATIS-0800002].
- The IPTV architecture is required to support mechanisms to block transmission of content to specified geographical areas whenever blackout requirements are applicable [ATIS-0800002].
- The IPTV architecture is required to support a mechanism that allows service signalling messages to be routed based on the capabilities of the end-user device and/or the application servers available to support services [ATIS-0800002].
- The IPTV architecture is required to support a mechanism that allows for service-based transport QoS to be managed across multiple network domains [ATIS-0800002].
- The IPTV architecture is required to support a mechanism for NAT traversal [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support mechanisms for allowing the integration of IPTV services and existing services (e.g. instant messaging, telephony).
- The IPTV architecture is recommended to allow seamless provision and operation of IPTV services across different administrative domains ([IETF RFC 1772]), which are defined in Clause 3.
- The IPTV architecture, if re-transmission broadcast service is supported, is recommended to support geographical regionalization of content.
- The IPTV architecture is recommended to support the ability to remotely configure and administer Network and Service elements [ATIS-0800002].
- The IPTV architecture is recommended to support mechanisms for the receipt of content from different sources, e.g., satellite, dedicated IP connections.
- IPTV architecture is recommended to support mechanisms for the exchange of information related to capabilities such as access condition user profile (e.g. ID information for DRM).
- The IPTV architecture is recommended to support for the establishment of sessions as a means of maintaining associations between users and the applications they use [ATIS-0800002].

Architecture options

- The IPTV architecture can optionally support mechanisms to capture and utilize user profiles and preferences to target/restrict content items [ATIS-0800002].
- The IPTV architecture can optionally convert video content from its stored format into one that is compatible with that required to be displayed on the ITF supporting device [ATIS-0800002].
- The IPTV architecture can optionally support mechanisms that allow private entities (e.g. residential users) to act as content-providers for the purpose of sharing their own content [ATIS-0800002].
- The IPTV architecture is required to support the ability for the service provider to prevent the sending of bulk unsolicited contents to the end-users.
- The IPTV architecture is required to support the ability to trace the source of incoming content (e.g. messages that has been a cause for complaint by an end-user).

6.1.3.1 Segmentation by role

6.1.3.1.1 Content Provider

Architecture recommendations

- The IPTV architecture is recommended to support mechanisms for the content provider to perform content management such as uploading content or deleting content or modifying the relevant attributes of content.
- The IPTV architecture is recommended to allow content usage statistics to be collected.

6.1.3.1.2 Service Provider

Architecture requirements

- The IPTV architecture is required to support mechanisms for the IPTV services Provider to Operate, Administer, Maintain, and Provision (OAMP) IPTV equipments [ATIS-0800002].
- The IPTV architecture is required to facilitate the ability of the Service Provider to manage the IPTV services with regards to Fault, Configuration, Accounting, Performance, and Security (FCAPS) [ATIS-0800002].
- The IPTV architecture is required to support the capability of monitoring the network elements (e.g. routers) and service elements (e.g. ITF) that report alarms in the event of faults.
- The IPTV architecture is required to support a means for the service provider to provide an integrated presentation of content received at the ITF via out-of-band (to IP) delivery methods and via IP networks – i.e., hybrid methods [ATIS-0800002].
- The IPTV architecture is required to support mechanisms that allow IPTV services delivery from a third party provider as defined in Clause 3 [ATIS-0800002].
- The IPTV architecture is required to support navigation capability for IPTV content
- The IPTV architecture is required to support the service provider to be able to authenticate, authorize and charge the subscriber.
- The IPTV architecture is required to support the service provider to be able to authenticate the end-user to authorize purchase of products, ordering VoD, or watching particular programs by using the appropriate controls – e.g. PIN number, login.
- The IPTV architecture is required to support the service provider to be able to distinguish between end-user and subscriber.

Architecture recommendations

- The IPTV architecture, if re-transmission broadcast service is supported, is recommended to provide comparable Quality of Experience to the end-user as the direct reception.
- The IPTV architecture is recommended to support mechanisms for the service provider to manage various services.
- The IPTV architecture is recommended to support mechanisms for the service provider perform subscriber management functions such as opening or cancelling or activating or freezing an account, searching user account's balance, searching user's consumption detail record, modifying user's information (e.g. accounts, login name, payment type), grouping users etc.
- The IPTV architecture is recommended to support mechanisms for the service provider to provide the functions for service usage and the prevention of the service abuse.
- P2P mechanism in IPTV is recommended to not preclude the use of client server mechanisms in IPTV.

Service provider requirements for Remote Management

Architecture requirements

- The IPTV architecture is required to support the service provider be able to upgrade the end-user device remotely.
- The IPTV architecture is required to support the service provider to be able to get QoS information from the end-user device.
- The IPTV architecture is required to support the service provider to be able to capture the end-user IPTV Terminal capabilities (e.g.: codecs, access limitations, etc.).

Architecture recommendations

- The IPTV architecture is recommended to support the service provider to be able to update the end-user device remotely, e.g. update software, firmware and virus list.

Service provider requirements for Push Content

Architecture requirements

- The IPTV architecture is required to support the service provider to be able to push content onto the end-user IPTV Terminal (content requested or not by the end-user).
- The IPTV architecture is required to support the service provider to be able to insert additional contents in content played from the end-user PVR.

6.1.3.1.3 Network Provider

Architecture requirements

- The IPTV architecture, if re-transmission of free-to-air broadcasting service is supported, is required to ensure the Network Provider to protect the end user's privacy at the same level of broadcasting network.

6.1.3.1.4 End-User

Architecture requirements

- The IPTV architecture is required to support mechanisms to filter unwanted contents.
- The IPTV architecture is required to support the end-user with the ability to move between a free-to-air (FTA) and pay per view (PPV) environment.
- The IPTV architecture is required to support the end-user with the ability to choose a preferred language option (audio, subtitle, captioning, supplementary video and supplementary descriptive audio) from various languages that the content provider pre-defined and the service provider delivered".
- The IPTV architecture is required to support the ability for the end-user to turn on and off the audio, the subtitle and captioning, supplementary video and descriptive audio at anytime without altering any of the default setting options.
- The IPTV architecture is required to support the capability to store and retrieve multiple profiles containing sets of user interface preference settings and language settings so that it will be easy to switch to different personal preferences for different viewers.

Architecture recommendations

- The IPTV architecture is recommended to support the capability for the subscriber to query their usage detail record lists.

- The IPTV architecture is recommended to support the capability to the end-user to alter his or her preferred language options at anytime.
- The IPTV architecture is recommended to support multiple languages audio, multiple language subtitles, multiple languages captioning, multiple language supplementary video and multiple language descriptive audio.
- The IPTV architecture is recommended to support the ability to independently select a default language for each of the following: audio, subtitle, captioning, supplementary video and supplementary descriptive audio.
- The IPTV architecture is recommended to support the capability for the end-user to watch with the preferred audio, subtitle, and captioning, supplementary video or descriptive audio.
- If the end-user's option can not match with the pre-defined content languages, the IPTV architecture is recommended to support the capability for the IPTV terminal device to present the content with default audio, default subtitle and captioning, default supplementary video and default descriptive audio.
- The IPTV architecture is recommended to support the capability for the end-user to switch audio, subtitles and captioning, supplementary video and descriptive audio back and forth when the user is watching the program without having to change his or her preferred language settings.

Architecture options

- The IPTV architecture can optionally support means for the content provider to define a set of language options for its content.

6.1.4 Relationship with other services and networks

Architecture requirements

- The IPTV architecture is required to support IPTV terminal devices which constantly listen for EAN messages [ATIS-0800002].
- The IPTV architecture is required to not preclude the use of the HSS, SLR, and/or related NGN functional components for all IPTV Subscriber Management functions [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support capabilities for the interoperability and user mobility between different IPTV networks allowing access to IPTV services by the customer either in motion or not.
- The IPTV architecture is recommended to allow network operators to leverage their existing network attachment capabilities [ATIS-0800002].
- The IPTV architecture is recommended to support means by which service/network providers can integrate IPTV subscriber management functions with a subscriber management system that can be used across multiple NGN services, including IMS-based services [ATIS-0800002].
- The integration of IPTV services in IMS-based environments is recommended to rely upon any relevant IMS-based NGN-specific capabilities, including (but not necessarily limited to) HSS/HLR and GUP [ATIS-0800002].
- The IPTV architecture is recommended to support real-time encoded and pre-encoded stored programs.
- The IPTV architecture is recommended to support capabilities for exchange of IPTV services information between different IPTV services providers. For instance, the service information can optionally include the source information, channel information, service start/end time, and QoS information.

6.2 QoS and Performance Aspects

Architecture requirements

- The IPTV architecture is required to allow the delivery of IPTV services with a defined Quality of Experience (QoE) for the IPTV end-user [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support consistent QoS for the duration of the service.
- The IPTV architecture is recommended to support a mechanism by which network operators can integrate IPTV QoS management functions into a common framework with other services and applications [ATIS-0800002].
- The IPTV architecture is recommended to rely upon any relevant QoS capabilities (e.g. RACF [ITU-T Y.2111] and DiffServ [IETF RFC 2475]) when integrating IPTV services into NGN-based environments.
- The IPTV architecture is recommended to support transmission of video or data with sufficient quality for sign language perception, including lip reading. This requires the transmission of a sufficient number of frames per second and sufficient spatial resolution to reproduce details of the signing person's hands, face, lips, eyes and body [ITU-T H.sup.1].
- The IPTV architecture is recommended to support the transmission and presentation of video and audio with sufficient synchronization for lip-reading [ITU-T H.sup.1].

Architecture options

- The IPTV architecture can optionally support the delivery of multiple services over the common IP transport with a manageable IP Quality of Service (QoS); services can optionally be delivered from multiple service providers or from a single provider [ATIS-0800002].

6.2.1 Quality of Experience

Architecture requirements

- The IPTV architecture is required to support mechanisms for supporting appropriate resiliency in the service provider infrastructure to maintain a high QoE [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support an appropriate QoE for end-users eligible for uploading content to the service provider's network [ATIS-0800002].
- The IPTV architecture is recommended to support means to provide channel changing times with sufficient QoE.
- The IPTV architecture is recommended to support means to support flexible channel changing times as a trade off to improve efficiency.
- The IPTV architecture is recommended to support the capability to monitor video quality.
- The IPTV architecture is recommended to support navigation of EPG menu items with sufficient QoE.

6.2.2 Performance

Network requirements

- Networks that support IPTV are required to support the IP QoS class and associated performance requirements specified in Y.1541 [ITU-T Y.1541], which recommends the selection of relevant specific QoS classes based on application requirements.

6.2.3 Traffic Management

Architecture requirements

- The IPTV architecture is required to support a mechanism for assigning traffic priorities [ATIS-0800002].
- The IPTV architecture is required to support the relevant mechanisms for IPTV traffic identification, classification and marking, policing and conditioning, scheduling and discarding.

Architecture recommendations

- The IPTV architecture is recommended to support mechanisms for dynamic IPTV traffic load balancing so as to dynamically accommodate with the network load and congestion conditions at any given time, so as to deliver the set of IPTV services to the end-users with the relevant level of quality.
- The IPTV architecture is recommended to offer an admission control solution for admission of IPTV services over the access and core network resources from the home network to the service source.

6.2.4 Bandwidth and constraints

Architecture requirements

- The IPTV architecture is required to support the capability for management of capacity on the services and network elements [ATIS-0800002].

Architecture options

- The IPTV architecture can optionally support mechanisms to support QoS/QoE parameter adjustment due to changes of content characteristics on a channel.

6.2.5 Application error recovery

Architecture recommendations

- The IPTV architecture is recommended to support an application layer error recovery mechanism to support sufficient QoE/QoS for unicast distribution of any IPTV service.
- The IPTV architecture is recommended to support an application layer error recovery mechanism to support sufficient QoE/QoS for multicast distribution of any IPTV service.
- Any application layer error recovery mechanism integrated in the IPTV architecture is recommended to be bandwidth efficient.
- Any application layer error recovery mechanism integrated in the IPTV architecture is recommended to be flexible to cover a range of networks conditions and IPTV services.

6.3 Service Security and Contents Protection Aspects

6.3.1 General IPTV security

- The IPTV architecture is recommended to take into account the influence/impact on performance, quality of service, usability, scalability and cost constraints on deployment of security.
- The IPTV architecture can optionally support SCP of end-user shared content [ATIS-0800002].

6.3.2 Content protection

Architecture requirements

- The IPTV architecture is required to support content protection as defined in Clause 3.
- The IPTV architecture is required to support associating content with protection and content management metadata in order to permit the expression of its rights of usage.
- The IPTV architecture is required to support the secure delivery of content protection and content management metadata, including usage rights metadata.
- The IPTV architecture is required to support content usage rights metadata that distinguishes between rights of use including rendering (viewing), storage, (re)distribution, and combinations thereof.
- The IPTV architecture is required to support protection of content that is distributed simultaneously to a very high number of subscribers (scalability).
- The IPTV architecture is required to support protection of content that is transferred over multicast and/or over unicast streams.
- The IPTV architecture is required to apply possible rights specifications and protect content for multiple common existing content formats (e.g., MP-3, MPEG-4).
- The IPTV architecture is required to support the securing of stored content according to granted usage.
- The IPTV architecture is required to support robust content tracing to content in an offline manner (e.g., VoD content).
- The IPTV architecture is required to support a means for conveyance of content tracing information (e.g. Watermark facilitation metadata).

  NOTE – Such provision may be made by the selection of appropriate standards profiles or by extensions to the existing standards.
- The IPTV architecture is required to support the application of content tracing technology within the output of an IPTV terminal device for the purpose of uniquely identifying a session (e.g., channel, time/date), IPTV terminal device and/or network operator. Examples of such content tracing technology can optionally include visible and invisible information.
- The IPTV architecture is required to allow the retrieval of all the content tracing information from the content.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability where only authorized user(s) or device(s) are allowed to use the IPTV content, even after content is transferred to another security system.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to keep identification information to identify IPTV content consistently, no matter which identification schemes are used and no matter to which security system the content is transferred to.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to not reduce the level of security when content is transferred to another security system.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to allow only trusted devices.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to provide a secure environment for exchanging service and content protection interoperability data (e.g. authentication information, metadata, key information, etc.).

- The IPTV architecture is prohibited from precluding support for service and content protection interoperability such that interoperability is not dependent on specific software or hardware.
- The IPTV architecture is prohibited from requiring a service and content protection mechanism of either side to be openly specified to achieve interoperability.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability which is flexible and extensible to support various business models.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability among multiple security systems which use different security mechanisms, respectively, where the purpose is to support the seamless time-shifting service (subscribers can store the content and retrieve it later) and place-shifting service (subscribers can see the content anywhere) although the security mechanisms are different.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to maintain transparency to users.
- The IPTV architecture is prohibited from precluding support for multiple content and service protection mechanisms regardless of specific hardware or software requirements.

Scrambling algorithm requirements

- Scrambling algorithms for IPTV are required to have sufficiently large key entropy to protect the content fully from plausible threats (e.g., at least 128 bits for the AES symmetric algorithms).
- Scrambling algorithms for IPTV are required to be built using publicly-available and standardized cryptographic algorithms.
- Scrambling algorithms for IPTV are required to not preclude support for either Simulcrypt or Multicrypt approaches. The purpose is to support multiple DRM vendors within a single network platform when required by the content distributor.
- Scrambling algorithms for IPTV are required to:
  - be designed with suitable, variable key lengths defined by the appropriate experts;
  - be an adaptable, technical solution which allows configurable, variable parameters (such as key length, crypto periods, etc.) for scalable and future proof levels of security in the same stream;
  - be designed by appropriate experts and is not broken within a reasonable amount of time, using "brute force" attacks;
  - be designed by appropriate experts and whose rationale is a cost/benefit analysis.
- Scrambling algorithms for IPTV are required to be efficiently implementable for both hardware and software implementations.

Architecture recommendations

- If IPTV content employs a content tracing technology, then it is recommended that the tracing technology be imperceptible.
- The IPTV architecture is recommended to support robust content tracing to content in real-time (e.g., broadcast content).
- The IPTV architecture is recommended to support the capability for authenticating and authorizing end-users for content sharing services (e.g. content export and content redistribution).

Architecture options

- The IPTV architecture can optionally support the inclusion of content tracing information. This content tracing information can optionally contain the operator ID, content owner ID, IPTV terminal device ID, and other information.

Scrambling algorithm options

- Scrambling algorithms for IPTV can optionally apply cryptographic algorithms of different strength to different content types.

6.3.3 Service Security

Architecture requirements

- The IPTV architecture is required to support Service Protection, as defined in Clause 3.
- The IPTV architecture is required to support authorization and authentication capabilities for the end-user.

  NOTE – This can optionally include the capability of a service provider to authenticate and authorize a subscriber (subscriber's IPTV terminal device) and a different service provider.
- The IPTV architecture is required to support a mechanism to signal the IPTV terminal device to utilize a specified scrambling algorithm based on a standardized framework.
- The IPTV architecture is required to have the ability to use standard key management systems (e.g., MIKE, EMM/ECM), to the extent that this is required for interoperability.
- The IPTV architecture is required to support the capability to the server side SCP interfaces to update and query the SCP System concerning scrambling algorithms for IPTV and any other operator-selected scrambling algorithms.
- The IPTV architecture is required to support rights management that is independent of specific content formats or specifications.
- The IPTV architecture is required to support a mechanism for secure delivery of entitlements to the IPTV terminal devices.
- The IPTV architecture is required to support content usage control (e.g. re-play entitlements).
- The IPTV architecture is required to support different modes of re-play entitlements, e.g., limit on number of plays, time limit on plays, restriction of fast forward or rewind.
- The IPTV architecture is required to support a mechanism for transmitting signalling messages securely between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to allow for the confidentiality of signalling messages between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to allow for the authenticity of signalling messages between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to allow for the integrity of signalling messages between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to securely retrieve the SCP parameters (e.g. configuration, status) from IPTV terminal device.
- The IPTV architecture is required to support a mechanism to securely update the SCP parameters (e.g. configuration) of the IPTV terminal device.
- The IPTV architecture is required to support the capability to turn on and off content tracing function with flexibility (e.g., based on time, an event, content, or channel).
- The IPTV architecture is recommended to support the capability for authenticating and authorizing end-users for content sharing services (e.g. content export and content redistribution).
- If the IPTV architecture employs a Key Management System, then it is required to be designed for scalability, reliability, and interoperability.
- If the IPTV architecture employs a Key Management System, then a hierarchical key management scheme is recommended to be considered to support scalability.

- If the IPTV architecture employs a Key Management System that uses a Group Key Management Protocol, then a hierarchical key management and key management algorithm alternative is recommended to be considered to support scalability.
- If the IPTV architecture employs a Key Management System that uses Short Term Keys, it is recommended that the media path is provisioned in such a way that NAT traversal and bandwidth constraints do not limit the key exchange.
- The IPTV architecture is recommended to support the joint transmission of content and content tracing information such that the content and its respective content tracing information remain synchronized during transport.
- The IPTV architecture is recommended to support at least the same degree of protection (for purposes of controlling unauthorized access) to content tracing information as is applied to the corresponding traced content.

Architecture recommendations

- The IPTV architecture is recommended to enable content confidentiality, i.e. support a capability to the head-end to support multiple scrambling algorithms.
- The IPTV architecture is recommended to support a "blackout mechanism": a mechanism for limiting viewing-rights of certain programs to certain groups of subscribers (e.g. block viewing by residents of a specific area (for example, this can optionally be useful for sporting events)).
- The IPTV architecture is prohibited from precluding support for the installation and operation of multiple service protection solutions without hardware replacements except removable devices (such as USB dongle and SIM cards).
- The IPTV architecture is prohibited from precluding support for an identification mechanism for available service protection solutions which are capable to satisfy the requirement that is specified for related content protection.
- The IPTV architecture is prohibited from precluding support fora SCP system discovery mechanism, such that whenever specific content requires a specific service protection system, the IPTV architecture may support a discovery method and adapt to it.
- The IPTV architecture is prohibited from precluding support a mechanism for the selection of a SCP system from the available SCP systems without any hardware replacement except removable devices.
- The IPTV architecture is prohibited from precluding support a secure downloading for a SCP system. The downloaded SCP system can optionally depend on specific service protection requirements.
- The IPTV architecture is prohibited from precluding support the verification and authentication of the downloaded SCP system mechanisms.

6.3.4 Network Security

Architecture requirements

- The IPTV architecture is required to support the capability of preventing the DoS attack to network.
- The IPTV architecture is required to support the provision of security measures to block illegal or unwanted traffic.
- The IPTV architecture is required to support network operators to prevent that the network topology and its resources are visible to unauthorized entities.
- The IPTV architecture is required to be capable of supporting a network which uses content label information in order to control access to content.

- The IPTV architecture is required to be hardened against attacks on multicast capabilities.
- The multicast architecture is required to support the capability of multicast protocol adjacency authentication in order to establish a reliable peer.

Architecture recommendations

- To protect the home network from malicious or unauthorized access, the IPTV architecture is recommended to support the ability for the DNGF to establish a firewall, with multiple levels of security and appropriate application level gateways [ATIS-0800002].

6.3.5 Terminal Security

Architecture requirements

- The IPTV architecture is required to support terminal device protection, as defined in clause 3.
- The IPTV architecture is required to support a method to authenticate IPTV terminal devices.
- The IPTV architecture is required to support physical tamper-resistance for terminal device.
- The IPTV architecture is required to support a means to detect when physical tampering has occurred for terminal device.
- The IPTV architecture is required to support secure download and installation of the SCP operating code to IPTV terminal devices.
- The IPTV architecture is required to support a secure means for performing security critical processes in IPTV terminal device, such as key management and media serialization, to abort playback of content in the event of a security related malfunction, detection of tampering, or other indication of misuse.
- The IPTV architecture is required to provide physical protection of sensitive security enabling processes and components involved in the processing transmission and storage of valued content in IPTV terminal device in case no logical protection (such as encryption or serialization watermarks) is present. These processes include descrambling and media serialization (content tracing).
- The IPTV architecture is required to recognize the need for physical protection of sensitive security enabling processes in IPTV terminal device, including descrambling and media serialization (content tracing), critical data supporting those processes, as well as for all components involved in the processing, transmission, and storage of any valued content lacking logical protections such as encryption or serialization watermarks.
- The IPTV architecture is prohibited from precluding to support the interchange of content between an IPTV terminal device and other (physical or logical) devices provided that the uses granted for this content includes such an interchange.

6.3.6 Subscriber Security

Architecture requirements

- The IPTV architecture is required to support User Privacy Protection, as defined in clause 3.
- The IPTV architecture is required to support a mechanism to allow an IPTV terminal device SCP component to authenticate the SCP servers.
- The IPTV architecture is required to allow a Subscriber to set an access control mechanism (e.g. a password) in order to restrict access to content and/or services.
- The IPTV architecture is required to support a mechanism for parental rating i.e., facilities for rating programs according to content.
- The IPTV architecture is required to be capable of indicating why access to content has been denied to the user.

- The IPTV architecture is required to allow for a mechanism for a Subscriber to request extensions (e.g. more plays, more play-time) to digital rights associated with specific content instances.

Architecture recommendations

- The IPTV architecture is recommended to allow the end user (as rights allow) to change, i.e. replace, an IPTV terminal device without inherently affecting its rights to consume content.

6.4 Network and Control Aspects

Architecture requirements

- The IPTV architecture is required to support mechanisms, inhibitors, and interfaces for the ITF to control the streaming of video content – i.e., trick modes [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for the ITF to decode EAN messages which communicate the following information, if required by national authorities [ATIS-0800002]:
  - A unique tag identifying the EAN event. This allows end devices to determine whether the event is new or a duplicate.
  - Originator of the EAN message.
  - EAN Priority (National, State, or local).
  - EAN Text for graphic overlay on current user programming
  - Network address (assumed to be IP multicast address) of Emergency Alert Video and associated audio.
  - Target Location ID – this is the geographic area that is compelled to handle the EAN it consists of State and county code. If the priority is National, then all areas are compelled to process the EAN.
  - Exempted Channels – the ID of content streams that are empted from the alert because they are direct processors of the EAN such that their content stream will contain the EAN without any intervention from the service provider.
  - An option to set a trigger for the start time and either duration or end time of the EAN.
- The IPTV architecture is required to support mechanisms to support the enforcement of parental controls in a manner consistent with ratings defined by each country [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for the service provider to support the enforcement of parental controls on a user profile basis or a policy basis – e.g. time limit [ATIS-0800002].
- The IPTV architecture is required to support mechanisms to forward notification messages to all, multiple, or a single user [ATIS-0800002].
- The IPTV architecture is required to support mechanism for forwarding and displaying notification messages based on pre-set preferences (e.g. do not disturb, service operator override).

Architecture recommendations

- The IPTV architecture is recommended to support the ability of both multicasting and unicasting transmission schemes.
- The IPTV architecture is recommended to support error handling capability for infrastructure components.
- The IPTV architecture is recommended to have the capability to support insertion of appropriately scoped advertisements (e.g. geographically or demographically) [ATIS-0800002].

- The IPTV architecture is recommended to support mechanisms for targeted advertising (e.g. based on user profile preferences) [ATIS-0800002].
- The IPTV architecture is recommended to support mechanisms for insertion of advertising content in non-video services [ATIS-0800002].
- The IPTV architecture is recommended to support service selection mechanism.

Architecture options

- The IPTV architecture can optionally support a PVR (DVR) function residing in either the end-user or service provider networks which supports content streaming control [ATIS-0800002].

6.4.1 Network

Architecture requirements

- The IPTV architecture is required to support the management and enforcement of the service providers' transport policies by the network provider [ATIS-0800002].
- The IPTV architecture is required to define mechanism to appropriately distinguish different forms of traffic – e.g. data and voice [ATIS-0800002].
- The IPTV architecture is required to support a mechanism for building associations between the non-video services and other stream types such as video and audio programs [ATIS-0800002].
- The IPTV architecture is required to support a mechanism for identifying the classification of the non-video service (independent, real time, and synchronized) [ATIS-0800002].
- The IPTV architecture is required to support a mechanism for the ITF to synchronize between different content streams [ATIS-0800002].
- The IPTV architecture is required to support the following triggers: [ATIS-0800002]
  - Time-in – Time used to trigger the consumption of the non-video service.
  - Time-out – The time to stop the use of the object.
  - Time-in and Time-out can also be used to indicate the window of relevance for the non-video service. For instance, IPG data would use this to indicate that the entries cover a specific time window.
- The IPTV architecture is required to support the capability for the ITF device to re-establish service without end-user intervention in the event of network outages [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to include interfaces that allow service elements within the architecture to obtain information about the location (e.g. postal address) of the end-user's end-point [ATIS-0800002].
- If the IPTV architecture is recommended to support mechanisms for accessing end-user location information in case of NGN-based IPTV, if the IPTV architecture includes them, which are compliant with emerging standards for such information – e.g. emerging ITU-T NGN standards for Network Attachment Control Function (NACF) interfaces [ATIS-0800002].
- The IPTV architecture is recommended to support the following flags related to non-video services [ATIS-0800002]:
  - Mandatory – The non-video service can not be ignored.
  - Discretionary – The ITF can optionally choose to ignore the non video service.
  - Advertisement – Declares the non-video service to be an advertisement.
  - Unsolicited – The data is not in response to a user request.

– Disposition – This indicates what is recommended to be done with the non-video service once it has been consumed. The disposition flag has several values including:

· Delete.

· Acknowledge – Send a message to the originator indicating it has been consumed.

· Persist – Stay resident for subsequent use, includes an expiration time (which can optionally be a value indicating never).

- The IPTV architecture is recommended to support redundancy and failover mechanisms for infrastructure components [ATIS-0800002].

Architecture options

- The IPTV architecture can optionally support a time reference that is traceable to national time standards [ATIS-0800002].
- The IPTV architecture is recommended not to put any constraint on latency sensitive services. [ATIS-0800002]
- The IPTV architecture can optionally require the ITF to provide mechanisms to detect and report service consumption events that are not detectable elsewhere in the IPTV infrastructure [ATIS-0800002].

6.4.1.1 Core and Metro Networks

6.4.1.1.1 Interworking between IPTV and PSTN/ISDN

Architecture recommendations

- The IPTV architecture is recommended to support the relevant network facilities for processing PSTN/ISDN incoming/outgoing calls.
- The IPTV architecture is recommended to support voice encoding/decoding capabilities, as per PSTN/ISDN incoming/outgoing calls.
- The IPTV architecture is recommended to be scalable as far as the processing of incoming/outgoing PSTN/ISDN calls per unit of time is concerned.
- The IPTV architecture is recommended to support real-time audio related to PSTN/ISDN incoming/outgoing calls, with a voice quality similar to that of PSTN/ISDN environments.
- The IPTV architecture is recommended to support call control service capabilities for the processing of incoming/outgoing PSTN/ISDN calls.

6.4.1.2 Access Network

Architecture requirements

- The IPTV architecture is required to support access networks in case of NGN-based IPTV as defined in NGN architecture.

6.4.2 Control protocol and signalling

Architecture requirements

- The IPTV architecture is required to support a means of signalling end users as to the occurrence of an emergency alert notification (EAN) regardless of the services currently being consumed by the end user [ATIS-0800002].

6.4.2.1 Transport protocol

Architecture recommendations

- The IPTV architecture is recommended to support mechanisms to assist in locating random access points in the media stream.

6.4.2.2 Roaming and Service Handover for mobility

Architecture requirements

- The IPTV architecture is required to support mechanisms for exchanging subscriber-related information between the visited service provider (where the end-user accesses the IPTV services) and the home IPTV service provider (where the end-user has its subscription to the IPTV services) in case mobility is supported.
- The IPTV architecture is required to support mechanisms for discovering and selecting end-user's service profile from the IPTV terminal device or the home service provider that will be used by the end-user whenever accesses such IPTV services from a visited service provider in case mobility is supported.
- The IPTV architecture is required to support mechanisms for discovering and selecting home provider IPTV services for roaming users in case mobility is supported.
- The IPTV architecture is required to support capturing the session control context information from the originating terminal device, and transferring them to the target terminal device by session transfer controller in case mobility is supported.

Architecture recommendations

- The IPTV architecture is recommended to allow service continuity over different networks.
- The IPTV architecture is recommended to support nomadism of end systems.
- The IPTV architecture is recommended to support device mobility that allows a mobile device to maintain its ongoing IPTV services while freely moving around.

6.4.2.3 Naming, addressing, and identification aspects

Architecture requirements

- The IPTV architecture is required to support a mechanism for assigning IP-addresses and subnet masks to an attaching DNG [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support both static and dynamic address allocation schemes, numbering and naming schemes.

6.4.3 Content distribution

Architecture requirements

- The IPTV architecture is required to support multicast means of communication to all end-users [ATIS-0800002].
- The IPTV architecture is required to allow the service provider to utilize the network providers' multicast delivery capabilities [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support mechanisms that allow IPTV services to be distributed to specific group of end-users.

- The IPTV architecture is recommended to support mechanisms for transmitting identification information related to end-users who want to receive or are selected to receive IPTV services.

6.4.3.1 Multicast and Broadcast distribution

Architecture requirements

- The IPTV architecture is required to define traffic management mechanisms for the differential treatment of IPTV traffic [ATIS-0800002].
- If IP transmission over power lines is supported in the Home Network, the IPTV architecture is required to support one or more instantiations of the IPI-1a interface [ATIS-0800002].
- The IPTV architecture is required to support channel change functionality in the ITF [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for transport of time of day to the Home Network [ATIS-0800002].
- The IPTV architecture is required to support IP filtering functions in the DNGF in order to prevent selected local multicast traffic on the HNS from appearing on the DN [ATIS-0800002].
- The IPTV architecture is required to support the ability to configure QoS rules at the DNGF that govern traffic mapping (upstream or downstream) for the different services [ATIS-0800002].

Home network requirements

- The Home Network (HN) is required to support at least one IPI-4 interface with sufficient bandwidth and QoS to support the IPTV services [ATIS-0800002].
- The Home Network (HN) is required to support at least one HNS IPI-1 interface with sufficient bandwidth to support the IPTV services [ATIS-0800002].
- The IPI-4a interface, if supported, is required to comply with the appropriate standard DSL specifications [ATIS-0800002].
- The IPI-4b interface, if supported, is required to comply with the appropriate optical access network specifications such as G.983, G.984 and IEEE802.3.
- The IPI-4c Interface, if supported, is required to support the transport of digital information, in packet format, over RF carriers over coax [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended support an IPTV terminal device with the capability to choose the desired format of the content if there are multiple formats available.
- The IPTV architecture is recommended to support the ability to simultaneously transport multiple video streams and voice and data over an IPI-4 interface [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to implement standard IP routing functions, per established IETF specifications [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to support routing functions per IPv4 specifications [ATIS-0800002].
- The IPTV architecture is recommended to support both IPV 6 and IPV4 [ATIS-0800002].
- The IPTV architecture is recommended to support static and dynamic address allocation schemes for both IPV4 and IPV6 [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to support the routing of IP packets between all interfaces toward the access/core network (WAN side of the HN), and toward the ITF (LAN side of the HN). Specifically, this means: [ATIS-0800002]
  - Routing is recommended to be supported from DN to HNS (downstream flow).

  - Routing is recommended to be supported from HNS to DN (upstream flow).
  - Routing is recommended to be supported from any HNS to any other HNS (bidirectional flows).
- The IPTV architecture is recommended to support the ability for the DNGF to support multiple logical IP interfaces (multiple attachment points at the IP layer) on any particular physical DN interface [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to assign IP addresses to devices in the Home Network [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to support channel change functions between the ITF and service provider [ATIS-0800002].
- The IPTV architecture is recommended to support automated configuration capabilities for the IPTV devices [ATIS-0800002].
- The DNG and ITF are recommended to support the status information report to the service provider [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support the ability to perform the bandwidth management of all HNS networks attached to the DNG [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support being the arbitrator for local traffic traversing from one HNS network to another HNS network, attached to the DNG [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support performing call admission functions to protect the home network from excessive and harmful traffic on any HNS, between two HNSs attached to the DNG, and between any HNS and any DN [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support the ability for the DNGF to perform policing functions on incoming traffic and drop offending traffic to protect the home network [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support routing IP traffic based on provision-able/manageable mechanisms to guarantee QoS for different service classes [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support mapping downstream traffic to corresponding local flows to provide QoS for the different services. This includes L3 to L2 mapping, based on the local HNS [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support mapping upstream traffic generated by the end-devices to corresponding outgoing flows to provide QoS for the different services. This includes L2 to L3 mapping [ATIS-0800002].

Home network recommendations

- The home network elements supporting IPTV services are recommended to support the authentication procedures required by the network and service providers [ATIS-0800002].
- The DNGF is recommended to support NAT/NAPT capability mapping IP address and port numbers between the public WAN and the LAN(s) [ATIS-0800002].
- If Ethernet over point-to-point CAT5 copper interface is supported in the home network, the IPI-1b Interface is recommended to comply with a standard such as IEEE 802.3 10/100/1000BaseT specifications. Multiple instances (multiple lines) may exist between the DNGF and the different devices implementing the ITFs [ATIS-0800002].
- If Ethernet over copper telephony wiring is supported in the home network, the IPI-1c Interface is recommended to comply with standard HomePNA over copper specifications, such as ITU-T G.9954 [ATIS-0800002] (additional resource may be HomePNA).

- If coaxial HNS networking is supported in the home network, the IPI-1d interface is recommended to comply with at least one of the coaxial transport specifications listed below: [ATIS-0800002] (Other technologies are possible)
  - HomePNA 3.0, per ITU-T G.9954.
  - Recommendation offered by the Multimedia over Coax Alliance (MoCA), which is a consortium of companies and not a formal standards organization. More information can be found at < http://www.mocalliance.org >.
  - TVnet technology offered by Coaxsys, which argues for a simple solution that does not require software to operate.

  NOTE – There are at least three competing technologies for the transport of digital data over coax.
- If wireless HNS interface is supported in the home network, the IPI-1e Interface is recommended to comply with standard WiFi specifications, such as IEEE 802.11 a/g/n [ATIS-0800002].
- Where the Home Network transports multiple latency sensitive traffic types (e.g., the IPTV services and frequency distribution protocols, or time distribution protocols), these protocols and the Home Network infrastructure is recommended to be configured such that they do not impact the latency requirements of each service [ATIS-080002]**.**

Architecture options

- The IPTV architecture can optionally support content sharing between devices in the home network.

6.5 End Systems and Interoperability aspects

Architecture requirements

- The IPTV architecture is required to provide the end-user the ability to select and switch between supplementary content that is associated with the main video content, if available.
- The IPTV architecture is required to support the end-user ability to select preferred supplementary content for sign language with a selectable preferred on-screen layout.
- The IPTV architecture is required to support the ability for the IPTV terminal device to decode video, audio, subtitles, captioning, supplementary video and descriptive audio and present them to the end-user.
- The IPTV architecture is required to support the capability of receiving and processing the metadata for content coming from content providers [ATIS-0800002].

Terminal device requirements

- The IPTV terminal device is required to support system start-up and initialization function.
- The IPTV terminal device is required to have the ability to select and receive multiples audio sources. (E.g. one with audio description)

Architecture recommendations

- The IPTV architecture is recommended to support content delivery in several yet optional versions to be selected according to the capabilities of the IPTV terminal device receiving the content (e.g. access rate, resolution, supported formats, etc.).
- The IPTV architecture is recommended to support the ability to identify wireless network characteristics information sent by the IPTV Terminal.

Terminal device recommendations

- The IPTV terminal device is recommended to be able to display the service logo.

- The IPTV terminal device is recommended to support skip forward and skip backward (e.g. by time period, interval, location in content) in broadcast TV with trick mode.
- The IPTV terminal device is recommended to support skip forward and skip backward (e.g. by time period, interval, location in content) in VoD service.
- The IPTV terminal device is recommended to support skip forward and skip backward (e.g. by time period, interval, location in content) in client PVR service.
- The IPTV terminal device is recommended to support skip forward and skip backward (e.g. by time period, interval, location in content) in network PVR service.
- The IPTV terminal device is recommended to allow the user the selection of subtitles or captions being displayed with a solid background or a transparent one.
- The IPTV terminal device is recommended to be able to declare its usage environment description to the service provider.

Architecture options

- The IPTV architecture can optionally support signalling capabilities for transmitting bandwidth related information.
- The IPTV architecture can optionally use the bandwidth related information to determine the appropriate content coding means to deliver the content.

Terminal device options

- The IPTV terminal device can optionally have the capability to provide information regarding its bandwidth availability.
- The IPTV terminal device can optionally have the capability to allow the end-user to adjust the size of the subtitles or captions displayed.
- The IPTV terminal device can optionally have the ability to select from a range of languages, speed and verbosity for subtitles and captions.

6.5.1 End-user

Architecture requirements

- The IPTV architecture is required to support the end-user ability to choose and select one subtitle or closed caption flow from several that might be delivered with the IPTV content.

Architecture recommendations

- The IPTV terminal device is recommended to select the preferred subtitle or closed caption flow when several such flows are available with the IPTV content.

6.5.1.1 End-user of Linear TV

Architecture requirements

- The IPTV architecture is required to support the end-user ability to switch from any IPTV content to another.
- The IPTV architecture is required to support the end-user ability to access different IPTV contents on different IPTV terminals devices if the delivery network allows the simultaneous delivery of several contents (e.g. different IPTV content).
- The IPTV architecture is required to support the end-user ability to select an additional audio associated with the main content, e.g. Audio Description.

Architecture recommendations

- The IPTV architecture is recommended to support the end-user with the ability to select an audio alternative to receiving textual information (e.g. scrollbars).

Terminal device recommendations

- The IPTV terminal device is recommended to have the ability to select the preferred main and supplementary content associated with the main content.
- The IPTV terminal device is recommended to have the ability to discover and display any additional information (such as subtitles) delivered with the TV channel.

6.5.1.2 End-user of Linear TV with trick mode

Architecture requirements

- The IPTV architecture is required to support the IPTV terminal device ability to record all available accessibility features (captions, subtitles, descriptive audio and multiple video streams such as for sign-language) with the main content, whilst retaining the synchronisation of the original information.
- The IPTV architecture is required to support the IPTV terminal device ability of synchronising multiple video streams, captions, and subtitles when the video stream is paused.
- The IPTV architecture is required to support the IPTV terminal device ability to restart the previously selected associated accessibility features after a pause.

Architecture recommendations

- The IPTV architecture is recommended to support the end-user ability to replay what has just been watched on a TV channel.
- The IPTV architecture is recommended to support the end-user the ability to pause and later play in fast forward mode to catch up with the normal delivery time.
- The IPTV architecture is recommended to support the IPTV terminal device ability to allow the end-user to select any of the recorded accessibility features.
- The IPTV architecture is required to support the availability of accessibility features (captions, subtitles, descriptive audio and multiple video streams such as for sign-language) and their synchronisation with the main content when viewing in normal playback.

Architecture options

- The IPTV architecture can optionally support the IPTV terminal device ability to render available accessibility features with the main content when viewing in high-speed playback.

6.5.1.3 End-user of Time-shift TV

Architecture requirements

- The IPTV architecture, if time-shift TV is supported, is required to support the end-user ability to easily identify the TV channels delivering the selected content and the relative progress position in the delivery of this content.
- The IPTV architecture, if time-shift TV is supported, is required to support the end-user ability to switch easily between the TV channels which are delivering or about to deliver the same content but at different delivery time using the remote control keys (e.g. channel up, channel down).

6.5.1.4 End-user of VoD

Architecture requirements

- The IPTV architecture, if VoD is supported, is required to support the end-user ability to discover and browse content catalogue(s).
- The IPTV architecture, if VoD is supported, is required to support the end-user ability to select contents using a single criterion or a combination of criteria (such as title, reference, genre, keyword, director, actor, etc.).
- The IPTV architecture, if VoD is supported, is required to support the end-user ability to get the selected content streamed after authorization.
- The IPTV architecture, if VoD is supported, is required to support the end-user ability to pause and then resume watching the selected content.
- The IPTV architecture, if VoD is supported, is required to support the end-user ability to rewind or fast forward, with or without watching capability, the VoD content.

Architecture recommendations

- The IPTV architecture is recommended to support video-on-demand (VoD).

6.5.1.5 End-user of Push VoD

Architecture requirements

- The IPTV architecture, if push video is supported, is required to support the end-user option to receive content without being disturbed (e.g. when watching a TV channel, recording a content on a PVR, downloading from the Internet, having a videoconference, etc.) and without disturbing activities of the devices engaged in providing a service (e.g. recording a content on a PVR, etc.).
- The IPTV architecture, if push video is supported, is required to support the end-user ability to receive content with no impact on the storage allocated to the end-user.

Architecture recommendations

- The IPTV architecture, if push video is supported, is recommended to support the end-user option to be informed after push VoD Content reception is completed if not otherwise stated.

6.5.1.6 End-user of Client PVR service

Architecture requirements

- The IPTV architecture, if PVR is supported, is required to support the end-user ability to pause live incoming content on a PVR so that it can be "resumed" later and allow the continued watching the content in time shift mode.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to view an on-screen menu of content already captured.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to view a schedule of forthcoming items so they can choose content to record.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to choose whether recording of a new version of content replaces the old version or will co-exist with it.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to amend the list of items "cued" for capture.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to set up and manage multiple personal profiles on their PVR associated with one or more service providers.

- The IPTV architecture, if PVR is supported, is required to support the end-user ability to navigate and explore content segments using indexes.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to capture content onto the portable device, if the portable device has recording capability, over a network and transfer that content with associated metadata to their home device and other mobile devices with the permission of the service or content provider.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to play games that include pre-recorded content and links to broadcast programming.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to capture a multi-stream offering in such a way that when playing the content at a later date the different streams remain synchronous.
- The IPTV architecture, If PVR is supported, is required to support the end-user ability to select either audio, subtitle text, or both to be recorded along with the video, and to store this selection as "preference".
- The IPTV architecture, if PVR is supported, is required to support the end-user's rightful ability to check if any content searched for is playable on the IPTV terminal device.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to check if the end-user IPTV terminal devices are suitable for playing back the recorded content.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to record the content according to the metadata received from a broadcaster and then discard unwanted elements when the broadcaster updates the metadata.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to set a preference to see or block a specific content or range of contents depending on the purchasing needs or habits or interests.
- The IPTV architecture, if PVR is supported, is required to support the end-user ability to obtain the content selected to be recorded, even if there is a schedule change recoverable by the PVR (delayed broadcast, no overlapping with other programmed recording, etc.) without any specific end-user action.

Architecture recommendations

- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to capture and play back content on a Personal video Recorder (PVR).
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to decide whether to capture single or multiple episodes of a series or other programmed groupings.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to record the content of the buffer and continue recording so the entire content is captured if the device is already tuned to a particular source and has been buffering that content in memory. The IPTV terminal device can optionally support an indication method for providing next availability of desired content if the IPTV terminal device was not tuned to the desired content.
- The IPTV architecture, if PVR is supported, is recommended to support both the user centric and service centric profile management on the IPTV terminal device.
- The IPTV architecture is recommended to support third parties metadata (e.g. content recommendations) in addition to metadata from service/content providers.
- The IPTV architecture is recommended to allow the user to exchange user profile information among various devices.

- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to manage the storage space on their PVR system or give an appropriate provider(s) permission to do so e.g. items to be deleted next, permanently stored, etc.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to allow the PVR to automatically capture content based on consumer viewing behaviour (profiling).
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to allow a service provider to remotely control the functionality of the consumer PVR system (e.g. to capture settings, profiles, etc.).
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to select programmes for recording based on information provided by the service or content provider.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to move personal profiles to different PVRs or PVR systems in other physical locations, e.g. when upgrading the devices or while viewing in a hotel when on holiday.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to have PVR information seamlessly and automatically update time sensitive content (such as news and advertising) recorded on the PVR.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to make purchases after seeing promotional or advertising features which are part of the PVR content.
- The IPTV architecture, if PVR is supported, is recommended to support an update of the PVR recordings, if possible.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to set preferences on the PVR that allows it to capture subtitles or audio description in the native language of the end-user when programmes are transmitted in a foreign language.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to select content to be recorded depending on its characteristics such as broadcast quality, aspect ratio etc.
- The IPTV architecture, if PVR is supported, is recommended to support the capability for a network PVR function.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to see relevant, timely interstitials (commercials and promotional) when time-shifted viewing of content.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to pay a premium to replace advertising interstitials in certain events (such as live sport) with relevant programme content.
- The IPTV architecture, if PVR is supported, is recommended to support the end-user ability to display text, images and other associated content that broadcasters make available as enhancements to their programmes.

Architecture options

- The IPTV architecture can optionally allow retrieval of content in a segmented manner.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to insert captured advertisements or promotions along with the content being played back.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to edit recorded content.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to store "personal" content on network storage devices, e.g. if the end-user disk is full.

- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to make available personal information to another end-user within or outside of the home network through an external transmission path, or any removable medium.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to capture, through a PVR, a complete interactive package such as interactive TV that contains applications, data, text, graphics, video and audio files and links.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to record content from trusted content providers and be presented with an index of the content.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to choose what to record using third party metadata services.
- The IPTV architecture, if PVR is supported, can optionally support the end-user ability to pause what is being watched, view any other material, and then resume the original material from where it was paused.

Terminal device recommendations

- The IPTV terminal device is recommended to support the end-user ability to set up and manage multiple user centric profiles.

6.5.1.7 Emergency Telecommunication Information services

Architecture requirements

- The IPTV architecture is required to implement robust mechanisms for handling emergency telecommunications throughout the network, service and transport layers.
- The IPTV architecture is required to support priority channel(s) for emergency telecommunications.
- The IPTV architecture is required to support a high-priority interface to existing emergency telecommunications services (e.g. through PSTN or ISDN).
- The IPTV architecture is required to support routing of emergency telecommunications from the end-user to appropriate emergency response service(s).
- The IPTV architecture is required to support routing of emergency telecommunications from an emergency response service to end-user(s).
- The IPTV architecture is required to support the capability to give session control to the emergency response service, thus only the emergency response service can terminate a call and not the end-user.
- The IPTV architecture is required to support the capability to give the end-user's geographical location to the emergency response service(s).
- The IPTV architecture is required to support both authenticated and unauthenticated access to emergency telecommunication services.
- The IPTV architecture is required to support emergency telecommunications with alternative and multimedia content e.g. video, real-time text, voice and any combination thereof, as well as other forms of messaging.

6.5.1.8 End-users of Service Information

Architecture requirements

- The IPTV architecture is required to support the end-user ability to see the associated information (e.g. by pressing a specific remote control key) and to act upon it (e.g. to follow the link, to make a choice, to bet, to return).

Architecture recommendations

- The IPTV architecture is recommended to support the end-user ability to tune to a TV channel from the displayed list of authorized TV channels.
- The IPTV architecture is recommended to support the end-user ability to configure or watch a short list of the TV channels among those authorized to watch (free or subscribed channels).
- The IPTV architecture is recommended to support the end-user ability to get information about the available TV channels (name, logos, owner, website).

6.5.2 IPTV terminal devices

Architecture requirements

- The IPTV architecture is required to support an extensible method for the service provider to query for the ITF's capabilities and status [ATIS-0800002].
- The IPTV architecture is required to identify mechanisms for the service provider to manage the ITF and associated peripheral devices (e.g., display or storage devices) and the physical devices that implement the ITF [ATIS-0800002].

Terminal device requirements

- The IPTV terminal user interface is required to not rely on colour alone to convey information.
- When no relevant national regulations apply, the IPTV terminal device can optionally support the ability of presenting emergency messages in text, alert video and audio over normal program media streams, and also the ability of interrupting any audio stream, including the supplementary audio.

  NOTE – When relevant national regulations apply, the IPTV architecture is required to support national regulations.
- For multi-channel audio transmissions, the IPTV terminal device is required to implement the transcoding feature, e.g. from HE-AAC to DTS Surround or Dolby Digital Plus to Dolby Digital, if it is a multi-channel capable terminal.
- For multi-channel audio transmissions, the IPTV terminal device is required to have an S/PDIF interface.
- The IPTV terminal device without multi-channel audio capabilities is required to implement multi-channel decoders and downmix from multi-channel to stereo.

Architecture recommendations

- The IPTV architecture is recommended to allow multiple services with different contents to be displayed on a single IPTV terminal device.

Terminal device recommendations

- The IPTV terminal device is recommended to offer to the end-user a service navigation capability based on the metadata for the services available through each network e.g. RF tuning information.
- The GUI API module is recommended to include the following functions:
  - Graphic design and display functions;
  - UI control interface design and display functions;
  - Set image and video attribute functions;
- The IPTV terminal device is recommended to provide a user setting enabling selection of an opaque background for any on-screen display, i.e., text that is overlaid onto video, thereby making it easier to read.

- The IPTV terminal device is recommended to provide a user setting to change the default colours of text and background for on-screen displays, i.e. as a minimum, a combination of white text on a black background is recommended to be offered.
- The IPTV terminal device is recommended to provide a user setting to change the default size of text for on-screen displays.
- The IPTV terminal device is recommended to inform the user of the timing when an action (for example, downloading content) is complete.
- The IPTV terminal device is recommended to display Arabic numerals (1, 2, 3, 4) rather than Roman numerals (I, II, III, IV) where applicable to the language used.
- The IPTV terminal device is recommended to support the ability to display subtitles and captions in any character set of the content provider's choosing.
- The IPTV terminal device is recommended to maintain the end-user's selected subtitle and caption styles/options/modes/formats, supplementary audio content and supplementary video content as far as possible when switching between services.
- Any On-Screen Displays are recommended to be available via external interfaces.
- The IPTV terminal device is recommended to support diagnostic for IPTV terminal. The IPTV terminal device is recommended to support subtitles and caption decoding and display.
- The IPTV terminal device, when permitted, is recommended to acquire and save the audience rating information and send it to the server.
- The IPTV terminal device is required to support the ability to ask for the end-user's permission when a non-anonymous use of the end-user privacy related information is involved.
- Multi-channel capable IPTV terminal device is recommended to utilize for audio control, i.e. Dynamic Range Control, Programme Reference Level or Dialogue Normalisation and Downmix in the audio decoder.
- The IPTV terminal device is recommended to support pause.
- The IPTV terminal device is recommended to support an IP-based 2-way communication channel.
- The IPTV terminal device is recommended to support distributed Personal Video Recording functionality.
- The IPTV terminal device is recommended to communicate with the network servers in order to be aware of service availability.
- The IPTV terminal device is recommended to have the capability to decode and display captions in a separate window or overlaid with different colours, colours for different speakers as signalled by the content provider.

Architecture options

- The IPTV architecture can optionally support the ability to store, cache, update, and run applications on devices that implement the ITF [ATIS-0800002].
- The IPTV architecture can optionally support the ability for applications to be delivered to ITF implementing devices with a video service (i.e., streamed with the video), by user request over the two-way network connection, and by the service provider at the service provider's direction [ATIS-0800002].
- The IPTV architecture can optionally support the ability of ITF implementing devices to serve as a master monitor or switcher application that can be updated by the service operator and that can manage the execution of other applications [ATIS-0800002].
- The IPTV architecture can optionally support the ability for service provider-managed applications to be stored and executed in the devices implementing the ITF [ATIS-0800002].

- The IPTV architecture can optionally support the ability for video service-associated applications to be stored and executed in the devices implementing the ITF [ATIS-0800002].
- The IPTV architecture can optionally support user-requested applications to be stored and executed in the devices implementing the ITF [ATIS-0800002].
- The IPTV architecture can optionally have the ability to arrange displays of multiple video sources in different layouts.

Terminal device options

- The IPTV terminal device can optionally enable the Service Provider to customize and/or recommend use of audio visual means to indicate when IPTV terminal device is performing any function.
- The IPTV terminal device can optionally enable the skins to contain properties of the graphical entities of the EPG interface such as the fonts, the icons, the pointer, the background pictures, and the sound effect.
- The IPTV terminal device can optionally enable the specified skin style to be further customized according the graphical entities such as the fonts, the icons, the pointer, the background pictures, the sound effect and etc.
- The IPTV terminal device can optionally download the skin on boot process.
- The IPTV terminal device can optionally enable the end-user to access the remote control functions via GUI.
- The IPTV terminal device can optionally render the UI with the end-user preferred skin.

6.5.2.1 Video

Terminal device recommendations

- The IPTV terminal device is recommended to support the rendering of multiple IPTV content and layouts.
- The IPTV terminal device is recommended to support a set of relevant decoding capabilities such as, but necessarily limited, to SD and HD.

6.5.2.2 Audio

Terminal device recommendations

- The IPTV terminal device is recommended to support audio services.
- The IPTV terminal device is recommended to support mono, stereo and multi-channel audio decoding capabilities.

6.5.2.3 Interfaces

Terminal device recommendations

- The IPTV terminal device is recommended to provide a human control interface (for example an infrared remote-control).
- The IPTV terminal device is recommended to provide means for feedback of control actions to the end-user by visual and/or audio indications selected by the end-user.
- The IPTV terminal device is recommended to provide end-user interface(s) for control and feedback of control actions by external devices or additional software, e.g. Braille interpretive device.

6.5.2.4 Provisioning

Terminal device recommendations

- The IPTV terminal device is recommended to be easy to install and configure for operation.
- The IPTV terminal device is recommended to support self- and remote provisioning of services, including network configuration and device-specific service enabling tasks.

6.5.2.5 PVR

Terminal device recommendations

- The IPTV terminal device is recommended to support both internal and/or external control of PVR functionality.

6.5.2.6 Mobile IPTV terminal devices

Mobile terminal device recommendations

- The mobile IPTV terminal device is recommended to support service continuity.
- The mobile IPTV terminal device is recommended to be able to extract its own wireless network characteristics from the current wireless network.

6.5.2.7 Security and Authentication Functionality

- The IPTV terminal device is required to support subscriber authentication and identification information management.
- The IPTV terminal device is recommended to support service application authorization.
- The IPTV terminal device is recommended to support software upgrade and download authentication.
- The IPTV terminal device is recommended to support network security policy management.
- The IPTV terminal device is recommended to support key, token and registration information management.
- The IPTV terminal device is recommended to support parental control related information management.
- The IPTV terminal device is recommended to support content purchasing information management.
- The IPTV terminal device is recommended to support API for service provider functions such as locking screen (which disables the displayed image to change for a certain amount of time until, e.g. all the resources needed to be shown are ready and can be synchronized).

6.5.2.8 Media Service Functionality

- The IPTV terminal device is required to support Media decoding management.

6.5.2.9 SCP Functionality

- The IPTV terminal device is recommended to support the SCP model specified by the IPTV FG.
- The IPTV terminal device is recommended to support licence management.
- The IPTV terminal device is recommended to support right management.
- The IPTV terminal device is recommended to support decryption of media stream and data stream.
- The IPTV terminal device is recommended to support access to security information.

6.5.2.10 End User Interaction Functionality

- The IPTV terminal device is recommended to support receiving and dispatching event from end-user to application.

6.5.2.11 Terminal Management API

Middleware recommendations

- The IPTV terminal device is recommended to support remote management.
- The IPTV terminal device is recommended to support log management.
- The IPTV terminal device is recommended to support software version management.
- The IPTV terminal device is recommended to support server parameter configuration.
- The IPTV terminal device is recommended to support access mode and parameter configuration.
- The IPTV terminal device is recommended to support media device parameter configuration, such decoder.
- The IPTV terminal device is recommended to support subscriber configuration, such as access account, service account.

6.5.2.12 System Resource Management Functionality

Middleware recommendations

- The IPTV terminal device is recommended to support monitoring and management of terminal resources.
- The IPTV terminal device is recommended to support allocation and scheduling of terminal resource to application.

6.5.2.13 Internet Access Functionality

- The IPTV terminal device can optionally support Internet client management, such as Web browser, e-mail and news client.

6.5.2.14 GUI Functionality

- The IPTV terminal device is recommended to support Graph design and display function.
- The IPTV terminal device is recommended to support UI control interface design and display function.
- The IPTV terminal device is recommended to support setting of image and video attribute.

6.5.3 Content Provision

Architecture recommendations

- The IPTV architecture is recommended to support transfer interfaces to content producer or content owner that are independent of content formats.
- The IPTV architecture is recommended to support common metadata for content provisioning.
- The IPTV architecture is recommended to support metadata for specifying re-encoding, trans-coding of content and their output formats.
- The IPTV architecture is recommended to support the ability to collect statistical information about content popularity, audience rating, connected time and other information according to user profiles.
- The IPTV architecture is required to support the ability to ask for the end-user's permission when a non-anonymous use of the end-user privacy related information is involved.

6.5.4 End-user domain (home and extensions)

Architecture requirements

- The IPTV architecture is required to define the minimal set of functions that constitute a DNGF [ATIS-0800002].
- The IPTV architecture is required to define the minimal set of functions that constitute an ITF [ATIS-0800002].
- The IPTV architecture is required to specify physical implementation of DNGF and ITF [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to support a mechanism through which end-users can make content they produced/created available to other end-users [ATIS-0800002].
- The IPTV architecture is recommended to support mechanisms for end-users to control who is able to view end-user originated content; everyone versus a specific subset of people [ATIS-0800002].
- The IPTV architecture is recommended to support an IPTV services for the whole end-user domain, which can optionally consist of multiple home networks and stationary or mobile end-devices with direct wireless interfaces with the network provider domain – i.e., the IPTV architecture must allow for the whole end-user domain to belong to the same service domain [ATIS-0800002].
- The IPTV architecture is recommended to allow multiple network providers for a single home network – i.e., the IPTV architecture is recommended to allow a single home network to connect to more than one transport domain [ATIS-0800002].
- The IPTV architecture is recommended to allow different providers for the transport and these service strata – i.e., the IPTV architecture must allow a single home network to belong to separate transport and service domains [ATIS-0800002].
- The IPTV architecture is recommended to allow for multiple providers for different or similar services – i.e., the IPTV architecture must allow a single home network to belong to multiple service domains [ATIS-0800002].

6.5.5 Remote management

Architecture recommendations

- The IPTV architecture is recommended to allow the service provider to retrieve device information such as manufacturer name, model name and number, software version, firmware version, and profiles and levels supported.
- The IPTV architecture is recommended to support the service provider to provide information relating to the service provider such as a URL for a home page or help desk. For example, to provide a means for the service provider to direct the user to a central information point which would allow the service provider to offer additional services or assistance in case of difficulty.
- The IPTV architecture is recommended to allow the service provider to retrieve statistical information of usage, e.g. channels watched and duration with the user's permission.
- The IPTV architecture is recommended to allow the service provider to access service transaction related information such as usage patterns, e.g. changing between linear IPTV channels.
- The IPTV architecture is recommended to allow the service provider to be able to configure and monitor device connectivity, e.g. access network and home network parameters.
- The IPTV architecture is recommended to allow the service provider to be able to access device, network and content metrics important for QoS, e.g. dropped packet rates, jitter, integrity of transport streams, etc.

6.6 Middleware, Application and Content Platforms

6.6.1 General

Architecture requirements

- The IPTV architecture is required to support the ability to search for available content [ATIS-0800002].
- The IPTV architecture is required to have the capability to support information about the content available to the end user [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to facilitate the acquisition of content – e.g., VOD, Advertising [ATIS-0800002].
- The IPTV architecture is not recommended to preclude supporting the requirements related to the retransmission of the existing terrestrial, satellite and cable broadcast such as regional and regulatory.

Architecture options

- The IPTV architecture can optionally support UMF (Uniform Media Formats) for content provision, discovery, delivery and consumption.

6.6.2 Middleware

6.6.2.1 General

Architecture requirements

- The IPTV architecture is required to support a means to present the ITF with the time of day reference [ATIS-0800002].

Middleware requirements

- The IPTV middleware is required to support terminal device start-up and initialization function.
- The IPTV middleware is required to support server-side device start-up and initialization function.

Terminal device requirements

- The IPTV middleware, if trick mode is supported, is required to support play, pause and stop.

Architecture recommendations

- The IPTV architecture is recommended to support middleware transparency aiming to decouple business functionality from middleware-specific functionality which allows developers to change middleware application elements without significantly modifying business functionality for IPTV services.
- The IPTV architecture is recommended to support mechanisms for the end-user to log advertisement information of interest [ATIS-0800002].

Middleware recommendations

- The IPTV middleware is recommended to support pause in a DVR capable terminal or system.
- The IPTV middleware is recommended to manage skip forward and skip backward (e.g. by time period, interval, location in content, etc.).
- The IPTV middleware is recommended to support executing of multiple simultaneous applications [DVB-MHP].

- The IPTV middleware components are recommended to facilitate service processes interaction among one or more IPTV devices (e.g. a server and its clients, such as STB, security system, or VoD server) in an IPTV system.
- The IPTV middleware is recommended to be able to manage the information about the applications.

Middleware options

- The IPTV middleware can optionally support the decoding of SI (Service Information).
- The IPTV middleware can optionally support capabilities to run value-added applications.
- The IPTV middleware can optionally support shortcut mechanism for selection.
- The IPTV middleware can optionally support the presentation engine for the multimedia data (e.g. audio, video, graphics, text and images) providing the browsing, the synchronization, the interaction with the user, of such data.

6.6.2.2 Application programming Interfaces (API)

Middleware requirements

- The IPTV middleware is required to provide an API for stopping and starting the presentation of video and audio.
- The IPTV middleware is required to provide an API to communicate with IPTV services providers to implement media transmission and media control function.
- The IPTV middleware is required to provide the API to access metadata information.

Architecture recommendations

- The IPTV architecture is recommended to support the APIs to manage the resources for applications [ATIS-0800002].

Middleware recommendations

- The IPTV middleware is recommended to support an API to access information on removable storage device (e.g. USB key).
- The IPTV middleware is recommended to support the API for controlling (e.g. selection, showing and hiding) subtitle and closed captioning display [ATIS-0800002].
- The IPTV middleware is recommended to provide an API for DRM function to communicate with DRM system.
- The IPTV middleware is recommended to include an API to access user preferences (e.g. accessibility features and display settings) available on a removable storage device (e.g. smartcard).
- The IPTV middleware is recommended to provide service enabling API.
- The IPTV middleware APIs are recommended to be open, flexible, granular, self-contained and components-based.
- The IPTV middleware is recommended to provide an API to support a variety of mixed media formats to be presented together (e.g. an HTML text page embedding a video stream).
- The IPTV middleware is recommended to provide an API to support picture-in-picture.
- The IPTV middleware is recommended to support application management (e.g. applications lifecycles, applications states).
- The IPTV middleware is recommended to be hardware and OS independent.

Middleware options

- The IPTV middleware can optionally support the API to communicate with IPTV services providers [ATIS-0800002].
- The IPTV middleware can optionally provide an API for recording programs locally.

6.6.2.3 Captioning

Middleware recommendations

- The IPTV middleware is recommended to provide an API to manage captioning including the selection from a range of languages, speed and verbosity.

6.6.3 Metadata

6.6.3.1 Metadata structure

Architecture requirements

- The IPTV architecture is required to be able to refer various content and services from different IP sources (e.g. terrestrial, satellite, mobile, cable and the internet).

Metadata requirements

- The IPTV metadata is required to support the indication of which accessibility features are available for a TV programme, i.e. captions, subtitles in various languages, supplementary video and descriptive audio.
- The IPTV metadata is required to support the description of accessibility features, including language etc.
- The IPTV metadata is required to be able to describe contents and be extensible.

Metadata recommendations

- The IPTV metadata is recommended to be able to describe legacy channel number information specified by content providers.
- The IPTV metadata is recommended to be able to describe user preferences (e.g. for personal favourite channels).
- The IPTV metadata is recommended to support one or more Uniform Media Formats (UMF) that integrate multiple representations about the content including media coding formats, SCP information and SCP tools information.
- The IPTV metadata for any given instance is recommended to be uniquely identified by an ID.
- The IPTV metadata is recommended to support packages.
- The IPTV metadata is recommended to be able to describe the date of the last modification and the expiration period of metadata instance.
- The IPTV metadata is recommended to be able to describe the target audience.
- The IPTV metadata is recommended to be able to describe the User Generated Content (UGC).

Metadata options

- The IPTV metadata can optionally provide the following configuration information: type of service, type of terminal device, type of transmission medium, user preferences, available QoS levels, codecs, profiles, encoding configurations, etc.
- The IPTV metadata can optionally be aligned with the metadata in existing broadcasting services.

6.6.3.2 Metadata for EPG service

Metadata requirements

- The IPTV metadata is required to provide general information about a piece of content that does not change regardless of how the content is published or broadcast, (e.g. title, synopsis, parental control, rating, encrypted or not, price and conditions of availability like the number of plays in duration, credit list, actors, characters, key talent, key characters, writer, composer, conductor, review, critic's review, identification of the original content provider, and access means to a pricing server).
- The IPTV metadata is required to support the description of various types groups of programs series, and shows. (GroupInformation)
- The IPTV metadata is required to support the description of service providers (e.g. name, owner, logo, etc.). (ServiceInformation)
- The IPTV metadata is required to support the description of groups of consecutive schedule events together, which spans a given time period on a single service. (Schedule)
- The IPTV metadata is required to support the description of contents that can be acquired on demand (as opposed to broadcast), including start time of which content is available, end time of which content is unavailable, etc. (OnDemandProgram)
- The IPTV metadata is required to support newly assigned channel numbers for the respective IPTV services and the legacy channel numbers and the (geographical) location of the original broadcasters when retransmitted from broadcast networks.
- The IPTV metadata is required to support the channel description including source type, service type, service provider, etc.

Metadata recommendations

- The IPTV metadata is recommended to be able to describe advertisement content (e.g. commercial video).
- The IPTV metadata is recommended to be able to describe usage restriction, including regional restriction, output and DRM export control, trick mode (e.g. rewind, fast forward) enabled, maximum buffering size or duration, etc.
- The IPTV metadata is recommended to be able to describe: metadata publisher, owner and copyrights.
- The IPTV metadata is recommended to support various content rating standards (e.g. PG, MPAA, etc.).

6.6.3.3 Metadata for package service

Metadata requirements

- The IPTV metadata are required to allow not only the description of single content items but also the description of collection of content components defined as "package".
- The IPTV metadata for package service is required to describe synchronization (temporal) and spatial information between contents to allow contents to be consumed as the service provider intended.

Metadata recommendations

- The IPTV metadata for package is recommended to support the description of the various types of components.

6.6.3.4 Metadata provisioning

Architecture requirements

- The IPTV architecture is required to be able to support the service provider with the capability of creating or amending the metadata associated with a particular content.

Architecture recommendations

- The IPTV architecture is recommended to allow the content provider to create and amend the metadata associated with its own contents.

Architecture options

- The IPTV architecture can optionally allow anyone with rights/permission to create and amend the metadata associated with a particular content (e.g. reviews, comments, synopsis, etc.).
- The IPTV architecture can optionally support the input of multiple metadata formats [ATIS-0800002].

6.6.3.5 Metadata delivery

Architecture requirements

- The IPTV architecture is required to have a means to deliver the content metadata to the user, including terms and conditions (e.g. duration the viewer is entitled to consume the content, PPV, related expenses, etc.), available accessibility features (captions, subtitles, descriptive audio, and multiple supplementary video streams), etc.

Architecture recommendations

- The IPTV architecture is recommended to support both multicast and unicast metadata delivery.
- The IPTV architecture is recommended to be able to support fragmented metadata delivery.
- The IPTV architecture is recommended to support metadata protection (e.g. user preferences, usage history).
- The IPTV architecture is recommended to allow metadata delivery independently of content delivery.
- The IPTV architecture is recommended to support both the push and pull model for metadata delivery.
- The IPTV architecture is recommended to support a mechanism for the terminal device to know about metadata instance modifications.
- The IPTV architecture is recommended to support a metadata delivery protocol over IP in addition to the already existing MPEG-2 TS-based transport.
- The IPTV metadata can optionally be provided in conjunction with the audiovisual contents.

Architecture options

- The IPTV architecture can optionally support a mechanism to allow the user-customized content list to be updated.

Middleware options

- The IPTV middleware can optionally support metadata compression.

6.6.4 Content

6.6.4.1 Content Coding

Codec recommendations

- The IPTV codecs are recommended to support various content resolutions.
- The IPTV codecs are recommended to support various content aspect ratios, e.g. 4:3, 16:9.
- The IPTV codec is recommended to be content format independent when handling segmentation.

6.6.4.2 Content delivery

Architecture recommendations

- The IPTV architecture is recommended to support mechanisms for content downloading.
- The IPTV architecture is recommended to support the delivery of multiple audio streams. (E.g. one with audio description)
- The IPTV architecture is recommended to support fast forward and fast rewind at different speeds.
- The IPTV architecture is recommended to support both a pull and a push method of content delivery.
- IPTV architecture is recommended to support the download of content that is not only audio and video but other content such as games, text, graphics, applications, etc.
- The IPTV architecture is recommended to be able to distinguish geographic regions to offer targeted services (important e.g. for targeted advertising).
- The IPTV architecture is recommended to allow the delivery of User Generated Contents (UGC).

6.6.4.3 General Video Requirements:

- The IPTV terminal device is recommended to output video in accordance with accepted international standards.
- The IPTV terminal device is recommended to support video scaling.
- The IPTV terminal device can optionally support VBI capabilities.
- The IPTV architecture is required to maintain video and audio in sync (accurate lip-sync) as judged by the general viewer at all times.
- The IPTV architecture is recommended to allow the playback of recorded content in the same way as the playback modes provisioned in a typical DVD, e.g.: Normal speed play, Fast forward (at various speeds), Fast rewind (at various speeds), Pause, Frame by frame advance, Slow forward, Slow backward
- The video format is required to support a wide range of temporal sampling standards, bit-rates and picture resolutions to support the range of (applications) contained in this document.
- The IPTV architecture is recommended to support channel change latency of less than 2.5 seconds.
- The IPTV architecture is recommended to support for live TV suitable-quality video while maintaining a transmission to decode latency of less than 2 second.
- Colorimetry of video is recommended to be in compliance with [ITU-R BT.1361] in all video formats.

6.6.4.4 Specific Video Requirements

- The SD video profile is required to have Standard Definition video resolutions equivalent to existing broadcasts.

- The IPTV terminal device is recommended to provide native mode video output support, if it supports high definition outputs.
- The IPTV terminal device is recommended to support a combination of video scaling and de-interlacing.
- The video format is recommended to support interlaced and progressive format.
- The IPTV terminal device is recommended to be capable of outputting SD and HD video signals according to one or more of the existing interface standards for video signals, if it is HD-capable.
- The IPTV architecture is required to achieve for live video quality at typical IP broadband video bandwidths an equivalent acceptable quality as competitive cable, satellite and terrestrial.
- The IPTV architecture is recommended to achieve for VOD and other off-line content encoded at typical IP broadband video bandwidths (typical target 1.5 Mbit/s) a quality equivalent to typical DVD quality.

6.6.4.5 General Audio Requirements:

- The IPTV architecture is recommended to support Single (mono), dual (stereo) and multi-channel (at least 5.1 surround sound) audio transmission; different modes may be supported using different codecs.
- The IPTV terminal device is recommended to support downmix from multi-channel to stereo.
- The IPTV terminal device can optionally be capable of responding to user preference for adjusting dynamic range compression and control based on audio meta-data.
- The IPTV terminal device can optionally be capable of supporting user or network selection among a minimum of three levels of audio compression of dynamic range: uncompressed, intermediate and heavy.
- The audio format is required to provide audio depth equivalent to existing broadcasts, i.e. requiring a sampling rate of 48 kHz at 16-bit. Other sample rates and bit-depths may also be supported.
- The IPTV terminal device can optionally support increased capabilities (e.g. 6.1, 7.1 or greater) audio profiles.
- The IPTV architecture can optionally support increased capabilities (e.g. 6.1, 7.1 or greater) audio profiles.
- The IPTV architecture is recommended to support multiple language audios streams associated with each video.
- The IPTV architecture can optionally support clean audio.

6.6.4.6 Content replay

Architecture options

- The IPTV architecture can optionally allow replacement of interstitial materials. (e.g. Advertisers and broadcasters will, on replay of recorded content, want to replace interstitial material with more relevant interstitials based on parameters such as time of viewing, environmental triggers (such as weather, season etc.) and number of times seen).
- The IPTV architecture can optionally allow the replacement of content (e.g. advertisement, expired content, etc.).
- The IPTV architecture can optionally allow advertisers to ensure that their commercials are seen only by the appropriate audience (e.g. where a minor is replaying content, a commercial for an alcoholic beverage is recommended to be skipped).
- Content provisioning and management

Architecture requirements

- The IPTV architecture is required to support a mechanism for the service provider to ingest and store VoD content [ATIS-0800002].

Architecture recommendations

- The IPTV architecture is recommended to provide content providers with content management capabilities, such as uploading, deleting and replacing content.
- The IPTV architecture is recommended to support the integration and interoperability of all platform and processing equipment necessary for the acquisition and processing of content during the ingestion phase (e.g., applying DRM, insertion of commercials, encoding, editing).
- The IPTV content provisioning is recommended to support a transfer interface between content provider and service provider that is independent of content formats.
- The IPTV Architecture is recommended to support content streaming overlapped with content pulling.

Content management recommendations

- The content management is recommended to be able to track each content program and segment location in the distributed media servers.
- The content management is recommended to be able to keep track of the distribution sessions among media servers.
- The content management is recommended to keep statistical and historic data of content delivery and copy sessions. These data could be used for calculating content popularity and guiding future content distribution.
- The content delivery protocols are recommended to support multiple policies for content distribution (e.g. Scheduled content pushing, dynamic content pulling, multiple sources for content pulling, etc.).

Architecture options

- The IPTV content provisioning can optionally offer the service provider and content provider the ability to specify and exchange content distribution metadata, including metadata for re-encoding, trans-coding of content and their output formats.

Content management options

- The content management can optionally support request bandwidth and congestion control capabilities.
- The content location management module can optionally keep track of the real time content distribution sessions in order to provide distribution bandwidth control in operator's core network.

6.6.5 Service navigation

Architecture requirements

- The IPTV architecture is required to support IPTV content selection through an Electronic Content Guide.
- The IPTV architecture is required to support IPTV service selection through an Electronic Service Guide.
- The IPTV architecture is required to support the ability of the ITF to display and allow user selection of program, content, and service descriptions.

Architecture recommendations

- The IPTV architecture is recommended to support the end-user capability to view the EPG content either sorted or filtered or both by time or other criteria.

Middleware recommendations

- The IPTV middleware is recommended to support a means to change the style of EPG.

Service navigation system recommendations

- The IPTV Service Navigation System is recommended to support exchange of information with other applications.
- The IPTV Service Navigation System is recommended to support consolidation of program/content information from multiple IPTV metadata service providers.
- The IPTV Service Navigation System is recommended to support IPTV service and content searching.
- The IPTV Service Navigation System is recommended to present always up-to-date information.

Service navigation system options

- The IPTV service navigation system can optionally support the customised presentation of the service and content information.
- The IPTV service navigation system can optionally adapt the information presentation to various terminal types.
- The IPTV service navigation system can optionally allow user to store metadata about user-customized content list.

6.6.6 Service/Content Discovery and Selection

Architecture requirements

- The IPTV architecture is required to support the mechanism for service discovery and delivery.
- The IPTV architecture is required to support a network based capability for the end-user to select the content to be delivered [ATIS-0800002].
- The IPTV architecture is required to support the ability for a user to interact with service operator-controlled server-side services through the 2-way network [ATIS-0800002].

Middleware recommendations

- The IPTV middleware is recommended to support the ability of the ITF to declare its usage environment description to the service provider.
- The IPTV middleware is recommended to support the ability of the ITF to obtain the usage environment description from the service provider.

Architecture recommendations

- The IPTV architecture is recommended to support several content selection modes (e.g. program navigation, channel switch, search, etc.).

Architecture options

- The IPTV architecture can optionally support profile/encoding negotiation capabilities to adapt to heterogeneous usage environments.

6.6.7 Returned data

Metadata recommendations

- The IPTV metadata is recommended to support the description of audience information. (e.g. channel number before and after channel change, time of change and user information for EPG service, and package identification, time of play and user information for package service).

Architecture options

- The IPTV architecture can optionally allow demographic data to be returned from the end-user device.

6.7 Public interest

6.7.1 Accessibility

Provide accessibility for people with disabilities or people with special needs and meet the minimum regulatory requirements.

Additionally, these requirements will provide accessibility for people with temporary environmental dysfunctions to include people with varied or different languages, to those with learning difficulties and to those whose capabilities are diminished by age and degeneration By 2015, it is estimated that 50% of the population will be over the age 50* and require accessibility features, therefore making such features mainstream requirements. It is also noted that some of these accessibility features are presently mainstream in their use and have been included in other clauses in this document. Appropriate references to those other clauses for such accessibility features are included in the list below as an aide for the implementer, as national regulation can optionally apply.

(NOTE – Some of the following requirements below may have regulatory implications in some countries and may not be required for all video IPTV applications, this may change over time. National regulations may place specific additional requirements that shall be honoured.)

As the high level requirements, the architecture and services is required to provide:

Architecture requirements

- The IPTV architecture is required to support mechanisms to support subtitles and closed captions.
- The IPTV architecture is required to support the ability of the ITF to decode and display subtitle or closed caption information.
- The IPTV architecture is required to support the subtitles and captions and vary its presentation in a separate window.
- The IPTV architecture is required to support the ability to select and receive two (related) video sources simultaneously (e.g. one with sign language translation).
- The IPTV architecture is required to support the ability to select and receive two audio sources (e.g. one with audio description).
- The IPTV architecture is required to support the end-user ability to be notified and receive regulatory information services, e.g. EAN messages (un-associated with TV channels) whenever the IPTV terminal device is active (e.g. displaying an EPG or a channel).
- The reception of regulatory information services is required to trigger mechanisms to draw the customer attention.

Terminal device requirements

- The IPTV applications and equipment is required to be designed using principles of Universal Design so that a wider population with users of varying capabilities can access such applications and equipment
- The IPTV Metadata is required to contain information about the provision of accessibility features.

Architecture recommendations

- The IPTV architecture is recommended to support good quality audio transmission and reproduction to make it possible for people to perceive the sound well. Reference needed.
- The IPTV architecture is recommended to support video transmission with sufficient quality for sign language perception if there is sign language in the contents [ITU-T H.Sup.1].
- The IPTV architecture is recommended to support video transmission with sufficient quality for lip reading perception [ITU-T H.Sup.1].
- The IPTV architecture is recommended to apply the ITU-T accessibility checklist to the work on IPTV [Accessibility Checklist].

Terminal device recommendations

- The IPTV terminal device is recommended to process emergency messages if they are available in the transmission infrastructure.
- The recording of accessibility features is recommended to be done in such a way that, when watching the recording, they can be both switched on and switched off. Therefore, it is a good idea to record all accessibility features streams and link them to the service as a whole.

6.7.2 Emergency telecommunications

Architecture requirements

- The IPTV architecture is required to support emergency alert service where required by regulation or law of the country – e.g., ANSI J-STD-042-2002 [ATIS-0800002].
- The IPTV architecture is required to support appropriate interfaces to support the receipt of suitably authorized emergency alert information where emergency alert service is provided [ATIS-0800002].
- The IPTV architecture is required to support the ability for the ITF to decode and display emergency alert information [ATIS-0800002].
- The IPTV architecture is required to support an open and standardized Interface to public emergency domains.

Architecture recommendations

- The IPTV architecture is recommended to support the capability of logging and forwarding emergency alert notifications when used as the emergency messages distribution system.
- The IPTV architecture is recommended to support the delivery of the specific emergency messages to the corresponding user groups based on pre-defined policies (e.g. geographic location).
- The IPTV architecture is recommended to support identification of the alerting messages sources and to support the classification of such messages upon pre-defined policies.

6.7.3 Provider Selection and Portability

Architecture recommendations

- The IPTV architecture is recommended to support a mechanism for customers to select IPTV network providers, IPTV services providers, and IPTV content providers with their preference.

Architecture options

- The IPTV architecture can optionally support number portability capabilities.

Bibliography

[b_EN 1332-4] CEN Identification Card Systems – Man-Machine Interface – Part 4: Coding of user requirements for people with special needs.

Appendix I – Public Services cross-reference

(This Appendix does not form an integral part of this document.)

Listed here are the items in the public services section with a cross-reference to the individual requirements clauses in the main body that they relate to.

The IPTV Architecture is required to support mechanisms to support closed captioning: Clauses **6.1, 6.5, 6.5.1, 6.5.2**

The IPTV Architecture is required to support the ability of the ITF to decode and display closed captioning information.

The IPTV Architecture is required to support the ability to view the captions and vary its presentation in a separate window: Clause **6.5.2**

The IPTV Architecture is required to support the ability to select and receive two (related) video sources simultaneously, (e.g. one with sign language translation): Clauses **6.4.1, 6.4.2, 6.5, 6.5.2, 6.5.2.1**

The IPTV Architecture is required to support the ability to select and receive two audio sources, (e.g. one with audio description): Clauses **6.4.1, 6.5, 6.5.1.1, 6.5.2.2**

The audio transmission and reproduction is recommended to be of good quality to make it possible for people to perceive the sound well.

Video is recommended to be transmitted with sufficient quality for sign language perception if there is sign language in the contents: Clause **6.2**

Video is recommended to be transmitted with sufficient quality for lip reading perception: Clause **6.2, 6.3**

The ITU-T accessibility checklist is recommended to be applied to the work on IPTV [2].

The IPTV Applications and equipments is required to be designed using principles of Universal Design so that a wider population with users of varying capabilities can access such applications and equipment: Clauses **6.1, 6.1.3.1.4, 6.2, 6.5.1.1, 6.5.2, 6.5.2.3, 6.5, 6.6.3.1, 6.6.5**

The IPTV Metadata is required to contain information about the provision of Accessibility Features: Clauses **6.1.3.1.4, 6.5.2, 6.6.2.2, 6.6.3.1, 6.6.3.5, 6.6.5**

Any recording that the IPTV Terminal makes is required to also include the appropriate Accessibility Features. The recording of Accessibility Features is recommended to be done in such a way that, when watching the recording, they can be both switched on and switched off. Therefore, it is a good idea to record all Accessibility Features streams and link them to the service as a whole: Clauses **6.5.1.2, 6.5.1.6**

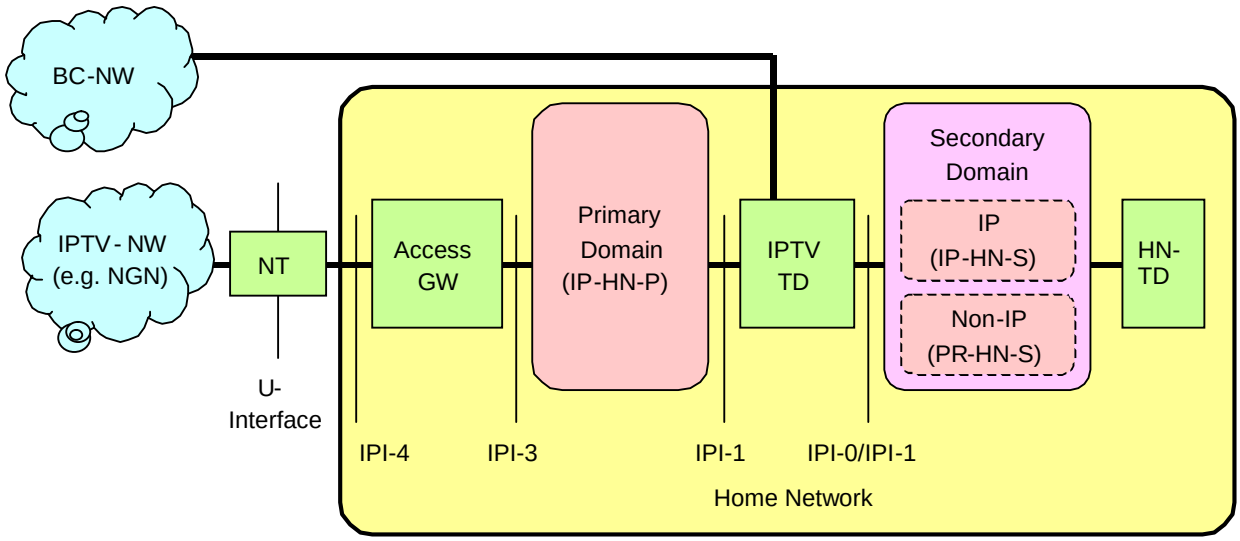
The IPTV architecture is required to support the end-user ability to be notified and receive regulatory information services (unassociated with TV channels) whenever the IPTV Terminal Device is active (e.g. displaying an EPG or a TV channel): Clause **6.4**

The reception of regulatory information services is required to trigger mechanisms to draw the customer attention: Clause **6.4.2**

The IPTV Terminal Device is recommended to process emergency messages if they are available in the transmission infrastructure: Clauses **6.1.4, 6.5.1.7**

Appendix II – Home Network (Consumer domain) Architecture

(This Appendix does not form an integral part of this document.)



IP-HN-P: Home network Primary
IP-HN-S: Home Network Secondary
PR-HN-S: Proprietary home Network Secondary

Figure II-1: Home Network architecture for IPTV end system

The each element can be defined as follows.

- Primary Domain (IP-HN-P)

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

- Secondary Domain

Secondary domain deals with IPTV related traffic between IPTV-TD and HN-TD. The devices and traffic dedicated to the secondary domain do not need to be configured to be reachable to/from access network. For example, there may be a case where locally assigned IP addresses are enough for this domain. Secondary domain can be divided into 2 parts, IP and non-IP, depending on the network layer protocol.

- IP Secondary Domain (IP-HN-S)

IP secondary domain is a part of secondary domain based on IP protocol.

- Non-IP Secondary Domain (PR-HN-S)

Non-IP secondary domain is a part of secondary domain based on non-IP protocol such as IEEE 1394.

The above architecture contains some interfaces indicating boundary between devices and domain. The interfaces are summarized in the table below.

Table II-1: Interfaces within Home Network

Interface		Note
IPI-0		Interface between IPTV-TD and HN-TD that has no direct connection with Access GW.
IPI-1		Upstream side interface of IPTV-TD or HN-TD. In case of HN-TD, the HN-TD has a direct IP connection with Access GW.
	IPI-1a	IPI-1 interface used for power line.
	IPI-1b	IPI-1 interface used for Ethernet (10/100 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 Access GW.
	IPI-3a	IPI-3 interface used for power line.
	IPI-3b	IPI-3 interface used for Ethernet (10/100 BASE-T).
	IPI-3c	IPI-3 interface used for Home PNA.
	IPI-3d	IPI-3 interface used for coaxial.
	IPI-3e	IPI-3 interface used for wireless.
IPI-4		Upstream side interface of Access GW.
	IPI-4a	IPI-4 interface used for connection with copper access network.
	IPI-4b	IPI-4 interface used for connection with optical access network through Ethernet interface.
	IPI-4c	IPI-4 interface used for connection with optical access network through coaxial interface.
	IPI-4d	IPI-4 interface used for connection with wireless access network.
U interface		Interface between IPTV-NW and Home Network. U interface and NT is outside of Home Network.

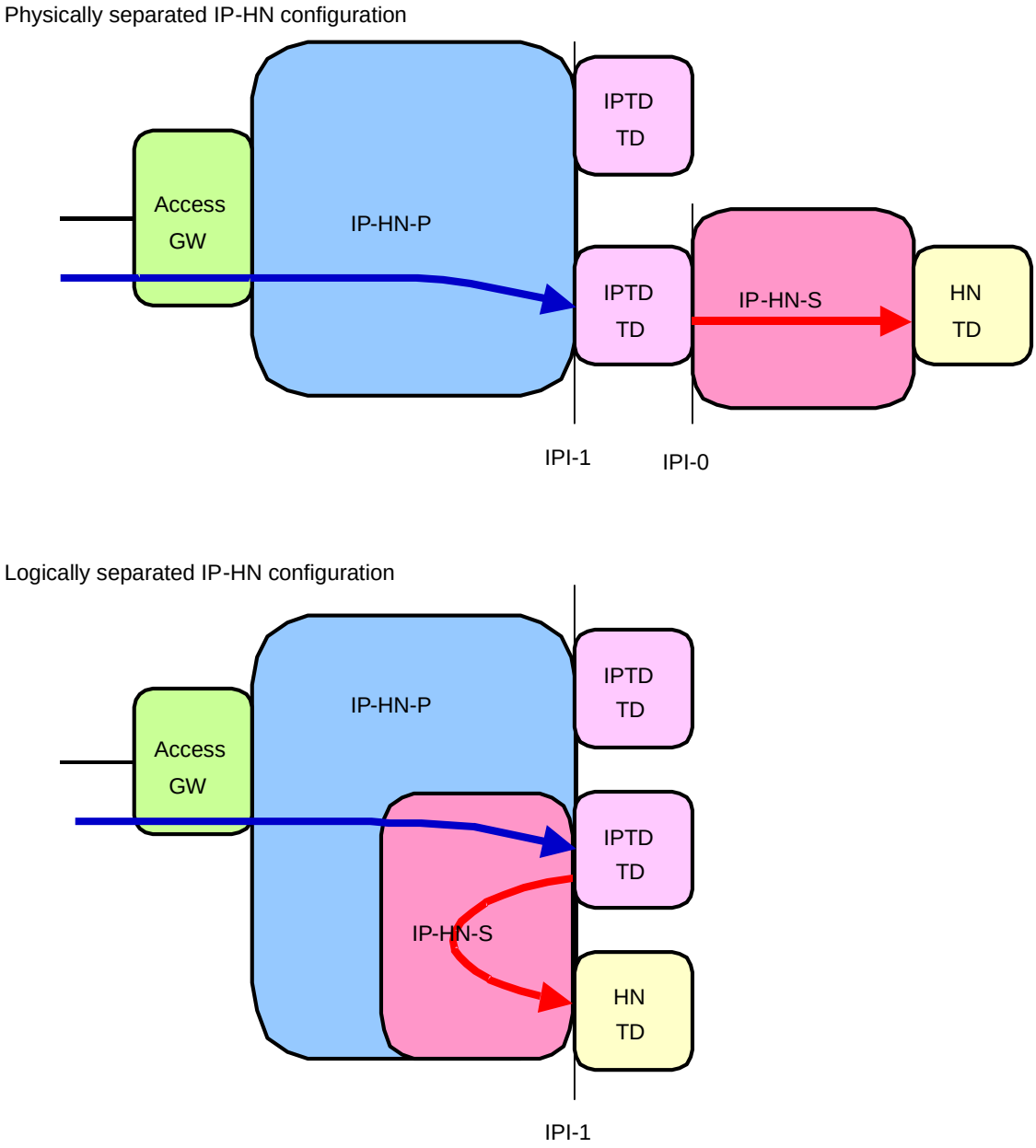


Figure II-2: Example configurations for IP-based home network

Figure II-2 shows an example of a physical configuration of IP-based Home Network. 2 Home Network areas, IP-HNP/IP-HN-S, can overlap physically as shown in the lower case of Figure II-2. HN-TD deals with IPTV related traffic only. Devices which do not handle IPTV traffic is required to be connected to IP-HN-S.

II.1.2 IPTV architecture

Summary

This document describes the IPTV functional architecture intended to support IPTV services based on the IPTV service requirements and definitions. Starting from a basic description of IPTV roles and services, a high level IPTV functional model is outlined. This model is then developed into a set of functional architectures which support NGN and non-NGN transport networks, as well as operation modes with or without IMS.

Keywords

IPTV, Architecture, IMS, NGN,

Current status

The document is complete, but there are still a number of areas where more work is required.

The following is a list of subject that were considered during discussions but that would warrant additional work for which there was no time:

- Content delivery of content streams and content files, and relative differences
- Multicast operation (address allocation, …)
- Third party applications, clarification of scope and functionality (relationship with legacy IPTV to be elaborated)
- Interworking between NGN non-IMS and NGN IMS architectural variants
- Restructuring of the document
- Better structure and use of procedures, and possible change to an Annex instead of appendix
- Relationship with other standards (ATIS IIF, ETSI TISPAN)

Dependency or relationship to other FG IPTV documents:

- IPTV service requirements document
- IPTV service scenarios document

CONTENTS

		Page
1	Scope	93
2	References	93
3	Definitions	94
	3.1 Terms defined elsewhere	94
	3.2 Terms defined within this document	94
4	Abbreviations and acronyms	94
5	Conventions	95
6	IPTV Domains	96
7	IPTV Architectural Approaches	97
8	IPTV Functional Architecture Framework	97
	8.1 End-User Functions	98
	8.2 Application Functions	98
	8.3 Content Delivery Functions	98
	8.4 Service Control Functions	98
	8.5 Management Functions	99
	8.6 Content Provider Functions	99
	8.7 Network Functions	99
9	IPTV Functional Architecture	99
	9.1 IPTV Architectural Overview	99
	9.1.1 End-User Functions	100
	9.1.2 Application Functions	101
	9.1.3 Service Control Functions	102
	9.1.4 Content Delivery Functions	102
	9.1.5 Network Functions	103
	9.1.6 Management Functions	104
	9.1.7 Content Provider Functions	104
	9.2 Architectural differences	104
	9.2.1 Differences between NGN-based and non-NGN-based IPTV architectures	104
	9.2.2 Differences between NGN-non-IMS-based and NGN-IMS-based IPTV architectures	104
	9.3 Description of Functions Specific to the Non-NGN IPTV Functional Architecture	104
	9.3.1 Control Client Functional Block	105
	9.3.2 IPTV Service Control Functional Block	105
	9.3.3 Service User Profile Functional Block	105
	9.3.4 Authentication and IP Allocation Functional Block	105
	9.3.5 Resource Control Functional Block	106

Page

9.4 Description of Functions Specific to NGN Non-IMS IPTV Architecture 106
9.4.1 Control Client Functional Block 106
9.4.2 IPTV Service Control Functional Block 106
9.4.3 Service User Profile Functional Block 106
9.4.4 Service Support Functions 107
9.4.5 NGN Service Stratum Functions 107
9.4.6 NGN Transport Stratum Functions 107
9.5 Description of Functions Specific to NGN IMS IPTV Architecture 108
9.5.1 Session Client Functional Block 108
9.5.2 Core IMS Functions 109
9.5.3 Service User Profile Functional Block 109
9.6 Description of Functions Common to the three Architectural Approaches 109
9.6.1 Application Functions 109
9.6.2 Application Client Functions 112
9.6.3 Content Delivery Functions 113
9.6.4 Network Functions 117
9.6.5 Content provider functions 117
9.7 Third Party Application Gateway Functional Block 117
9.8 Inter-working between NGN variants of the IPTV architecture 119
9.9 Reference Points 119
9.9.1 Reference Points common to all three IPTV Architectures 122
9.9.2 Reference Points specific to Non-NGN IPTV Architecture 125
9.9.3 Reference Points specific to NGN Non-IMS IPTV Architecture 126
9.9.4 Reference Points specific to NGN IMS IPTV Architecture 127

10 Interconnection between different IPTV networks 129
10.1 Interconnection between two NGN-based IPTV networks 129
10.1.1 Interconnection with the visited network 129
10.1.2 Interconnection with third party providers 130
10.2 Interconnection between Non-NGN IPTV network and NGN IPTV network 131
10.2.1 Interconnection with Non-NGN IPTV network 131
10.2.2 Interconnection with the third party provider network 132

Annex A – Relationship Between IPTV and NGN Architectures 133
A.1 IPTV related components in the NGN architecture 133
A.2 Functional Mapping between NGN-based IPTV and NGN architectures 134
A.3 Application Support Functions & Service Support Functions 135

Page

Appendix I – Procedural Flows Relating to IPTV Services 136
I.1 High level flows 136
I.1.1 High level procedural flows for loosely coupled Content-on-Demand 137
I.1.2 High level procedural flows for tightly coupled Content-on-Demand 138
I.1.3 High level procedural flows for loosely coupled Linear TV 140
I.1.4 High level procedural flows for tightly coupled Linear TV 142
I.1.5 High Level Procedural Flows for Initialization of IPTV Application Access 143
I.1.6 High Level Procedural Flows for Content Distribution 144
I.2 Procedural Flows for IPTV Services based on Non-NGN IPTV Architectures 147
I.3 Procedural Flows for IPTV Services based on NGN Non-IMS IPTV Architectures 147
I.3.1 Procedural Flows for Content On-Demand with Loose Coupling and Redirect 147
I.3.2 Procedural Flows for Content On-Demand with Loose Coupling and Proxy 149
I.3.3 Procedural Flows for Content On-Demand with Tight Coupling and Redirect 151
I.3.4 Procedural Flows for Content On-Demand with Tight Coupling and Proxy 153
I.3.5 Procedural Flows for Local Program adaptation for NGN linear IPTV 155
I.4 Procedural Flows for IPTV Services based on NGN IMS IPTV Architecture 156
I.4.1 Procedural Flows for VoD Service 156
I.4.2 Linear TV service procedural flows in NGN IMS IPTV 158
I.5 Procedural flows for IPTV interconnection between two NGN networks 159
Appendix II – IPTV Physical Network Hierarchy 162
Appendix III – Overlay Networking Function for IPTV Services and Multicast 163
Appendix IV – Adaptation of the IPTV Architecture for HFC Networks 164

IPTV architecture

1 Scope

This document describes the IPTV functional architecture intended to support IPTV services based on the IPTV service requirements and definitions [IPTV.REQ]. Starting from a basic description of IPTV roles and services, a high level IPTV functional model is outlined. This model is then developed into a more detailed functional architecture. Specific cases are also described in more detail.

The IPTV functional architecture may be based on use of existing network components and technologies, as well as on NGN architectures. This leads to three possible options for the architectural representations:

1. IPTV functional architecture for non-NGN network components (including existing networks)
2. IPTV functional architecture based on the NGN functional architecture, but not based on IMS
3. IPTV functional architecture based on NGN and its IMS component

The common elements between these alternatives as well as the differences are described in this document.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.112] ITU-T Recommendation J.112 (1998), *Transmission systems for interactive cable television services*

[ITU-T M.1400] ITU-T Recommendation M.1400 (2006), *Designations for interconnections among operators' networks*

[ITU-T Q.1290] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*

[ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in next generation networks*

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *NGN Framework Reference Architecture*

[ITU-T Y.2021] ITU-T Recommendation Y.2021 (2006), *IMS for Next Generation Networks*

[ITU-T J.700] ITU-T Recommendation J.700IPTV Service Requirements and Framework for Secondary Distribution

[IPTV.REQ] ITU-T FG IPTV working document (FG IPTV-DOC-0147r1), IPTV services requirements

[IPTV.WD-ALERM] ITU-T FG IPTV working document (FG IPTV-DOC-0186), Application Layer Error Recovery Mechanisms for IPTV Services

[ATIS-0800002] ATIS standard ATIS-0800002 (2006), IPTV Architecture Requirements

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.2 Functional architecture [ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE 1 – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

NOTE 2 – This definition is taken from [ITU-T Y.2012] and therefore relates to NGN. However, it is also valid for other networks, e.g. networks supporting IPTV.

3.1.3 Reference point [ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

NOTE – A reference point may correspond to one or more physical interfaces between pieces of equipment.

3.2 Terms defined within this document

This document defines the following terms:

3.2.1 Linear TV: A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed.

3.2.2 VoD: A service in which the subscriber can view video content whenever desired. The operating assumption is that the content is stored on the provider's VoD server. Subscriber accesses the movie from a library directory which may include search engine that accesses movie description and rating. Subscribers typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time when using this service.

4 Abbreviations and acronyms

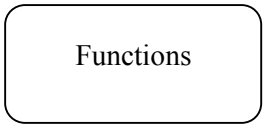
This document uses the following abbreviations and acronyms:

AS-FE	Application Support – Function Entity
CDF	Content Delivery Functions
CD&SF	Content Delivery & Storage Functions
CMTS	Cable Modem Termination System
CoD	Content on Demand
CP	Content Protection
CPF	Content Provider Functions
DNG	Delivery Network Gateway
DOCSIS	Data Over Cable Service Interface Specifications

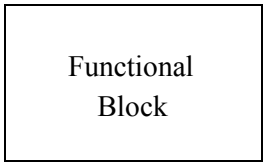
EPG	Electronic Programme Guide
FE	Functional Entity
HFC	Hybrid Fibre Coax
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IPTV	Internet Protocol TV
ITF	IPTV Terminal Function, IPTV TF
NACF	Network Attachment Control Functions
NGN	Next Generation Network
PVR	Personal Video Recorder
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RACF	Resource Admission Control Functions
RF	Radio Frequency
RTP	Real-time Transport Protocol
SC&DF	Service Control & Delivery Functions
SCF	Service Control Functions
SCP	Service and Content Protection
SIP	Session Initiation Protocol
SP	Service Protection
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VoD	Video on Demand

5 Conventions

Functions: In the context of IPTV architecture, "Functions" are defined as particular groupings of functions. It is represented by the following symbol:



Functional block: In the context of IPTV architecture, a "Functional Block" is defined as a group of function(s) that has not been further subdivided at the level of detail described in this document. It is represented by the following symbol:



NOTE – In the future other group or other document may possibly further subdivide these Functional Blocks.

Data Source: In the context of IPTV architecture, "Data Sources" are defined as particular sources of content, metadata and content protection information. They are represented by the following symbol:



6 IPTV Domains

Figure 6-1 shows the main domains that are involved in the provision of an IPTV Service. These domains do not define a business model. This decomposition does not preclude that one provider may be involved in the support of any given IPTV service across more than one domain.

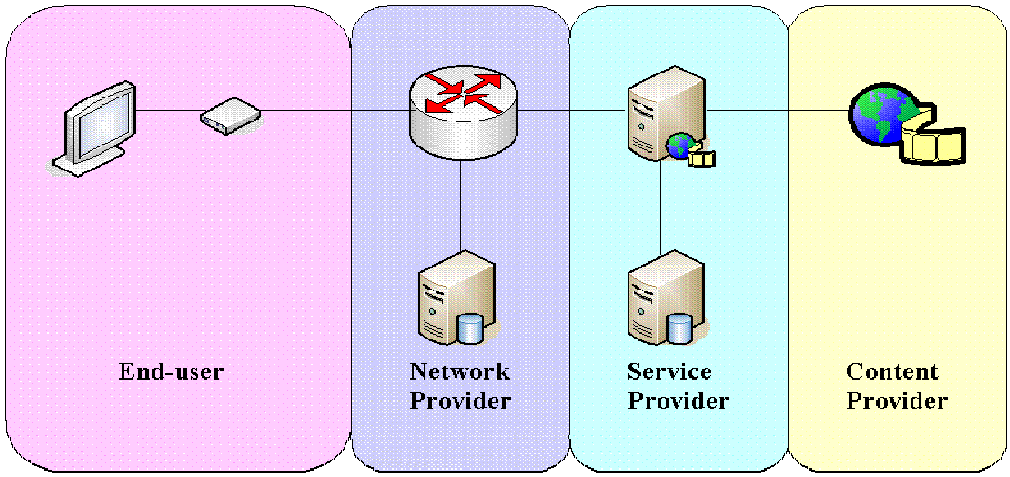


Figure 6-1: IPTV Domains

NOTE – In Figure 6-1, conventions defined in clause 5 are not used as this is not a functional architecture diagram.

The four IPTV domains are as described below:

Content Provider: The entity that owns or is licensed to sell content or content assets.

Service Provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider can optionally be a customer of another service provider.

NOTE – Typically, the service provider acquires or licenses content from content providers and packages this into a service that is consumed by the end-user.

Network Provider [ITU-T Q.1290]: The organization that maintains and operates the network components required for IPTV functionality. A network provider can optionally also act as service provider.

NOTE – Although considered as two separate entities, the Service Provider and the Network Provider may in fact be one organizational entity.

End User [ITU-T J.112]: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

NOTE 1 – An end-user is not necessarily a subscriber

The functional elements constituting these domains above will be described in more detail in section 8, of this document.

7 IPTV Architectural Approaches

This document identifies three IPTV architecture approaches that enable service providers to deliver IPTV services:

- (1) "Non-NGN IPTV functional Architecture" (Non-NGN IPTV): The Non-NGN IPTV architecture is based on existing IPTV network components and protocols/interfaces. The technology components, protocols and interfaces used in this IPTV architecture are already in widespread use and hence this approach is a representation of typical existing IPTV networks and services. This architectural approach may be used as the basis for evolution towards the other IPTV architectures listed below.

- (2) "NGN-based non-IMS IPTV Functional Architecture" (NGN-Non-IMS IPTV): The NGN Non-IMS IPTV architecture utilizes components of the NGN framework reference architecture as identified in [ITU-T Y.2012] to support the provision of IPTV services, in conjunction with other NGN services if required.

- (3) "NGN IMS-based IPTV Functional Architecture" (NGN-IMS-IPTV): The NGN-IMS based IPTV architecture utilizes components of the NGN architecture including the IMS component to support the provision of IPTV services, in conjunction with other IMS services if required.

In the following clauses, this document identifies the commonalities of the three architectural approaches identified above. This document also describes the main specifics of each architectural approach. This allows to facilitate the inter-working and to identify potential evolutionary paths between these architectural approaches.

8 IPTV Functional Architecture Framework

The IPTV Functional Architecture Framework shown in Figure 8-1 identifies the principal functional groups for IPTV. These functional groups provide a more detailed breakdown of the IPTV domains that are defined in clause 6.

The domains of Content Provider and End-User remain the same. The domains of Service Provider and Network provider are not used in the architecture as the commercial and operational boundaries that this implies are not appropriate to an architectural decomposition.

The functional groups in the architecture are derived by grouping related functions. How these functional groups are allocated across operational and organizational boundaries is out of scope of this document.

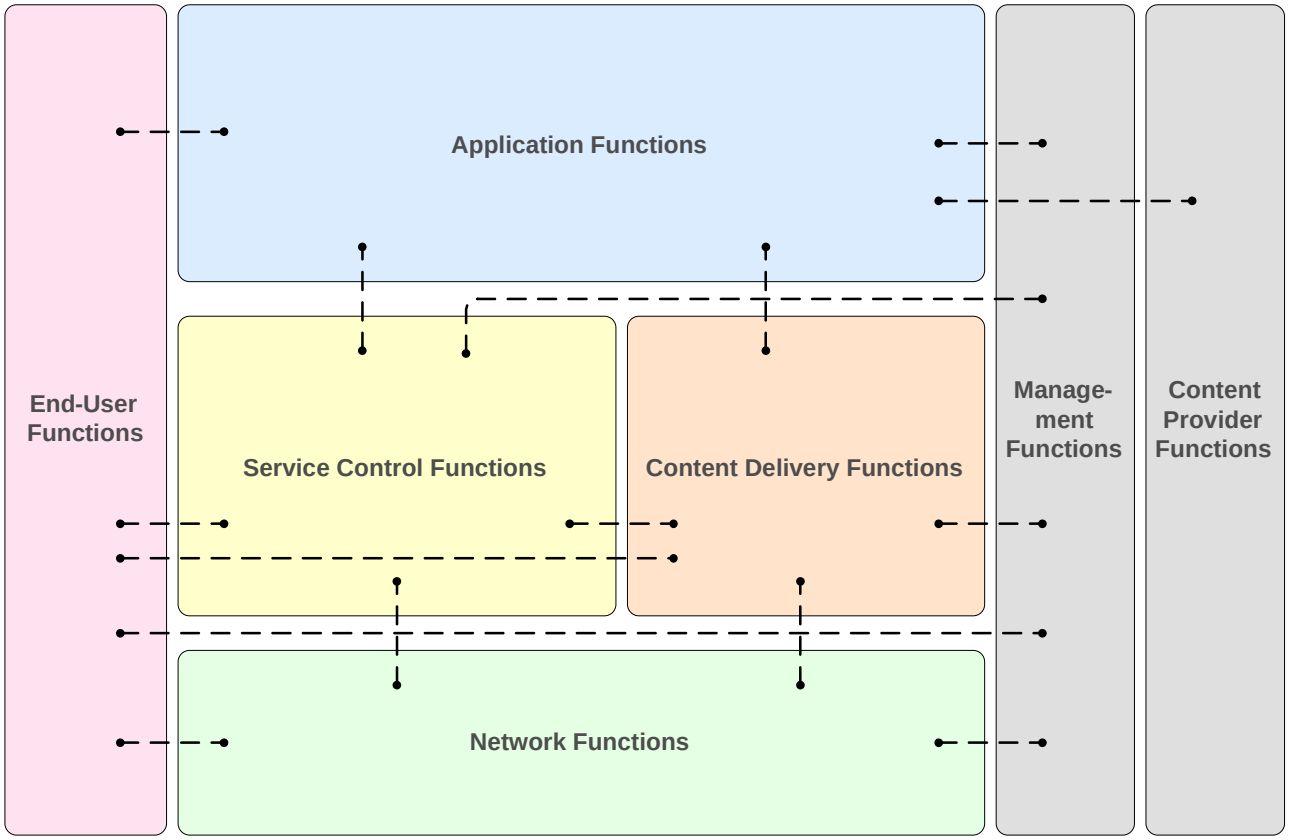


Figure 8-1: IPTV Functional Architecture Framework

The following sub-clauses give a description of each functional group. The related functions in each functional group are further decomposed in clause 9.

8.1 End-User Functions

The End-User Functions perform mediation between the end-user and the IPTV infrastructure.

8.2 Application Functions

The Application Functions enable the End-User Functions to select and purchase a content item.

8.3 Content Delivery Functions

The Content Delivery Functions (CDF) facilitate delivery of content from the Application Functions to the End-User Functions using the capabilities of the Network Functions.

Content is distributed from the Application Functions to the Content Delivery Functions before or during the service offering process.

Content Delivery Functions also support End-User Functions with the capability for playback control (e.g. trick mode play functionality with VoD and Network PVR).

8.4 Service Control Functions

The Service Control Functions provide the functions to request and release network and service resources required to support the IPTV services.

The Service Control Functions can request the Content Delivery Functions to allocate content delivery and storage capabilities and request the Network Functions to reserve network bandwidth for the content stream. The Service Control Functions may also obtain end user's current location from the Network Functions.

8.5 Management Functions

The Management Functions perform overall system management, status monitoring and configuration.

8.6 Content Provider Functions

The Content Provider Functions are provided by the entity that owns or is licensed to sell content or content assets (i.e. owner of the content, metadata and usage rights).

8.7 Network Functions

The Network Functions provide IP layer connectivity between the IPTV service components and the End-User functions. The Network Functions are shared across all services delivered by IP to an end-user.

The Network Functions contribute to provision of the Quality of Service (QoS) required by the IPTV services.

9 IPTV Functional Architecture

The functional architectures, shown in Figures 9-1 to 9-4, are based on Figure 8-1. The Functions identified in Figure 8-1 are used to structure their layouts. These functional architectures are expected to provide functionality for IPTV services. Figure 9-1 provides IPTV architecture overview while Figures 9-2, 9-3 and 9-4 respectively provide Non-NGN IPTV functional architecture, NGN-based non-IMS IPTV functional architecture and NGN IMS-based IPTV functional architecture.

Key to Figures

- The rectangular blocks represent functional blocks in the IPTV architecture.
- The rounded rectangular areas represent the particular grouping of functions.
- The solid lines represent direct relationships between either Functions or Functional Blocks.
- The dotted lines represent logical associations between End-User Functions and either Functions or Functional Blocks located outside the End-User Functions.

9.1 IPTV Architectural Overview

Figure 9-1 provides an overview of the IPTV functional architecture. Functions and Functional Blocks described in this clause are common to all architectural approaches as detailed in clause 7 except where stated differently.

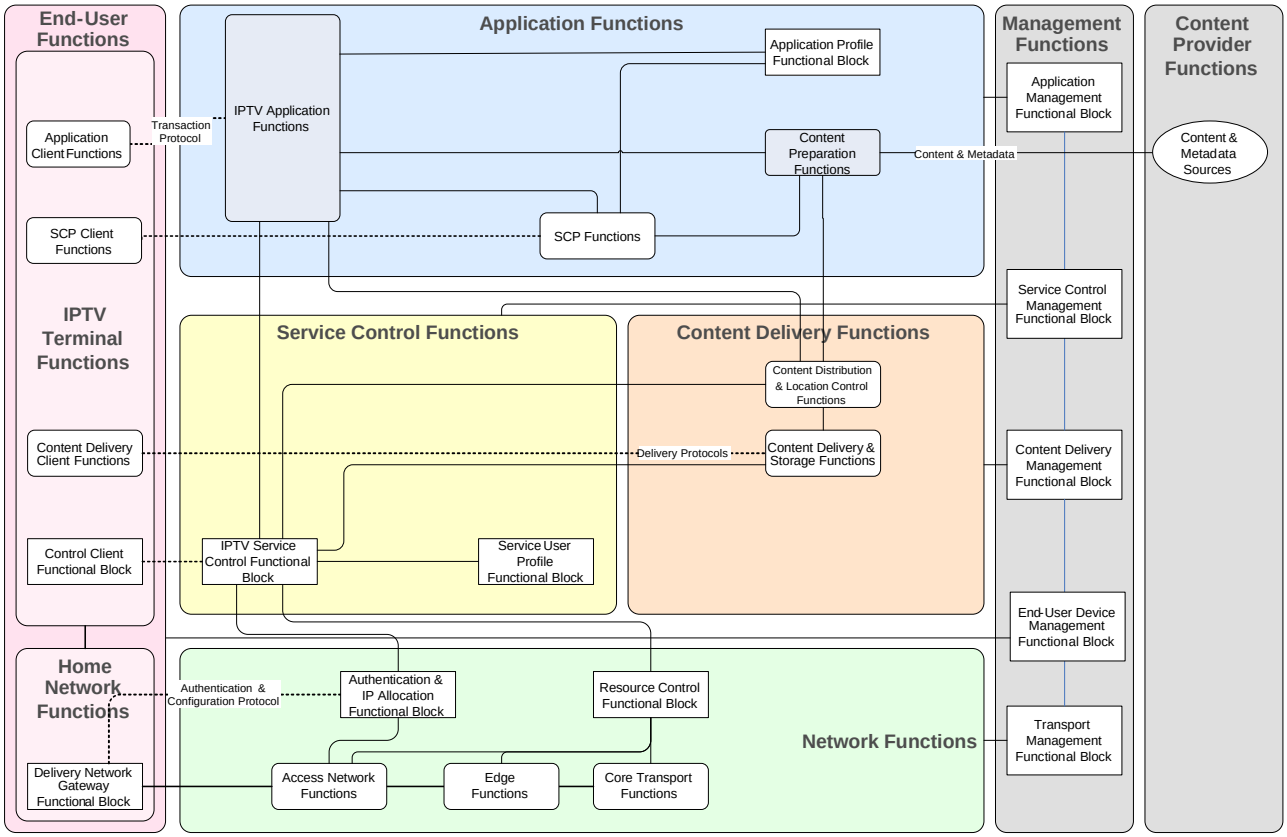


Figure 9-1: IPTV Architectural Overview

9.1.1 End-User Functions

The End-User Functions are comprised of IPTV Terminal Functions and the Home Network Functions.

9.1.1.1 IPTV Terminal Functions

The IPTV Terminal Functions (ITF) are responsible for collecting control commands from the end-user, and interacting with the Application Functions to obtain service information (e.g. EPG), content licences, and keys for decryption. They interact with the Content Delivery Functions to receive the IPTV services. They also provide the capability for content reception, decryption, and decoding.

9.1.1.1.1 Application Client Functions

The Application Client Functions exchange information with the Application Functions to support IPTV and other interactive applications.

9.1.1.1.2 Service and Content Protection (SCP) Client functions

These functions interact with the server side SCP functions to provide Service Protection and Content Protection.

9.1.1.1.3 Content Delivery Client Functions

The Content Delivery Client Functions receive and control the delivery of the content from its source. The Content Delivery Client Functions acquire the content data from the Content Delivery & Storage Functions. After acquiring the content, the Content Delivery Client Functions decrypt and decode it, and may also support playback control optionally.

9.1.1.1.4 Control Client Functional Block

The Control Client Functional Block allows the ITF to initiate service requests to IPTV Service Control Functional Block, in order to prepare for the connection to the Content Delivery Functions.

9.1.1.1.5 SCP Client Functions

The SCP Client Functions verifies the usage rights and decrypts the content.

These functions interact with the server side SCP functions to provide Service Protection and Content Protection.

9.1.1.2 Home Network Functions

The Home Network Functions provide the connectivity between the external network and each IPTV terminal device. These functions include IP connectivity, IP address allocation and configuration from the Network Functions to the IPTV terminal devices. All data, content, and control traffic must pass through the Home Network Functions in order to enter or exit the end-user's IPTV Terminal Device. The Home Network Functions serves as the gateway between the IPTV Terminal Functions and the Network Functions.

The Home Network Functions are comprised of the following Functional Blocks.

9.1.1.2.1 Delivery Network Gateway Functional Block

The Delivery Network Gateway Functional Block provides IP connectivity between the external network and the IPTV terminal device.

The Delivery Network Gateway Functional Block manages the IP connectivity, obtaining IP address(s) and configuration for the Home Network Functions and IPTV terminal devices.

9.1.2 Application Functions

The Application Functions are comprised of the following Functions and Functional Blocks:

- IPTV Application Functions
- Application Profile Functional Block
- Content Preparation Functions
- SCP Functions

9.1.2.1 IPTV Application Functions

The IPTV Application Functions provide the server side functions of the IPTV Applications. One of the roles of these Functions is to allow the IPTV Terminal Functions to select, and purchase if necessary, content.

When receiving requests from IPTV Terminal Functions, the IPTV Application Functions perform application authorization and execution of IPTV service logic based on user profile, content metadata and other information retrieved from relevant entities. The IPTV Application Functions also communicate with Content Delivery Functions to prepare the delivery of media content to IPTV Terminal Functions through Content Delivery Functions.

9.1.2.2 Application Profile Functional Block

The Application Profile Functional Block stores the profiles for the IPTV Applications.

9.1.2.3 Content Preparation Functions

The Content Preparation Functions prepare and combine the content such as VoD programs, TV channel streams, metadata, EPG data, as delivered by the Content Provider Functions, into the required delivery format.

9.1.2.4 Service & Content Protection (SCP) functions

The SCP functions control the protection of the services and content. Content Protection includes control of access to content and the protection of content using methods such as encryption. Service protection includes authentication and authorisation of access to services and optionally protection of the services using methods such as encryption.

9.1.3 Service Control Functions

9.1.3.1 IPTV Service Control Functional Block

The IPTV Service Control Functional Block provides the functions to handle service initiation, modification and termination requests, perform service access control, establish and maintain the network and system resources required to support the IPTV services requested by the IPTV Terminal Functions.

The Service Control Functions may:

- provide registration, authentication and authorization functions for the End-User Functions.
- process request from IPTV Applications and forward it to the Content Delivery Functions in order that the Content Delivery Functions select the most appropriate Content Delivery and Storage Functions, for delivering content to the End-User Functions.
- request the Content Delivery Functions or Application Functions to get charging information.

9.1.3.2 Service User Profile Functional Block

The Service User Profile Functional Block is used for storing service profiles and generating responses to queries for service profiles. The Service User Profile Functional Block also performs basic data management and maintenance functions.

9.1.4 Content Delivery Functions

The Content Delivery Functions receive content which was sent from the Content Preparation Functions and deliver it to the End-User Functions using the capabilities of the Network Functions.

For example, in case of On-Demand application, the Content Delivery Functions receive and distribute content items, e.g. a digital video file, to a set of video servers. The distribution may be rule based and/or usage based. The Content Delivery Functions also provide the mapping between the Content identifier provided by the IPTV Application Functions and the actual video server and content instance to be allocated to the Content Delivery Client Functions.

For example, in case of Linear TV application, the Content Delivery Functions receive one or more digital video streams and output these as IP multicast streams. The Content Delivery Functions may also provide the mapping between a logical channel number and the multicast address that the IPTV Terminal Functions will use for receiving the corresponding channel.

The Content Delivery Functions are comprised of the following Functions:

- Content Distribution & Location Control Functions
- Content Distribution & Storage Functions

9.1.4.1 Content Distribution & Location Control Functions

The Content Distribution & Location Control Functions include:

- Control the distribution of content from the Content Preparation Functions to the Content Delivery and Storage Functions.
- Gather the information regarding Content Delivery and Storage Functions, e.g. resources utilization, resources status (e.g. in-service and out-of-service), content distribution information, load status, etc.
- Perform the selection of a suitable Content Delivery and Storage Functions according to some criteria, e.g. the gathered information, the terminal capability, etc.

9.1.4.2 Content Delivery & Storage Functions

The Content Delivery & Storage Functions store and cache the content from Content Preparation Functions, and transfer the content data among peers.

The Content Delivery & Storage Functions are responsible for streaming and delivering (e.g. via RTP over UDP, Unicast or Multicast) content streams to the Content Delivery Client Functions via the Network Functions.

9.1.5 Network Functions

The Network Functions are shared across all services delivered by IP to an End-User Functions. The Network Functions provide the IP layer connectivity in order to support IPTV Services.

NOTE – the conventions defined in Clause 5 are not used in sub-clauses 9.1.5.3, 9.1.5.4 and 9.1.5.5 in order to maintain alignment with the terminology used in the NGN framework.

9.1.5.1 Authentication & IP Allocation Functional Block

The Authentication & IP Allocation Functional Block provides the functions to authenticate the Delivery Network Gateway Functional Block which connects to the Network Functions, as well as allocation of IP address to the IPTV Terminal Functions.

9.1.5.2 Resource Control Functional Block

The Resource Control Functional Block provides control of the resources which allocated for the delivery of the IPTV services through the Access Network, Edge and Core Transport Functions.

9.1.5.3 Access Network Functions

Access Network Functions are responsible for (1) aggregating and forwarding the IPTV traffic sent by the End-User Functions into the edge of the core network and (2) forwarding the IPTV traffic from the edge of the core network towards the End-User Functions.

9.1.5.4 Edge Functions

Edge Functions are responsible to forward the IPTV traffic aggregated by the Access Network Functions (as defined in sub-clause 9.1.5.2.1 above) towards the core network, and also to forward the IPTV traffic from the core network to the End-User Functions.

9.1.5.5 Core Transport functions

Core Transport Functions are responsible for forwarding IPTV traffic throughout the core network.

9.1.6 Management Functions

The Management Functions manage overall system status monitoring, configuration. This set of functions may be deployed in a centralized or distributed manner.

Management Functions are required for each of the main functional groups:

- Application Management Functional Block
- Content Delivery Management Functional Block
- Service Control Management Functional Block
- End User Device Management Functional Block
- Transport Management Functional Block

9.1.7 Content Provider Functions

Content Provider Functions provide the content and associated metadata to Content Preparation Functions, they contain the following sources:

9.1.7.1 Content and metadata Sources

The Content and Data Sources include content protection right sources, content sources and metadata sources for the IPTV services.

9.2 Architectural differences

9.2.1 Differences between NGN-based and non-NGN-based IPTV architectures

The NGN-based IPTV architecture is based on the NGN architecture defined in [**ITU-T Y.2012**] and uses the components and functions of the NGN. The non-NGN-based IPTV architecture does not necessarily require these components and functions and uses conventional and/or legacy network technologies for the delivery of IPTV services. The main differences are described below.

- The NGN-based IPTV architecture uses Network Attachment Control Functions (NACF) [presently under discussion in ITU-T SG13 to provide functions such as authentication and IP configuration.
- The NGN-based IPTV architecture uses Resource & Admission Control Functions (RACF) defined in [ITU-T Y.2111] to provide resource and admission control functions.
- The NGN-based IPTV architecture uses Service Control Functions defined in [ITU-T Y.2012] to provide service control functions.

9.2.2 Differences between NGN-non-IMS-based and NGN-IMS-based IPTV architectures

The NGN-IMS-based IPTV architecture uses Core IMS Functions and associated functions such as Service User Profile Functional Block defined in [ITU-T Y.2021] to provide service control functions. The NGN-non-IMS-based IPTV architecture uses Service Control Functions other than Core IMS Functions to provide service control functions.

9.3 Description of Functions Specific to the Non-NGN IPTV Functional Architecture

Functions and Functional Blocks described in this sub-clause are specific only to the non-NGN IPTV architecture except where stated otherwise.

Figure 9-2 shows the non-NGN IPTV functional architecture.

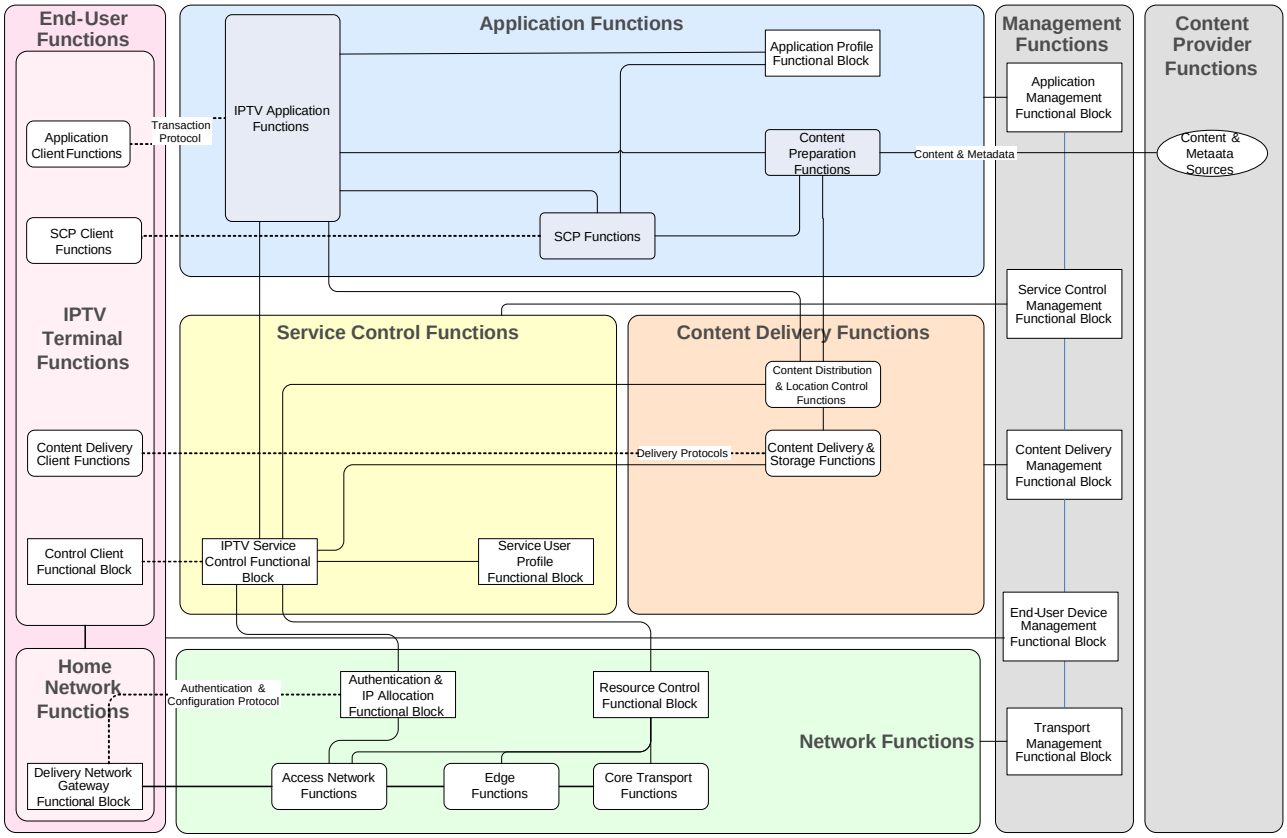


Figure 9-2: Non-NGN IPTV Architecture

9.3.1 Control Client Functional Block

The Control Client Functional Block allows the ITF to initiate service requests to IPTV Service Control Functional Block, in order to prepare for the connection to the Content Delivery & Storage Functions.

NOTE – This functional block is common with its counterpart in NGN Non-IMS IPTV functional architecture.

9.3.2 IPTV Service Control Functional Block

The IPTV Service Control Functional Block provides the functions to handle service initiation and/or termination requests, perform service access control, establish and maintain the network and system resources required to support the IPTV services requested by the IPTV Terminal Functions.

NOTE – This functional block is common with its counterpart in NGN Non-IMS IPTV functional architecture

9.3.3 Service User Profile Functional Block

The Service User Profile Functional Block is used for storing service profiles, subscriber-related data, such as location data, and presence status data, etc. The Service User Profile Functional Block generates responses to queries for service profiles. The Service User Profile Functional Block also performs basic data management and maintenance functions.

9.3.4 Authentication and IP Allocation Functional Block

The Authentication and IP Allocation Functional Block provides the functions to authenticate the Delivery Network Gateway Functional Block which connects to the Network Functions, as well as allocation of IP address.

9.3.5 Resource Control Functional Block

The Resource Control Functional Block provides control of the resources in the Access Network, Edge and Core Transport Functions to allow appropriate resources to be provided for content delivery.

9.4 Description of Functions Specific to NGN Non-IMS IPTV Architecture

Functions and Functional Blocks described in this sub-clause are specific only to the NGN Non-IMS IPTV architecture except where stated otherwise.

Figure 9-3 shows the NGN Non-IMS IPTV functional architecture.

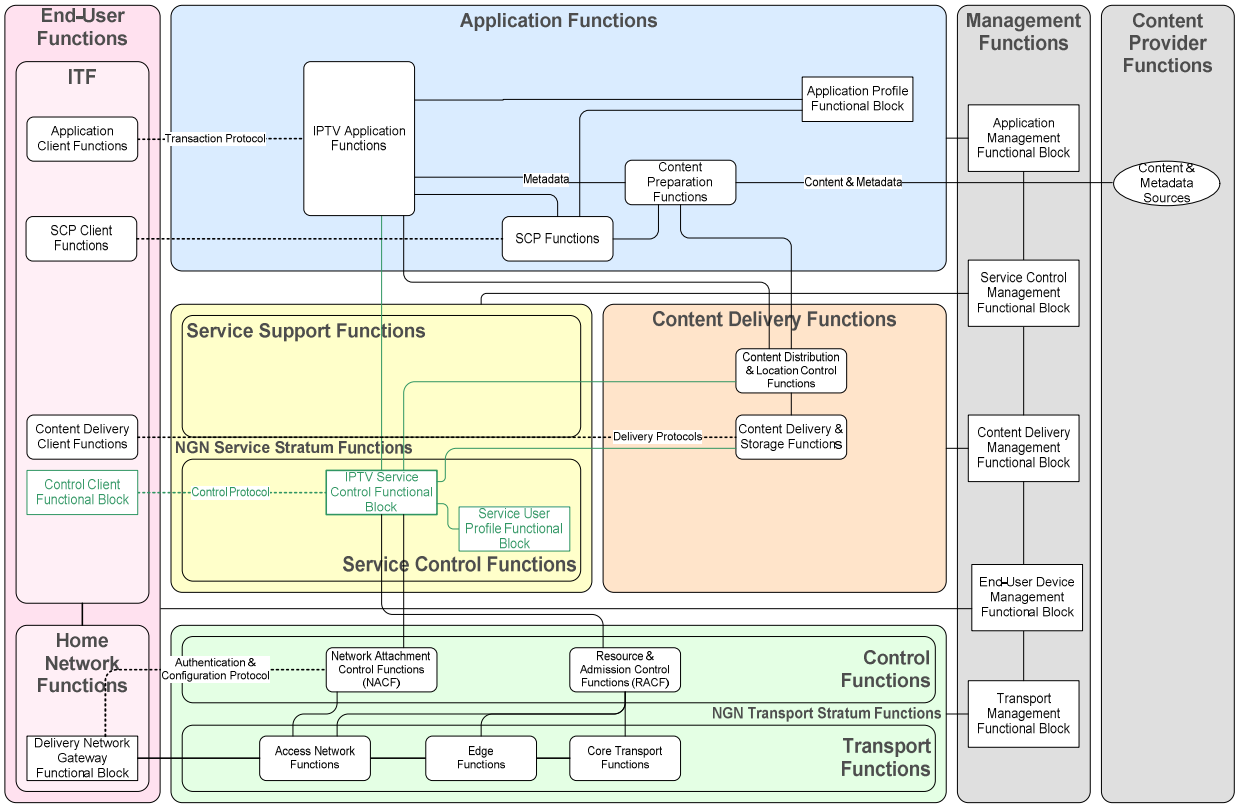


Figure 9-3: NGN Non-IMS IPTV Architecture

9.4.1 Control Client Functional Block

This functional block is common with its counterpart in Non-NGN IPTV functional architecture. See sub-clause §9.3.1 for further details.

9.4.2 IPTV Service Control Functional Block

This functional block is common with its counterpart in Non-NGN IPTV functional architecture. See sub-clause §9.3.2 for further details.

9.4.3 Service User Profile Functional Block

The Service User Profile Functional Block can be used for storing user profiles, subscriber-related data, such as location data, and presence status data in the NGN Service Stratum. The Service User Profile Functional Block also performs basic data management and maintenance functions as well as generating responses to queries for user profiles.

This Functional Block corresponds to the Service User Profile Functional Entity as defined in [ITU-T Y.2012].

9.4.4 Service Support Functions

The Service Support Functions provide some generic functions to facilitate the provisioning of IPTV services.

9.4.5 NGN Service Stratum Functions

For IPTV service that based on NGN, the main layers in the decomposition are application layer, service layer and network layer. The application layer aligns to the Applications Functions described above. The Service Stratum includes the Service Control Functions and the Network Stratum includes the Transport Functions and Control functions.

The NGN Service Stratum includes Application Support Functions & Service Support Functions as well as Service Control Functions:

- **Service Support Functions** – These include gateway functions to the Service Control Functions. However these are not shown at this level of decomposition.
- **Service Control Functions –** These include the functions for the control of the network to ensure the delivery of the media content from the source to the IPTV Terminal.

9.4.6 NGN Transport Stratum Functions

The NGN Transport Stratum Functions include Transport Functions and Transport Control Functions.

9.4.6.1 Transport Control Functions

The Transport Control Functions include Resource and Admission Control Functions (RACF) as well as Network Attachment Control Functions (NACF).

9.4.6.1.1 RACF

The Resource and Admission Control Functions are described in [ITU-T Y.2111].

9.4.6.1.2 NACF

Network Attachment Control Functions are described in [ITU-T Y.2012].

9.4.6.2 NGN Transport Functions

The NGN Transport Functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of content information, as well as the transfer of control and management information.

The NGN Transport Functions include Access Network Functions, Edge Functions, Core Transport Functions, and gateway functions.

9.4.6.2.1 Access Network Functions

The Access Network Functions are described in [ITU-T Y.2012].

9.4.6.2.2 Edge Functions

The Edge Functions are described in [ITU-T Y.2012].

9.4.6.2.3 Core Transport Functions

The Core Transport Functions are described in [ITU-T Y.2012].

9.5 Description of Functions Specific to NGN IMS IPTV Architecture

Functions and Functional Blocks described in this sub-clause are specific only to the NGN IMS IPTV architecture except where stated otherwise.

Figure 9-4 shows the NGN IMS IPTV functional architecture.

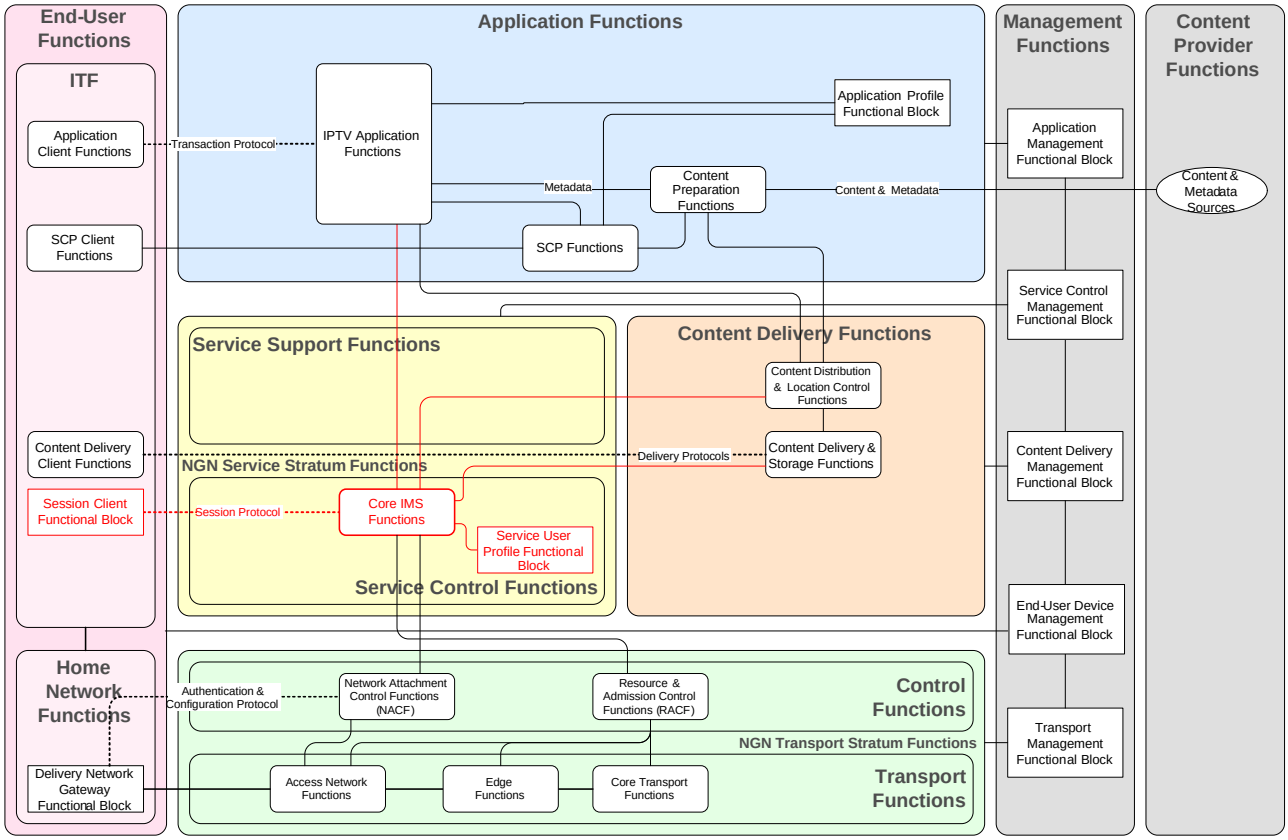


Figure 9-4: NGN IMS IPTV Architecture

9.5.1 Session Client Functional Block

The Session Client Functional Block provides the functions to handle service requests, such as session initiation, modification and termination.

This Functional Block communicates with IPTV applications via Core IMS Functions to prepare for the connection to the Content Delivery Functions. In the VoD case, the Session Client Functional Block initiates requests to IPTV Application Functions to select a suitable Content Delivery & Storage Functions which can provide the required content. For the Linear TV case, the Session Client Functional Block initiates requests to the IPTV Application Functions for the relevant network parameters (e.g. multicast address and port), to enable delivery of the required Linear TV content.

9.5.2 Core IMS Functions

In the NGN-IMS IPTV architecture, the IPTV Service Control Functional Block described in clause § 9.1.3.1 is supported by Core IMS Functions, which offers a session control mechanism, and provides functions for the authentication and authorization of IPTV Terminal Functions based on user profile, as well as functions for the interaction with RACF for resource reservation.

Core IMS Functions also provides interactions between IPTV Terminal Functions, IPTV Application Functions and Content Delivery Functions. The Core IMS Functions can be used for Service Discovery. Functions such as charging and roaming can also be supported by IMS mechanisms.

9.5.3 Service User Profile Functional Block

The Service User Profile Functional Block can be used for storing user profiles, subscriber-related data, such as location data, and presence status data in the Service stratum. The Service User Profile Functional Block also performs basic data management and maintenance functions, as well as generates responses to queries for user profiles.

This Functional Block corresponds to the Service User Profile Functional Entity as defined in [ITU-T Y.2012].

9.6 Description of Functions Common to the three Architectural Approaches

The Functions further decomposed in this sub-clause are common to the three architectural approaches.

9.6.1 Application Functions

The following sub-clauses provide a breakdown of the Application Functions of the IPTV Architecture. Figure 9-5 applies to all three architecture approaches, and extends the IPTV Functional Architecture to include the detailed Functions and Functional Blocks that relate to Application Functions and their relationship to the peer Application Client Functions and the Content Provider Functions.

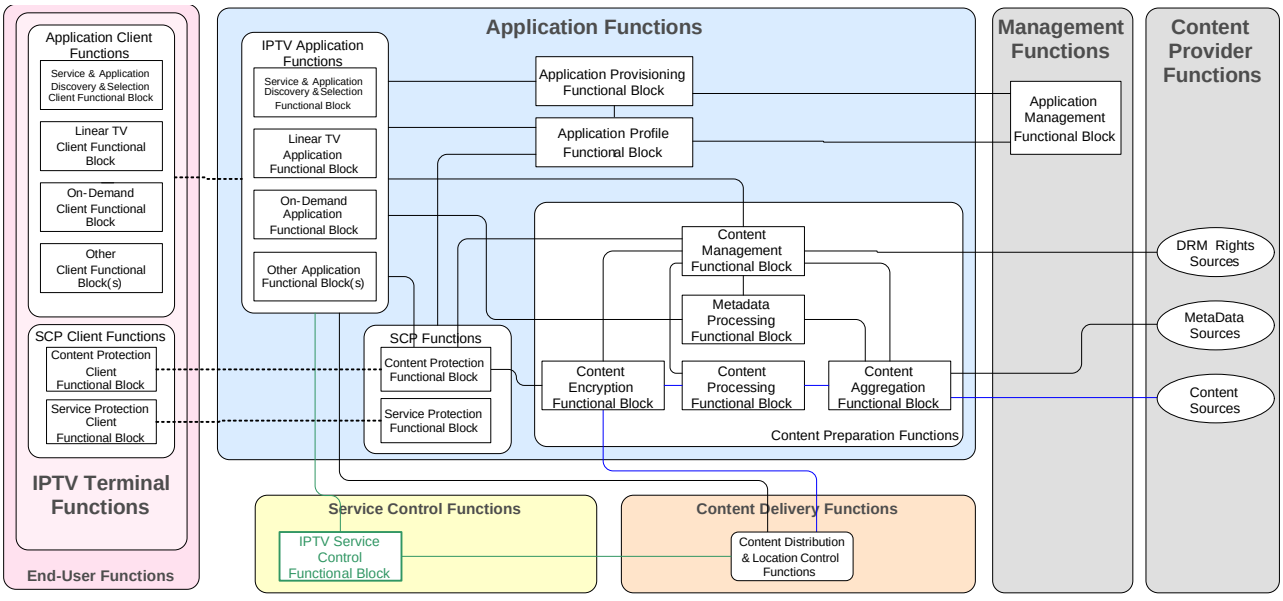


Figure 9-5: Detailed Application Functional Architecture

The following sub-clauses describe the decomposition of IPTV Application Functions into its constituent Functional Blocks.

The constituent Functional Blocks of Application Client Functions and Content Provider Functions are described in sub-clause 9.6.2 and 9.6.5 respectively.

9.6.1.1 IPTV Application Functions

An IPTV Service is offered to an end-user by a Service Provider, it may contain one or more Applications that provide different features to the End User such as Linear TV, Content on Demand, Communications, etc.

Applications make use of a set of underlying support functions that provide common facilities for example Content Delivery Functions, Service Control Functions. These functions are built from functional blocks, for example Unicast Delivery Functional Block.

An End User may have access to IPTV Services from different Service Providers and will then need to be able select the IPTV Service they wish to use. Once an End User has selected an IPTV Service they may need to be able to select the application they wish to use. The End User may subsequently select another application from the same or a different Service Provider

9.6.1.1.1 Service and Application Discovery & Selection Functional Block

The Service and Application, Discovery and Selection (SADS) functional block provides for the discovery and selection of IPTV services and applications. This can include the discovery and selection of services from multiple Service Providers. The ordering of service selection or provider selection is not specified, this is then followed by application selection.

The SADS functional block generates and provides the service discovery information to SADS client functional block. The service discovery information may consist of one or more entry points to Service Selection Applications. The entry points may be in the form of a URL. Service Discovery may be performed using the service control function.

The SADS functional block generates and provides the description information about the available applications, for example Linear TV and Content on Demand, to the SADS client functional block. The SADS client functional block presents this to the end user for browsing and selection. The SADS functional block receives metadata information about services and applications from the Metadata Processing Functional block.

9.6.1.1.2 On-Demand Application Functional Block

This Functional Block performs session management, service authorization, presentation of the content metadata, and execution of the service logic for the On-Demand application.

9.6.1.1.3 Linear TV Application Functional Block

This Functional Block performs session management, service authorization, presentation of the content metadata, and execution of the service logic for the Linear TV application.

9.6.1.1.4 Other Application Functional Blocks

These Functional Blocks provide for the delivery and presentation of additional IPTV services and their content, e.g. games, distant learning, etc.

All the IPTV Application Functions may communicate with the Application Profile Functional Block to support the customization of the IPTV services.

9.6.1.2 SCP Functions

The SCP functions controls the protection of the services and content. This are divided into Content Protection and Service Protection functional blocks.

9.6.1.2.1 Content Protection Functional Block

This Functional Block controls the protection of the content and is responsible for the management of the content rights and the keys used to encrypt and decrypt the content. It acquires the content rights (or content licence, originated from Content Provider) from the Content Preparation Functions, generates and distributes this security information (rights object or keys) to the SCP Client Functions. It may also provide keys for content encryption.

For example, when it receives a request for security information from IPTV Terminal Functions, it interacts with Application Profile Functional Block for the user related security subscription information, e.g. time limited, whether Fast Forward/Fast Rewind are allowed etc., generates the right object and delivers it to the IPTV Terminal Functions.

It also provides keys for service and content protection to IPTV Application Functions, which then deliver the keys to relevant functions, e.g. IPTV Terminal Functions and the content encryption function.

9.6.1.2.2 Service Protection Functional Block

This functional block controls the protection of services. Service protection includes authentication and authorisation of access to services and the protection of the services using methods such as encryption.

9.6.1.3 Application Profile Functional Block

The Application Profile Functional Block stores the profiles for the IPTV applications. The application profile may be located either within Service User Profile Functional Block or within IPTV Application Functions depending on implementation.

9.6.1.4 Application Provisioning Functional Block

Application Provisioning Functional Block add or withdraw applications manages the life-cycle of IPTV applications.

9.6.1.5 Content Preparation Functions

The Content Preparation Functions include Content Aggregation, Content Management, Metadata Processing, Content Processing and Content Encryption Functional Blocks. These Functional Blocks may be used to prepare and combine the content, as delivered by the content owner, into the required delivery format.

The Content Preparation Functions may be subject to commercial agreements with content owners, not all content are subject to the functions described below.

First the content is acquired by Content Aggregation Functional Block. The metadata and rights information are delivered to the Metadata Processing Functional Block. Content may be re-coded and encrypted in Content Processing and Content Encryption Functional Block before being delivered to Content Delivery Functions. The program related metadata is delivered to IPTV applications. If the original content from the content owner is modified or re-coded in any way, it may be necessary to also edit the programme related metadata.

9.6.1.5.1 Content Management Functional Block

This Functional Block manages the life-cycle of the content in compliance with commercial agreements with the content owner. This management function may be triggered by request from the IPTV Application Functions. The Content Management Functional Block directs the Content Processing Functional Block to process the content, e.g. to perform packaging, scheduling or re-coding.

9.6.1.5.2 Metadata Processing Functional Block

This Functional Block obtains, manages and processes the program related metadata from the metadata sources, via the Content Aggregation Functional Block, and provides it to the IPTV Applications Functions. The metadata may include title, brief introduction and content tracing information (such as watermark), etc., from the Content Provider, as well as price, time schedule, etc., from the Service Provider.

9.6.1.5.3 Content Aggregation Functional Block

This Functional Block aggregates content and metadata delivered by the Content Provider Functions.

9.6.1.5.4 Content Processing Functional Block

This Functional Block includes re-coding and other functions such as packaging, ad-insertion into streams, format conversion, resolution conversion, editing, etc.

The Content Processing Functional Block performs all or some of the following functions:

- Re-coding: In order to achieve bandwidth efficiency, content encoded in one compression format may be encoded into a more efficient format, e.g. ITU-T Recommendation H.262 to ITU-T Recommendation H.264;
- Content packaging: Content packaging is the selection and combination of multiple items of content into a single item of content for delivery (e.g., packaging a movie with different subtitles);
- Content scheduling: Content scheduling is the provision of timing information for ad-insertion or for the scheduling of content delivery;
- Other functions such as ad-insertion into streams, format conversion, resolution conversion, editing, etc.

9.6.1.5.5 Content Encryption Functional Block

This Functional Block encrypts the content.

9.6.2 Application Client Functions

9.6.2.1 Service and Application Discovery & Selection Client Functional Block

The SADS Client Functional Block provides for the end user's discovery and selection of IPTV services and applications.

9.6.2.2 On-Demand Client Functional Block

This Functional Block interacts with the On-Demand Application Functional Block to perform session management, service authorization, presentation of the content metadata, and execution of the service logic for the On-Demand application.

9.6.2.3 Linear TV Client Functional Block

This Functional Block interacts with the Linear TV Application Functional Block to perform session management, service authorization, presentation of the content metadata, and execution of the service logic for the Linear TV application.

9.6.2.4 Other Client Functional Blocks

These Functional Blocks interact with the Other Application Functional Blocks for the delivery and presentation of additional IPTV services and their content, e.g. games, distant learning etc.

9.6.2.5 SCP Client Functions

9.6.2.5.1 Content Protection Client Functional Block

The Content Protection Client functional block performs integrity checking, usage rights verification and content decryption.

9.6.2.5.2 Service Protection Client Functional Block

The Service Protection Client functional block performs the authentication and authorisation of access to services and, optionally, protection of the services using methods such as encryption.

9.6.3 Content Delivery Functions

The following sub-clauses provide a breakdown of the Content Delivery Functions of the IPTV Architecture. Figure 9-6 applies to all three architecture approaches, and extends the IPTV Functional Architecture to include the detailed functional blocks that relate to Content Delivery Functions and their relationship to the Network Functions. The details for unicast delivery and multicast delivery are considered.

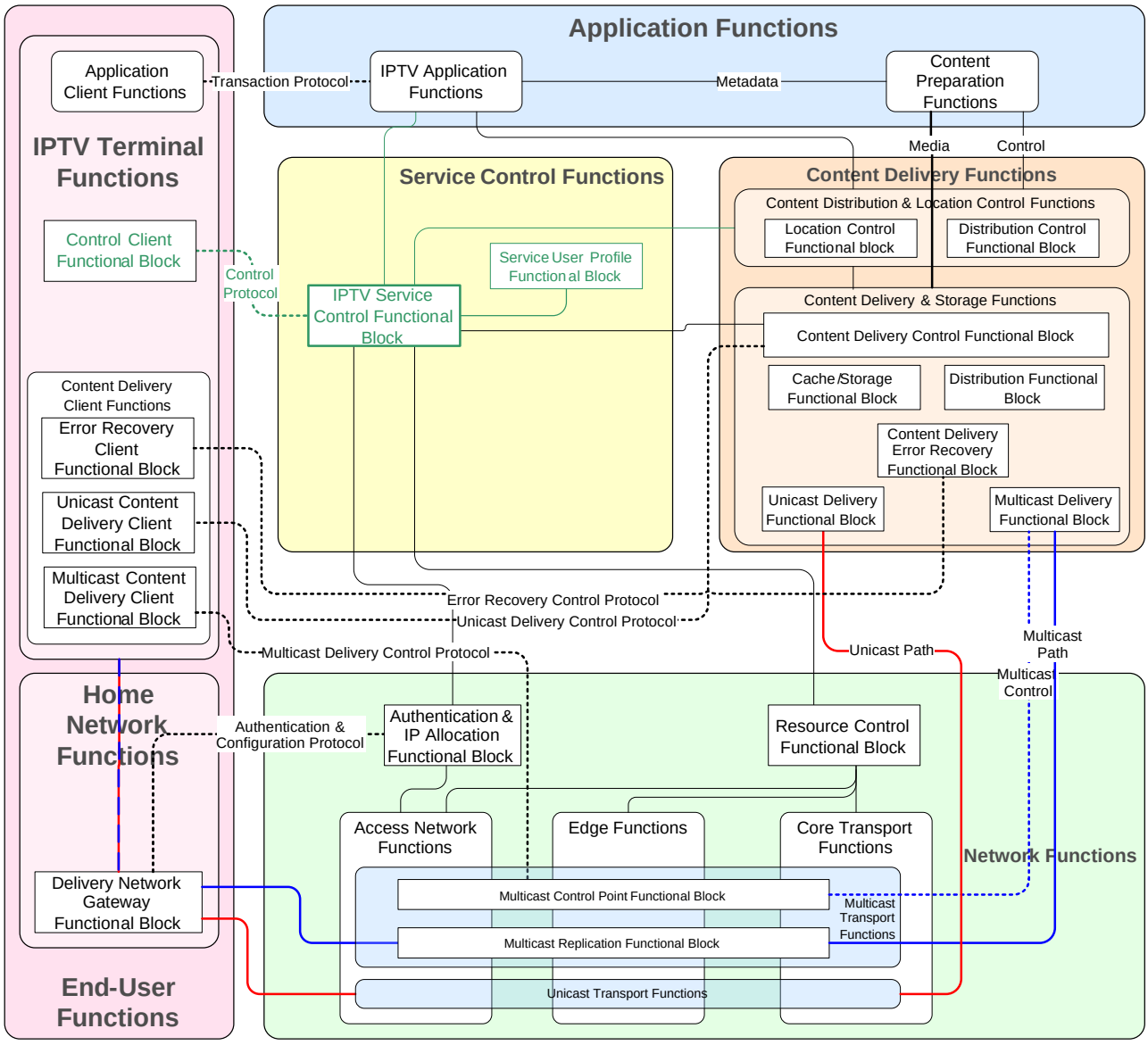


Figure 9-6: Content Delivery Functional Architecture

The following sub-clauses describe the decomposition of Content Delivery Functions into its constituent Functional Blocks.

The constituent Functional Blocks of Content Delivery Client Functions and Network Functions are described in sub-clauses 9.6.3.3 and 9.6.4 respectively.

The high-level functionality for Applications, Service Control and Content Delivery Functions was described previously.

9.6.3.1 Content Distribution & Location Control Functions

The Content Distribution & Location Control Functions control the Content Delivery & Storage Functions to optimize content distribution, selection and deliver content to the IPTV Terminal Functions.

It includes two Functional Blocks: Distribution Control Functional Block and Location Control Functional Block.

9.6.3.1.1 Distribution Control Functional Block

The Distribution Control Functional Block coordinates the delivery & storage resources and establishes the optimal distribution policy for distributing file content and live stream content from Content Preparation Functions to Content Delivery & Storage Functions. It is also responsible for distributing file content among the Content Delivery & Storage Functions.

The distribution policy for content distributed as files or streams may be different.

The Distribution Control Functional Block use and maintain the distribution information about how the content is distributed among the Content Delivery & Storage Functions. The Distribution Control Functional Block may also use the information obtained from Location Control Functional Block to optimize the distribution policy.

The Distribution Control Functional Block may also use information such as load status of Content Delivery & Storage Functions to optimize the distribution policy.

9.6.3.1.2 Location Control Functional Block

The Location Control Functional Block is used to process the request from IPTV Service Control Functional Block or IPTV Application Functions to select a suitable Content Delivery & Storage Functions which can provide the required content. Then the selected Content Delivery & Storage Functions can deliver the content to the Content Delivery Client Functions. The selection criteria include the distribution information and load status of Content Delivery & Storage Functions, the terminal information, e.g. terminal location and capability, and other possible criteria. The IPTV Service Control Functional Block or IPTV Application Functions then request the identified Content Delivery & Storage Functions to allocate resources for content delivery.

The Location Control Functional Block resolves the application information, such as logical content identifier, into the content location information, such as the address of the Content Delivery & Storage Functions which can provide the requested content.

In the case where multicast is used, the Location Control Functional Block may:

- manage and allocate multicast network parameters (e.g. multicast address);
- associate and maintain the mapping between logical channel identifiers and these parameters;
- provide this mapping to IPTV Application Functions or IPTV Service Control Functional Block when requested.

9.6.3.2 Content Delivery & Storage Functions

These functions are described in sub-clause 9.1.4.2. The detailed functional blocks contained in these functions are described below.

9.6.3.2.1 Content Delivery Control Functional Block

The Content Delivery Control Functional Block handles control functions on Content Delivery and Storage Functions, such as control of the media resources, and handling of VCR commands.

9.6.3.2.2 Unicast Delivery Functional Block

The Unicast Delivery Functional Block is responsible for streaming and delivering (e.g. via RTP over UDP) content streams to the Content Delivery Client Functions via the Network Functions based on the use of the unicast protocol and mechanisms.

It may also provide other functions, such as file downloading and uploading to and from the Content Delivery Client Functions.

9.6.3.2.3 Multicast Delivery Functional Block

The Multicast Delivery Functional Block is responsible for streaming and delivering (e.g. via RTP over UDP) content streams to the Content Delivery Client Functions via the Network Functions based on the use of the multicast protocol and mechanisms.

9.6.3.2.4 Cache & Storage Functional Block

The Cache & Storage Functional Block is responsible for caching the content, e.g. in order to support time-shifted linear TV. It is also responsible for storing the file content, e.g. in order to support VoD or other file-based IPTV services.

9.6.3.2.5 Distribution Functional Block

The Distribution Functional Block receives the content from the Content Preparation Function. It distributes the content, which include live streams or files, residing among the separate instances of Content Delivery & Storage Functions.

9.6.3.2.6 Error Recovery Functional Block

The Content Delivery Functions may optionally include an Error Recovery Function [reference to WD-ALERM]. This functional block serves to improve reliability in case that the IPTV Network Functions cannot provide sufficient QoS. The Error Recovery Functional Block generates additional information for a content stream, either proactively or on request, such that the Error Recovery Client Functional Block in the Content Delivery Client Functions can recover the content.

The Error Recovery Functional Block relies on the Content Delivery Functions to deliver the additionally generated information.

The Error Recovery Functional Block relies on the availability of an Error Recovery Client Functional Block in the Content Delivery Client Functions. The Error Recovery Functional Block may for example be realized by Forward Error Correction (FEC) or by Retransmission.

9.6.3.3 Content Delivery Client Functions

The Content Delivery Client functions are responsible for the content reception in the IPTV terminal Functions.

9.6.3.3.1 Multicast Content Delivery Client Functional Block

The Multicast Client Functional Block receives the content from the Multicast Delivery Functional Block within the Content Delivery & Storage Functions. This functional block communicates with the Multicast Control Point Functional Block for the selection of the multicast stream.

9.6.3.3.2 Unicast Content Delivery Client Functional Block

The Unicast Content Delivery Client Functional Block receives the content from the Unicast Delivery Functional Block within the Content Delivery & Storage Functions.

9.6.3.3.3 Error Recovery Client Functional Block

The Content Delivery Client Functions may optionally include an Error Recovery Client Functional Block. This functional block performs error recovery on the content streams in conjunction with the Error Recovery Functional Block within the Content Delivery Functions.

9.6.4 Network Functions

These functions are described in sub-clause 9.1.5. The detailed functional blocks contained in these functions are described below.

Multicast Control Point Functional Blocks and Multicast Replication Functional Blocks may exist in Access Network Functions, Edge Functions, or Core Transport Functions.

9.6.4.1 Multicast Transport Functions

9.6.4.1.1 Multicast Control Point Functional Block

This Functional Block is responsible for the selection of the individual multicast streams to be delivered, over the access network, to the IPTV End-User Functions. The request for a multicast stream may need to be authorised before it is accepted.

9.6.4.1.2 Multicast Replication Functional Block

This Functional Block is responsible for replicating multicast streams from a Multicast Delivery Functional Block to all the instances of the Multicast Control Point Functional Blocks.

9.6.4.2 Unicast Transport functions

The Unicast Transport Functions are responsible for transport of unicast content streams from the Unicast Delivery Functional Block to the End-User Functions.

9.6.5 Content provider functions

The Content Provider Functions provide a number of different types of sources to the Content Preparation Functions, e.g. Content Protection metadata sources, Metadata sources and Content sources. The physical interfaces and content formats may be different depending on the type of the sources. It may include functions for access control based on rating of the content.

9.6.5.1 Content protection metadata sources

Content Protection Metadata defines the usage rules and rights for protected IPTV content.

9.6.5.2 Metadata sources

A metadata source is an entity that provides content provider metadata associated with the IPTV content.

9.6.5.3 Content sources

A content source is an entity that provides IPTV content

9.7 Third Party Application Gateway Functional Block

The third Party Application Gateway Functional Block is responsible for support of third Party Application Functions as shown in Figure 9-7.

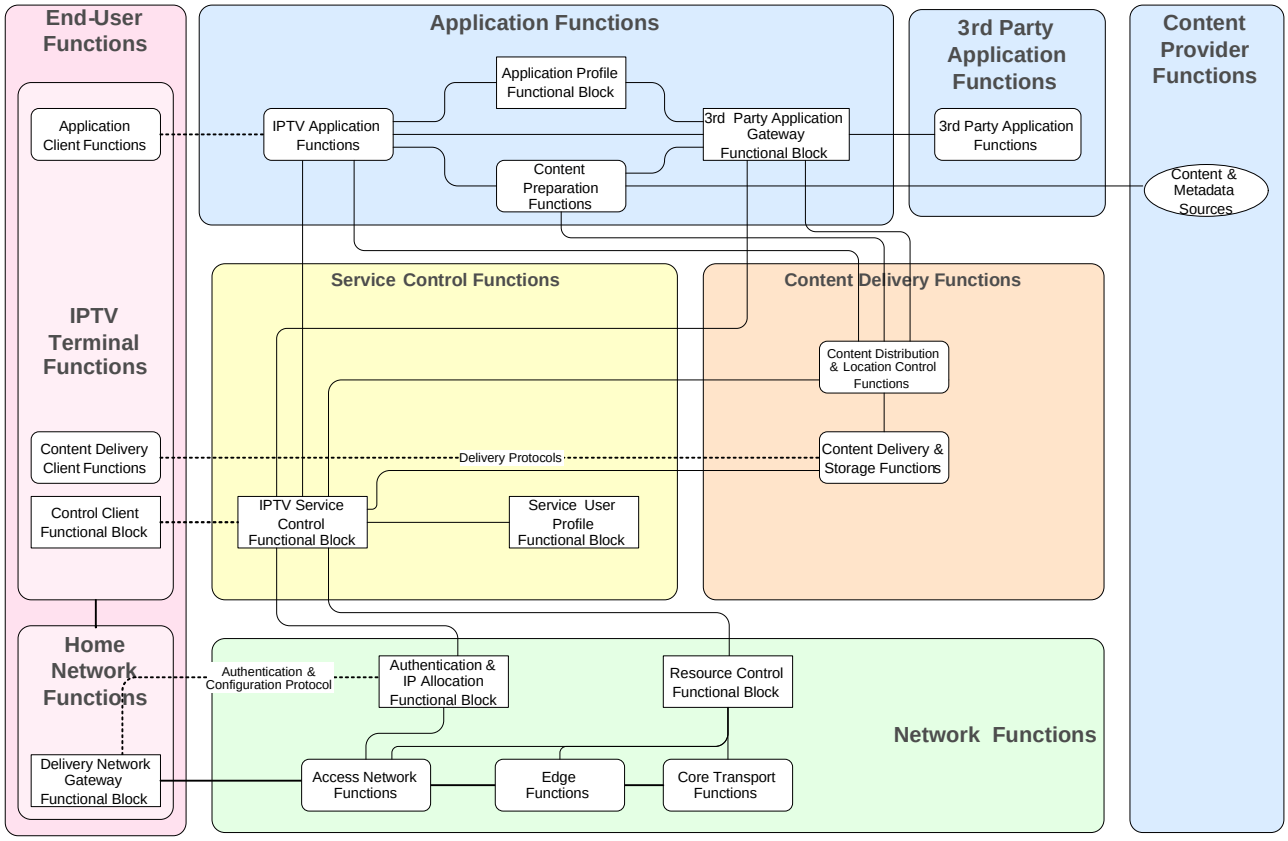


Figure 9-7: Third Party Application Gateway Functional Block in IPTV Architecture

Third Party Application Functions invoke application interfaces to make use of IPTV functionality. The reference point between third Party Application Gateway Functional Block and third Party Application Functions is intended to support the development of third party applications.

Third Party Application Gateway Functional Block

This Functional Block provides a controlled interface for the Third Party Application Functions to utilise the IPTV related capabilities and resources. The functions of the Third Party Application Gateway Functional Block are as follows:,

- Policy control
- Access to user profiles
- Access to IPTV presence information (e.g., the requested service status, channel currently accessed, content currently accessed)
- Content play control

- Access to the status and position within a content stream

- Translation of protocols between IPTV Service Control Functional Block and Third Party Applications, in case the protocols adopted by the two sides are different.

9.8 Inter-working between NGN variants of the IPTV architecture

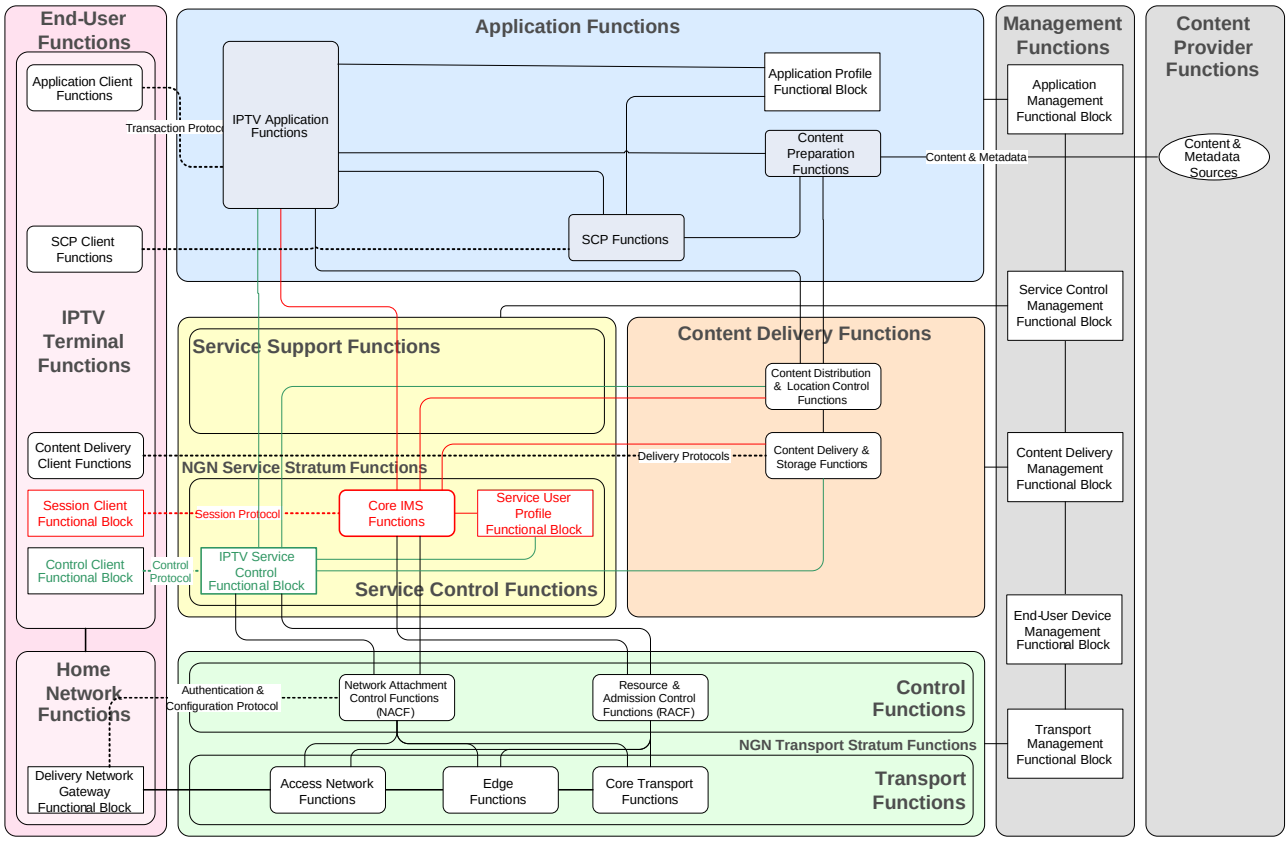


Figure 9-8: Inter-working Between NGN Variants of the IPTV Architecture

[EDITOR'S NOTE – further clarification is required on what inter-working between the two variants can happen in the same IPTV system.]

9.9 Reference Points

Figures 9-9, Figure 9-10 and Figure 9-11 respectively identify the IPTV reference points for the Non-NGN, NGN Non-IMS and NGN IMS architectures.

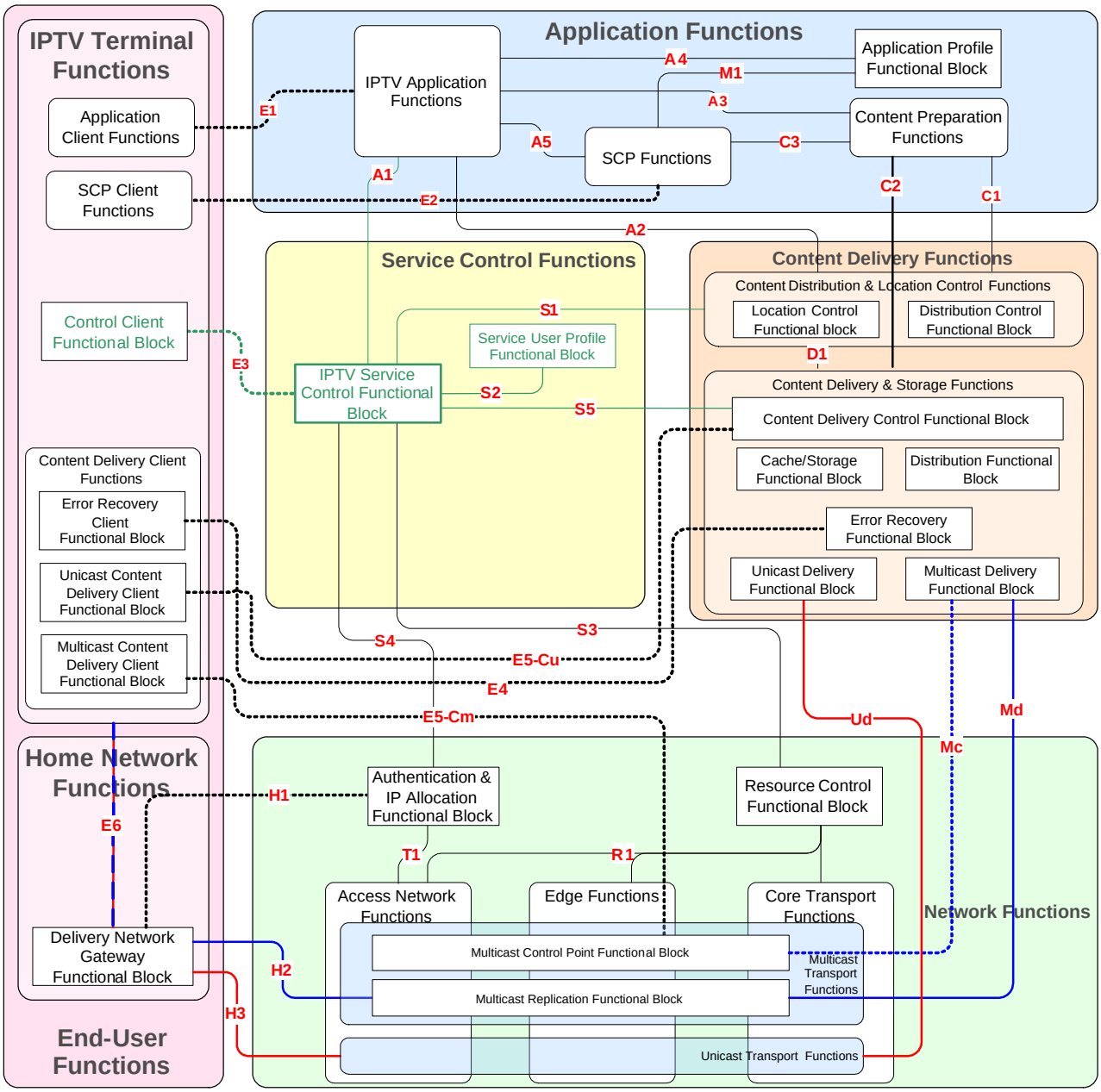


Figure 9-9: Reference Points of Non-NGN IPTV Architecture

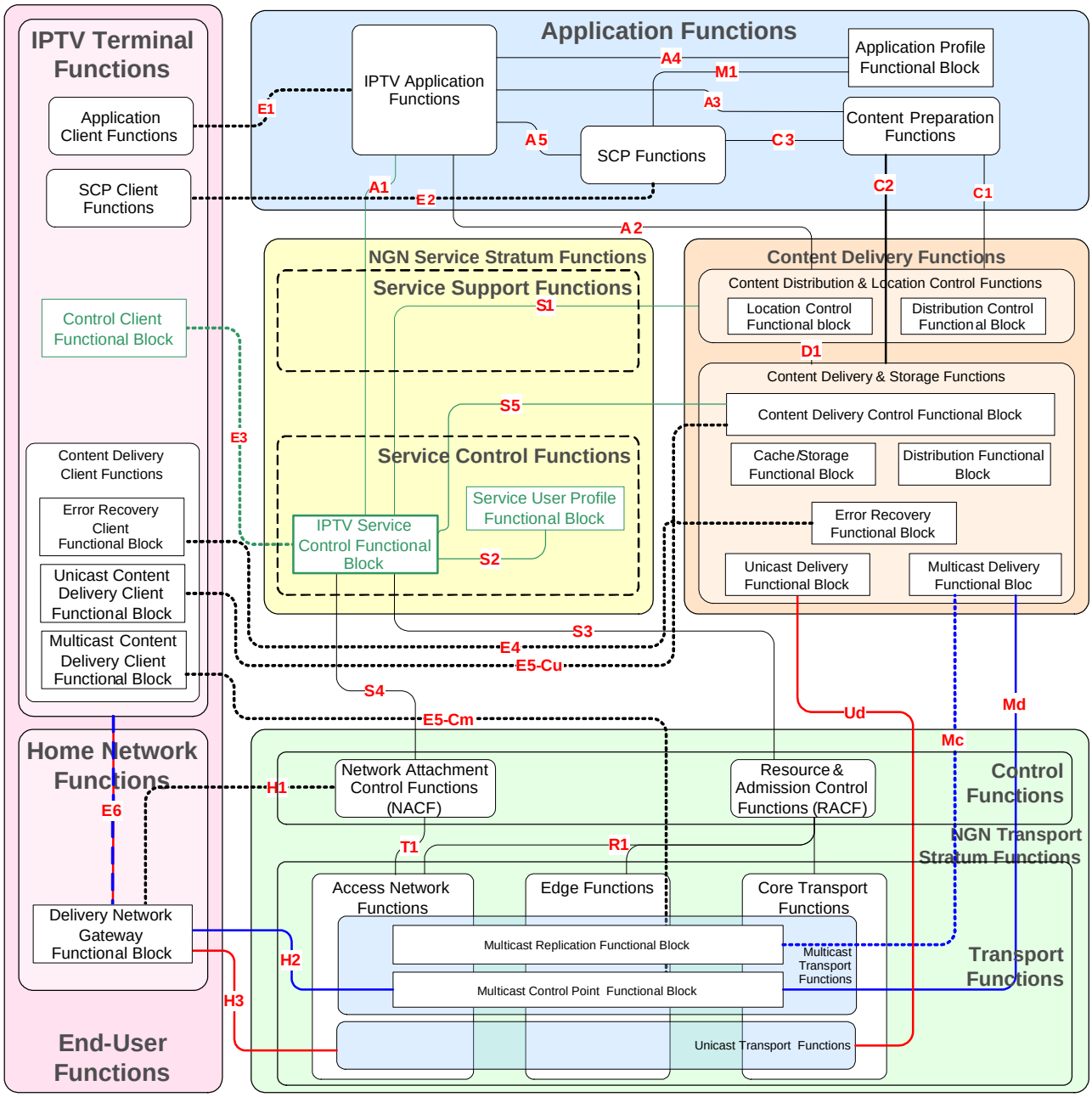


Figure 9-10: Reference Points of NGN Non-IMS IPTV Architecture

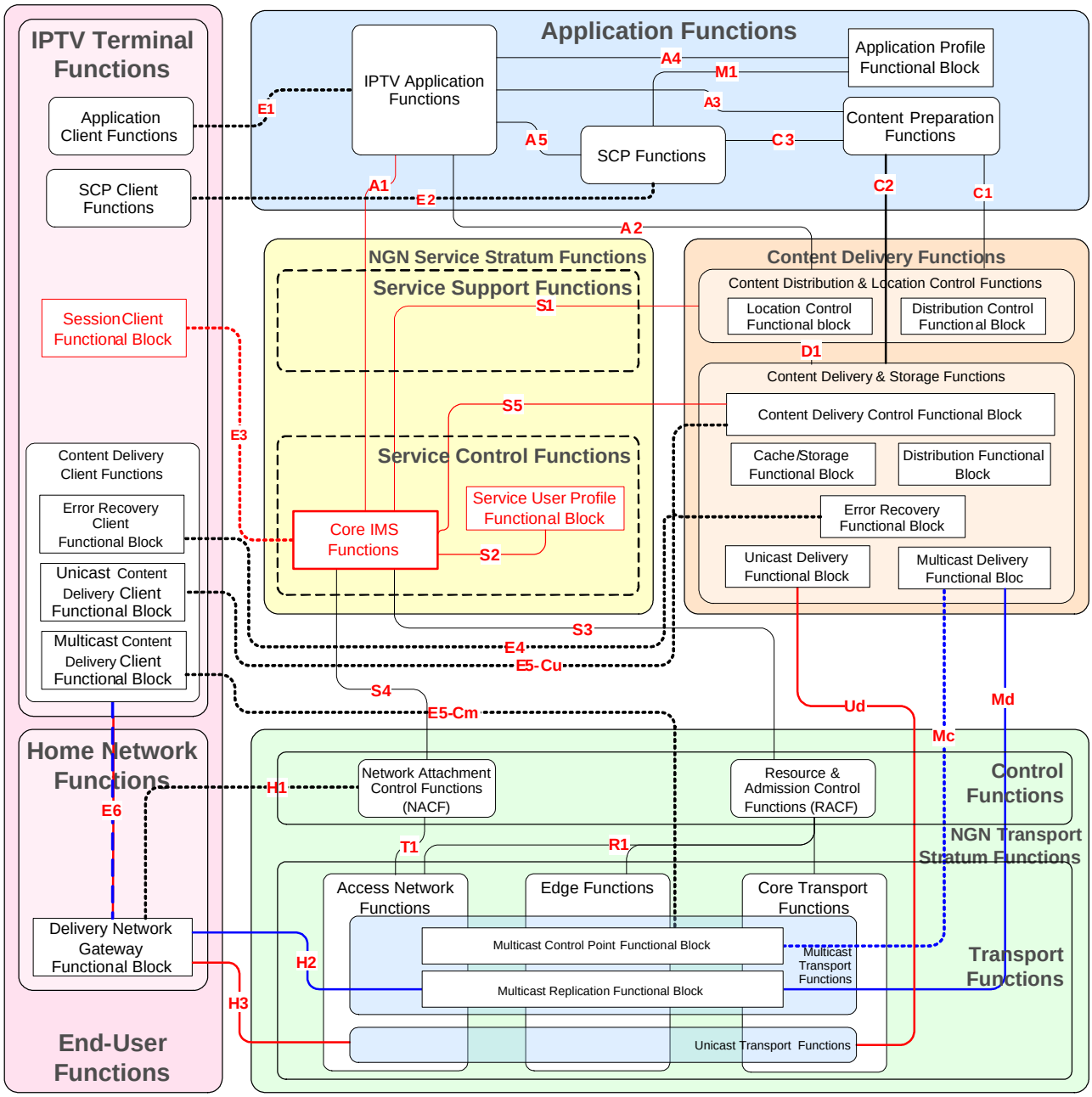


Figure 9-11: Reference Points of NGN IMS IPTV Architecture

9. 9 .1 Reference Points common to all three IPTV Architectures

The reference points below are common to all three IPTV Architectures which can be found in Figure 9-9, Figure 9-10 and Figure 9-11.

9.9.1.1 Reference point E1

The E1 reference point is a reference point between ITF Application Client Functions and IPTV Application Functions that are used by ITF to browse and select IPTV services as well as to support service configuration.

9.9.1.2 Reference point E5-Cu

The E5-Cu reference point is a reference point between the Unicast Content Delivery Client Functional Block and the Content Delivery Control Functional Block that is used to exchange content control message, e.g. VCR commands.

NOTE – The information exchanged between the Unicast Content Delivery Client Functional Block and the Content Delivery Control Functional Block may be transferred via the IPTV Service Control Functions, e.g. in the case where the IPTV Service Control Functions proxy all requests between the Unicast Content Delivery Client Functional Block and the Content Delivery Control Functional Block.

9.9.1.3 Reference point E5-Cm

The E5-Cm reference point is a reference point between the Multicast Content Delivery Client Functional Block and Multicast Control Point Functional Block that is used to exchange messages for joining multicast channels, e.g. IGMP messages.

9.9.1.4 Reference point E4

The E4 reference point is a reference point between Error Recovery Functional Block and Error Recovery Client Functional Block that is used to exchange messages for requesting and delivering error recovery information, for example FEC repair data or retransmission data.

9.9.1.5 Reference point E6

The E6 reference point is a reference point between Content Delivery Client Functions and the Delivery Network Gateway Functional Block in order to deliver control messages and content streams.

9.9.1.4 Reference point H2

The H2 reference point is a reference point providing multicast-based IP connectivity between Delivery Network Gateway Functional Block and Access Network Functions in order to deliver control messages and content streams.

9.9.1.5 Reference point H3

The H3 reference point is a reference point providing Unicast-based IP connectivity between Delivery Network Gateway Functional Block and Access Network Functions in order to deliver control messages and content streams.

9.9.1.6 Reference point A2

The A2 reference point is a reference point between IPTV Applications Functions and Content Distribution & Location Control Function (CD&LCF) that is used by IPTV Applications Functions to request service parameters from CD&LCF.

For Linear TV Applications, the A2 reference point is used to request multicast network parameters, e.g. multicast address. For On-Demand applications, the A2 reference point is used to request the CD&LCF to identify a suitable CD&SF for content delivery.

9.9.1.6 Reference point A3

The A3 reference point is a reference point between IPTV Applications Functions and Content Preparation Functions that is used to transmit the metadata stored in Content Preparation Functions to IPTV Applications Functions.

9.9.1.7 Reference point A4

The A4 reference point is a reference point between IPTV Applications Functions and Application Profile Functional Block that is used by IPTV Application Functions to retrieve application profiles. The application profile may include end-user subscription information. An example is for SAD&S Functional Block to get personalized profiles.

9.9.1.8 Reference point C1

The C1 is a reference point between Content Preparation Functions and Content Delivery Distribution & Control Location Functions (CD&LCF) that is used by Content Preparation Functions to configure policies such as content distribution rules, selection criteria, etc., in the CD&LCF and to send stream content or file content distribution request to CD&LCF for selecting suitable CD&SF to receive the content.

9.9.1.9 Reference point C2

The C2 reference point is a reference point between Content Preparation Functions and Content Delivery & Storage Functions (CD&SF). It is used to transfer stream content or file content from Content Preparation Functions to CD&SF.

9.9.1.10 Reference point D1

The D1 reference point is a reference point between Content Distribution & Location Control Function (CD&LCF) and Content Delivery & Storage Functions that is used by CD&LCF to get the status information of CD&SF such as load status, the contents catalogue on each CD&SF, etc. The CD&LCF identifies a suitable CD&SF according to some criteria when receiving request from IPTV Application Functions or IPTV Service Control Functional Block. In IMS case, IPTV Service Control Functional Block is replaced by Core IMS Functions.

9.9.1.11 Reference point Ud

The Ud reference point is a reference point between Unicast Delivery Functional Block and Unicast Transport Functions that is used by the CD&SF to deliver content streams in unicast mode.

9.9.1.12 Reference point Md

The Md reference point is a reference point between Multicast Delivery Functional Block and Multicast Transport Functions that is used by the CD&SF to deliver content streams in multicast mode.

9.9.1.13 Reference point Mc

The Mc reference point is a reference point between Multicast Delivery Functional Block and Multicast Replication Functional Block/Multicast Control Point Functional Block that is used for the dynamic computation, establishment and maintenance of multicast trees.

9.9.1.14 Reference point E2

The E2 reference point is a reference point between Content Protection Client Functional Block and Content Protection Rights & Key Management Functional Block that is used for delivering security information (rights object or keys) from Content Protection Rights & Key Management Functional Block to Content Protection Client Functional Block.

9.9.1.15 Reference point A5

The A5 reference point is a reference point between IPTV Application Functions and Content Protection Rights & Key Management Functional Block that is used for providing keys of service and content protection information from Content Protection Rights & Key Management Functional Block to the IPTV Application Functions.

9.9.1.16 Reference point C3

The C3 reference point is a reference point between Content Preparation Functions and Content Protection Rights & Key Management Functional Block. Content Protection Rights & Key Management Functional Block acquires the content rights or licence from the Content Preparation Functions. Content Protection Rights & Key Management Functional Block may also provide generated keys to Content Preparation Functions.

9.9.1.17 Reference point M1

The M1 reference point is a reference point between Content Protection Rights & Key Management Functional Block and Application Profile Functional Block that is used by Content Protection Rights & Key Management Functional Block to get security related information from the Application Profile Functional Block.

9.9.2 Reference Points specific to Non-NGN IPTV Architecture

The reference points below are specific to Non-NGN IPTV Architecture which is depicted in Figure 9-9.

9.9.2.1 Reference point S1

The S1 reference point is a reference point between IPTV Service Control Functional Block and CD&LCF that is used to forward the service signalling messages, e.g. service requests, content resource requests, between ITF/IPTV Application Functions and CD&LCF.

9.9.2.2 Reference point S2

The S2 reference point is a reference point between IPTV Service Control Functional Block and Service Profile Functional Block that is used by IPTV Service Control Functional Block to access service profiles.

The service profile includes end-user information, e.g. end-user identity, security information, etc., and may as well include service profile specific to an IPTV application.

9.9.2.3 Reference point S3

The S3 reference point is a reference point between IPTV Service Control Functional Block and the Resource Control Functional Block that is used by IPTV Service Control Functional Block for requesting control of network resources.

9.9.2.4 Reference point S4

The S4 reference point is a reference point between IPTV Service Control Functional Block and Authentication & IP Allocation Functional Block that is used by the IPTV Service Control Functional Block to get information from Authentication & IP Allocation Functional Block such as the ITF location.

9.9.2.5 Reference point S5

The S5 reference point is a reference point between IPTV Service Control Functional Block and Content Delivery Control Functions (CDCF) Functional Block that is used to exchange messages for session management, e.g. session establishment, modification, or termination, etc.

It may also be used to exchange content control messages, e.g. VCR commands.

9.9.2.6 Reference point T1

The T1 reference point is a reference point between Authentication & IP Allocation Functional Block and Access Network Functions that is used for management of network configuration parameters as well as authentication data.

9.9.2.7 Reference point R1

The R1 reference point is a reference point between Resource Control Functional Block and network transport functions (e.g. Access Network Functions) that is used by the Resource Control Functional Block to control network resources within the network transport functions.

9.9.2.8 Reference point E3

The E3 reference point is a reference point between the Control Client Functional Block and the IPTV Service Control Functional Block that is used to exchange session signalling information, e.g. session establishment, modification, and termination. It may also be used to exchange content control messages, such as VCR commands.

9.9.2.9 Reference point A1

The A1 reference point is a reference point between IPTV Applications Functions and IPTV Service Control Functional Block used for:

- forwarding service signalling information between IPTV Service Control Functional Block and IPTV Applications Functions;
- forwarding signalling information between IPTV Applications Functions and other functions, such as ITF, CD&LCF.

Service requests from ITF are forwarded to Application Functions, and service responses, including service parameters, are sent from Applications Functions and forwarded to ITF via the A1 reference point.

9.9.2.10 Reference point H1

The H1 reference point is a reference point between Delivery Network Gateway Functional Block and Authentication & IP Allocation Functional Block that is used to perform authentication, and obtain necessary network parameters, e.g. IP address, etc., when the ITF within End-User Functions attaches to the network**.**

9.9.3 Reference Points specific to NGN Non-IMS IPTV Architecture

The reference points below are specific to NGN Non-IMS IPTV Architecture which is depicted in Figure 9-10.

9.9.3.1 Reference point S1

The S1 reference point is the same as the S1 reference point in the Non-NGN architecture (see Clause 9.9.2.1).

9.9.3.2 Reference point S2

The S2 reference point is the same as the S2 reference point in the Non-NGN architecture (see Clause 9.9.2.2).

9.9.3.3 Reference point S3

The S3 reference point is a reference point between IPTV Service Control Functional Block and RACF. The S3 reference point corresponds to the Rs reference point in [ITU-T Y.2111].

9.9.3.4 Reference point S4

The S4 reference point is a reference point between IPTV Service Control Functional Block and NACF. The S4 reference point corresponds to the S-TC1 reference point in [ITU-T Y.2012].

9.9.3.5 Reference point S5

The S5 reference point is the same as the S5 reference point in the Non-NGN architecture (see Clause 9.9.2.5).

9.9.3.6 Reference point T1

The T1 reference point is a reference point between NACF and Access Network Functions. The T1 reference point corresponds to the TC-T1 reference point in [ITU-T Y.2012].

9.9.3.7 Reference point R1

The R1 reference point is a reference point between RACF and Access Network Functions. The R1 reference point corresponds to the Rw reference point in [ITU-T Y.2111]

9.9.3.8 Reference point E3

The E3 reference point is the same as the E3 reference point in the Non-NGN architecture (see Clause 9.9.2.8).

9.9.3.9 Reference point A1

The A1 reference point is the same as the A1 reference point in the Non-NGN architecture (see Clause 9.9.2.9).

9.9.3.10 Reference point H1

The H1 reference point is a reference point between Delivery Network Gateway Functional Block and NACF that is used to perform authentication, and get necessary network parameters, e.g. IP address, etc., when the ITF within End-User Functions attaches to the network.

The H1 reference point corresponds to the TC-U1 reference point in [ITU-T Y.2012].

9.9.4 Reference Points specific to NGN IMS IPTV Architecture

The reference points below are specific to NGN IMS IPTV Architecture which is depicted in Figure 9-11.

9.9.4.1 Reference point S1

The S1 reference point is a reference point between Core IMS Functions and CD&LCF that is used to forward the service signalling messages, e.g. service requests, content resource requests, between ITF/IPTV Application Functions and CD&LCF.

This reference point corresponds to the ISC reference point defined in [ITU-T Y.2021].

9.9.4.2 Reference point S2

The S2 reference point is a reference point between Core IMS Functions and Service User Profile Functional Block.

It is used for Core IMS Functions to store and get service profiles. The profile includes end-user information, e.g. end-user identity, security information, etc., as well as service profile specific to an IPTV application.

This reference point corresponds to the Cx reference point defined in [ITU-T Y.2021].

9.9.4.3 Reference point S3

The S3 reference point is a reference point between Core IMS Functions and RACF.

It is used by Core IMS Functions to request RACF for the control of transport resources. This reference point corresponds to the Rs reference point as defined in [ITU-T Y.2111].

9.9.4.4 Reference point S4

The S4 reference point is a reference point between Core IMS Functions and NACF.

It is used by Core IMS Functions to interact with NACF in order to retrieve information related to the IP connectivity access information (e.g. physical location of the ITF).

This reference point corresponds to the S-TC1 reference point as defined in [ITU-T Y.2012].

9.9.4.5 Reference point S5

The S5 reference point is a reference point between Core IMS Functions and Content Delivery Control Functional Block that is used to exchange messages for session management, e.g. session establishment, modification, or termination, etc.

It may also be used to exchange content control messages, e.g. VCR commands.

9.9.4.6 Reference point T1

The T1 reference point is a reference point between NACF and Access Network Functions.

This reference point corresponds to the TC-T1 reference point as defined in [ITU-T Y.2012].

9.9.4.7 Reference point R1

The R1 reference point is a reference point between RACF and network Transport Functions. The R1 reference point corresponds to the Rw reference point in [ITU-T Y.2111]

9.9.4.8 Reference point E3

The E3 reference point is a reference point between Session Client Functional Block and Core IMS Functions.

It is used by Session Client Functional Block to initiate a service request to IPTV Applications Functions via Core IMS Functions, to identify and prepare for the connection to the Content Delivery Functions, e.g. request for a suitable Content Delivery & Storage Functions in VoD case, and request for network parameter in Linear TV case, etc.

This reference point corresponds to the Gm reference point defined in [ITU-T Y.2021].

9.9.4.9 Reference point A1

The A1 reference point is a reference point between IPTV Applications Functions and Core IMS Functions used for:

- forwarding service signalling information between Core IMS and IPTV Applications Functions;
- forwarding signalling information between IPTV Applications Functions and other functions, such as ITF, CDLCF.

Service requests from ITF are forwarded to Application Functions, and service responses, including service parameters, are sent from Applications Functions and forwarded to ITF via this reference point.

This reference point corresponds to the ISC reference point defined in [ITU-T Y.2021].

9.9.4.10 Reference point H1

The H1 reference point is the same as the H1 reference point in the NGN Non-IMS architecture (see Clause 9.9.3.10).

10 Interconnection between different IPTV networks

This clause describes the extensions of the IPTV architecture to include the interconnection between two NGN networks, as well as between NGN and Non-NGN networks. These extensions cover:

1) inter-working

2) roaming

3) access to third party services.

Note that in this clause, the use of the terms "home network" and "visited network" is based on the context of mobile (e.g. cellular) networks or networks supporting nomadism. These terms shall not be confused with the use of the term "home network" as used in the context of residential (home) networks.

10.1 Interconnection between two NGN-based IPTV networks

10.1.1 Interconnection with the visited network

Figure 10-1 illustrates the case where IPTV Terminal Functions are connected to the visited network and are accessing the Application Functions in the home network. In this figure, either the Core IMS Functions or the IPTV Service Control Functional Block is used depending on the capabilities of the home network and the visited network, respectively. The Service Control Functions of each network request network resources via its own RACF. Network functions in each network may be interconnected to other networks and the RACF-to-RACF reference point can be used to request resource and admission control.

NOTE – The detailed procedures and information for RACF-to-RACF communication are under study in ITU-T.

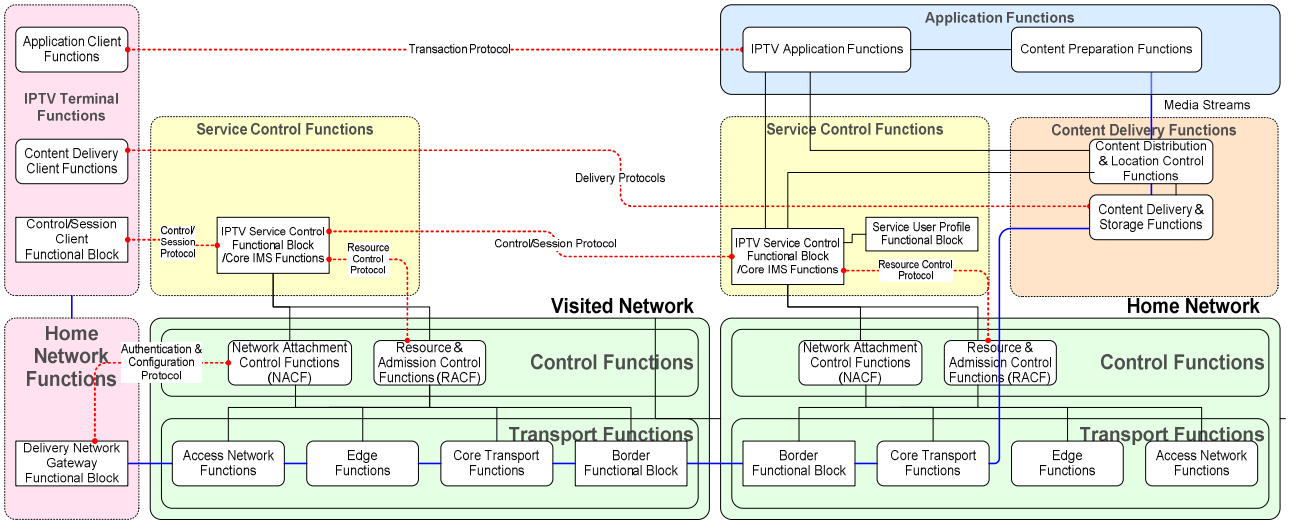


Figure 10-1: Interconnection with the visited network

Figure 10-2 illustrates the case where IPTV Terminal Functions are connected to visited network and are accessing the Application Functions in the home network without using Service Control Functions in the visited network. In this figure, either the Core IMS Functions or the IPTV Service Control Functional Block is used, depending on the capabilities of the home network. The RACF of the home network requests the network resources from the visited network via the RACF-to-RACF reference point.

If no Service Control Functions are applicable due to the absence of compatible Service Control Functions or mutual agreement between network providers, the RACF-to-RACF reference point is used to request network resources in the visited network.

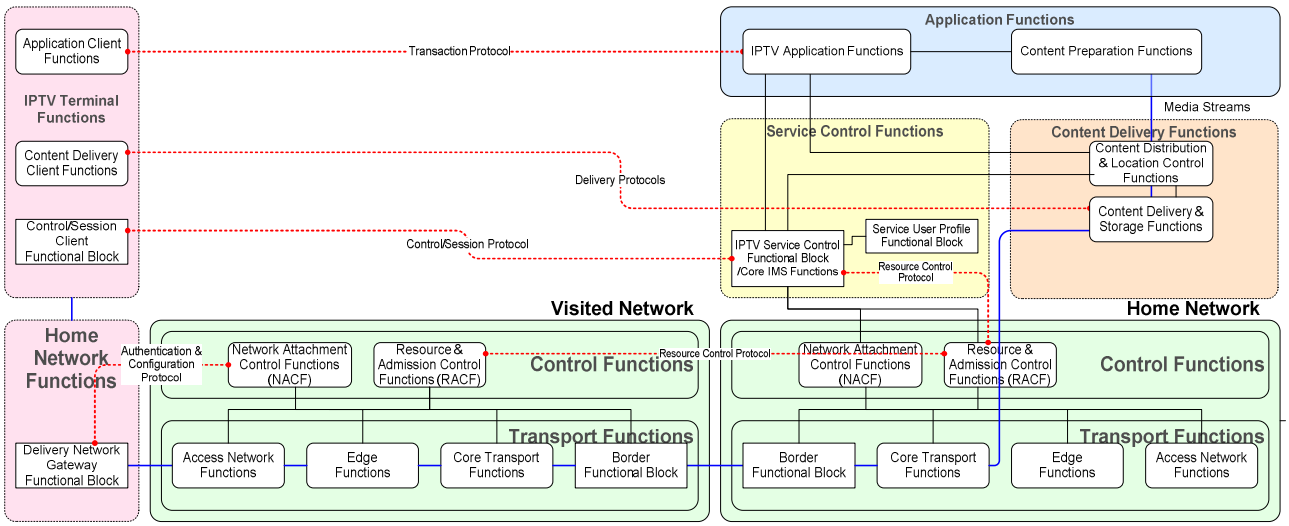


Figure 10-2: Interconnection with the visited network without service control functions

10.1.2 Interconnection with third party providers

Figure 10-3 illustrates the interconnection with a third party provider. In this figure, either Core IMS Functions or IPTV Service Control Functional Block is used, depending on the architecture variants used in the home network and the third party provider, respectively. The Application Functions and Content Delivery Functions of the third party provider are involved in providing IPTV services. The Service Control Functions of each provider request the network resources from their respective RACF.

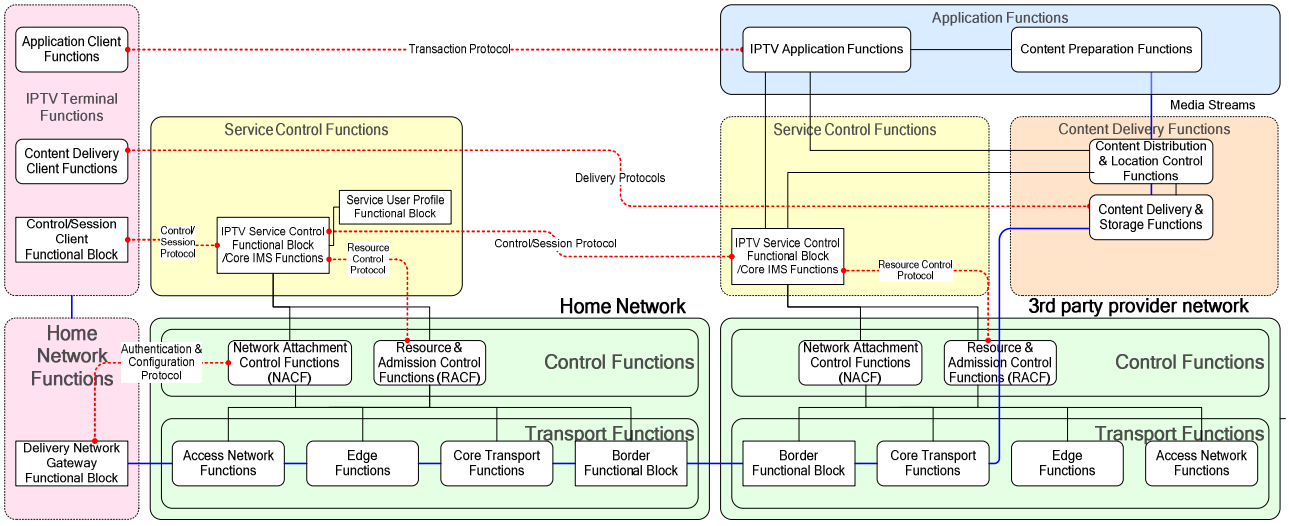


Figure 10-3: Interconnection with the third party provider

10.2 Interconnection between Non-NGN IPTV network and NGN IPTV network

10.2.1 Interconnection with Non-NGN IPTV network

Figure 10-4 illustrates the case where IPTV Terminal Functions connected to Non-NGN network are accessing Application Functions in the NGN network. In this figure, either Core IMS Functions or IPTV Service Control Functional Block are used in the NGN network (depending on which architecture variant is used in the NGN network) and are requesting network resources from its own RACF. For the Non-NGN side, the Resource Control Functional Block may or may not be supported. It is expected that Inter-working Gateway Functional Block be placed between Non-NGN and NGN for both content format and signalling message conversion. The Inter-working Gateway Functional Block may also coordinate QoS control between Non-NGN and NGN.

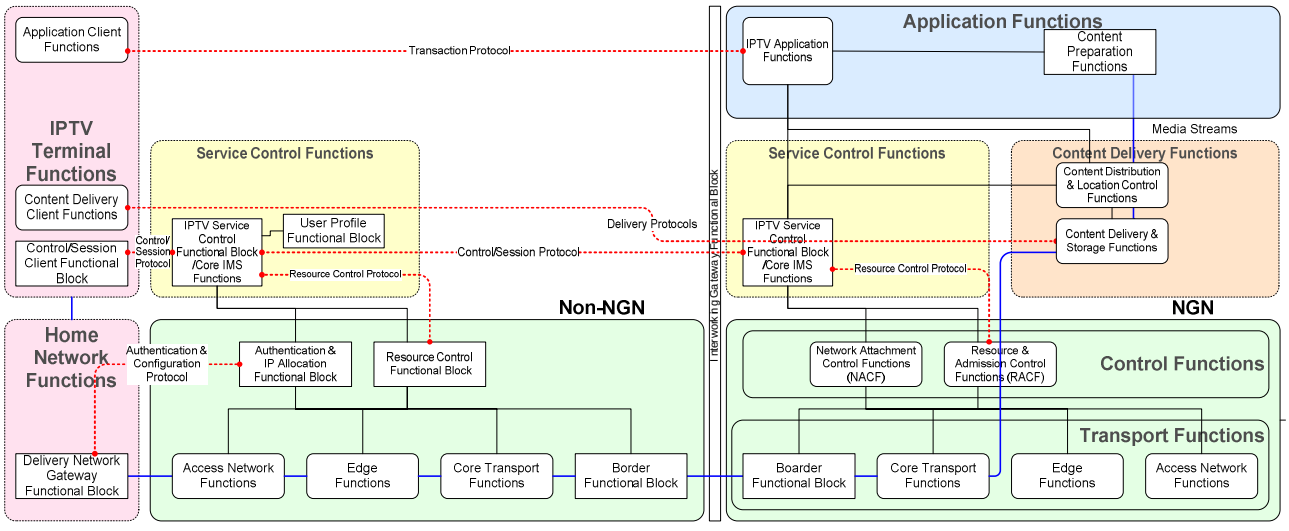


Figure 10-4: Interconnection with the Non-NGN network

Figure 10-5 also illustrates the case where IPTV Terminal Functions connected to Non-NGN network are accessing Application Functions in the NGN network.. In this figure, the Service Control Functions in Non-NGN network are not used. For the NGN side, either Core IMS Functions or IPTV Service Control Functional Block is used, depending on which architecture variant is used in the NGN network. . For the Non-NGN side, the Resource Control Functional Block may or may not be supported. It is expected that Interworking Gateway Functional Block be placed between Non-NGN and NGN for both content format and signalling message conversion. The RACF of the NGN network requests the network resources of the Non-NGN network from the Resource Control Functional Block of the Non-NGN network, through the Interworking Gateway Functional Block. The Interworking Gateway Functional Block could also coordinate QoS control between Non-NGN and NGN.

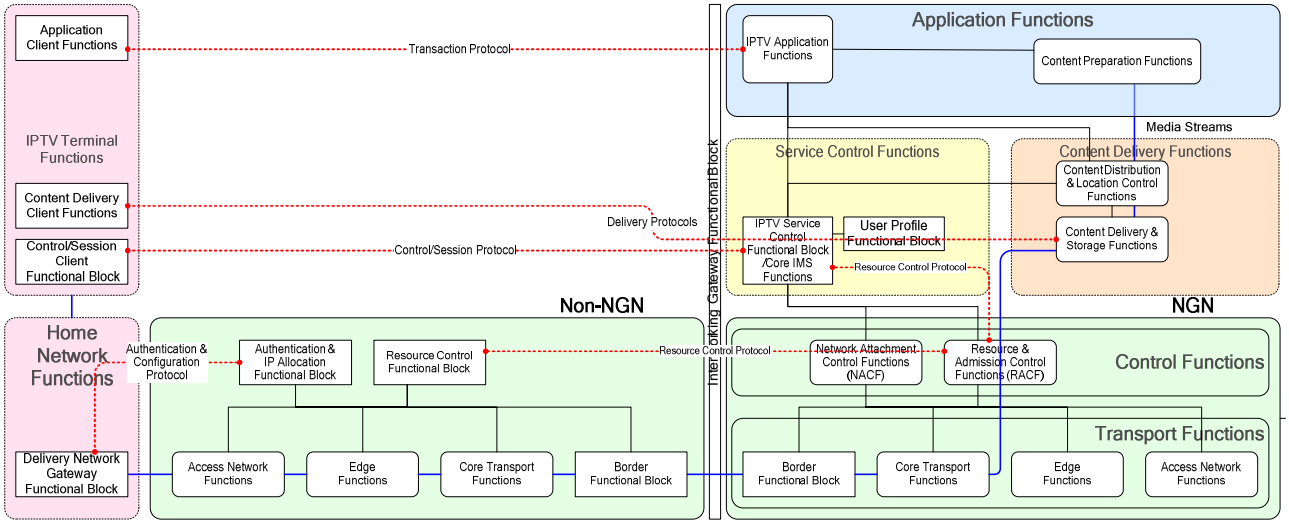


Figure 10-5: Interconnection with the Non-NGN without Service Control Functions

10.2.2 Interconnection with the third party provider network

Figure 10-6 illustrates the interconnection with the Third Party Provider Network. In this figure, the home network is a Non-NGN network. Either Core IMS Functions or IPTV Service Control Functional Block is used, depending on which architectural variant is used in the Third Party Provider Network.

The Application Functions and Content Delivery Functions of the third party provider are involved in providing IPTV services. The Service Control Functions of third party provider request the network resources to its RACF, while the Service Control Functions of the home network request the network resources from its Resource Control Functions.

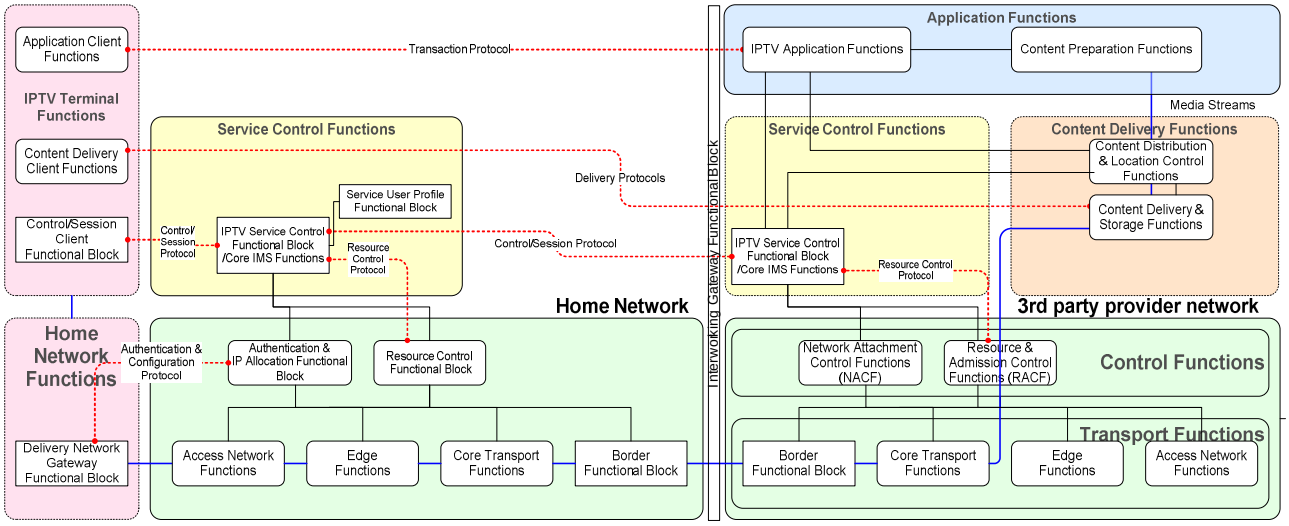


Figure 10-6: Interconnection with the third party provider

Annex A

Relationship Between IPTV and NGN Architectures

A.1 IPTV related components in the NGN architecture

It is useful to relate the IPTV architecture to the general NGN framework architecture and other networks to clarify the similarities and differences, as well as provide a reference for the more detailed description of IPTV specific components. The "NGN-based" architecture means the IPTV architecture in accordance with [ITU-T Y.2012] for providing IPTV services. The NGN components described in [ITU-T Y.2012] are shown in Figure A-1.

As the Non-NGN IPTV functional architecture mentioned in the scope and detailed later in the main body of this document does not necessarily require NGN components, and uses conventional and/or legacy technology networks for delivery of IPTV services, Figure A-1 should not be construed as the only basis for IPTV services.

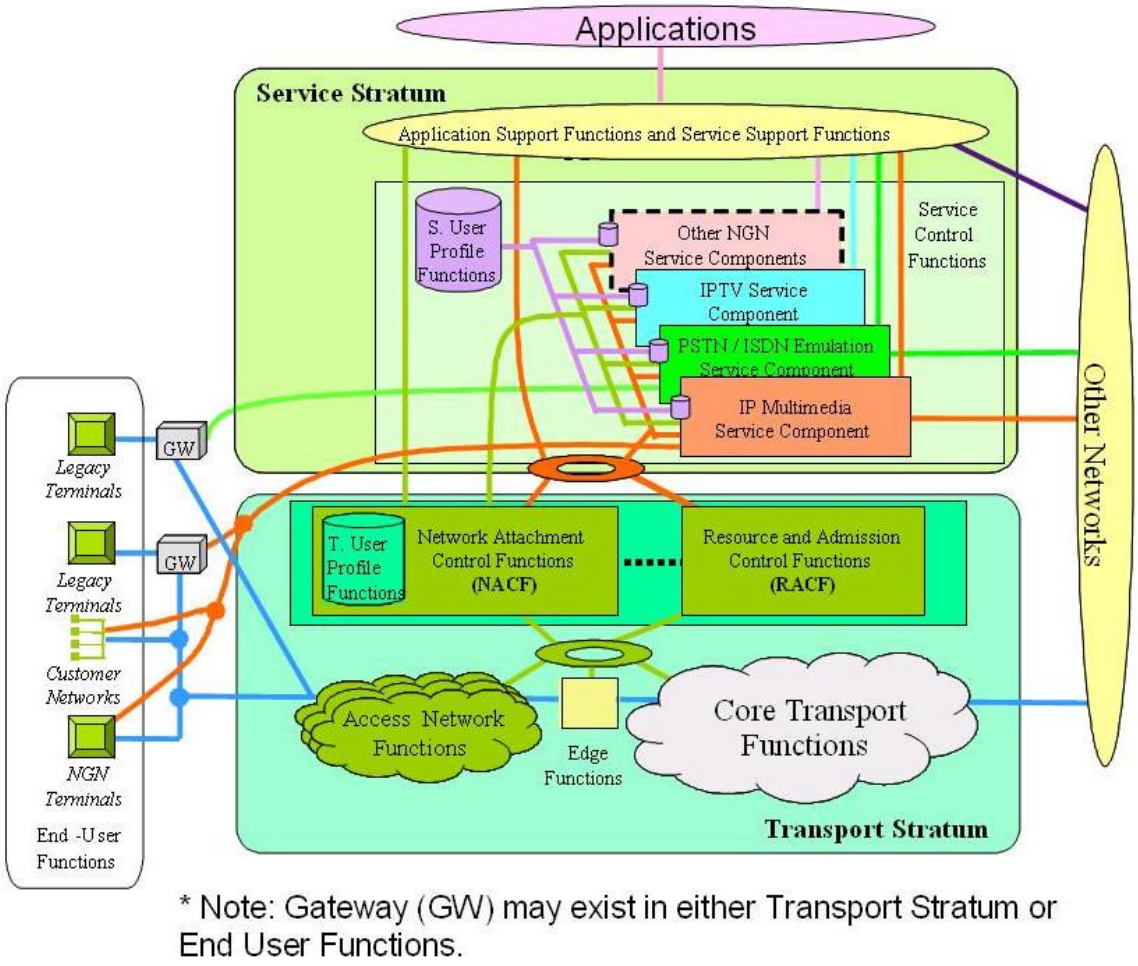


Figure A-1: Transport and service configuration of the NGN

NOTE – There is an oversight in diagram A-1: service components are not purely service control but also comprise service delivery functions. To remedy this problem, the diagram from [ITU-T Y.2012] should have a service control function box that stops halfway into the underlying components, with another "service delivery functions" box covering the remaining space."

A.2 Functional Mapping between NGN-based IPTV and NGN architectures

The NGN-based IPTV architecture is defined in accordance with [ITU-T Y.2012] for providing IPTV services. Therefore, its functionalities have a correspondence relationship with the NGN architecture.

Application Functions may be included in Application Support Functions & Service Support Functions of NGN shown in Figure A-1. Service Control Functions and Content Delivery Functions may be included in the IPTV service component of NGN of Figure A-1. Thus, Application Functions, Service Control Functions, and Content Delivery Functions are included in the Service Stratum of the NGN architecture.

NOTE – Provided that Figure A-1 is modified so that the IPTV service components contain both a service control and a service delivery part.

Table A-1 (Functional mapping between NGN-based IPTV and NGN architectures) provides the relationships between the functions of these two architectures.

Table A-1: Functional mapping between NGN-based IPTV and NGN architectures

No.	IPTV architecture	NGN architecture	Comments
1	Network Functions	Transport Stratum	These correspond to each other.
2	End-user Functions	End-User Functions	These correspond to each other.
3	Management Functions	Management Functions	These correspond to each other.
4	Service Control Functions	Service Control Functions (in Service Stratum)	IPTV Service Control Functional Block corresponds to NGN Service Control Functions. However, NGN Service Control Functions may include other functionalities.
5	Content Delivery Functions	Somewhere in the service stratum (possibly "Service Delivery Function" if created in ITU-T Recommendation Y.2012 [ITU-T Y.2012]).	Content Delivery Functions may reside outside the NGN in cases like a third party service provider.
6	Application Functions	Application Support Functions & Service Support Functions (in Service Stratum)	Application Functions may reside outside the NGN in cases like a third party service provider.

NOTE – Content Provider Functions are out of scope and not included in this mapping table.

A.3 Application Support Functions & Service Support Functions

The Application Support Functions & Service Support Functions which is defined in ITU-T Recommendation Y.2012 [ITU-T Y.2012] include four functional entities such as Application Support Functional Entity (AS-FE), Application Gateway Functional Entity (APL-GW-FE), Application Service Coordination Manager Functional Entity (APL-SCM-FE) and Service Switching Functional Entity (SS-FE).

Among these functional entities, AS-FE has the closest relationship with the Application Functions of the IPTV Architecture. The guidelines for selecting functions as the AS-FE are as follows:

- A function that is used in common in two or more applications is recommended to be included in AS-FE.
- From the viewpoint of personal information and privacy protection, a function that handles the user profile managed within NGN is recommended to be included in the AS-FE.
- From the viewpoint of security, a function that handles the inside information of network, such as network control signalling, is recommended to be included in the AS-FE.
- A function that can be located in application support functions and service support functions to provide an efficient service is recommended to be included in the AS-FE to improve QoE.

Appendix I

Procedural Flows Relating to IPTV Services

(This Appendix does not form an integral part of this document.)

The functional architecture in clause 9 describes the functions and functional blocks of the IPTV architecture. The following clauses describe the interactions between the functions and functional blocks by illustrating the related procedural flows.

NOTE – These procedural flows are intended as illustrative examples of interactions between functional blocks and functions, and should not be taken as mandatory when implementing the IPTV architectures defined in this document.

[EDITOR'S NOTE – The content of the appendices has not been checked in depth during the last review. Its content should be checked for consistency and technical accuracy.]

I.1 High level flows

The high-level procedural flows describe the high level interactions between the functions in the IPTV architecture.

In this description the Content Delivery Functions and Service Control Functions are combined, represented as a single group of functions called "Content Delivery & Service Control Functions, so that the different interaction between the Application Functions and these functions can be illustrated. Detailed breakdown of the functions, and their associated procedural flows, are described later.

In general, a transactional protocol is used between the ITF and the Application Functions, this protocol is used for the selection and, if required, purchase of content. A streaming control protocol is used between the ITF and the Content Delivery & Service Control Functions to establish the delivery and control the content. A delivery protocol is used to carry the content from a delivery function to the ITF.

There are two main approaches to timing of the allocation resources:

- **Tightly Coupled:** The delivery and network resources are allocated on request of the application during the transactional phase of the service. They are released by a request from the application after viewing has been completed. This requires a session to be maintained with the transaction protocol. This approach is called "tightly coupled" as the application layer is tightly coupled to the control and delivery layer.
- **Loosely coupled:** The delivery and network resources are allocated in response to the establishment of the streaming protocol session. They are released when this streaming protocol session is terminated. This approach is called "loosely coupled" as the application layer is only loosely coupled to the control and delivery layer.

The principal differences between Tight and Loose Coupling of the application with the Service Control Functions are the timing of the allocation of delivery and network resources. Close coupling may be more appropriate for the immediate consumption of content as delivery can be guaranteed. Loose coupling may be more appropriate for delayed consumption of content as resources are not allocated until actually needed.

Although the event sequences for the Tightly Coupled Content On-Demand and Loosely Coupled Content On-Demand operation for Content On-Demand are different the sequence of messages sent by the ITF are the same. The same is true for the two Linear TV cases. This should allow an ITF to interoperate with either style of application to Service Deliver and Control operation.

NOTE – In cases where there is no clear distinction between the application functions and the content delivery and service control functions, these diagrams may not accurately represent the procedural flows. For specific IMS-based procedural flows, refer to clause I.4.

I.1.1 High level procedural flows for loosely coupled Content-on-Demand

The following procedural flows represent the high-level sequence of flows for a Content-on-Demand application that uses the Unicast Content Delivery Functions where the application is loosely coupled to the Service Control Functions.

Pre Conditions: It is assumed that provisioning, network attachment and service selection have been completed.

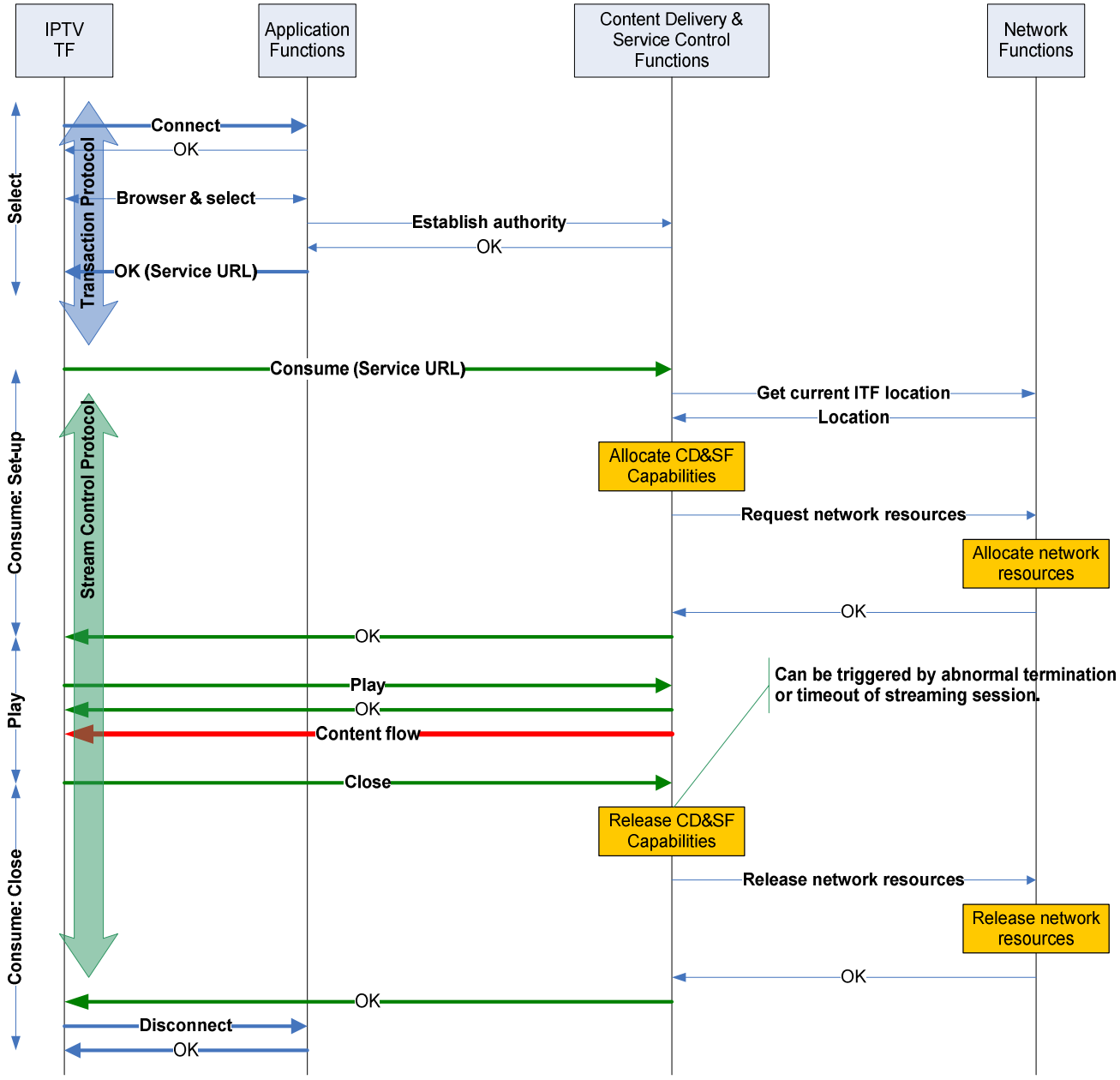


Figure I-1: High level procedural flows for loosely coupled Content-on-Demand

1. IPTV Terminal Functions, ITF, connects to and interacts with the Application Functions to select the content item that the customer wishes to receive.

2. The Application connects to the Content Delivery & Service Control Functions, to establish the authority for the ITF to consume the content.

3. The application returns the URL of the Content Delivery & Service Control Functions and content item.

4. ITF connects to the Content Delivery & Service Control Functions to request the delivery of the content item.

5. The Content Delivery & Service Control Functions determined the location of the ITF, for example by querying the Network Control function.

6. The Content Delivery & Service Control Functions determines which delivery function has the requested content and can be connected to the ITF and allocates this.

7. The Content Delivery & Service Control Functions requests the allocation of the network resources needed to support the network path from the delivery function to the ITF.

8. The ITF issues a Play request.

9. The Content Delivery & Service Control Functions streams the content to the ITF.

10. At the end of the viewing session the ITF closes the Streaming Session.

11. The Content Delivery & Service Control Functions releases the delivery resources.

12. The Content Delivery & Service Control Functions requests the release of network resources.

13. The Content Delivery & Service Control Functions confirms that the session is closed.

I.1.2 High level procedural flows for tightly coupled Content-on-Demand

The following procedural flows represent the high-level sequence of flows for a Content-on-Demand application that uses the Unicast Content Delivery Functional Block, where the application is tightly coupled to the Service Control Functions.

Pre Conditions: It is assumed that provisioning, network attachment and service selection have been completed.

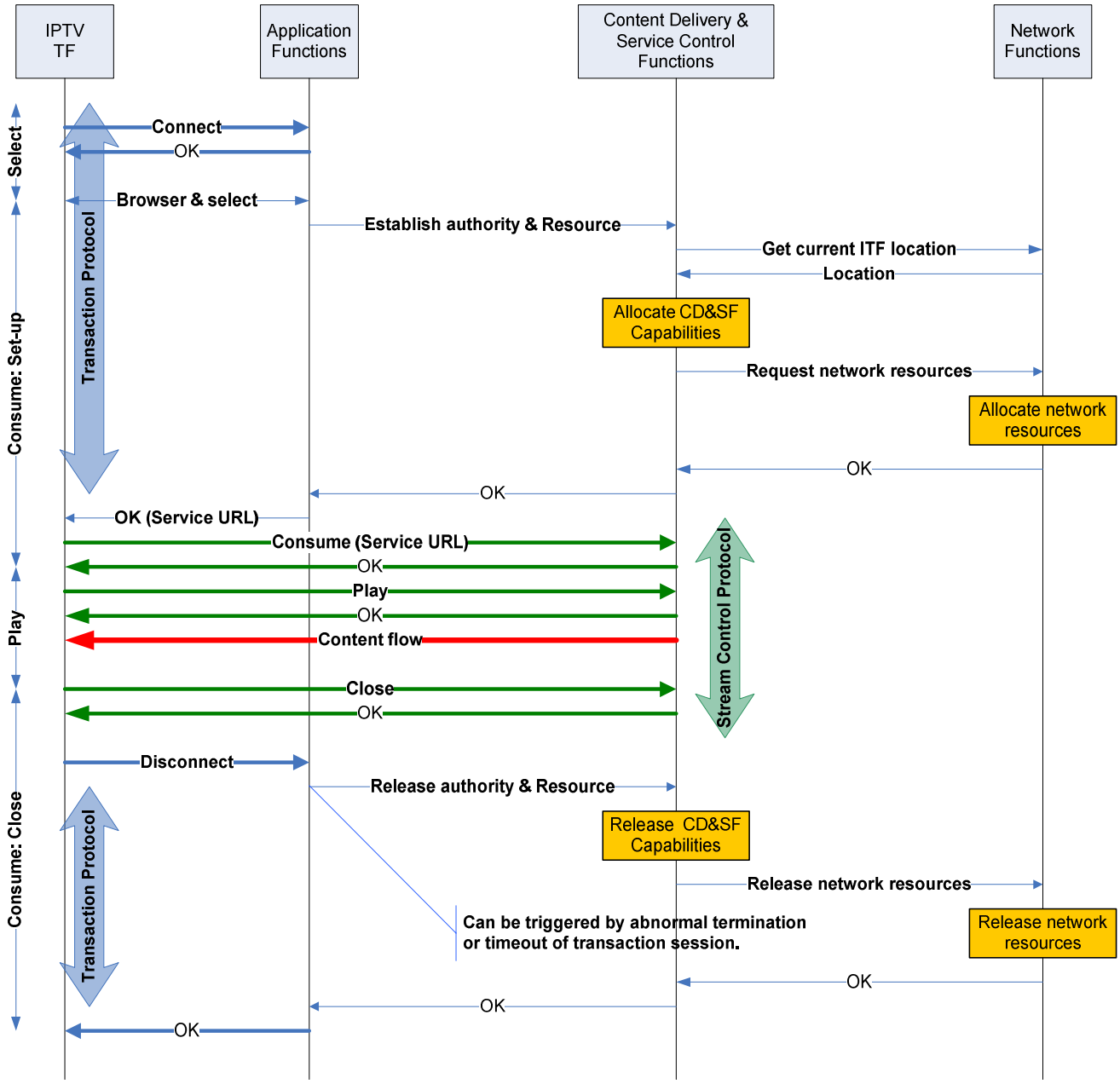


Figure I-2: High level procedural flows for tightly coupled Content-on-Demand

1. The IPTV Terminal Function, ITF, connects to and interacts with the Application to select the content item that the customer wishes to receive.

2. The Application connects to the Content Delivery & Service Control Functions to establish the authority for the ITF to consume the content and reserve the delivery and network resources.

3. The Content Delivery & Service Control Functions determines the location of the ITF, for example by querying the Network Control Functions.

4. The Content Delivery & Service Control Functions determines which content delivery function has the requested content and could be connected to the ITF and allocates this.

5. The Content Delivery & Service Control Functions requests the allocation of the network resources needed to support the network path from the Content Delivery Functions to the ITF.

6. The application returns the URL of the Content Delivery & Service Control Functions and content item.

7. The ITF connects to the Content Delivery & Service Control Functions to request the delivery of the content item.

8. The ITF issues a Play request.

9. The Content Delivery & Service Control Functions streams the content to the ITF.

10. At the end of the viewing session the ITF closes the Streaming Session.

11. The ITF closes the transaction session with the Application.

12. The Application informs the Content Delivery & Service Control Functions that the session has ended.

13. The Content Delivery & Service Control Functions releases the delivery resources.

14. The Content Delivery & Service Control Functions requests the release of network resources.

I.1.3 High level procedural flows for loosely coupled Linear TV

The following procedural flows represent the high-level sequence of flows for a Linear TV application that uses the Multicast Delivery Functions where the application is loosely coupled to the Service Control Functions.

Pre Conditions: It is assumed that provisioning, network attachment and service selection have been completed.

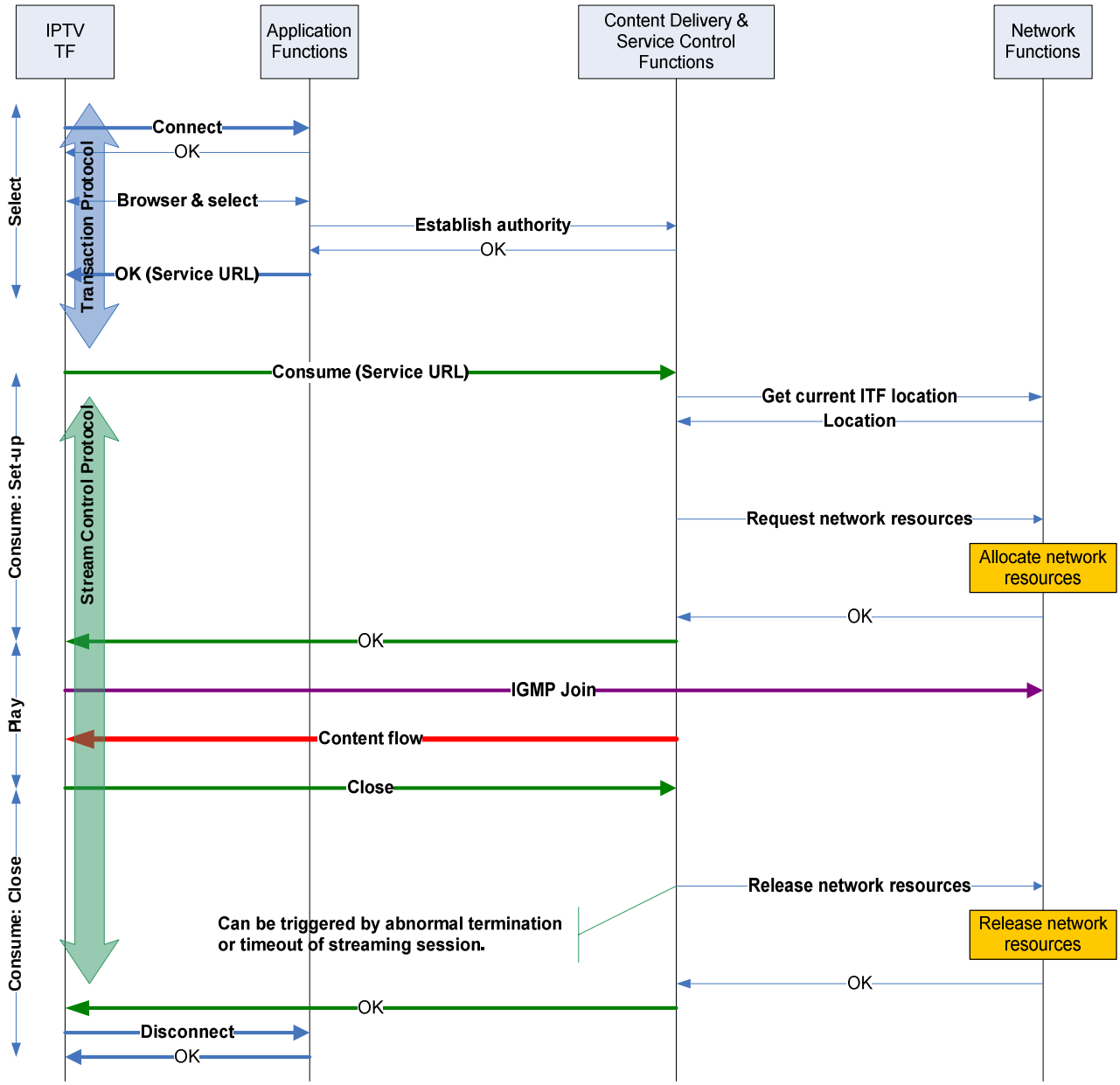


Figure I-3: High level procedural flows for loosely coupled Linear TV

1. The IPTV Terminal Function, ITF, connects to and interacts with the Linear TV Application to obtain the list of channels that the customer wishes to receive.
2. The Application connects to the Content Delivery & Service Control Functions, to establish the authority for the ITF to consume the channels.
3. The application returns the URL of the Content Delivery & Service Control Functions and the list of multicast addresses.
4. The ITF connects to the Content Delivery & Service Control Functions to request the network resources for the reception of the channels.
5. The Content Delivery & Service Control Functions determined the location of the ITF, for example by querying the Network Control function.
6. The Content Delivery & Service Control Functions requests the allocation of the network resources needed to support the network path from the delivery function to the ITF.
7. The ITF issues a Multicast Group Join request to receive the channel

8. At the end of the viewing session the ITF closes the Streaming Session.
9. The Content Delivery & Service Control Functions requests the release of network resources.
10. The Content Delivery & Service Control Functions confirms that the session is closed.

I.1.4 High level procedural flows for tightly coupled Linear TV

The following procedural flows represent the high-level sequence of flows for a Linear TV application that uses the Multicast Delivery Functional Block where the application is tightly coupled to the Service Control Functions.

Pre Conditions: It is assumed that provisioning, network attachment and service selection have been completed.

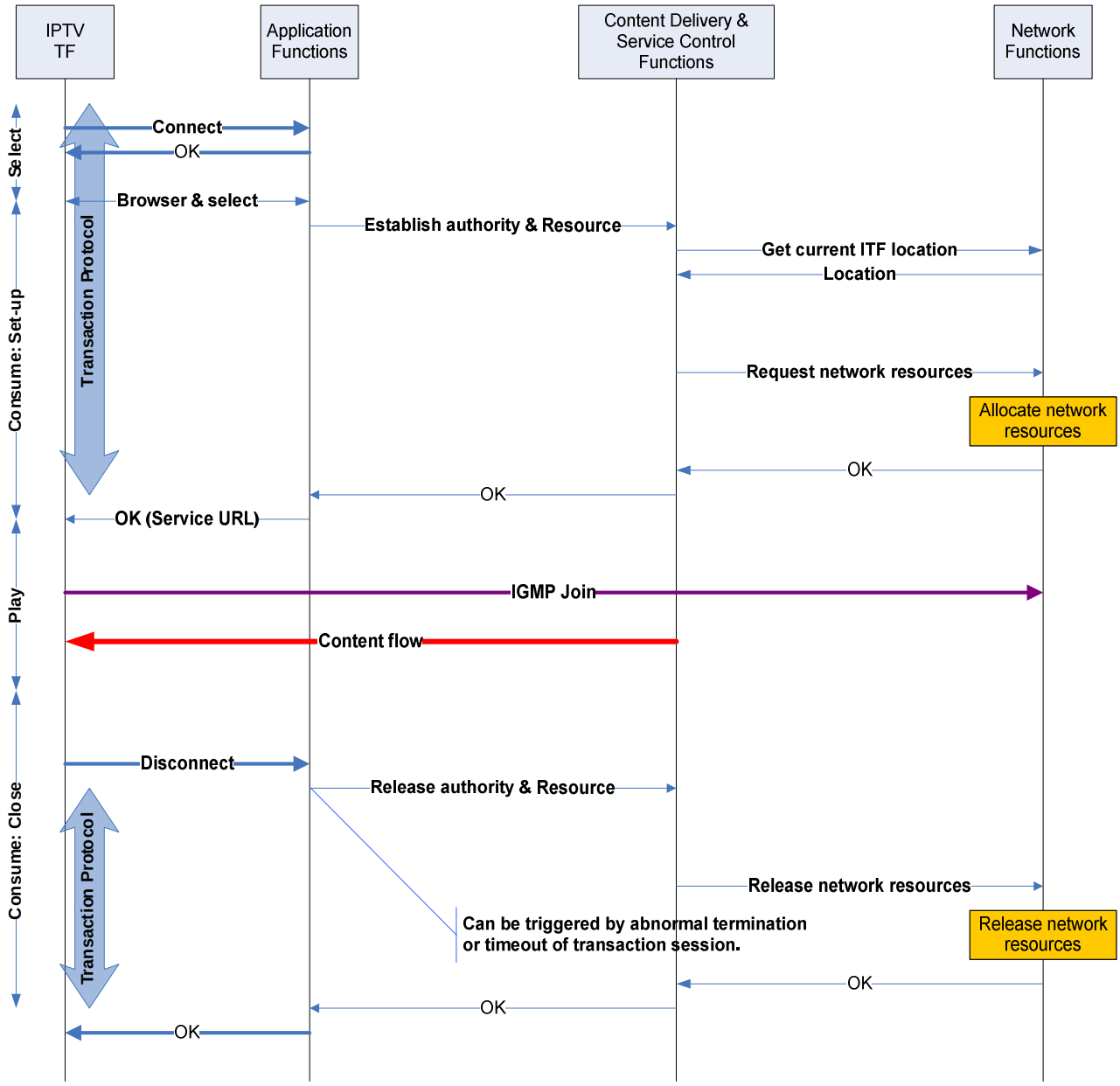


Figure I-4: High level procedural flows for tightly coupled Linear TV

1. The IPTV Terminal Function, ITF, connects to and interacts with the Linear TV Application to obtain the list of channels that the customer wishes to receive.
2. The Application connects to the Content Delivery & Service Control Functions, to establish the authority for the ITF to consume the channels and reserve the network resources.
3. The Content Delivery & Service Control Functions determined the location of the ITF, for example by querying the Network Control function.
4. The Content Delivery & Service Control Functions requests the allocation of the network resources needed to support the network path from the content delivery function to the ITF.
5. The Application returns the URL of the Content Delivery & Service Control Functions and the list of multicast addresses.
6. The ITF issues a Multicast Group Join request to receive the channel.
7 At the end of the viewing session the ITF closes the Application Session.
8. The Application informs the Content Delivery & Service Control Functions that the session has ended.
9. The Content Delivery & Service Control Functions requests the release of network resources.

I.1.5 High Level Procedural Flows for Initialization of IPTV Application Access

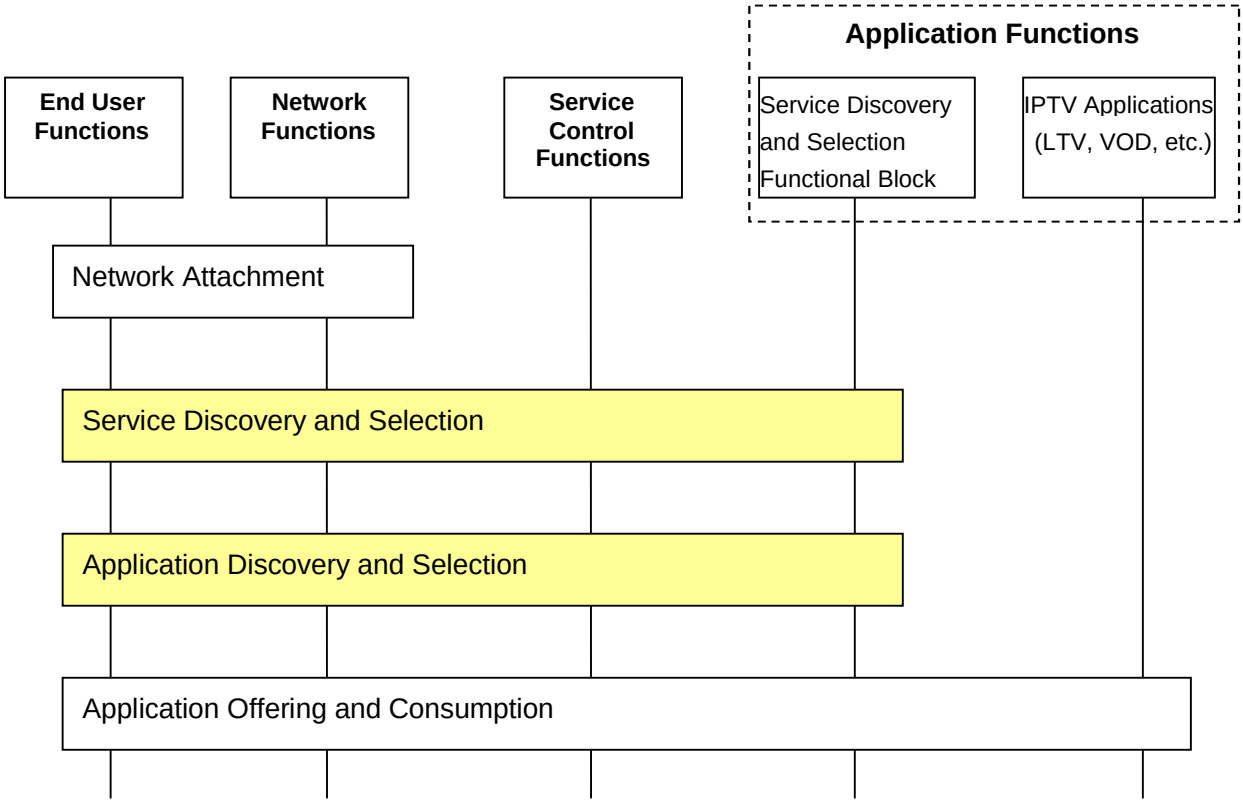


Figure I-5: High Level Procedural Flow for Initialization of IPTV Application Access

1. The user first selects a network provider and a network access mode, and the End User Functions execute the network attachment operation with the Network Functions.

2. After the user accesses the network, the Service Control Functions provide the user the initial information of the available IPTV service providers, and the user selects an IPTV service provider. The Network Functions may be involved in this procedure.

3. The Service Discovery and Selection Functional Block finds available applications (such as Linear TV, VoD, etc.), and provides these to the user for selection.

4. The user accesses the selected application.

I.1.6 High Level Procedural Flows for Content Distribution

I.1.6.1 Procedural Flows for File-based Content Distribution

File-based content distribution is mainly used in CoD services.

The procedures above the dotted line of Figure I-6 refer to file-based content distribution from the Content Preparation Functions to the Content Delivery & Storage Functions.

The procedures below the dotted line of Figure I-6 refer to file-based content distribution from Content Delivery & Storage Functions which already have received the required file-based content, and hence can distribute it to other Content Delivery & Storage Functions.

The procedures below the dotted line are intended for the case when efficiency can be enhanced for the content delivery.

Pre Conditions: It is assumed that content metadata and content protection rights information have been delivered from Content Provider Functions to Content Preparation Functions.

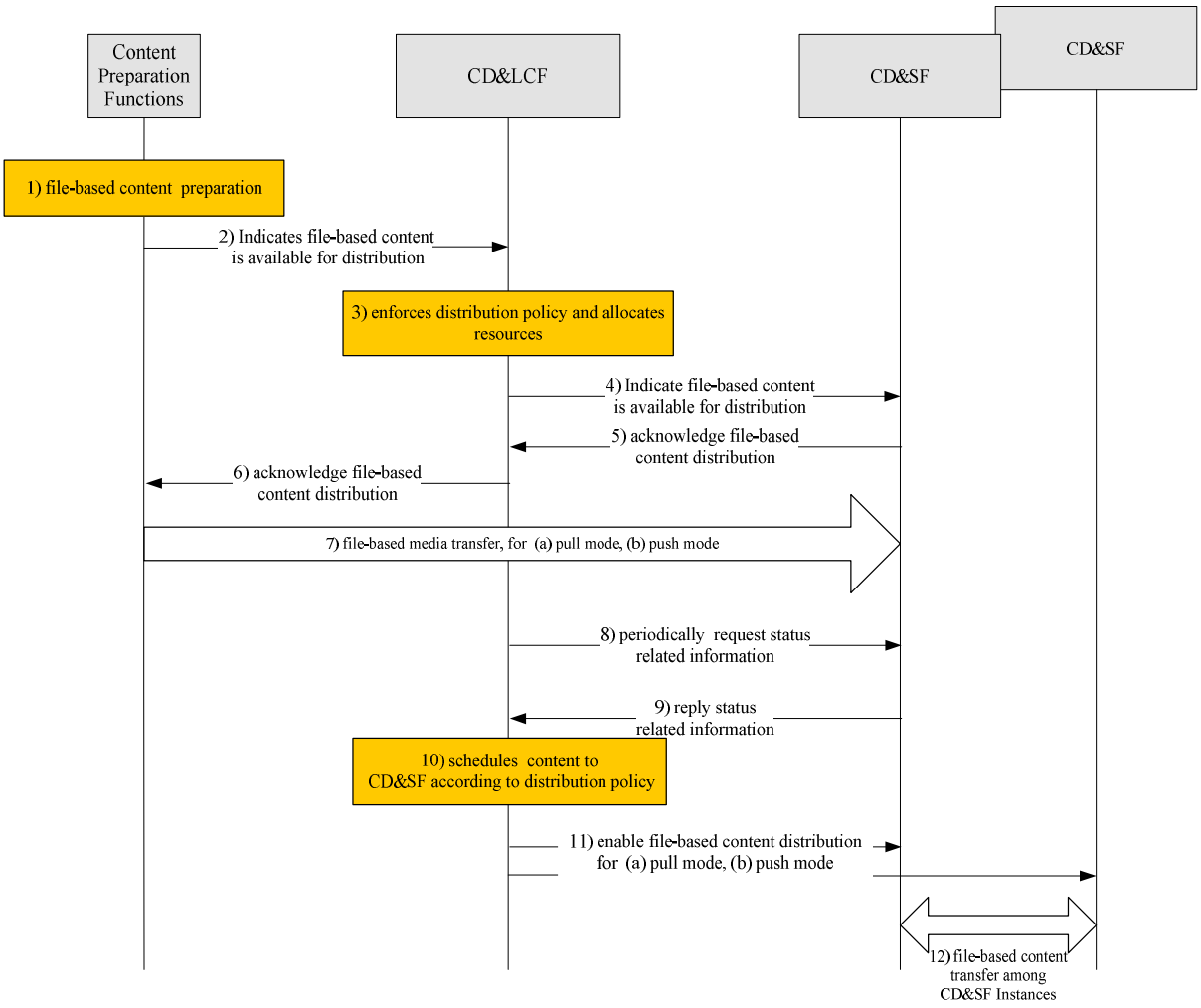


Figure I-6: Procedural Flows for File-based Content Distribution

1. File-based content preparation procedures include content aggregation, content management, metadata processing, content processing and content encryption, which may need to be completed before file-based content is distributed.
2. Content Preparation Functions indicate file-based content is available for distribution to CD&LCF.
3. CD&LCF enforce distribution policy and allocates resources (i.e. select suitable CD&SF to receive file-based content).
4. CD&LCF indicate to the CD&SF that file-based content is available for distribution..
5. CD&SF acknowledge to the CD&LCF that file-based content can be distributed.
6. CD&LCF acknowledge to the Content Preparation Functions that file-based content can be distributed.
7. Content Preparation Functions proceeds to transfer the file-based content to CS&DF.
   a) The file-based content transport method can be PULL mode, i.e. CD&SF download the file content initially from the Content Preparation Functions.
   b) The file-based content transport method can be PUSH mode, i.e. Content Preparation uploads the file content initiatively to CD&SF.

8. In order to maintain information such as file content distribution information, load status of CD&SF, CD&LCF periodically send "status" request messages to the CD&SF.
9. CD&SF return "status" related information back to CD&LCF.
10. CD&LCF schedule content to CD&SF according to distribution policy.
11. Enable file-based content distribution for (a) push mode, (b) pull mode.
12. File-based content is transferred among CD&SF instances.

I.1.6.1.2 Procedural Flows for Stream-based Content Distribution

Stream-based Content Distribution mainly used in Linear TV and Time-shifted linear TV.

Pre Conditions: It is assumed that content metadata and content protection rights information have been delivered from Content Provider Functions to Content Preparation Functions.

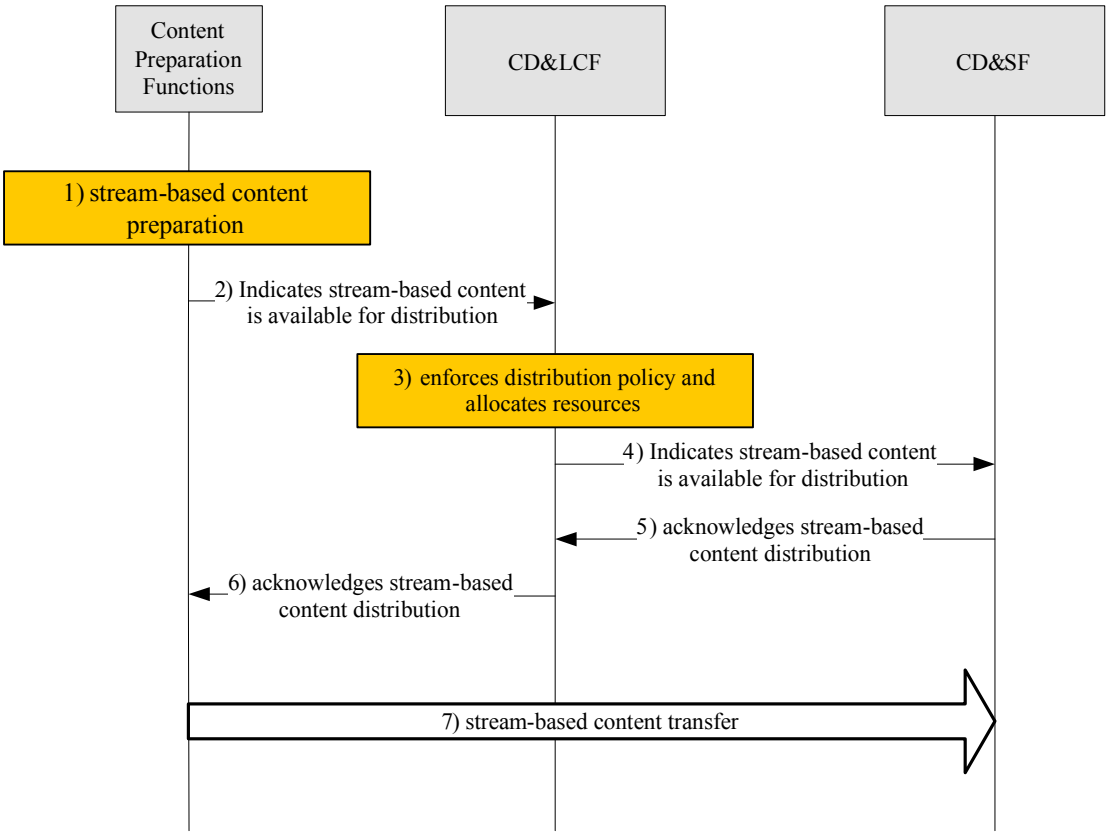


Figure I-7: Stream Content Distribution Flow

1. Stream-based content preparation procedures include content aggregation, content management, metadata processing, content processing and content encryption, which may need to be completed before file-based content is distributed.
2. Content Preparation Functions indicate stream-based content is available for distribution to CD&LCF.
3. CD&LCF enforce distribution policy and allocates resources (i.e. select suitable CD&SF to receive stream-based content).
4. CD&LCF indicate to the CS&DF that stream-based content is available for distribution.
5. CD&SF acknowledge to the CD&LCF that stream-based content can be distributed.

6. CD&LCF acknowledge to the Content Preparation Functions that stream-based content can be distributed.

7. Content Preparation Functions proceeds to transfer the stream-based content to CS&DF.

I.2 Procedural Flows for IPTV Services based on Non-NGN IPTV Architectures

The following clauses provide detailed descriptions of the procedural flows in the case of non-NGN IPTV architecture.

TBD.

I.3 Procedural Flows for IPTV Services based on NGN Non-IMS IPTV Architectures

The following clauses provide detailed descriptions of the procedural flows in the case of NGN non-IMS IPTV architecture.

There are two ways in which the IPTV Control and the Content Delivery functions may interoperate:

- **Proxy:** One approach is for IPTV Service Control Functional Block to proxy all requests between the ITF and the Content functions. In this way IPTV Control can request the allocation of delivery and network resources, track the progress of the streaming session and request the release of resources at the end of the session.
- **Redirect:** The other approach is for IPTV Service Control Functional Block to request the allocation of delivery and network resources and then redirect the ITF to communicate directly with the actual Content Storage and Delivery Functions that has been allocated.

The Proxy approach has the advantage that a single function, IPTV Service Control Functions, keeps track of the allocated resources. The Redirect approach has the advantage that the ITF communicates directly with the Content Storage and Delivery function, reducing latency and resource usage.

The Redirect approach requires that the streaming control protocol can be redirected during session establishment. This is supported by most protocols, and if supported means that a single ITF implementation can communication to ITPV services using either proxy or redirect.

The following figures show the procedural flows for the four use-cases resulting from the combination of Lose and Tight Coupling with Proxy and Redirect. In all cases the Content On-Demand Application is shown making use of the Unicast Content Delivery Functions.

Pre Conditions: It is assumed that provisioning, network attachment and service selection have been completed.

I.3.1 Procedural Flows for Content On-Demand with Loose Coupling and Redirect

The following **procedural flows** show the interaction between the ITF and the IPTV Application Functions, IPTV Service Control Functions and the Content Delivery Functions, where the Application Functions and the IPTV Service Control Functional Block do not communicate with each other, and the IPTV Service Control Functional Block redirects the ITF to the allocated Content Storage and Delivery Functions.

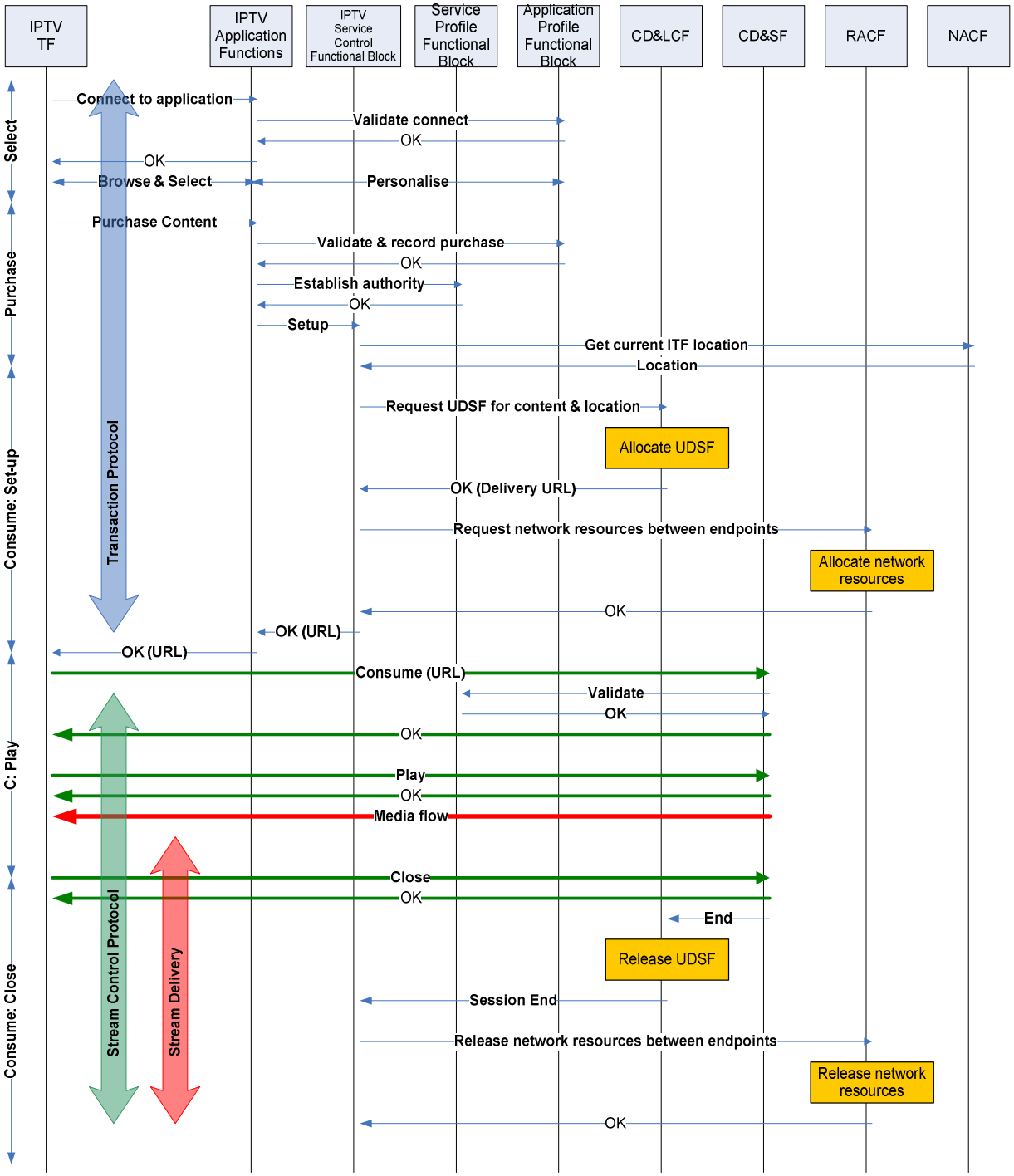


Figure I-8: On-Demand Procedural Flows with Loose Coupling and Redirect

1. The ITF runs the On-Demand Client which connects, using a transactional protocol, to On-Demand Application to obtain the URL of the IPTV Service Control Functional Block with a reference to the content item that the customer wishes to receive. During this interaction that application will authorize the ITF's connection, it may use the application profile to personalise the service, it may record the transaction and any associated purchase in the application profile. The application will establish, within the service profile, the authority for the ITF to subsequently consume the content.

2. The ITF connect to the IPTV Service Control Functional Block, using a session control protocol, passing it the reference to the content item to be consumed. The IPTV Service Control Functional Block authorizes the ITF's connection request against the authority that has been established.

3. The IPTV Service Control Functional Block determines the location of the IPTV Device, for example by querying the NACF. It passes this information and the content reference to the Unicast Delivery Control Functional Block to request the allocation of delivery resources.

4. The Content Delivery Control Function determines which Unicast Delivery Functional Block has the requested content and could be connected to the IPTV Device. It queries, or maintains the state of, the Unicast Delivery Functional Block to identify one that has free capacity and allocates this to the ITF. It returns the URL of physical server containing the allocated content item to the IPTV Service Control Functional Block.

5. The IPTV Service Control Functional Block requests the network resources needed to support the network path from the Unicast Delivery Functional Block to the IPTV device. IPTV Service Control Functional Block returns the ITF a redirect containing the URL of physical server and content item.

6. The ITF redirects its session control connection to the identified Unicast Delivery Functional Block to control and receive the content.

7. The Unicast Delivery Functional Block uses a delivery protocol to send the content to the ITF.

8. At the end of the viewing the ITF terminates the streaming control session with the Unicast Delivery Functional Block.

9. The Unicast Delivery Functional Block informs the Unicast Delivery Control Function that the session has ended.

10. The Unicast Delivery Control Function releases the delivery resources and informs the IPTV Control Function that the session has ended.

11. The IPTV Control Function requests the release of network resources that were allocated to the network path from the Unicast Delivery Functional Block to the ITF.

In the exception case where the ITF does not perform step 8 the Unicast Delivery Functional Block monitors the session and if this fails performs step 9. Steps 10 and 11 would also follow.

I.3.2 Procedural Flows for Content On-Demand with Loose Coupling and Proxy

The following **procedural flows** show the interaction between the ITF and the IPTV Application Functions, IPTV Service Control Functions and the Content Delivery Functions, where the Application Functions and the IPTV Service Control Functional Block do not communicate with each other and the IPTV Service Control Functional Block proxies the communications between the ITF and the allocated Content Storage and Delivery Function.

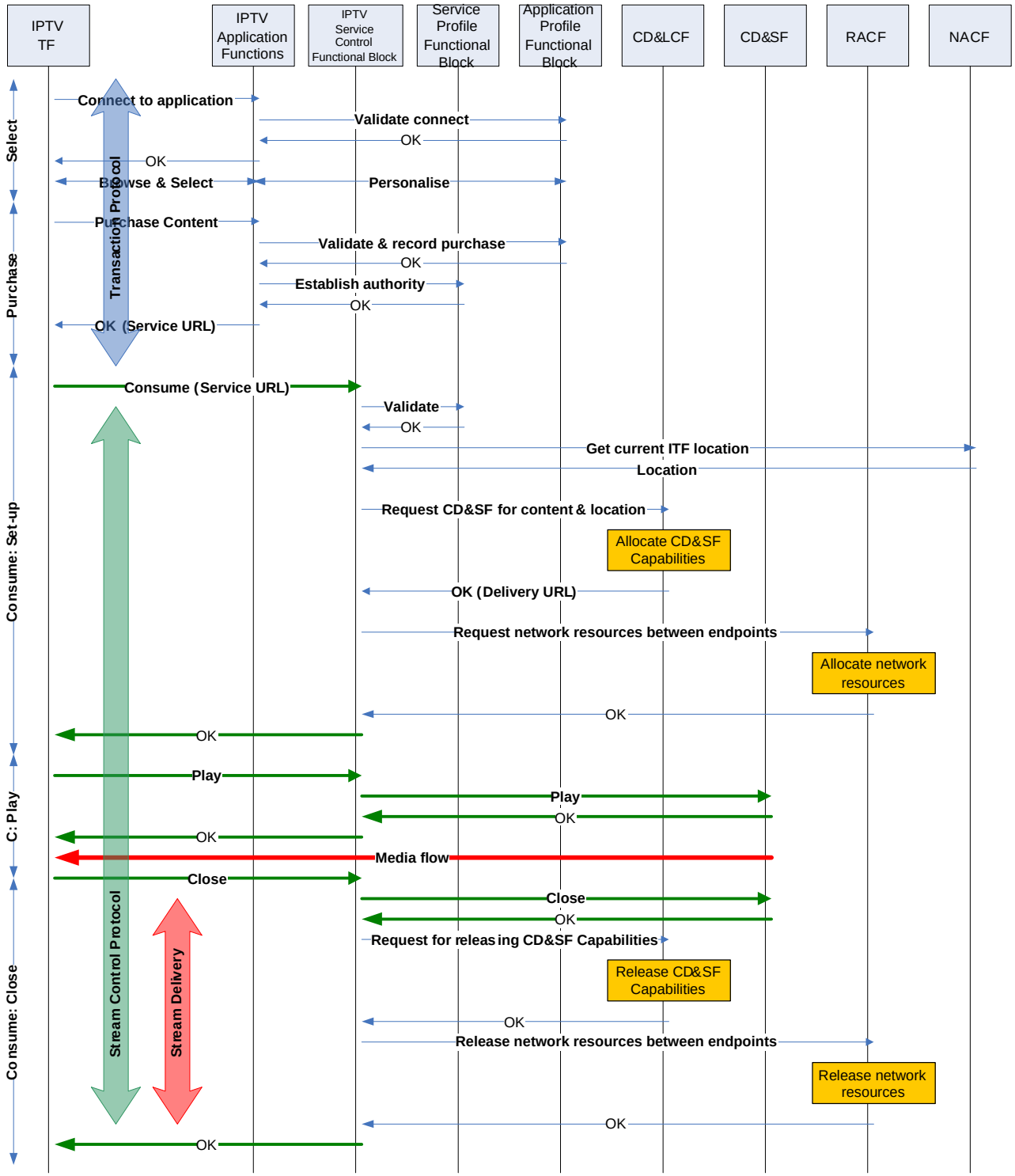


Figure I-9: On-Demand Procedural Flows with Loose Coupling and Proxy

1. The ITF runs the On-Demand Client which connects, using a transactional protocol, to On-Demand Application to obtain the URL of the IPTV Service Control Functional Block with a reference to the content item that the customer wishes to receive. During this interaction that application will authorize the ITF's connection, it may use the application profile to personalise the service, it may record the transaction and any associated purchase in the application profile. The application will establish, within the service profile, the authority for the ITF to subsequently consume the content.

2. The ITF connect to the IPTV Service Control Functional Block, using a session control protocol, passing it the reference to the content item to be consumed. The IPTV Service Control Functional Block authorizes the ITF's connection request against the authority that has been established.

3. The IPTV Service Control Functional Block determines the location of the IPTV Device, for example by querying the NACF. It passes this information and the content reference to the Unicast Delivery Control Function to request the allocation of delivery resources.

4. The Content Delivery Control Function determines which Unicast Delivery Functional Block has the requested content and could be connected to the IPTV Device. It queries, or maintains the state of, the Unicast Delivery Functional Block to identify one that has free capacity and allocates this to the ITF. It returns the URL of physical server containing the allocated content item to the IPTV Service Control Functional Block.

5. The IPTV Service Control Functional Block requests the network resources needed to support the network path from the Unicast Delivery Functional Block to the IPTV Device.

6. The IPTV Service Control Functional Block starts to proxy the ITF's session control connection to the identified Unicast Delivery Functional Block to control and receive the content

7. The Unicast Delivery Functional Block uses a delivery protocol to send the content to the ITF.

8. At the end of the viewing the ITF terminates the streaming control session which the IPTV Service Control Functional Block proxies to the Unicast Delivery Functional Block.

9. The IPTV Service Control Functions informs the Unicast Delivery Control Function that the session has ended

10. The Unicast Delivery Control Function releases the delivery.

11. The IPTV Control Function requests the release of network resources that were allocated to the network path from the Unicast Delivery Functional Block to the ITF.

In the exception case where the ITF does not perform step 8 the IPTV Service Control Functions monitors the session and if this fails terminates the connection to the Unicast Delivery Functional Block and performs step 9. Steps 10 and 11 would also follow.

I.3.3 Procedural Flows for Content On-Demand with Tight Coupling and Redirect

The procedural flows show the interactions between the ITF and the IPTV Application Functions, the IPTV Service Control Functional Block and the Content Delivery Functions, where the Application communicates with the IPTV Service Control Functional Block to pre-allocate resources. As the delivery resources have already been allocated, the ITF communicates directly to the allocated Content Storage and Delivery Functions.

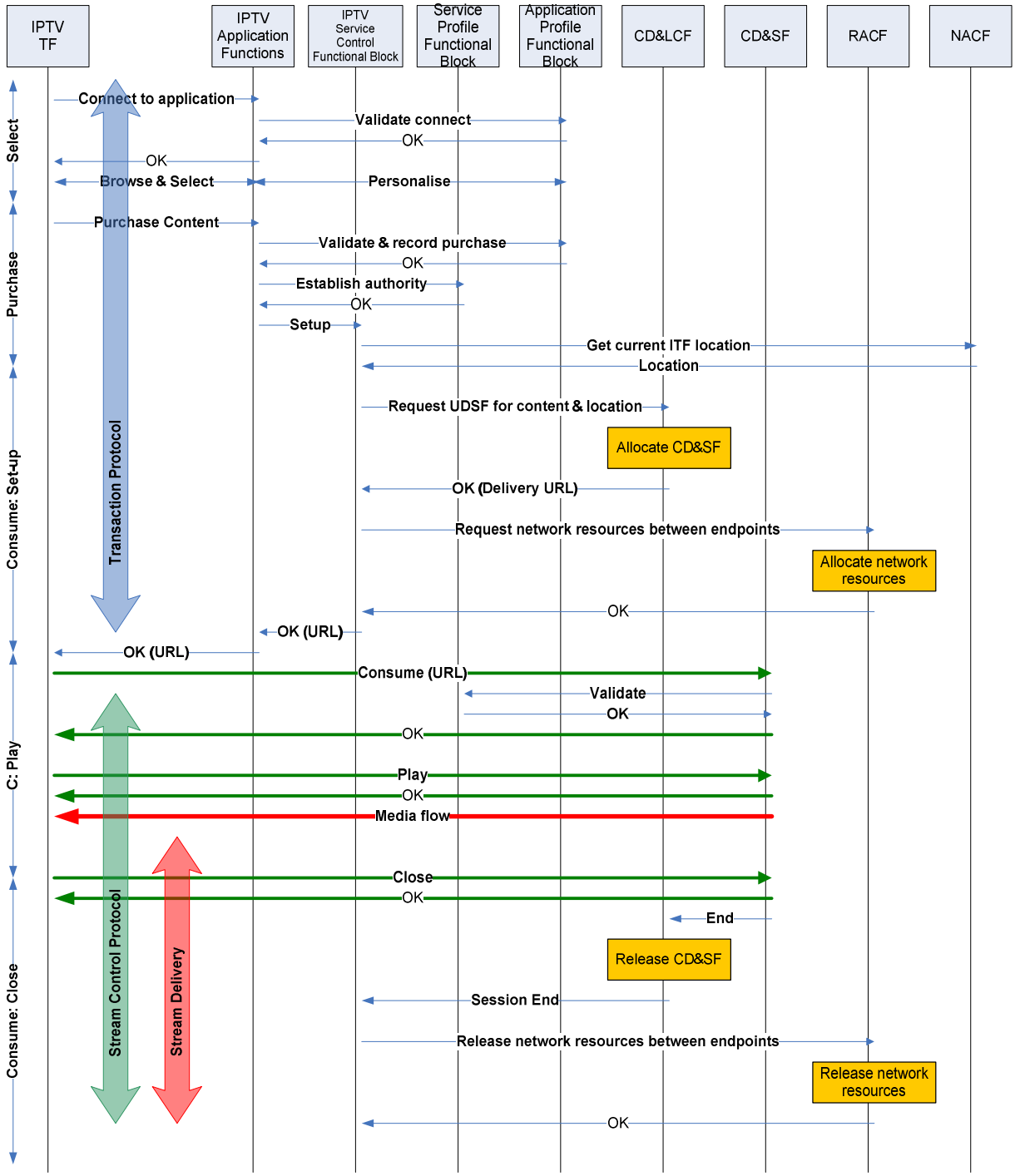


Figure I-10: Procedural Flows for On-Demand Procedural Flows with Tight Coupling and Redirect

1. The ITF runs the On-Demand Client which connects, using a transactional protocol, to On-Demand Application to obtain the URL of the IPTV Service Control Functional Block with a reference to the content item that the customer wishes to receive. During this interaction that application will authorize the ITF's connection, it may use the application profile to personalise the service, it may record the transaction and any associated purchase in the application profile. The application will establish, within the service profile, the authority for the ITF to subsequently consume the content.

2. The Application connects to the IPTV Service Control Functional Block passing it the reference to the content item to be consumed and the ITF.

3. The IPTV Service Control Functional Block determines the location of the ITF, for example by querying the NACF. It passes this information and the content reference to the Unicast Delivery Control Function to request the allocation of delivery resources.

4. The Content Delivery Control Function determines which Unicast Delivery Functional Block has the requested content and could be connected to the IPTV Device. It queries, or maintains the state of, the Unicast Delivery Functional Block to identify one that has free capacity and allocates this to the ITF. It returns the URL of physical server containing the allocated content item to the IPTV Service Control Functional Block.

5. IPTV Service Control Functional Block requests the network resources needed to support the network path from the Unicast Delivery Functional Block to the IPTV Device. IPTV Service Control Functional Block returns to the Application the URL of physical server and content item, which in turn pass this to the ITF.

6. The ITF establishes session control connection to the identified Unicast Delivery Functional Block to control and receive the content The Unicast Delivery Functional Block authorizes this request by checking with the service profile.

7. The Unicast Delivery Functional Block uses a delivery protocol to send the content to the ITF.

8. At the end of the viewing the ITF terminates the streaming control session with the Unicast Delivery Functional Block.

9. The ITF then terminates that connection to the Application with in turn informs the IPTV Service Control Functions that the session has ended.

10. The IPTV Service Control Functional Block informs the Unicast Delivery Control Function that the session has ended so that it can release the delivery resources.

11. The IPTV Control Function requests the release of network resources that were allocated to the network path from the Unicast Delivery Functional Block to the ITF.

In the exception case where the ITF does not perform step 9 the IPTV Application Functions is monitoring the session and if this fails, it request terminates the session and notifies the IPTV Control Functional Block. Steps 10 and 11 would also follow.

I.3.4 Procedural Flows for Content On-Demand with Tight Coupling and Proxy

The following flow shows the interaction between the ITF and the application, the IPTV Service Control Functions and the Content Delivery Function elements, where the Application calls the IPTV Service Control Functions to pre-allocated resources. The IPTV Service Control Functions acts as a proxy for the communications between the ITF and the allocated Content Storage and Delivery Function.

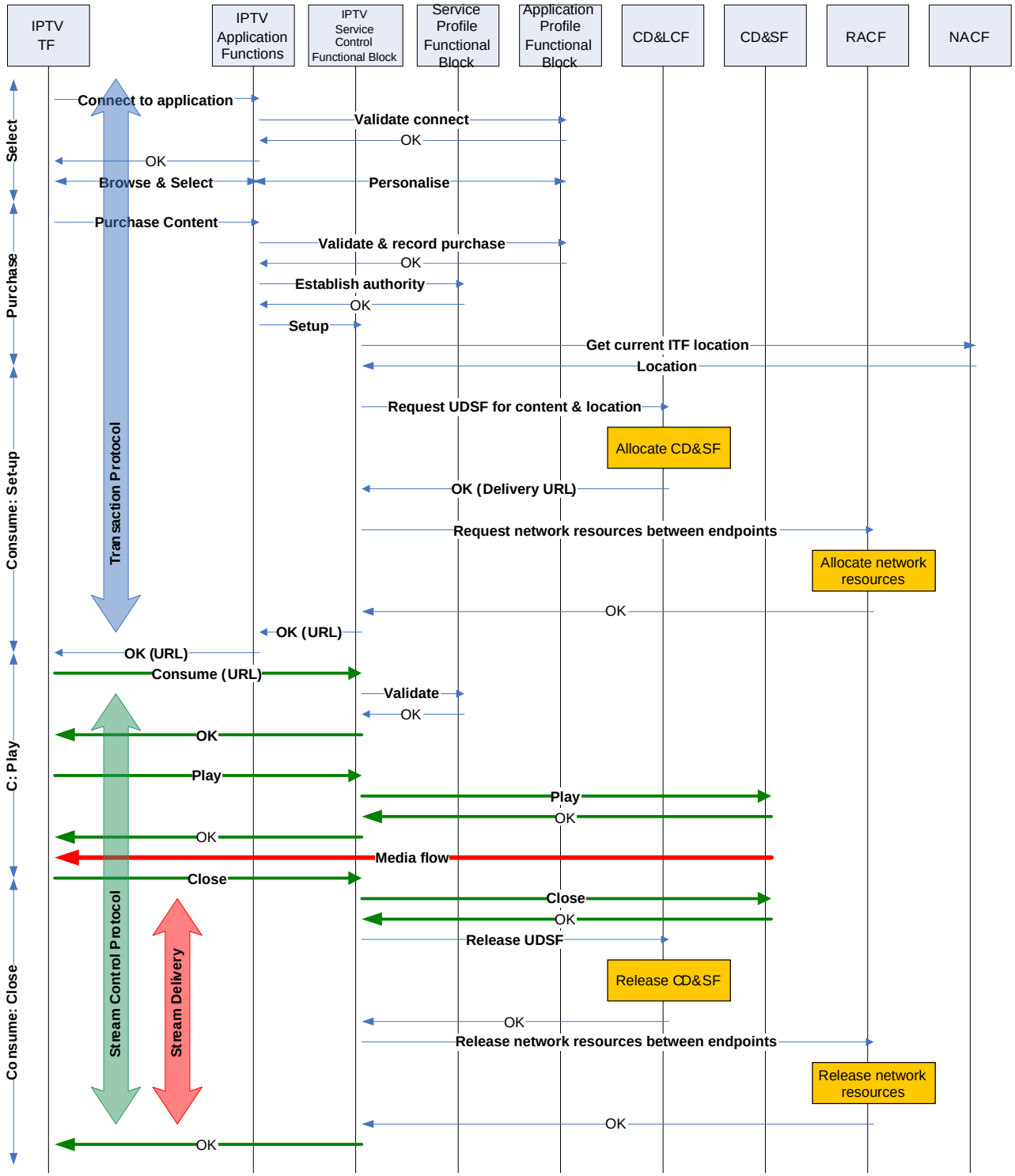


Figure I-11: Procedural Flows for On-Demand Procedural Flows with Tight Coupling and Proxy

1. The ITF runs the On-Demand Client which connects, using a transactional protocol, to On-Demand Application to obtain the URL of the IPTV Service Control Functional Block with a reference to the content item that the customer wishes to receive. During this interaction that application will authorize the ITF's connection, it may use the application profile to personalise the service, it may record the transaction and any associated purchase in the application profile. The application will establish, within the service profile, the authority for the ITF to subsequently consume the content.

2. The Application connects to the IPTV Service Control Functional Block, passing it references to the content item to be consumed and the ITF.

3. The IPTV Service Control Functional Block determines the location of the IPTV Device, for example by querying the NACF. It passes this information and the content reference to the Unicast Delivery Control Function to request the allocation of delivery resources.

4. The Content Delivery Control Function determines which Unicast Delivery Functional Block has the requested content and could be connected to the IPTV Device. It queries, or maintains the state of, the Unicast Delivery Functional Block to identify one that has free capacity and allocates this to the ITF. It returns the URL of physical server containing the allocated content item to the IPTV Service Control Functional Block.

5. The IPTV Service Control Functional Block requests the network resources needed to support the network path from the Unicast Delivery Functional Block to the IPTV Device. IPTV Service Control Functional Block returns to the Application the URL of physical server and content item, which in turn pass this to the ITF.

6. The ITF starts to session control connection to the IPTV Service Control Functional Block which proxies the request to the selected Unicast Delivery Functional Block.

7. The Unicast Delivery Functional Block uses a delivery protocol to send the content to the ITF.

8. At the end of the viewing the ITF terminates the streaming control session which the IPTV Service Control Functions is still proxying to the Unicast Delivery Functional Block.

9. The ITF then terminates that connection to the Application with in turn informs the IPTV Service Control Functions that the session has ended.

10. The IPTV Service Control Functions requests that the Unicast Delivery Control Function releases the delivery.

11. The IPTV Control Function requests the release of network resources that were allocated to the network path from the Unicast Delivery Functional Block to the ITF.

In the exception case where the ITF does not perform step 9 the IPTV Application Functions is monitoring the session and if this fails, it request terminates the session and notifies the IPTV Service Control Functional Block. Steps 10 and 11 would also follow.

I.3.5 Procedural Flows for Local Program adaptation for NGN linear IPTV

The following diagram illustrates how location-specific content can be proposed to end-users after determining the location of the terminal.

NOTE – This diagram depicts optional behaviour when program is adapted to local constraints.

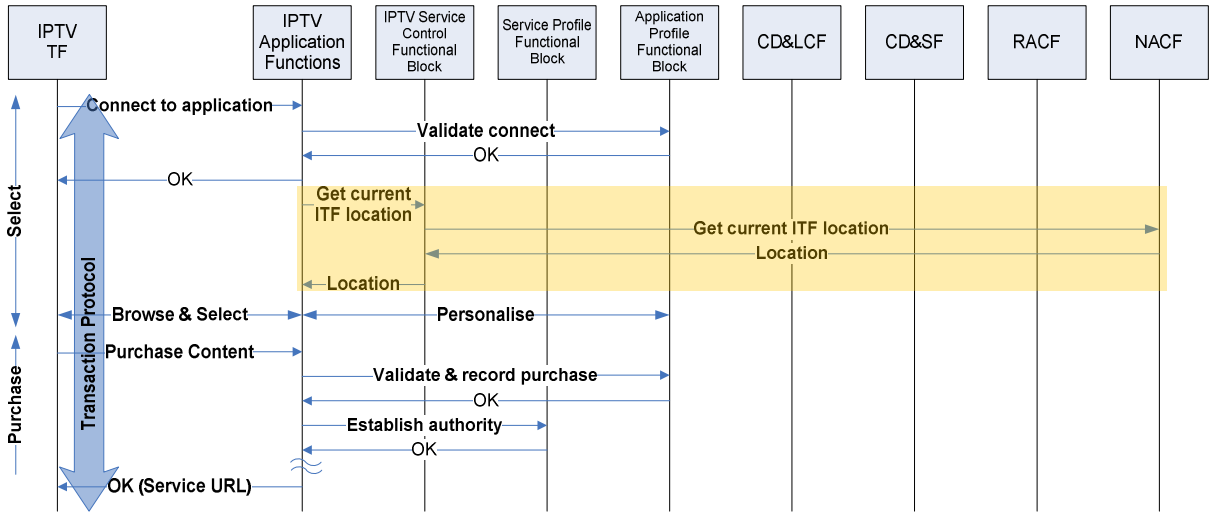


Figure I-12: Procedural Flows of Local Program adaptation for NGN-based linear IPTV

I.4 Procedural Flows for IPTV Services based on NGN IMS IPTV Architecture

The following clauses provide detailed descriptions of the procedural flows in the case of NGN IMS IPTV architecture.

[EDITOR'S NOTE – This sub-clause has not been checked for consistency.]

I.4.1 Procedural Flows for VoD Service

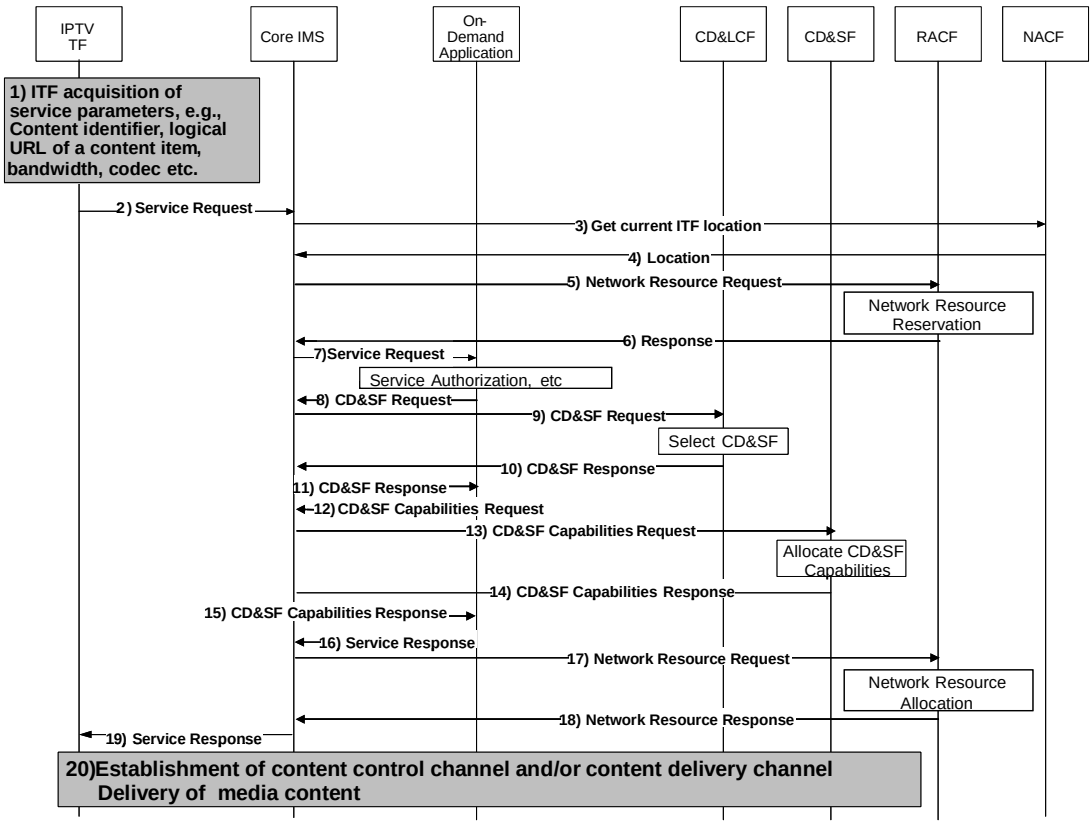


Figure I-13: Procedural Flows for VoD Service

Pre Conditions: It is assumed that provisioning, network attachment has been completed.

1. The IPTV Terminal Functions obtain the Content Identifier, logical URL, bandwidth, and codec information for a content item that the end-user wishes to receive. This may be achieved by interaction with the Program Guide Function, or by other means. In this step, the IPTV Terminal Functions may obtain content delivery parameters such as bandwidth, codec, etc. by using content control messages.
2. The IPTV Terminal Functions initiate a service request to the Core IMS Functions.

3-4. The Core IMS Functions optionally determine the location of the IPTV Terminal Functions, for example by querying the NACF.

5. The Core IMS Functions send a network resource request to the RACS in order to reserve network resources for content control and content delivery.
6. The RACF performs network resource reservation and sends the response to the Core IMS Functions.
7. The Core IMS Functions send the service request with content identifier, logical URL to the On-Demand IPTV Application Functional Block.
8. The On-Demand Application Functional Block performs service authorization. If the IPTV Terminal Functions are allowed to access the content, the On-Demand IPTV Application Functional Block sends the request to the CD&LCF via Core IMS Functions in order to select the CD&SF.
9. The Core IMS Functions forward the request to the CD&LCF.
10. The CD&LCF selects a suitable CD&SF based on some criteria, e.g. the state of the CD&SFs (e.g. load state etc.), the knowledge of distributed content among the CD&SF etc. The CD&LCF resolves the logical URL of Content into the physical URL of an allocated CD&SF, and responds the URL of selected CD&SF to On-Demand Application Functional Block via Core IMS Functions.
11. The Core IMS Functions forward the response to the On-Demand Application Functional Block.
12. The On-Demand Application Functional Block sends the content resource request to the selected CD&SF via Core IMS Functions in order to allocate content resources.
13. The Core IMS Functions forward the content resource request to the selected CD&SF.
14. The CD&SF performs content resource allocation and sends the response to the Core IMS Functions.
15. The Core IMS Functions forward the response to the On-Demand Application Functional Block.
16. The On-Demand Application Functional Block sends the service response to the Core IMS Functions.
17. The Core IMS Functions send a network resource request to the RACF.
18. The RACF performs network resource allocation and sends the response to the Core IMS Functions.
19. The Core IMS Functions send the service response to the IPTV Terminal Functions.
20. The ITF connects to the identified CD&SF to receive the content.

NOTE – 3GPP may allow direct interactions between On-Demand Application Functional Block and CD&LCF.

I.4.2 Linear TV service procedural flows in NGN IMS IPTV

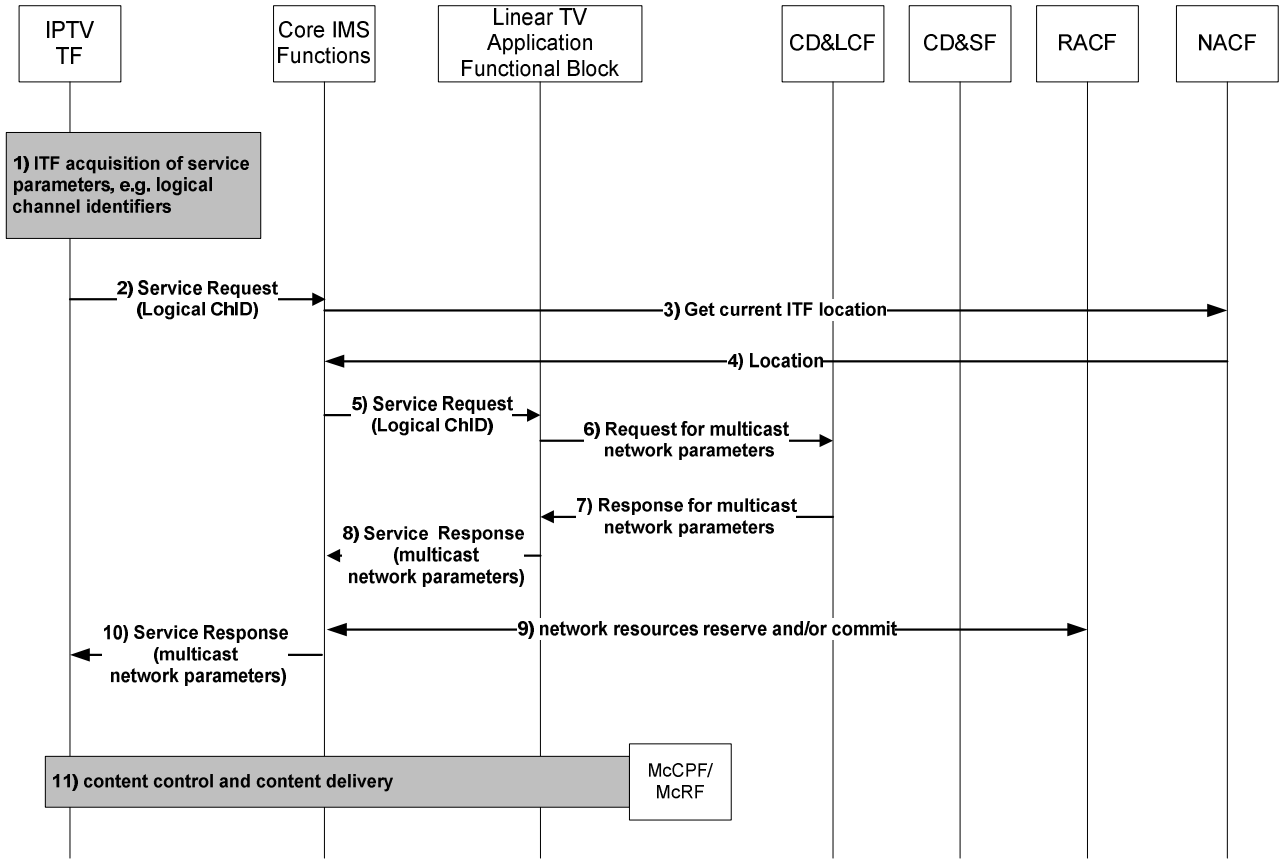


Figure I-14: Linear TV service procedural flows in NGN IMS IPTV

Pre Conditions: It is assumed that provisioning, network attachment has been completed. The channel streams have been delivered to Multicast Replication Point Function (McRF)/ Multicast Control Point Function (McCPF).

NOTE – Multicast is assumed in this diagram, terminals at the end of unicast links should be further studied.

1. The ITF acquires linear TV service parameters (such as a logical channel identifier or a list of logical channel identifiers), e.g. by a service selection procedure;

2. The ITF initiates a service request with logical channel identifier(s) to the Core IMS.

3 and 4. The Core IMS Functions determines the location of the IPTV Device, for example by querying the NACF.

5. The Core IMS Functions forwards the request to the LTV application with ITF location and logical channel identifier(s).

6. The Linear TV application passes the ITF location and the logical channel identifier(s) to the Content Delivery Control Function.

7. The Content Delivery Control Function determines the multicast addresses, which Content Delivery & Storage Function uses to output the required channels and has multicast network paths to the IPTV Terminal based on the association between logical channel identifiers and multicast addresses. It returns of the corresponding multicast address (es) to the Linear TV application.

8. The Linear TV application returns the multicast network parameters to the Core IMS.

9. The Core IMS Functions requests the network resources to support the network path from the Content Delivery & Storage Function to the IPTV Device.

10. Core IMS Functions forwards response to ITF.

11. ITF receives the one or a list of logical channels and their multicast addresses and maintains this mapping for the duration of the Multicast session. After that, ITF initiate channel control request by initialling a multicast join request and receives the multicast stream. When the user exits the Linear TV Application, i.e. they stop watching TV. The ITF will request to end the session and release any requested resources.

I.5 Procedural flows for IPTV interconnection between two NGN networks

The following scenarios show how network attachment process and service session establishment process can be coordinated in order to realize the roaming case in Figure 10-2, where the Service Control Function in the visited network is not used. Some NGN related interfaces (e.g. RACF-RACF interaction, NACF-NACF interaction) require further standardization work in the future. Figure I-15 illustrates a session setup procedure specific for CoD in the NGN IMS based IPTV in the case of a visited network without IMS control function (as in Figure 10-2).

The network attachment procedure may be independent from the service establishment procedure.

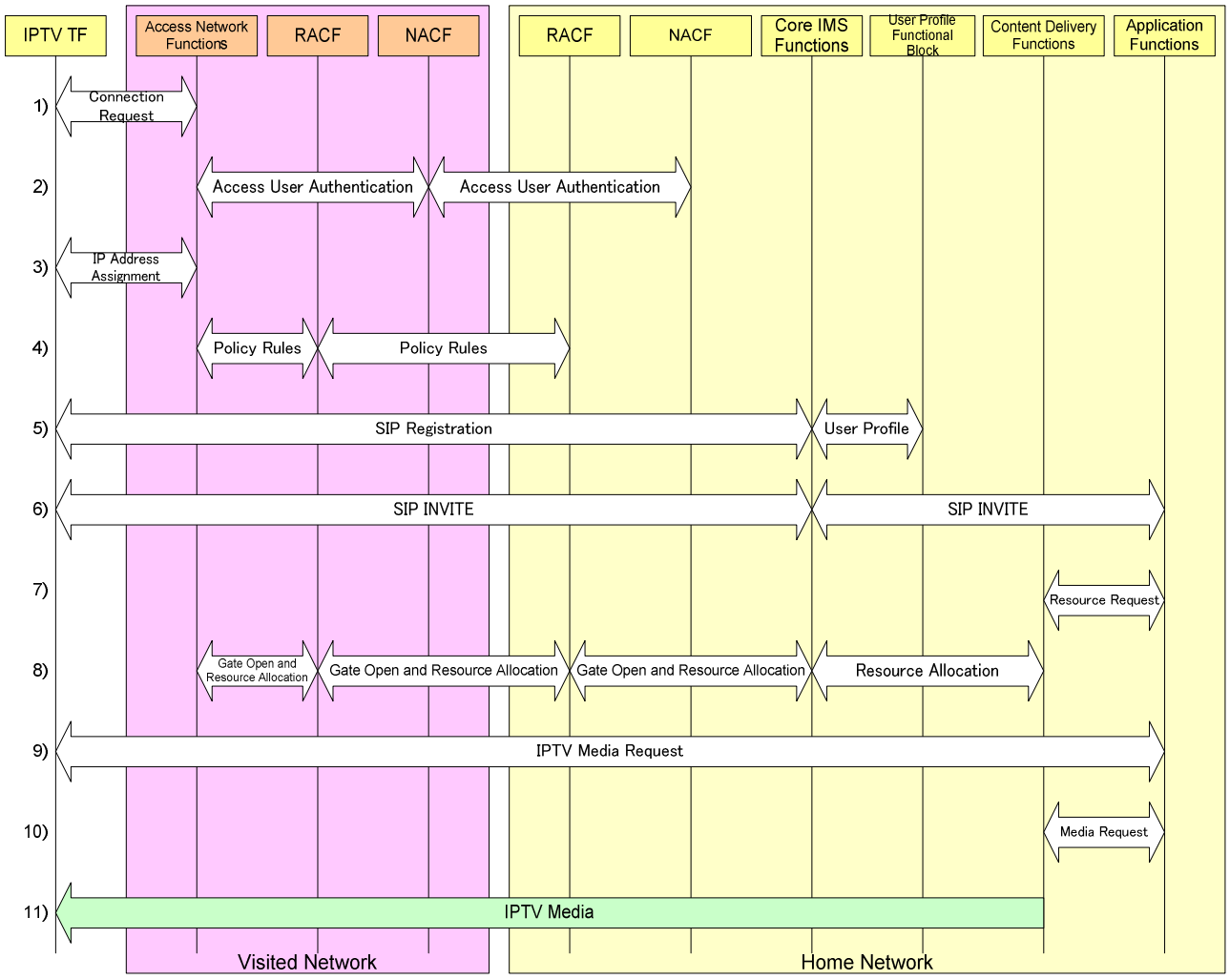


Figure I-15: Basic setup procedure for IMS-based IPTV in Figure 10-2

1. The IPTV Terminal attaches to the Access Network and requests the user authentication and authorization in order to obtain the valid IP address and establish the link.

2. The Access Network sends the user authentication request to the home NACF through the visited NACF.

3. After the completion of the user authentication and authorization, the Access Network assigns the valid IP address to the IPTV Terminal and establishes the link.

4. The Access Network obtains the user policy rules from the home RACF through the visited RACF and opens the gate for signalling messages (e.g., SIP port number) based on the provider's agreement.

5. The IPTV Terminal executes the SIP registration mechanism with the Core IMS Functions including the User Profile.

6. The IPTV Terminal sends a SIP INVITE message to the Core IMS Functions in order to request the IPTV application session. The Core IMS Functions then sends it to the Application Functions.

7. The Application Functions requests the resource allocation for the IPTV Terminal to the Content Delivery Functions.

8. The Content Delivery Functions requests the resource allocation for the IPTV Terminal to the Core IMS. The Core IMS Functions then sends the IPTV content information (e.g., IP address, port number, content type and bandwidth) to the home RACF so that the home RACF can request the visited RACF to open the gate on the Access Network for the IPTV content. Policy rules may be allocated to the Access Network.

9. The IPTV Terminal requests the Application Functions to send the content.

10. The Application Functions requests the Content Delivery Functions to start sending the content.

11. The IPTV Terminal receives the IPTV content from the Content Delivery Functions.

Figure I-15 illustrates basic CoD session setup procedure for NGN non-IMS based IPTV in the case of a visited network without IPTV Service Control Functions (as in Figure 10-2).

The network attachment procedure may be independent from the service establishment procedure.

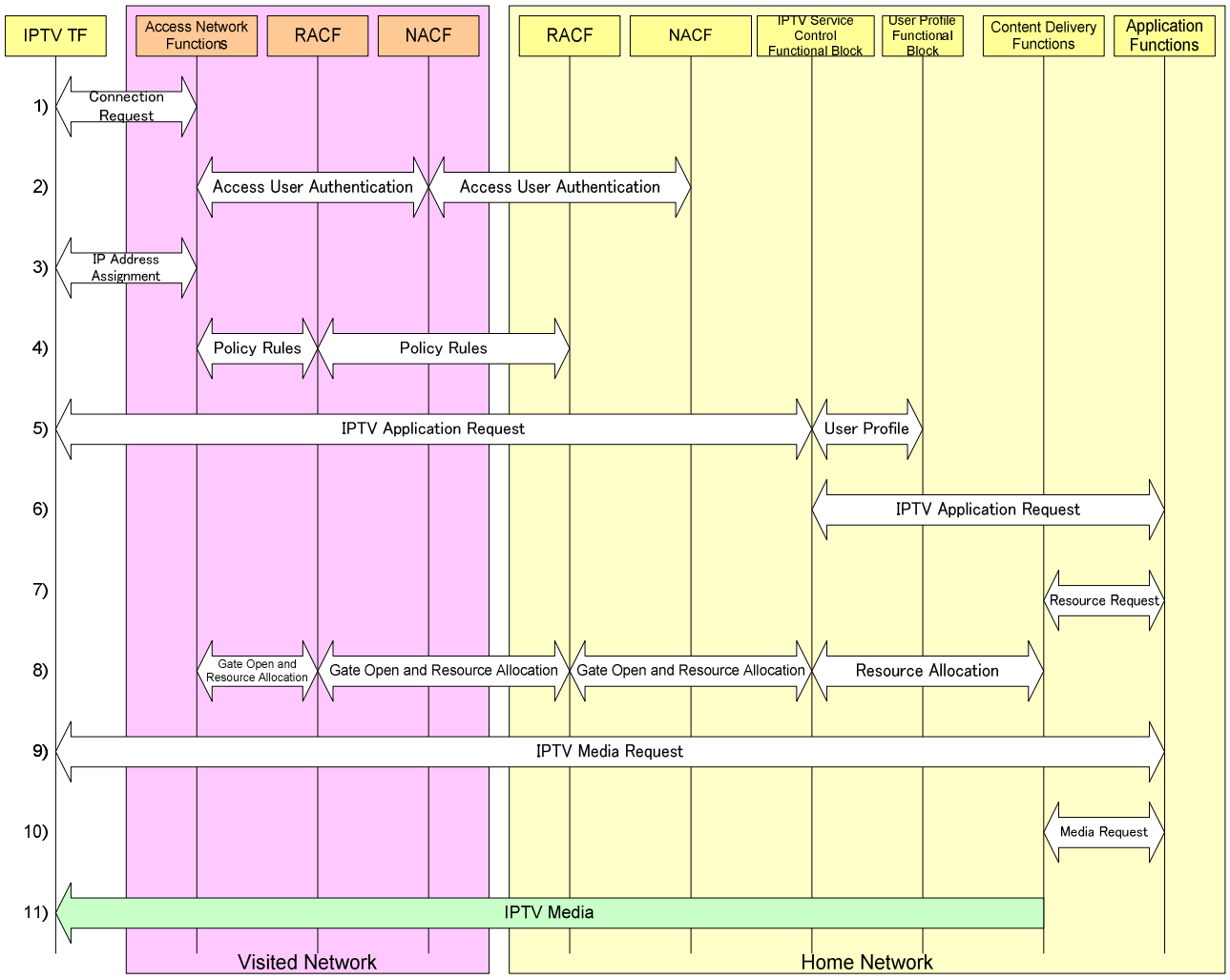


Figure I-16: Basic setup procedure for non-IMS-based IPTV in Figure 10-2

1. The IPTV Terminal attaches to the Access Network and requests the user authentication and authorization in order to obtain the valid IP address and establish the link.

2. The Access Network sends the user authentication request to the home NACF through the visited NACF.

3. After the completion of the user authentication and authorization, the Access Network assigns the valid IP address to the IPTV Terminal and establishes the link.

4. The Access Network obtains the user policy rules from the home RACF through the visited RACF and opens the gate for signalling messages (e.g., IPTV control port number) based on the provider's agreement.

5. The IPTV Terminal requests the IPTV content to the IPTV Service Control Functions including the User Profile.

6. The IPTV Service Control Functions requests the IPTV application session to the Application Functions.

7. The Application Functions requests the resource allocation for the IPTV Terminal to the Content Delivery Functions.

8. The Content Delivery Functions requests the resource allocation for the IPTV Terminal to the IPTV Service Control Functions. The IPTV Service Control Functions then sends the IPTV content information (e.g., IP address, port number, content type and bandwidth) to the home RACF so that the home RACF can request the visited RACF to open the gate on the Access Network for the IPTV content. Policy rules may be allocated to the Access Network.
9. The IPTV Terminal requests the Application Functions to send the content.
10. The Application Functions requests the Content Delivery Functions to start sending the content.
11. The IPTV Terminal receives the IPV content from the Content Delivery Functions.

Appendix II

IPTV Physical Network Hierarchy

(This Appendix does not form an integral part of this document.)

The IPTV Architecture needs to allow for IPTV Network, Service and Application Components to exist at different physical and logical points in a network. This is common for many operators where the network and service components are hierarchically distributed.

The functional elements of the IPTV Architecture can be mapped to a physical network hierarchy as shown in Figure II-1.

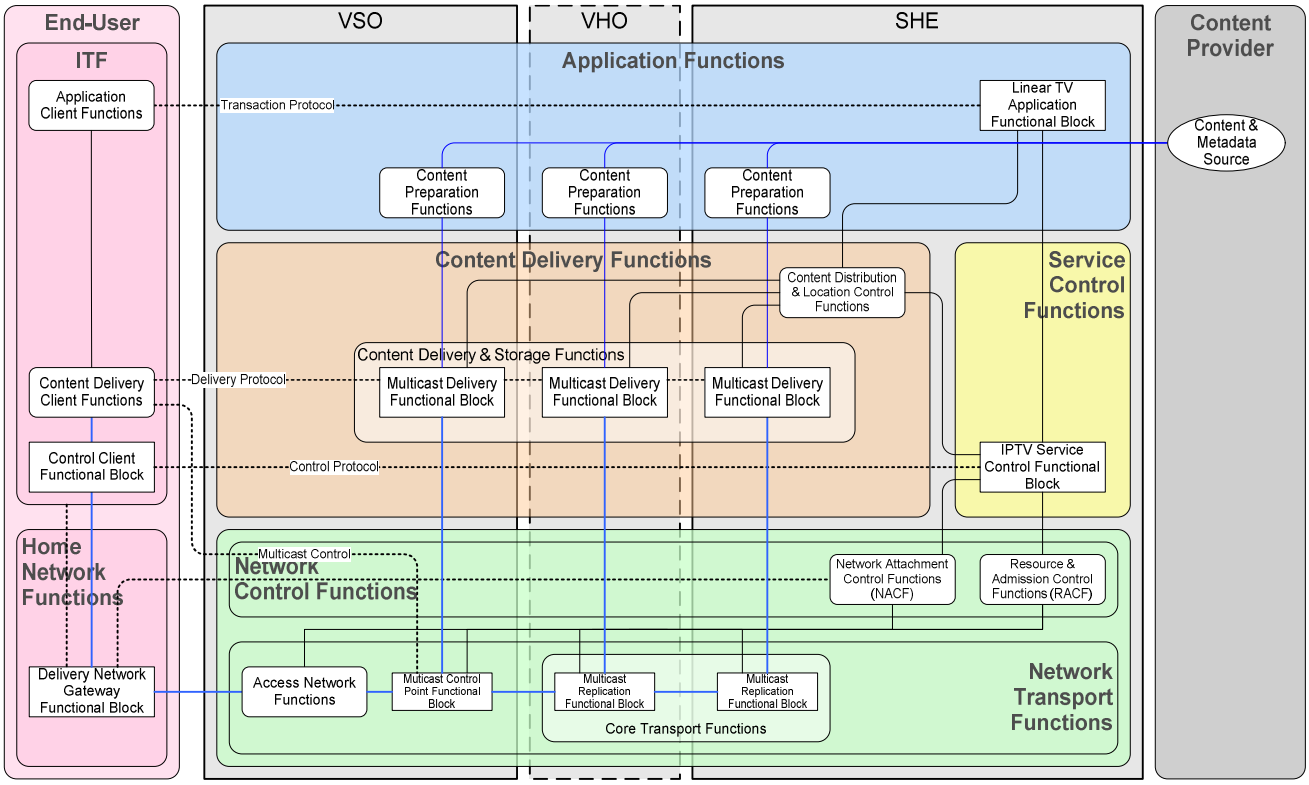


Figure II-1: Network Hierarchy for an IPTV Network (Linear TV example)

Figure II-1 includes a network hierarchy as content and control flows from content provider to the end-user. This hierarchy is an example, with larger networks having more levels and smaller networks having fewer. The figure shows the components and flows for a Linear TV service example. The Access network functions must be located between VSO and end-user and the IP multicast replication functions may be located in VSO, but they are not illustrated in the figure.

Super Head End (SHE) Network node(s) with the broadest content scope: The SHE sources content to an entire IPTV network. Intended uses include primary storage for off-line content and transmission of region-independent off-air content (e.g. premium and specialty programming).

Video Hub Office (VHO) Network node(s) with a local/regional content scope: The VHO sources region-dependent off-air content (e.g. local programming) and houses local off-line storage of content.

Video Serving Office (VSO) Network node(s) that connect end-users (via access systems) to the IPTV network: The VSO (typically a Central Office) hosts or connects all access systems for interconnection to end-users. In addition, the VSO contains aggregation equipment to enable efficient interconnection of access systems to the IPTV network. The option to locate content interconnection and/or content processing equipment is shown, though perhaps not typical.

NOTE – SHE can be called central server, VHO is regional or metro servers, and VSO is local servers.

Appendix III

Overlay Networking Function for IPTV Services and Multicast

(This Appendix does not form an integral part of this document.)

One means for providing an overlay networking function for IPTV services and multicast and the functions of overlay networking may be performed under the Content Delivery Control Function.

One way of controlling QoS enabled multicast delivery is to utilize the concept of overlay network.

The following functions may be present in the Content Delivery Control Function:

a) Control overlay networking configuration and topology management and overlay multicast tree management, etc. The overlay network will be created virtually with the control of "Content Delivery Control".

b) Provide multi-homed "Contents Delivery Control Function" through constructed overlay networks to meet efficient content delivery with high quality service requirements for IPTV services.

c) Support overlay network configurations to ensure that clients are not connected / disconnected from the delivery function in case of failures. In addition, the "Content Delivery Control Function" will provide control functions that support redundancy in case of multiple servers in order to reduce the impact of server delivery failures.

Appendix IV

Adaptation of the IPTV Architecture for HFC Networks

(This Appendix does not form an integral part of this document.)

Figure IV-1 shows the function functional architecture for IPTV where the network layer is provided by a HFC Cable network. Detail decomposition of the diagram is shown in Draft Recommendation J.700 [ITU J.700].

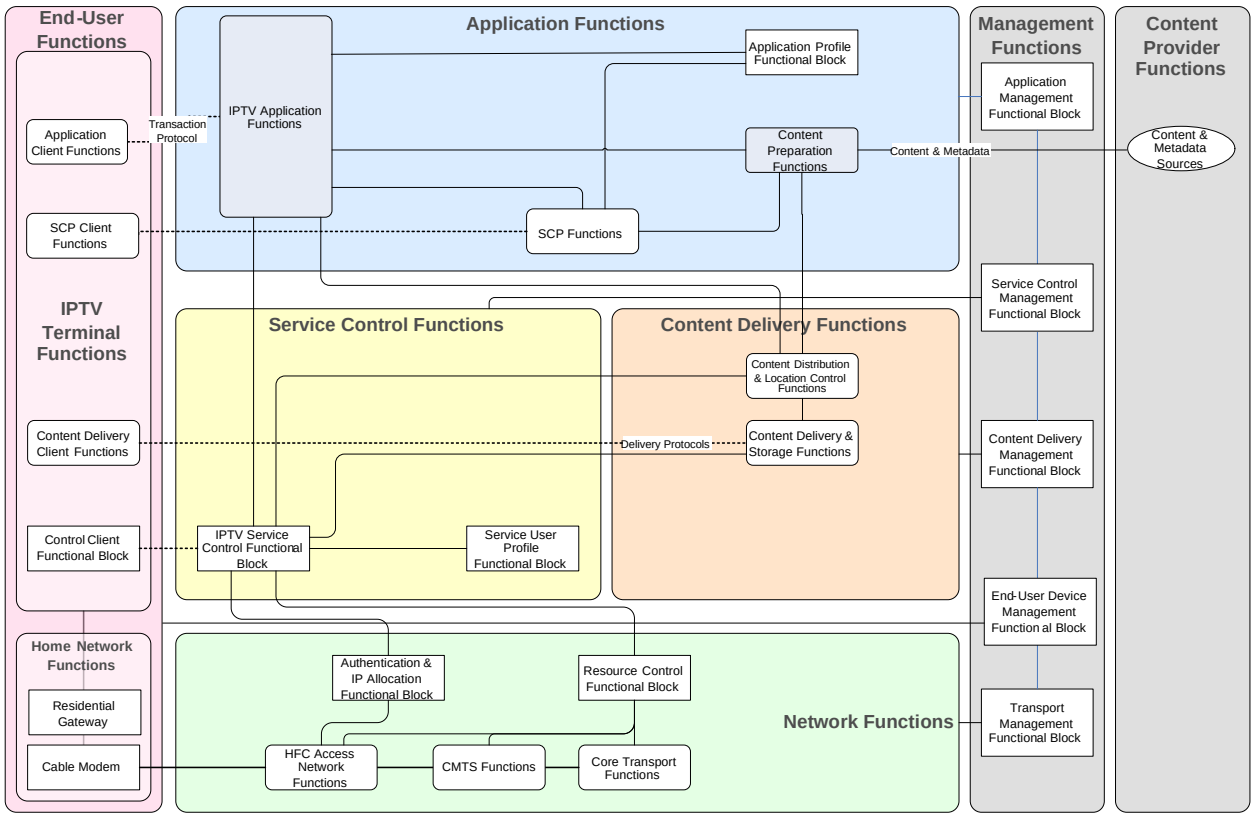


Figure IV-1: High-Level Functional Architecture for Cable delivered IPTV

The descriptions of the functional elements that are common to all IPTV architectures are presented in clause 9 above. The cable specific functions are described below. It should be noted that the nature of the interfaces to the common functional elements may differ between cable delivered IPTV and NGN or non-NGN delivered IPTV.

HFC Access Network

The Hybrid Fibre Coax, HFC, access network is defined as the network between the CMTS and the Cable Modem. Attributes of the HFC access network include:

- Supported or required DOCSIS versions
- DOCSIS Set top box Gateway (DSG)
- Edge QAMs
- Modular CMTS

- Optical Distribution Network
- RF Network

CMTS

The cable modem termination system, CMTS, provides support for IP based data services, such as Internet or Voice over IP.

II.1.3 IPTV service scenarios

Summary

The purpose of this document is:

- to identify, classify and define some examples of IPTV services by means of elaborated use cases,
- to identify the different players and roles in the corresponding value chain,
- to further illustrate the requirements for the different players involved in the provisioning and the operation of these IPTV services, and which have been listed in the IPTV Services Requirements document edited by FG IPTV,
- to elaborate on the communication flows between the different functional domains and entities involved in the deployment and the operation of the corresponding IPTV service.

Keywords

IPTV, service scenarios, use cases, communication flows.

Introduction

The IPTV service scenarios document provides a list of IPTV use cases that are informative illustrations of how IPTV services can be designed, deployed and operated. From this perspective, use cases have been classified according to an IPTV service taxonomy that includes (but is not limited to) on-demand services, advertising services and broadcast services.

NOTE – some of the terminology and notions discussed in this document may be used in a different way than that used by the other documents produced by the IPTV Focus Group. Further study is required to align this terminology.

Current status

The document has been reviewed thoroughly during the corresponding editing session. WG1 members believe it is now complete and ready for submission to SG13 for further review and consideration.

Dependency on or relationship to other FG IPTV documents:

The IPTV service scenarios document relies upon the IPTV architecture document, as far as the taxonomy that identifies the different domains (end-user, network provider, service provider, and content provider, as per Figure 6-1 of the IPTV architecture document) is concerned.

CONTENTS

Page

1 Scope 170

2 References 170

3 Definitions 170

3.1 Terms defined elsewhere 170

3.2 Terms defined in this document 171

4 Abbreviations and acronyms 171

5 Conventions 172

6 IPTV services description and use cases 172

6.1 IPTV service list 172

6.2 Broadcast services 173

6.2.1 Linear TV 173

6.2.2 Linear TV with trick mode 175

6.2.3 Pay per view 176

6.2.4 Electronic program guide (EPG) 176

6.2.5 Personal Broadcast Service 178

6.2.6 Hybrid: Online and Off-air TV Delivery 180

6.2.7 Linear TV with Multi-View service 180

6.3 On-demand service 180

6.3.1 VoD 181

6.3.2 Near VoD (NVoD) 182

6.3.3 Reserved Delivery service 183

6.3.4 On-demand with Multi-View service 184

6.3.5 Music on demand (MoD) 184

6.4 Advertising service 185

6.4.1 Traditional advertising service 185

6.4.2 Targeted Advertising 186

6.4.3 On-demand Advertising 186

6.4.4 Interactive Advertising 187

6.4.5 Advertising message logging 187

6.5 Public interest service 188

6.5.1 Support for end-users with disabilities 188

6.5.2 Emergency communications 188

6.5.3 Community related information 188

Page

6.6 Tele-services 191
6.6.1 Tele-learning 191
6.6.2 Tele-medicine 191
6.6.3 Monitoring services 191
6.7 Portal services 192
6.7.1 Data portal (walled garden, Internet access, etc.) 192
6.7.2 Web-based IPTV Portal 192
6.8 Hosting services 193
6.8.1 Business-to- business 193
6.8.2 User created content (UCC) hosting 193
6.9 IPTV interactive service 193
6.9.1 Information (news, weather, transportation, local community, etc.) 194
6.9.2 Commerce (banking, stock, shopping, ticketing, auction, product delivery, event, etc.) 194
6.9.3 Communication (e-mail, messenger, SMS, channel chatting, VoIP, web surfing, multiple video conference, video phone, etc.) 194
6.9.4 Entertainment (games, karaoke, photo album, lottery, blog, etc.) 195
6.10 Presence services 195
6.10.1 Basic Presence Service 196
6.10.2 Channel based Presence Service 196
6.10.3 Targeted Advertising based on Presence Service 197
6.11 Time-shifting and Place-shifting service 197
6.12 Session mobility service 198
6.13 Supplementary content 199

7 Payment Methods for accessing IPTV services 200

Bibliography 200

IPTV service scenarios

1 Scope

The IPTV service scenarios document provides a list of IPTV use cases that are informative illustrations of how IPTV services can be designed, deployed and operated. From this perspective, use cases have been classified according to an IPTV service taxonomy that includes (but is not limited to) on-demand services, advertising services and broadcast services.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[IPTV.ARCH] ITU-T FG IPTV working document (FG IPTV-DOC-0181), IPTV architecture

[ITU-T F.703] ITU-T Recommendation F.703 (2000), *Multimedia Conversation Service Description*

[ITU-T F.790] ITU-T Recommendation F.790 (2007), *Telecommunications accessibility guidelines for older persons and persons with disabilities*

[ITU-T M.1400] ITU-T Recommendation M.1400 (2006), *Designations for interconnections among operators' networks*

[ITU-T Q.1290] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*

[ITU-T Accessibility checklist] ITU-T FSTP-TACL (2006), Telecommunications Accessibility Checklist

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Network provider [ITU-T Q.1290]: The organization that maintains and operates the network components required for IPTV functionality. A network provider can optionally also act as service provider.

3.1.2 Service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider can optionally be a customer of another service provider

3.2 Terms defined in this document

This document defines the following terms:

3.2.1 **Application provider:** The application provider is the entity providing IPTV-related user applications.

3.2.2 **Content aggregator:** A player in the IPTV service delivery chain whose role is to aggregate content, e.g. to form a TV bouquet composed of several TV channels.

3.2.3 **Content provider:** The content provider is the entity owning content or being licensed to sell content assets. Their role is content delivery.

3.2.4 **Electronic program guide (EPG):** A structured set of data, intended to provide information on available content that may be accessed by end-users.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

A/V	Audio / Video
ADSL	Asymmetric Digital Subscriber Line
BSS	Business Support Systems
C2C	Customer-to-Customer
CAS	Conditional Access System
CD	Compact Disc
CRM	Customer Relationship Management
DVD	Digital Versatile Disk
DVR	Digital Video Recorder
EAN	Emergency Alert Notification
ECG	Electronic Content Guide
ECI	Emergency Communications Information
ECN	Emergency Communications Notifications
ECR	Emergency Communication Report
EPG	Electronic Program Guide
FTP	File Transfer Protocol
HD	High Definition
IM	Instant Messaging
IPG	Interactive Program Guide
IPPV	Impulsive PPV
IPTV	IP-based TV
iTV	Interactive TV
MoD	Music on Demand
NVoD	Near VoD

OPPV	Order-ahead PPV
OSS	Operational Support Systems
PC	Personal Computer
PDA	Personal Digital Assistant
PPU	Pay Per Use
PPV	Pay Per View
PVR	Personal Video Recording
RVoD	Real VoD
QoS	Quality of Service
SMS	Short message service
STB	Set Top Box
TV	Television
UCC	User Created Content
UGC	User Generated Content
VCR	Video Cassette Recorder
VoD	Video on demand
VoIP	Voice over IP

NOTE – In the context of this document, the abbreviation VoD includes video, audio and associated metadata.

5 Conventions

In this document, there are no specific conventions.

6 IPTV services description and use cases

6.1 IPTV service list

This clause provides a list of IPTV services, which is not an exhaustive list. It is categorized by their service characteristics from an end-user's perspective.

- Content services
    1. Linear TV (audio, video and data)
    2. Linear Broadcast Audio
    3. Linear TV with Trick Modes
    4. Multi-View service
    5. Pay Per View (PPV)
    6. Personal Broadcast Service
    7. PVR service (network or client-based)
    8. Time-shift TV
    9. Video on Demand (VoD)
    10. Near VoD (Video on Demand) broadcasting
    11. Content Push

12. Music on Demand (MoD) including Audio book
13. Content download service
14. Service Information (EPG: Electronic Program Guide, ECG: Electronic Content Guide, etc.)
15. third party content services
16. End-user Originated content (Video, etc. and applications)
17. Regulatory Information services
18. Advertising
19. Hybrid services

- Interactive services
  1. Interactive TV (iTV)
  2. Learning services (education for children, elementary, middle and high school student, languages and estate, etc.)
  3. Information services (news, weather, traffic, etc.)
  4. Entertainment services (photo album, games, karaoke and blog, etc.)
  5. Portal services
  6. Commerce services (security, banking, stock, shopping, auction and ordered delivery, etc.)
  7. Interactive Advertising
- Communication services
  1. Communication service (e-mail, instant messaging, SMS, channel chatting, VoIP, Web, multiple video conference and video phone, etc.)
  2. Communications Messaging
  3. Presence service

6.2 Broadcast services

Broadcast services comprise a one-way transmission of content from one point (the source) to two or more points (the receivers), whereas the end-user has no control over the content or timing of what he receives, apart from the ability to select a particular channel.

6.2.1 Linear TV

Linear TV is a broadcast TV service that is the same as the classic form of television services that are provided by cable, terrestrial and direct-to-the-home satellite operators, where the programme content is transmitted according to a defined schedule and is intended for real-time consumption by the end-user. The service therefore provides an essentially continuous stream flowing from the content provider to the terminal device located in the end-user network.

Linear TV includes (but is not necessarily limited to) the following approaches:

- **Linear TV with audio and video:** Audio and video (audiovisual) signals are broadcasted and distributed to the downlink without control of the broadcast.
- **Audio only:** Audio signals are broadcasted and distributed to the downlink without control of the broadcast.

- **Linear TV with audio, video, and data:** These services are A/V services which are combined with interactive data for the related or supplementary information of A/V program using bi-directional link. The end-user can watch the downlink A/V stream and can access more detailed or value-added information via uplink simultaneously.

Figure 6-1 shows an example of a Linear TV service with local PVR capabilities.

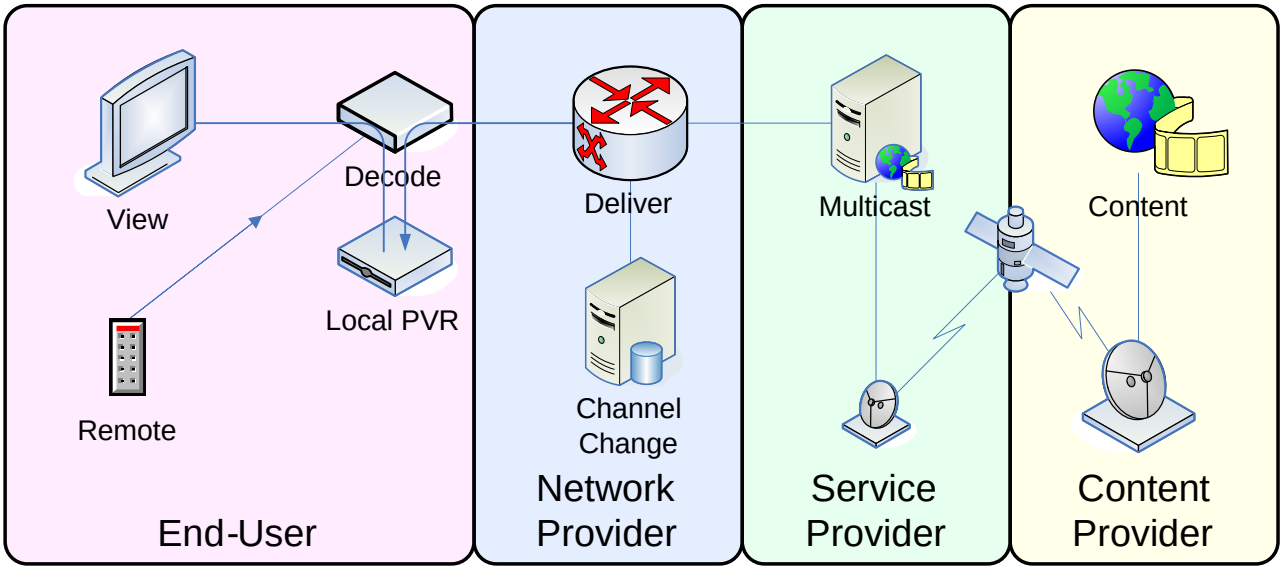


Figure 6-1: Linear TV with Local PVR

Figure 6-2 shows a scenario for a Channel-based Linear TV service.

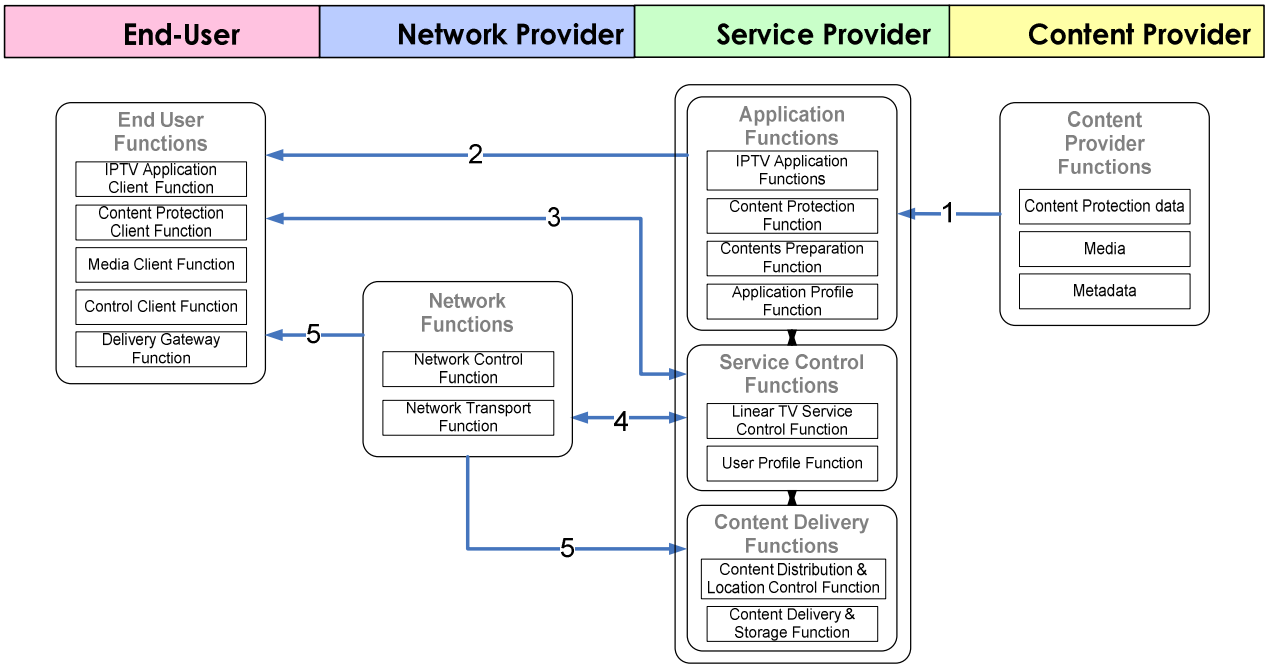


Figure 6-2: Channel-based Linear TV Service Scenario

1. Contents (video, audio, data, etc.) with related metadata, and Content Protection (CP) data are produced and managed by the Content Provider, and are delivered to the Service Provider.

2. Then the Service Provider formats the data prepared by the content provider into IP packets and controls program schedule and distribution. Then, the scheduled channel information is provided to the end-users indicating the content is ready for consumption.

3. When an end-user wants to access the channel-based Linear TV service or selects a channel, the request is sent to the Service Provider. This procedure may include service negotiation (e.g., QoS, price, etc.) and service availability confirmation procedures.

4. If the end-user is granted access to the channel-based linear TV service, then the Service Provider interacts with the Network Provider for transmitting the requested content. This procedure may include network resource reservation and allocation to guarantee the contracted service level.

5. Upon completion of the above step 4, the Service Provider supplies channel access information (e.g. the multicast address assigned to the requested channel) and then the end-user can watch the channel.

6.2.2 Linear TV with trick mode

- Linear TV with Trick Mode allows the end-user to pause linear TV. For the ability to skip content and other capabilities (e.g. instant replay), the use of PVR or DVR is required.

- PVR service (network or client-based)

- The Personal Video Recorder service is an end-user-controlled electronic device service that records linear TV and stores it in a digital storage facility, either in standalone set-top boxes or in the network. This service can support "time shifting", "trick modes", and complementary convenience functions such as, programming and remote control by PDA, networked PC, or web browser.

Figure 6-3 shows a scenario for Channel-based Linear IPTV Service with trick mode:

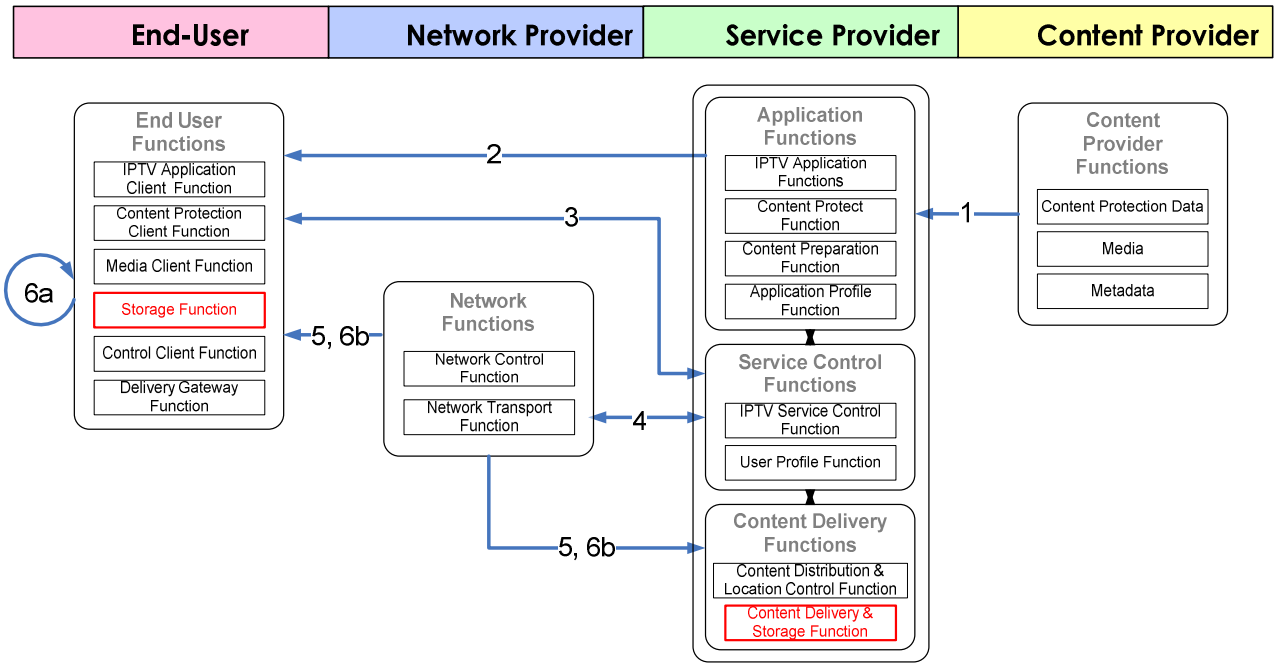


Figure 6-3: Channel-based Linear IPTV Service Scenario with trick mode

Steps 1 to 5 are similar to those depicted in Figure 6-2.

6a. When the End User's IPTV terminal has its own storage capability and the end-user requests any trick mode function, the programmed content is recorded by the Storage Function and may be displayed later according to the end-user's selection or the constraints provided by the content protection metadata.

6b. If the end-user requests the trick mode service without any local storage capability (e.g. embedded in their IPTV terminal), then the programmed content is recorded in the storage facility managed by the Service Provider. The selected content can then be displayed later by the end-user, according to the constraints provided by the content protection metadata.

6.2.3 Pay per view

Pay per view is a streaming service where end-users can purchase events or programs to be seen on TV. The user can buy the PPV service e.g. via an on-screen guide, a telephone, or through the Internet and see the events or program at any time within the expiration date.

- **Order-ahead PPV (OPPV):** The ability to order PPV programming ahead of time.
- **Impulsive PPV (IPPV):** The ability to order PPV programming impulsively.

6.2.4 Electronic program guide (EPG)

Electronic program guide (EPG) is an on-screen guide to scheduled programs, contents with additional descriptive information, allowing a viewer to navigate, select and discover content by time, title, channel, genre, etc., by using a remote control, a keyboard, a touchpad or even a phone keypad. Generally, EPG can be displayed in several types such as Mosaic EPG, Box EPG, Text EPG, Mini EPG, Tree EPG and so forth, possibly depending on the service provider's business model.

Traditionally, in Broadcast Services, Electronic Programming Guide services have been provided to allow end-users to easily browse television or live video content listings in an effort to easily find and select television content to view and/or record. According to today's typical use of the EPG service, an EPG is an on-screen guide used to display scheduled broadcast television programs, allowing a viewer to navigate, select, and discover content by time, title, channel, genre, etc. In the future, IPTV services would support an EPG that will display all available content. In other service offerings detailed in this document, EPG is not relevant. On-Demand Services may utilize some form of content catalogue to allow easy browsing and selection of content, but this is not live content and certainly an EPG would not be used in this "catalogue" type of scenario. Also, EPG may be an end-user Interactive Service but it is not a bi-directional interactive service for end-user interaction with a server or head-end.

Figure 6-4 shows a scenario of EPG

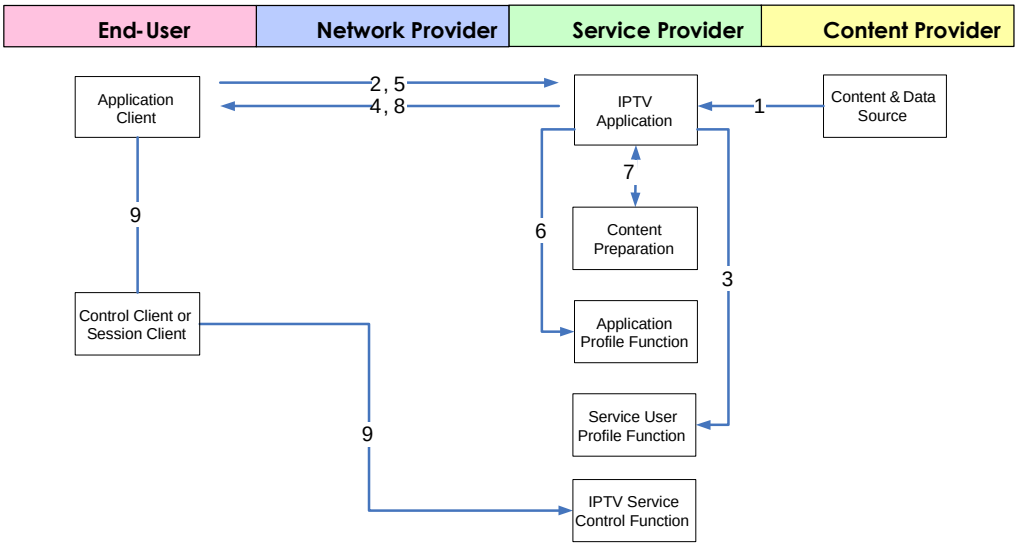


Figure 6-4: EPG Service Scenario

1. The content provider delivers the content to the service provider.

2. The end-user turns on the user terminal.

3. The service provider's IPTV Application retrieves the available service list for the user according to the service user profile.

4. The IPTV application delivers the list of available services and content to the end-user terminal.

5. The end-user selects one of the available services like a broadcast service, an on-demand service, etc. Moreover, the end-user can search for certain programs and contents using specific criteria such as genre, channel number, etc. In case of the search service, steps 5, 7 and 8 are repeated until the user finds the desired programs and contents.

6. The IPTV application must provide the user with the detailed information (EPG) for the selected service. To do so, the IPTV application first retrieves the preferred program and content information (i.e., genre, channel, etc.) through the Application Profile function. The end-user's preferences can be derived from the history of the program and content which the user frequently chooses.

7. The IPTV application retrieves the content metadata through the content preparation function based on the program and content information preferred by the user or the search conditions of the user.

8. The IPTV application generates the EPG screen including the scheduled service program and content lists using the preferred program and content information or the search condition as well as the retrieved content metadata. Finally, it delivers the EPG screen to the end-user's terminal.

9. The end-user selects content from the EPG screen which is received from the IPTV Application. Once the content has been selected by the end-user, the provisioning of the selected content is performed by the IPTV Service Control Functions as defined in the IPTV Architecture document edited by the FG IPTV.

6.2.5 Personal Broadcast Service

The personal IPTV broadcast service provides the end-user with a way to advertise personal content (possibly including scheduling information) description so that other end-users can access such content. This service makes the IPTV end-user a content provider. The service provider is responsible for relaying session information between the broadcasting end-user and the receiving end-users, possibly assuming some access control functions operated by the service provider so as to make sure that a given end-user is entitled to broadcast his/her personal content.

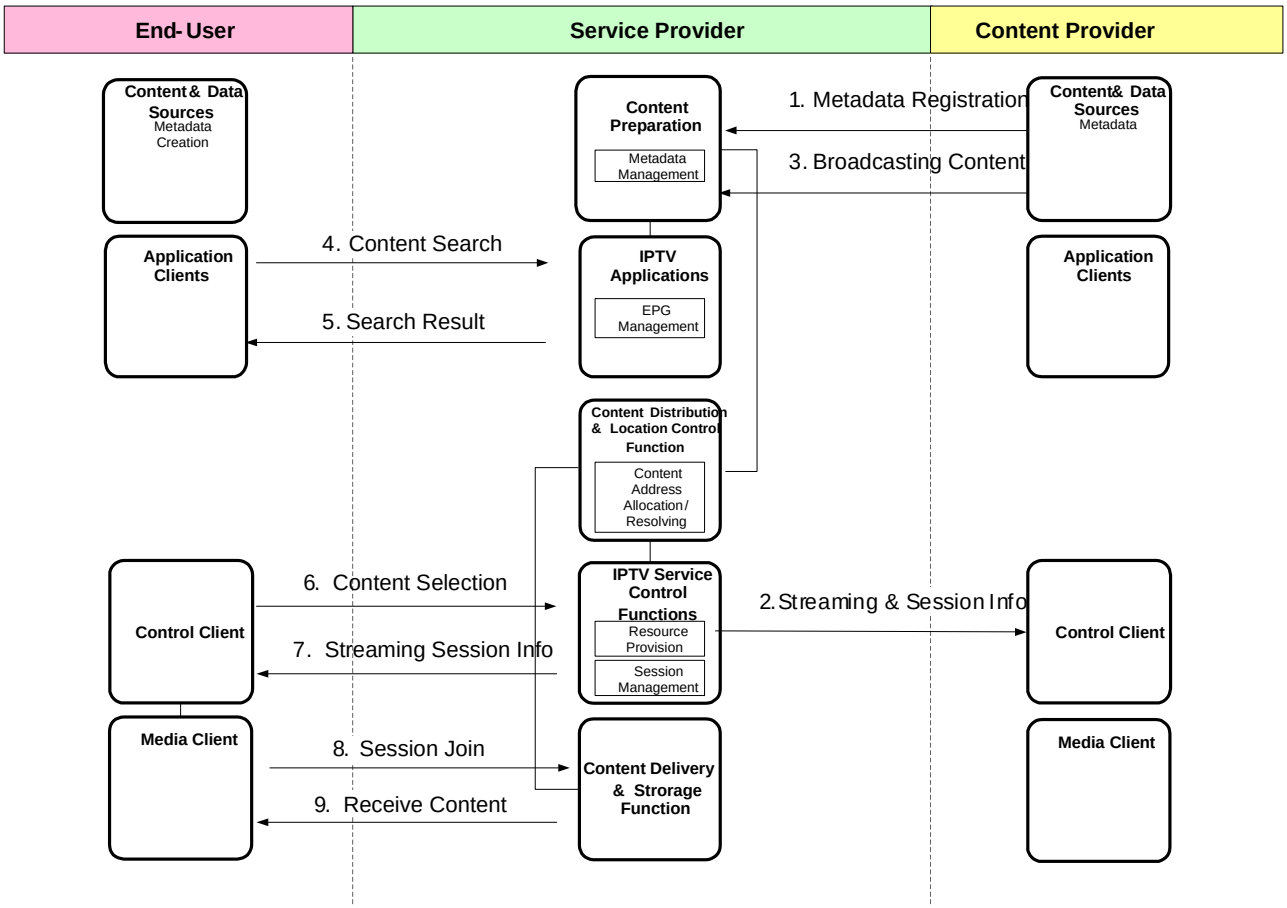


Figure 6-5: Use case of Personal Broadcast Service

1. **Metadata Registration:** The content providing end-user prepares information about the content. He will broadcast and register it in the metadata distribution server. This can be done by uploading a metadata file (generated e.g. by means of some authoring tools). The metadata may contain source information like client ID, content ID, and other content-related information.

2. **Streaming & Session Info:** Once the content providing end-user registers the metadata with the server, the service provider may allocate some network resources for the streaming (e.g., bandwidth, multicast address), and then give this information back to the content providing end-user.

3. **Broadcast Content:** The content providing end-user sends the corresponding content stream, possibly using a 1-to-n group communication scheme (multicast) or n 1-1 communication flows (unicast).

4. **Content Search:** The receiving client makes a search (e.g. with keyword).

5. **Search Result:** The metadata server responds to this search request and provides a result accordingly.

6. **Content Selection:** The receiving client may be able to select a specific content with the source information provided by content search result. In this process, service control functions may participate in the session routing or gathering of charging information.

7. **Streaming & Session Info:** This message contains the actual content address and session information for receiving it.

8. **Session Join:** The receiving client requests from the content delivery function to join the session with session info (including real location).

9. **Receive content:** The receiving client receives the content from the content delivery system.

6.2.6 Hybrid: Online and Off-air TV Delivery

An alternative approach for the delivery of Linear TV is to enable the end-users' IPTV device to receive the broadcast signal from the broadcaster, e.g. via traditional distribution techniques like digital satellite TV, or terrestrial digital TV. This will then be combined with On-Demand content delivered over the network from the Network Provider.

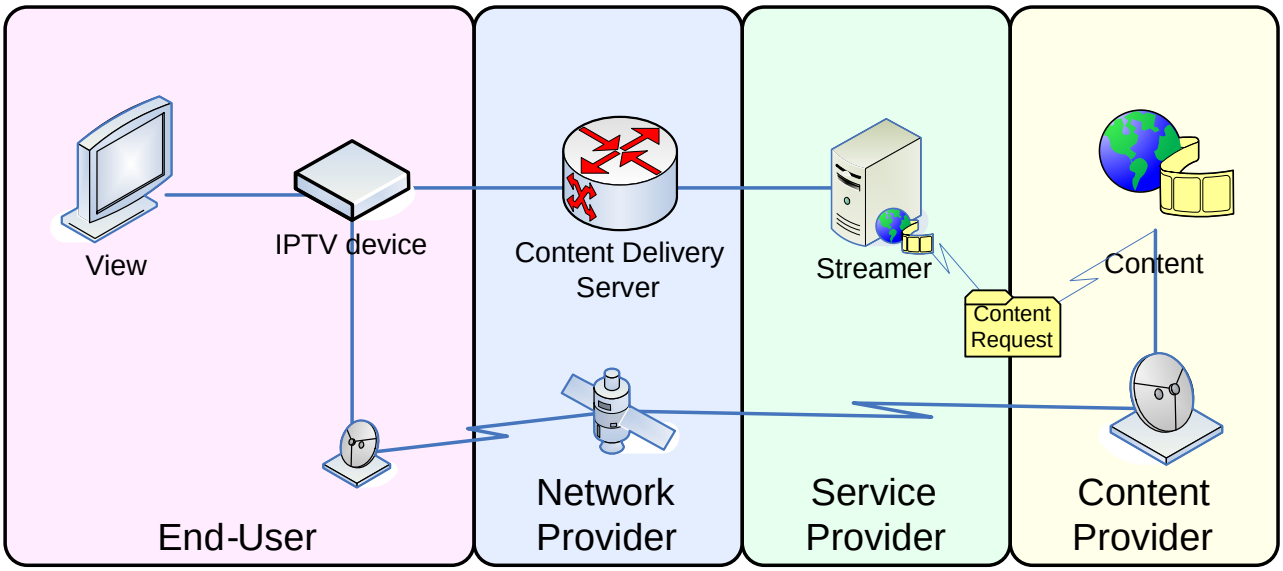


Figure 6-6: Hybrid: Online and Off-air TV Delivery

6.2.7 Linear TV with Multi-View service

Linear broadcast TV with Multi-View is a service that consists in providing one scene with different camera angles. The user can select this angle which he likes to watch. For example, when the end-user watches a linear broadcast of a baseball game, he can see the first base, third base, or backfield according to his wishes, not the angle the channel director prefers.

6.3 On-demand service

Content prepared and delivered by the content provider for retrieval is received and stored by the service provider. If necessary, trans-coding can be performed to accommodate with the storage device characteristics. The end-user can then select and retrieve such contents from this storage at any time, according to the constraints provided by the content protection metadata.

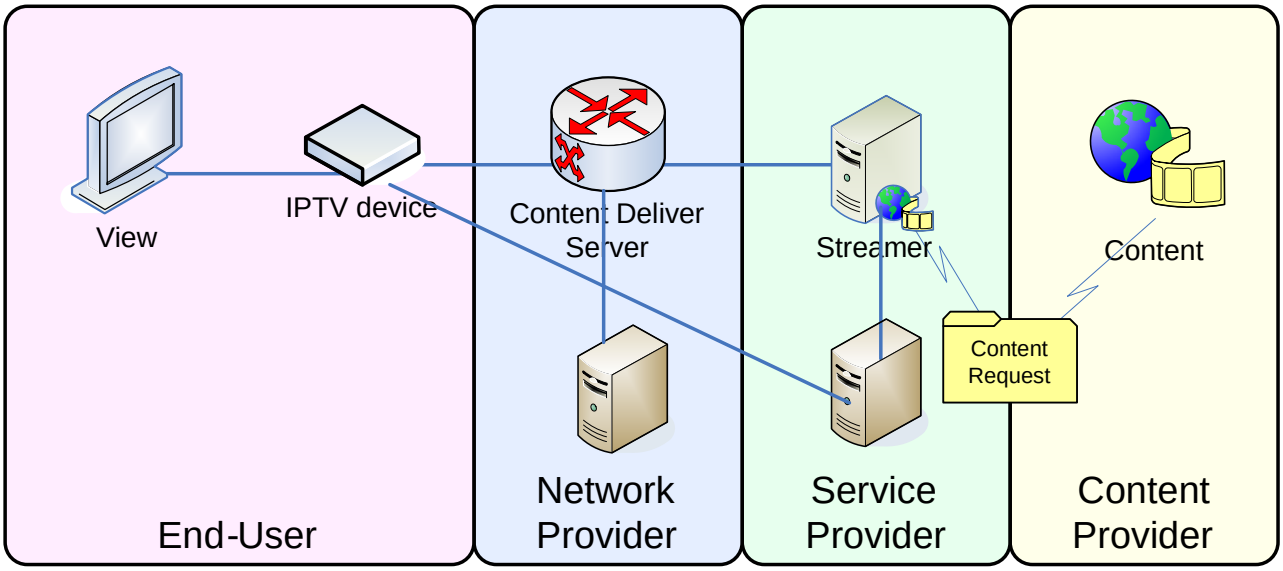


Figure 6-7: Content on Demand

6.3.1 VoD

VoD is a video service which allows the end-users to select and watch video content at any point of time. The end-user has full control over choosing which program or clips to watch and when starting to watch. A service scenario for VoD is shown in Figure 6-8.

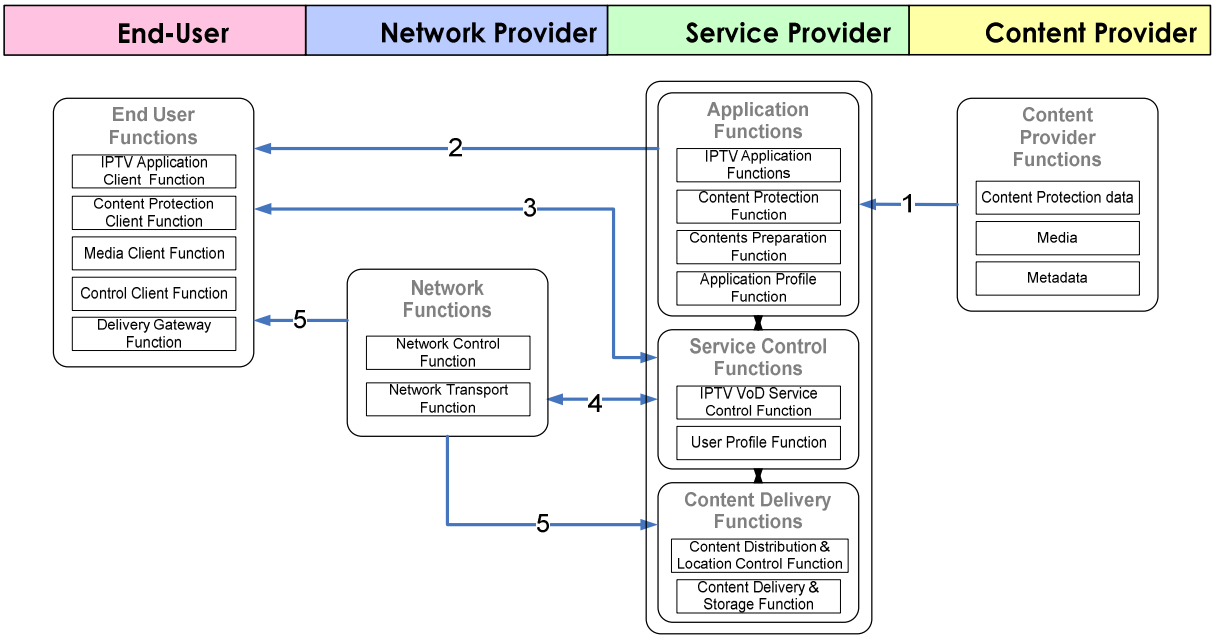


Figure 6-8: Service Scenario for VoD

1. Video content with its metadata and Content Protection data that are produced and managed by the content provider are delivered to the service provider.

2. The service provider prepares the content as per the agreement between the content provider and the service provider.

3. When an end-user selects a VoD content, the request(s) is sent to the service provider. This procedure may include service negotiation (e.g., QoS, price, packaging option, etc.).

4. If the end-user is granted access to the content (e.g. by the service provider), then the service provider interacts with the network provider to possibly negotiate the conditions of forwarding the content to the end-user. This procedure may include the network resource reservation to guarantee the contracted service level.

5. Upon completion of the above step 4, the service provider supplies the content access information (e.g., the multicast address that will be used to forward the content) and the end-user can then receive the video.

6.3.2 Near VoD (NVoD)

Near VoD is a video service where multiple copies of a program are broadcast at short time offsets (typically 10-20 minutes) providing convenience for the end-users. The end-user can watch the program by tuning in to a specific point in time. The end-user waits a maximum offset time to get the start of the program. The end-user has no control over the session except in choosing which program to watch. A service scenario for Near VoD is shown in Figure 6-9.

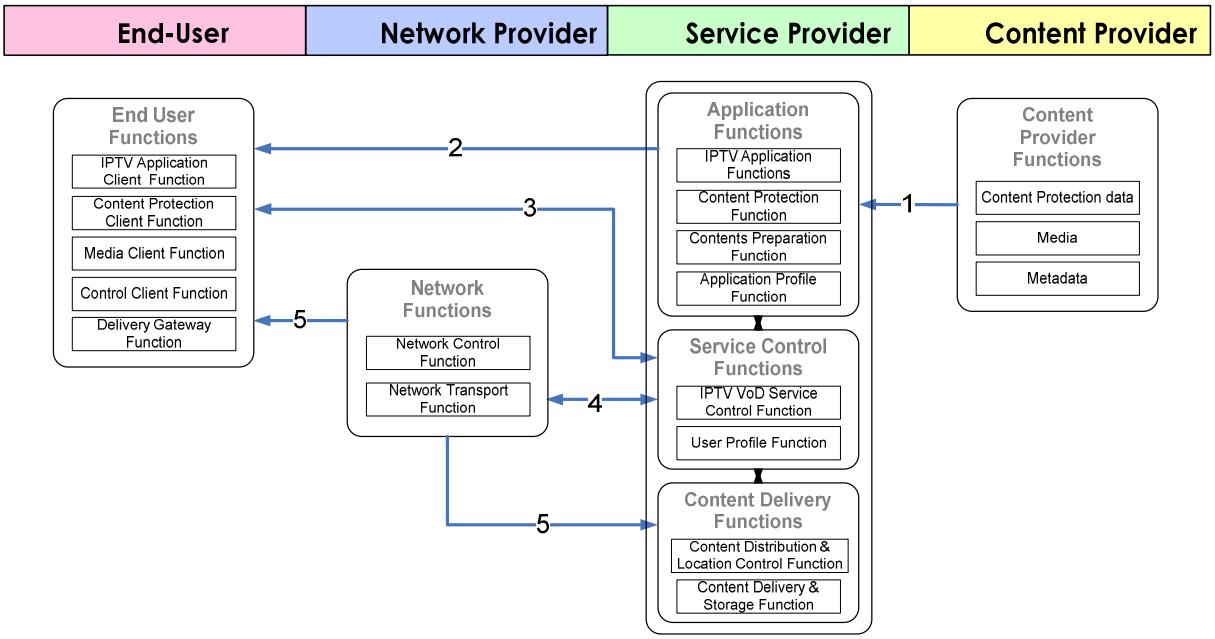


Figure 6-9: Service Scenario for Near VoD

1. Video contents with its metadata and Content Protection data that are produced and managed by the content provider are delivered to the Service Provider.

2. The service provider prepares the content according to the offset timing, as per the agreement between the content provider and the service provider.

3. When an end-user selects a Near VoD content, the request(s) is sent to the service provider. This procedure may include service negotiation (e.g., QoS, price, packaging option, etc.).

4. If the end-user is granted access to the content (e.g. by the service provider), then the service provider interacts with the network provider to possibly negotiate the conditions of forwarding the content to the end-user. This procedure may include the network resource reservation to guarantee the contracted service level.

5. Upon completion of the above step 4, the Service Provider supplies the content access information (e.g., the multicast address that will be used to forward the content) and the end-user can then receive the video.

6.3.2.1 VoD

6.3.3 Reserved Delivery service

There are several cases where reserved delivery services can be used:

- In VoD when the video delivery can not be immediately satisfied, following the end-user request but will be triggered at a later stage by some wake-up mechanism.
- When an end-user has subscribed to an automatic video delivery service based on some criteria (e.g. the end-user has subscribed for the delivery of the new movies from a specific director or with a specific actor, etc.).
- When the Service Provider offers a network PVR functionality. After an end-user record request, the Network PVR waits for the event to be recorded. When the Content is available in the network PVR, then in some cases, it is of interest to deliver the content to an end-user Equipment without waiting for the end-user request.
- When the Service Provider, based on known user preferences, decides to download contents which are likely to be requested by the end-users, to a CPE having recording features, in order to avoid later network congestion.
- When the Service Provider decides to download commercials for insertion at content replay time.

This scenario is described in the following Figure 6-10:

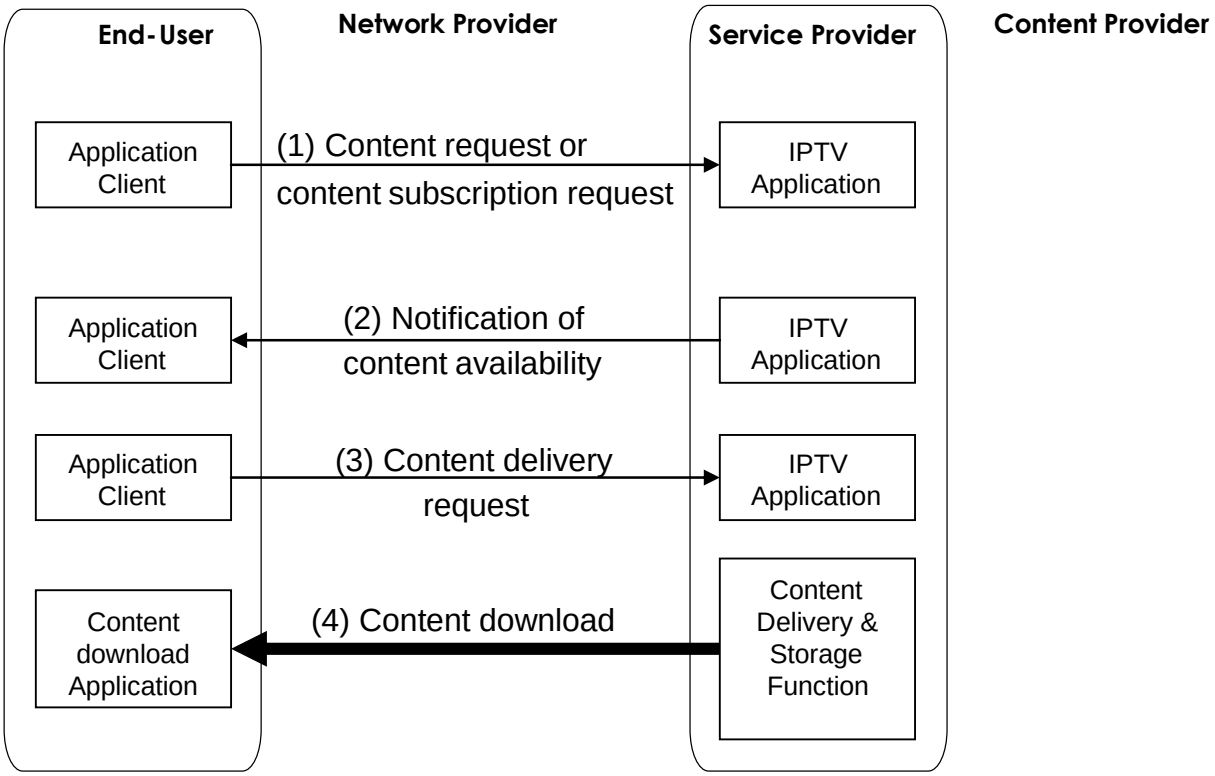


Figure 6-10: Reserved Delivery Scenario

(1) This scenario can start with a catalogue browsing and content selection. It can also start with the access to an IPTV portal proposing specific content subscription (e.g. new movies, week-end football best-of, etc.).

This step does not exist in the case of contents pushed to the Terminal Device without prior end-user request. This use case is valid only when Terminal Devices are provided by the Service Provider.

(2) When a content to be delivered to the Terminal Device is available and possibly depending on other conditions (e.g. server load, subscription rate, etc.) then the Service Provider issues a Notification of Content Availability.

(3) The Terminal Device will issue a content delivery request depending on end-user environment conditions (e.g. availability of storage capacity, Terminal Device activity and load, etc.).

(4) The content download starts upon reception of the content delivery request. If the content delivery request does not follow the notification of content availability, the server conditions might have changed and the server may reject the delivery request, giving a delay to reissue another delivery request.

6.3.4 On-demand with Multi-View service

The on-demand service with Multi-View consists in providing various camera angles in addition to the one station view provided by the Video on-demand service. The viewer can select the camera angle which he would like to watch. For example, when the end-user watches a baseball game, he can see the first base, third base, or backfield according to his wishes, not only those predefined by a channel.

6.3.5 Music on demand (MoD)

Music on demand (MoD) is an audio service which allows the end-user to select music or audio contents as an interactive enhanced service like VoD (see clause 6.3.1).

6.4 Advertising service

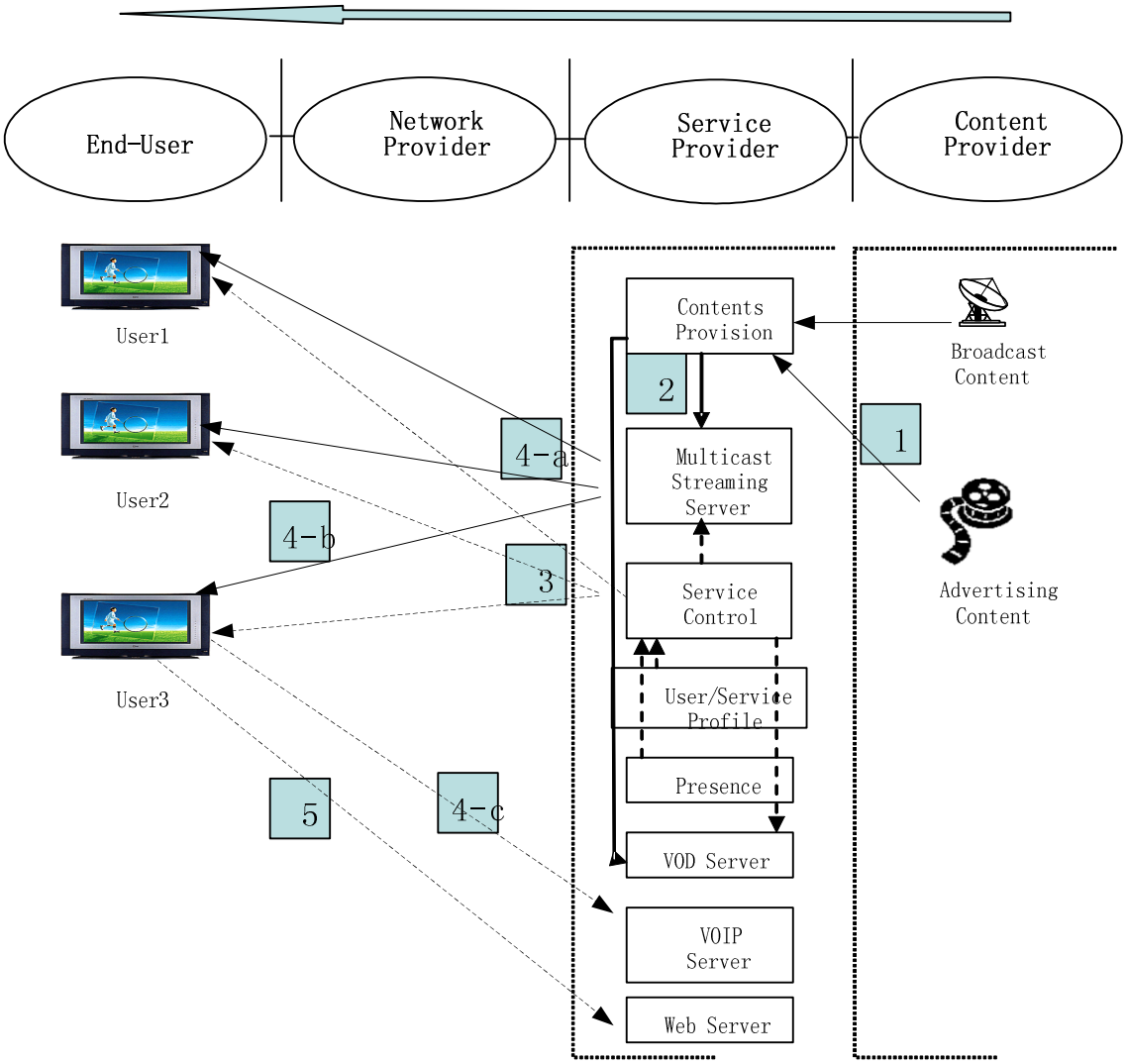


Figure 6-11: Advertising Service

6.4.1 Traditional advertising service

Traditional advertising consists in broadcasting commercial advertising or public promotion of goods, services, companies and ideas. Every end-user located in a certain region will receive such advertisements, which are usually inserted into or between A/V programs. Each advertising service can be provided on a national basis or regionally/locally, either in the form of a video clip or within an exclusive channel according to the service type and contract.

Ad insertion is accomplished using an ad insertion system that inserts advertisements in the video stream prior to being ingested by the IPTV acquisition system. This is typically applied to a Linear service.

Advertisement content is created by content providers and delivered to the service provider. An advertisement is inserted into the video stream and delivered to the end-user. The end-user can see the advertisement while watching the TV program.

1 The content provider produces and manages content for TV channel program with its metadata and delivers them to the service provider. The advertiser produces advertising contents and provides it also to the service provider.

2 The service provider inserts the advertisement contents in the proper TV channel contents stream. The contents (with the advertisement included) can then be delivered to the end-user by a multicast stream.

3 When an end-user triggers or selects the channel service following the channel information, the end-user IPTV terminal device connects to the broadcast/multicast server through the IPTV Control/Session Client. This procedure may include the exchange of multicast messages, as well as service level negotiation for QoS delivery purposes.

4-a See Figure 6-11. The end-user IPTV terminal device receives the channel stream and the end-user can then watch the TV channel program with advertisement.

6.4.2 Targeted Advertising

Targeted Advertising is a commercial advertising or public promotion of goods, services, companies and ideas, usually personalized according to the end-user's preferences or centres of interest, based upon the end-user's profile characteristics in order to match the audience with the campaign objective requirements. Targeted advertisements are defined according to the end-user's preferences, usage history, personal characteristics (biographic and accessibility) and usage environments (terminals, networks and natural environmental characteristics).

Advertisers want to ensure their commercials are only seen in areas where their products or services are available.

End-users want to set a preference to see only specific products or ranges of products depending on their purchasing needs or habits or interests.

End-users want to set a preference to block specific products or range of products based on their purchasing needs, habits or lifestyle.

1 2 Similar to the traditional broadcast advertising service, as depicted in clause 6.4.1.

3 When a user triggers or selects the channel service following the channel information, Service Provider's Service Control function checks the user profile, presence and control to sending different advertisement depending on the end-user characteristics (end-user profile and presence). This procedure may include the exchange of multicast messages, as well as service level negotiation for QoS delivery purposes.

4-b See Figure 6-11. The end-user's IPTV terminal device receives the channel stream with advertisements included. The end-user can then watch the TV channel program with advertisement.

6.4.3 On-demand Advertising

On-demand Advertising is a commercial advertising or public promotion of goods, services, companies and ideas, where the service provider delivers business advertising directory information for the end-user to navigate and select. After navigating and selecting within the advertisement list, the end-user can watch the advertisement that he/she selected.

The IPTV service may also be used to deliver business advertising directory information (e.g., "Yellow Pages" information) regarding available business services. This information may include simple directory listings.

1 The advertiser produces advertising contents and provides it to the service provider.

2 The service provider transmits the received advertisement contents to the proper storage components through the Media Delivery interacting with the IPTV Control. Then, the contents list and relevant information are distributed via the network to the end-users.

3 An end-user navigates and selects any on-demand advertisement contents.

4-c See Figure 6-11. The end-user receives the stream and can watch the advertisement.

6.4.4 Interactive Advertising

Interactive Advertising is a commercial advertising or public promotion of goods, services, companies and ideas, which lets end-users send various types of requests and receive feedback with interactivity.

The end-user clicks on an icon during advertising in order to connect to a website to get additional information on the product.

After pressing a "click-to-call" button (or click on an icon) the end-user initiates a free call to purchase a certain product.

1 2 3 The steps are identical to those described in clause 6.4.3.

4-c The end-user receives the stream and can watch the advertisement. The end-user can also click on an icon for connecting to a web server.

5 See Figure 6-11. The end-user can initiate a free call to purchase a certain product (or get more information on the product and buy it online.)

6.4.5 Advertising message logging

Advertising message logging is a tool used to record information about advertising messages, such as message text and click-times, etc. If necessary, advertising messages can be captured into a log file. The naming of the log file is recommended to use an absolute pathname. This is necessary, as the log file is opened at each point that a message needs to be written to it. For the sake of convenience and easiness, the advertising message log window can be designed. It displays the information of the advertising message logging in the form of a menu. Options on the Message Log window include:

1. View message log information

2. Operating record

3. Copy a message

4. Clearing the Message Log

Message log information includes advertising message text, time, and channel. Some ads relate to interactive advertising services. Purchasing can be made by clicking on an icon.

6.5 Public interest service

6.5.1 Support for end-users with disabilities

End-users with and without disabilities can benefit from supplementary content alongside and in synchronisation with the main content. The most familiar services are subtitling, which provides language translation of the dialogue, and captioning, which provides a transcript of sound effects as well as the dialogue to aid people who cannot hear the sound. The subtitling and captioning services can come in one of two forms: either as a text stream that must be rendered in the receiver with a local font or as a series of graphical bitmaps. There are advantages and disadvantages of each.

Another form of supplementary content is visual sign language translation for deaf people. A sign language interpreter appears in-vision, using hand gestures and mouth movements to convey the dialogue to viewers. Ideally, the position of the interpreter can be set by the end-user, as well as whether there is a solid or transparent background.

Audio description is a commentary explaining the significant visual aspects of the main content, primarily for the benefit of people who cannot see it, though it is also useful for people with learning difficulties. The commentary fits between the dialogue so as not to interfere with the main content, but to work in conjunction with it. Ideally the volume level and positioning of the audio description can be adjusted by the end-user.

Digital television equipment usually provides a user interface comprising a remote control and on-screen display. Some end-users need clearer, larger text or alternative colour combinations in order to read it. Others cannot see the screen at all and need alternative forms of information, such as spoken. The remote control also presents a challenge to those who cannot see or have dexterity limitations. Voice control or a much simpler form of button control can be provided.

6.5.2 Emergency communications

People have different preferences, perhaps based on need, for delivery of notifications. As examples, output should be spoken, text, sign language, and output at different rates. The ITU-T Accessibility Checklist and [ITU-T F.790] should be consulted.

Message content should include all pertinent details presented in a way that is easily and quickly understood by the population. This includes multiple languages in some cases, as well as the use of multimedia for illiterate or hearing/visually impaired individuals.

Spoken messages are particularly useful where the natural language text is not well supported by technology, and for reaching anyone who is unable to read at the moment.

The terminal notifies the user of an incoming Emergency Alert Notification (EAN) message both visually and audibly, or according to the user's preferences and capabilities if they specify otherwise.

6.5.3 Community related information

These are services providing community related information, such as announcements, bus routes, weather and government services related information.

One of the example services is the government service treats civil appeal, tax payment, public poll, Government Issue notice and etc. It could enhance the government productivity and transparency by unifying and opening administration service.

6.5.3.1 Emergency Communications Scenarios and Use Cases over IPTV Systems

6.5.3.1.1 Emergency Communications Generic Service Components

Under Emergency Communications circumstances, public authorities and citizen communities generally act as emergency message providers. The public authority is in charge of emergency messages generation, audit and distribution. Figure 6-10 shows how the authority and community interact with each other and the messages in between them.

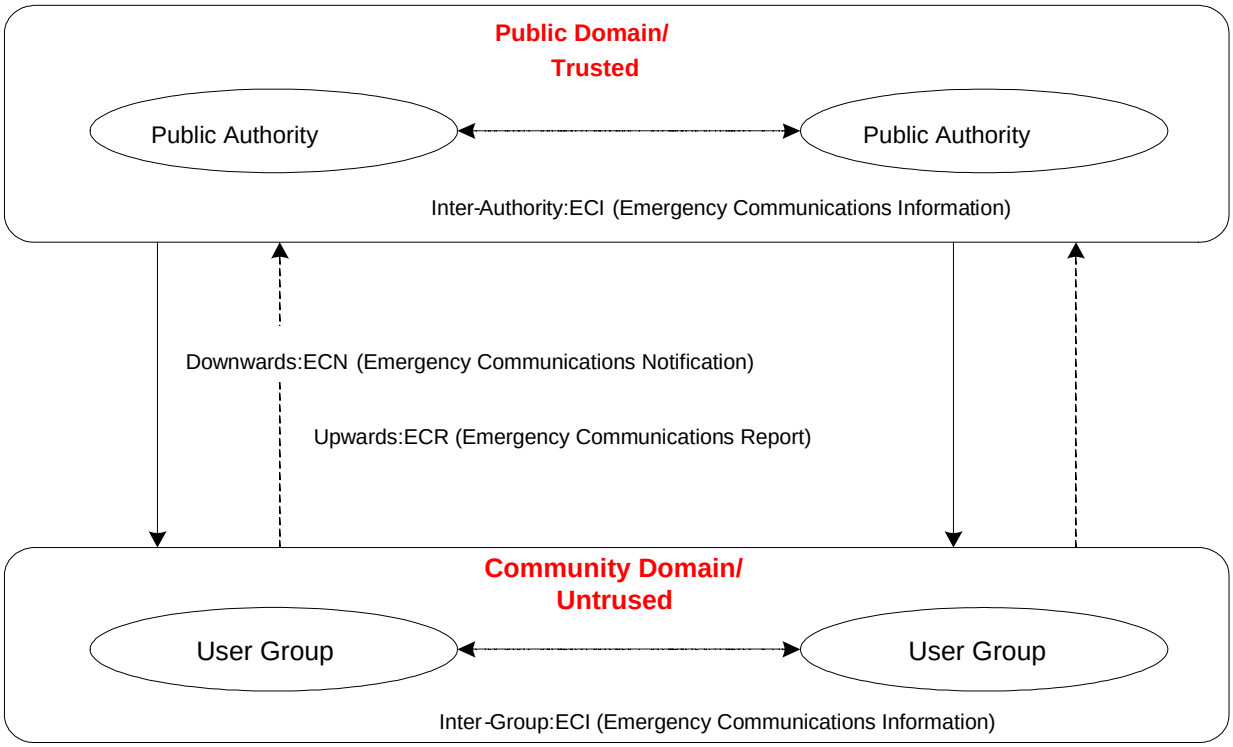


Figure 6-12: Emergency communications components and message interaction

Present emergency messages and typical use cases across IPTV systems can be divided in four modes:

1) Downwards with ECN usage scenario

2) Upwards with ECR usage scenario

3) Inter-group with ECI usage scenario

4) Inter-authority with ECI usage scenario (irrelevant to IPTV systems, hence not described in this document)

6.5.3.1.2 Downwards with ECN Usage Scenario

The public authority authenticated the emergency communication notification message. The ECN would then be distributed to a specific community group or just broadcast. In that case, Emergency Communications would be interleaved with other IPTV services, such as VoD streaming. In this scenario, ECN could work in PUSH or PULL mode. In PUSH mode, the top priority event messages should be forced into IPTV broadcast systems, regardless whether the end-users subscribe to such asynchronous events or not. In PULL mode, end-users can synchronously request the specific interested ECN, such as traffic event in the specified districts or cities, or weather warning from public departments.

The key points of the Downwards usage scenario are:

1) ECN broadcasting in IPTV domain;

2) ECN distribution toward specific communities according to the service they have subscribed to;

3) ECN distributed in PUSH or PULL mode;

4) ECN media streaming has the priority over other content delivery (text, audio and video);

5) ECN distribution community groups correlate with IPTV end-users and multicast groups;

6.5.3.1.3 Upwards with ECR Usage Scenario

The Emergency Communication report (ECR) would be passed through IPTV systems into the public authority (such as fire station or medical centre), which is in addition to legacy emergency communications. Fire warning report, illegal house intrusion event report could be passed into the public authority. Amount of personalized notices or warnings are delivered to the corresponding authority. Types of personalized and customised emergency services can be implemented, such as personal medical services, home visual surveillance services, or global remote medical systems. In this scenario, IPTV systems would be flexibly integrated with other service systems, such as medical or fire centres.

In ECR mode, IPTV systems work as emergency communication message sources with their interactive channels. These multi-media ECR would be forwarded to a specific public authority, where ECR is authenticated and audited.

Upwards usage scenario key points:

1) Multi-media ECR

2) IPTV systems forward the ECR to a specific public authority

3) IPTV end-user location and identification information can also be delivered to a public authority

6.5.3.1.4 Inter-group with ECI Usage Scenario

ECI is part of User-Generated Content (UGC) in IPTV systems. Aside ECR, Emergency Communications reports going to the public authority, ECI from one user group could be delivered to another group for inter-group warning or notifications.

6.5.3.2 Emergency Communications Scenarios in IPTV Systems

6.5.3.2.1 Downwards with ECN Usage Scenario

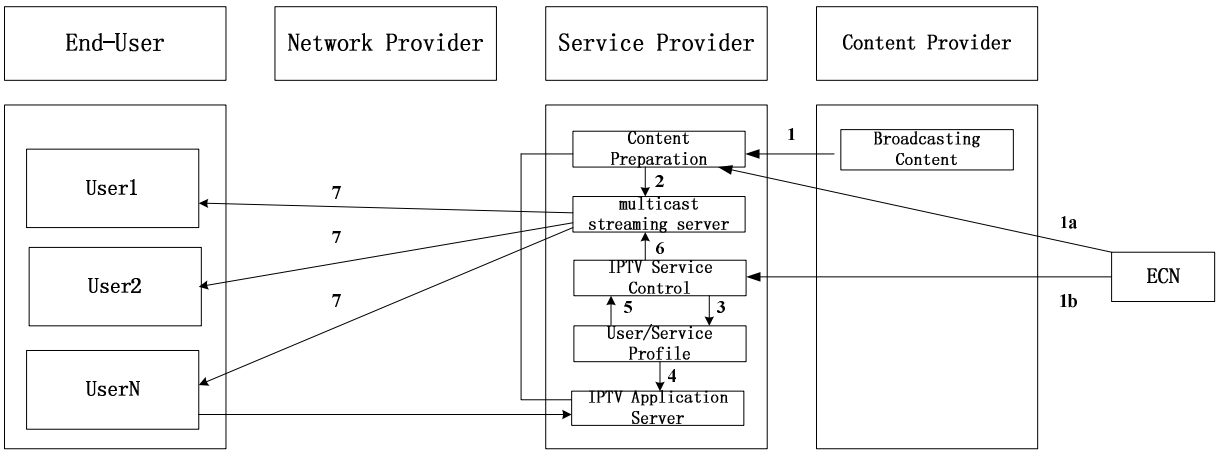


Figure 6-13: Downwards with ECN Usage Scenario

1) Content enter the IPTV Service Provider domain from the Content Provider:

   i. 1a. ECN messages are forwarded to the IPTV Service Provider domain, and the media content is processed by the content preparation function;

   ii. 1b. The public authority informs the IPTV service control function about the ECN entering the IPTV system;

2) Upon ECN receipt, the content preparation function interleaves the ECN with the other content or interrupts the forwarding of the other content, and aggregated content is ready for delivery by (multicast) streaming server:

   i. 2a. Aggregated content is delivered to the IPTV application server instead of the (multicast) streaming servers;

3) The IPTV service control checks the available ECNs, then checks end-user or group profile and service information to instruct the aggregated content where it needs to be sent;

4) The end-user and service profile instructs the IPTV application server to deliver the media (ECN receipt user group mapping to IPTV application user group);

5) The end-user and service profile informs the IPTV service control about the (multicast) streaming delivery (ECN receipt user group mapping to an IPTV multicast group);

6) The aggregated content is ready for delivery by the (multicast) streaming server with destination group information and service information;

7) The media is forwarded to the end-users and user groups. It could be multicast streaming or any other application format, such as VoD, presence, VoIP or web servers.

6.6 Tele-services

6.6.1 Tele-learning

Tele-learning is an instructional service for delivering educational contents e.g. infant, children, school student, languages, financial skill, etc., to students who are physically located in different geographic areas. Teachers and students can communicate in real time (i.e. both present at the same time) and/or non-real time (i.e. at time of their own decision using a messaging capability) using video, audio, pictures and text, etc.

6.6.2 Tele-medicine

Tele-medicine is a medical service which is provided to doctors and patients who are in different geographic areas from each other. Doctors can deal with patients by remote diagnosis, remote consultation, remote medical examination, medical education etc., in real time (i.e. both present at the same time) and/or non-real time (i.e. at time of their own decision using a messaging capability) using video, audio, pictures and text, etc.

6.6.3 Monitoring services

Monitoring services are services which provide monitoring and surveillance capability. Examples of such services include health monitoring, surveillance of places, etc.

6.7 Portal services

A portal service is a branded aggregation of products and services designed to satisfy a large majority of end-users' needs, such as VoD, shopping, banking, communication, entertainment and other interactive services with portal menu. Portal service can target end-users with broadcasting of commercials, advertisements and interactive response advertising.

6.7.1 Data portal (walled garden, Internet access, etc.)

Data portal service is a branded aggregation of content with wall garden access for information, shopping, banking, learning and other communication service with interactivity. Also, it can support direct Internet access for more specific information search.

6.7.2 Web-based IPTV Portal

The web-based IPTV portal is a platform that allows an organization to integrate its business information, applications, and services in a web-based IPTV Portal for easy navigation and access.

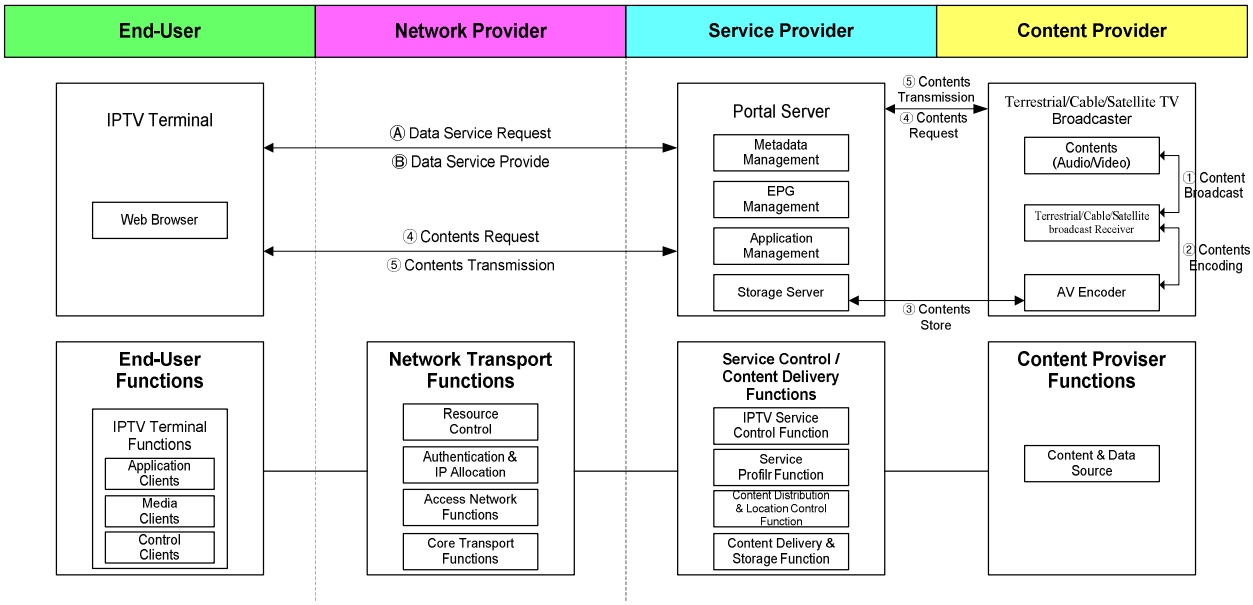


Figure 6-14: Web-based IPTV Portal Service Scenario

1. Terrestrial/Cable/Satellite TV Broadcaster provide the contents to the service provider (Web-based IPTV Portal)
2. Service provider encodes the received audio/video source from Terrestrial/Cable/Satellite TV Broadcast receiver.
3. Store the contents to the storage after additional process such as contents packaging, encryption, etc.
4. End-user selects the contents via EPG based on web which are provided by portal server.
5. Portal server transmits the contents which are requested by end-user.

Ⓐ End-user request the web data services on Internet such as E-mail, FTP, messenger and Instant Messaging (IM).

Ⓑ Portal server provides the web data services.

6.8 Hosting services

Hosting services consist of IPTV platforms with hosting capabilities that provide organizations and end-users with on, off-line system and network for storing information, image, video, or any content accessible via the IPTV hosting service.

6.8.1 Business-to- business

The business-to-business hosting service is an IPTV hosting service for the special group or business unit subscriber. It connects the channel, VoD, and portal service made by end-user business unit to the IPTV platform to supply particular groups with real time broadcasting channels, and value-added interactive services.

6.8.2 User created content (UCC) hosting

User Created Contents (UCC) hosting service is an IPTV hosting service for the individual end-user like a user- generated Video, or interactive content data. This service allows the end-user to operate his/her own channel, like personal web TV by uploading A/V, application and other contents that he/she generates through the IPTV hosting platform.

6.9 IPTV interactive service

Interactive services let end-users send various types of requests and receive feedback with interactivity.

The integrated Internet service in IPTV consists of integrating current Internet based on-line services and provides them within the IPTV service as per the following examples.

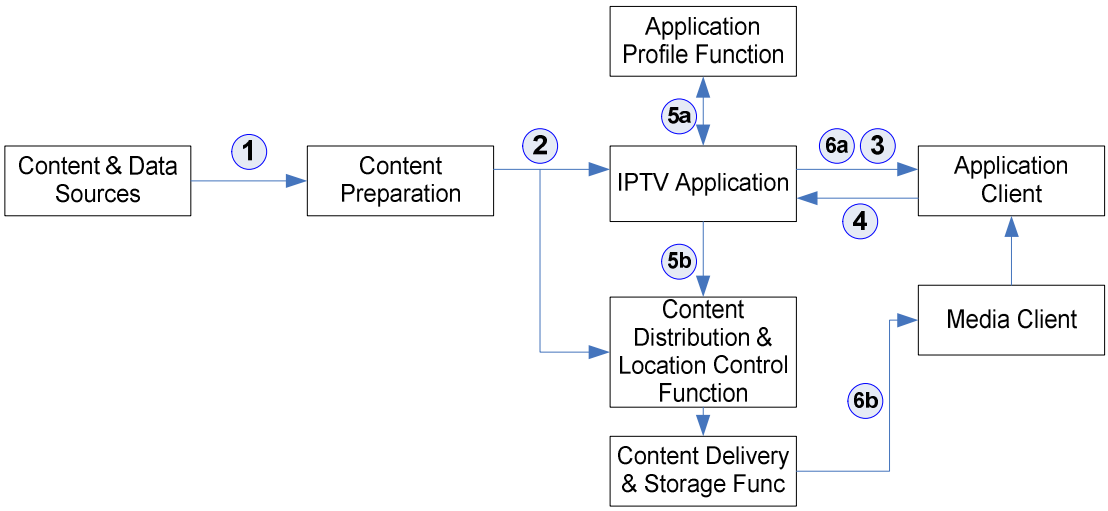


Figure 6-15: Example of an Interactive IPTV Service Scenario

1 The original content and data are produced and delivered to the Content Preparation Function.

2 Received and processed by the Content Preparation function, its metadata is delivered to the IPTV Application function and its content is delivered to the Content Delivery & Storage Function under the control of the Content Delivery Control Function.

3 When an end-user uses the IPTV terminal device, the updated IPTV service EPG is transmitted based on the end-user's profile.

4 When the end-user selects one of the integrated Internet services, the corresponding information is transmitted from the Application Client to the IPTV Application.

5 **a.** If the selection includes end-user-specific requests, it is transmitted and processed by the Application Profile Function.

5 **b.** If the selection requests more data or content than that can be stored in the service provider's storage facility, then the request is forwarded to the Content Delivery & Storage Function for further processing (e.g. reserve extra storing or buffering capacity, delete the content and send a notification to the end-user, etc.).

6 **a.** Proper response is provided by the IPTV Application.

6 **b.** If necessary, the requested content or data are transmitted by the Content Delivery & Storage Function under the control of the Content Delivery Control Function.

6.9.1 Information (news, weather, transportation, local community, etc.)

IPTV Interactive Information service is an information service that supports various types of content such as news, weather, traffic forecasts, and advertisements. The end-user can choose content through an independent menu. An example of the information service is a program survey service.

6.9.2 Commerce (banking, stock, shopping, ticketing, auction, product delivery, event, etc.)

IPTV Interactive Commerce service is a commercial service that allows the end-user to purchase goods and use financial services such as banking, stock, auction, etc. For example, personal banking service can help the end-user to view account balances, review past account activity, pay bills, and transfer money between accounts from the IPTV terminal device.

6.9.3 Communication (e-mail, messenger, SMS, channel chatting, VoIP, web surfing, multiple video conference, video phone, etc.)

IPTV Interactive Communication service is a converged service of telecommunication and broadcasting that compounds phone services (VoIP, video phone, multiple video conference, etc.) and Internet-based communication services (Instant Messaging, Short Messaging Service, Email, Web, etc.) with television services. It is usually provided by controlling multiple sessions for a phone service, an Internet-based communication service and a television service. IPTV Interactive Communication services have a few combinations. Thus end-users can access the converged services that provide "a phone service and a TV service" or "a communication service and a television service" or "a phone service and a communication service and a television service" simultaneously.

IPTV Interactive Communication is a communication service that enables the end-user to exchange information such as voice, video, and data. End-users can send (or receive) the mail and message while watching TV. In addition, end-users can simultaneously interact with other people via two-way video and audio transmissions using video conference.

– Videoconference

A videoconference service is service providing bidirectional symmetric real-time transfer of motion video, text and voice between end-users in two or more locations. This real time text differs from instant messaging systems because it is the bidirectional transmission of one character at a time. This gives the end-user the impression of real-time communications, just like voice or video systems that transport streaming media over IP. The concept is aimed at providing for rich media real time conversation for all people in various situations. This includes but is not limited to people that are disabled in some way, e.g. the deaf or hearing impaired, blind people, etc., but also people who find themselves in a situation where the complementing media video, real-time text and voice together fulfils the conversation needs much better than only voice.

ITU-T Rec. F.703 covers videophone with real time text. Ideally all videophones should offer this service, but in many cases only video and audio are provided. F.703 is useful not only for the disabled but for anyone who can benefit from the textual back-up of for example technical data, language translations, verbal or signed conversations. It can be used for people who are not only deaf or disabled but people who can't communicate in either of the two mediums or do not have the command of the spoken language used. This service is useful to document information within videophone calls (e.g. phone numbers and addresses) without searching for pen and paper. An example would be to get a flight booking reference when making a travel arrangement.

– Messaging

Messaging is an interactive service which offers user-to-user telecommunication between individual users. Messaging services may be immediate (e.g. instant messaging (IM)) or of a store-and-forward type (e.g. email and voice mail).

6.9.4 Entertainment (games, karaoke, photo album, lottery, blog, etc.)

IPTV Interactive Entertainment is a service that is designed for the end-user's amusement by providing content such as games, karaoke, and photo album. Games can be sub-divided into single player and multi-player games depending on the number of players. Moreover, games can be classified into network games and non-network games depending on the level of interaction. In the case of a photo album, the end-users can enjoy pictures they uploaded or transfer them to other people's IPTV terminal devices, mobile phones, etc.

6.10 Presence services

Presence Service is an IPTV service that manages presence information between end-users (watchers, [IETF RFC2778]) and presentities, in order to enable applications and services to make use of presence information.

The presence service provides information about the end-user's location.

The presence service provides access to presence information to be made available to other users or services including IPTV services.

A presence service, as observed by the end-user, is a service in which the end-user can control the dissemination of his presence information to other end-users and services, and also be able to explicitly identify what are the other end-users and services to which he provides presence information.

Presence Service is the capability to support management of presence information between watchers and presentities, in order to enable applications and services to make use of presence information.

Presence information is a set of attributes characterizing current properties such as status (online, offline, meeting, on the phone, etc.), place (home, office, library, etc.), communication means (audio, video, text, etc.), and so on. [3GPP TS 22.141]

Presentity is an entity that provides presence information.

Watcher is an entity that requests presence information about a presentity. [IETF RFC2778]

Example services might include:

- Electronic Program Guide (EPG) personalization based on presence on top of locally stored data
- Targeted advertising based especially when correlated with time of day
- Chatting with friends watching the same channel

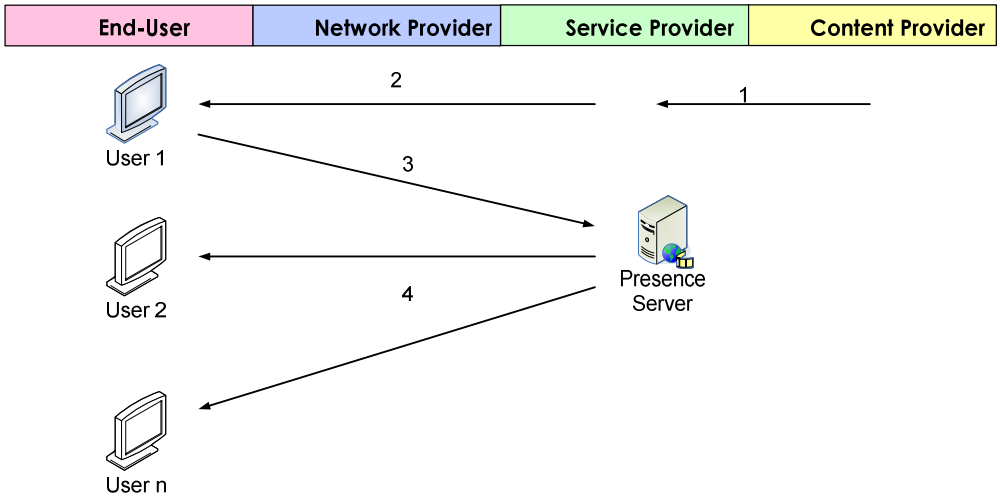


Figure 6-16: Presence Service Scenario

1. Content is acquired by the service provider from some sources such as a satellite downlink or a content library.
2. The content is delivered to the end-users.
3. The presence information of users and information on users' devices, services and service components is provided to the Presence Server. The information might be content information (Broadcast TV channel, VoD content, Commercial Advertising, etc.) currently accessed.
4. The presence information can be distributed to other end-users.

6.10.1 Basic Presence Service

End-user A is watching TV.

End-user B logs in TV at home.

Now, user A knows that user B is at home and calls him.

6.10.2 Channel based Presence Service

End-user A is watching the football game on the IPTV terminal device.

He/she would like to chat with friends who are watching the same channel.

He/she opens the presence service client and pushes the button marked as "Search for friends".

On a mask on the screen he/she specifies the search criteria, which are "buddies watching the same channel now, and available for chatting".

He/she gets a list and invites them all to a multi-point messaging session.

6.10.3 Targeted Advertising based on Presence Service

The presence server gathers the presence information of end-users and stores their log into a database with the approval of them. The presence information could be content information they watches, shopping habits, etc.

An advertiser requests the end-user log of end-users from the presence server and can make targeted advertisements.

6.11 Time-shifting and Place-shifting service

– Time-shifting service

An IPTV service in which subscribers can access and control (pause, rewind, fast forward, etc.) IPTV contents without time limitation. Therefore, this service is assuming that the IPTV contents are saved in a repository for later use.

In a traditional TV service the time shifting service has been provided by the recording functionality such as VCR (Video Cassette Recorder). Then, some products using hard drive instead of tape are starting to prevail while supporting some capabilities such as automatic recording with key words, the name of actor, etc., which is referred to as DVR (Digital Video Recorder) or PVR (Personal Video Recorder).

Note that the content should be stored so that end-users can retrieve it later. The PVR devices are storing the contents in local hard drive. We can call this approach "end-user-based time-shifting service". However, we can consider some cases in which it is not appropriate to save the contents locally. For example, if the IPTV terminal is PDA, the size of the hard drive is limited. The network-based time-shifting mechanism is needed for those kinds of cases, which is also called NVR (Network Video Recorder). In those solutions, hard drives are located in the service provider's domain as opposed to the end-user's set-top box. In the network-based time-shifting service, the broadcasting traffic is transformed into on-demand traffic and service providers can leverage their existing VOD infrastructure already in place. Subscribers sign up for specific network-based time-shifting service and storage limits, and the service provider gives end-users access to the IPTV content as it is delivered to their own terminals.

In summary, we can define two types of time-shifting service, subscriber-based and network-based time-shifting services in IPTV.

– Place-shifting service

An IPTV service in which subscribers can access (pause, rewind, fast forward, etc.) IPTV contents without place limitation. That is, the end-user sees his or her subscribed IPTV contents anywhere. The place-shifting basically addresses requirements of end-users who move from one place to another, the former being the place where he or she originally subscribed to the service. This service is assuming that an end-user's terminal device can be a mobile phone.

Depending on who is taking care of redistributing the IPTV traffic, two types of place shifting services can be defined, subscriber-based place-shifting and network-based place-shifting service. In subscriber-based place-shifting, an end-user device redistributes traffic to the place where the end-user is currently located. In network-based place-shifting, the IPTV service provider forwards the IPTV traffic to the moved place.

6.12 Session mobility service

An IPTV service in which an on-going multimedia session can be transferred seamlessly between different devices based on user preferences. That is, the service makes subscriber see his or her subscribed real time IPTV content seamlessly. It is different from Place-Shifting service for it is more suited for transferring on-going or real time sessions.

Figure 6-17 illustrates the details of session and media transfer for session mobility. In this scenario, we assume that Corresponding Device is in a real time session with the originating terminal device on a mobile host and want to move session to target device on a fixed host. Originating terminal device and target device share the same Content relay A which is controlled by the Content transfer controller A. Similarly, Content relay B provides content relay service to Correspondent Device. Session mobility can be used to achieve session and content transfer.

The session mobility basically is to support capturing the session control context information from the originating terminal device and transferring them to the target terminal device by a media transfer controller in case of receiving session transfer request. The exchange between the media transfer controller and media relay can also be used to negotiate capabilities and transfer the session. And it also supports suspending and resuming the session based on the subscriber's requirements. This service allows for an end-user's terminal to be a mobile device.

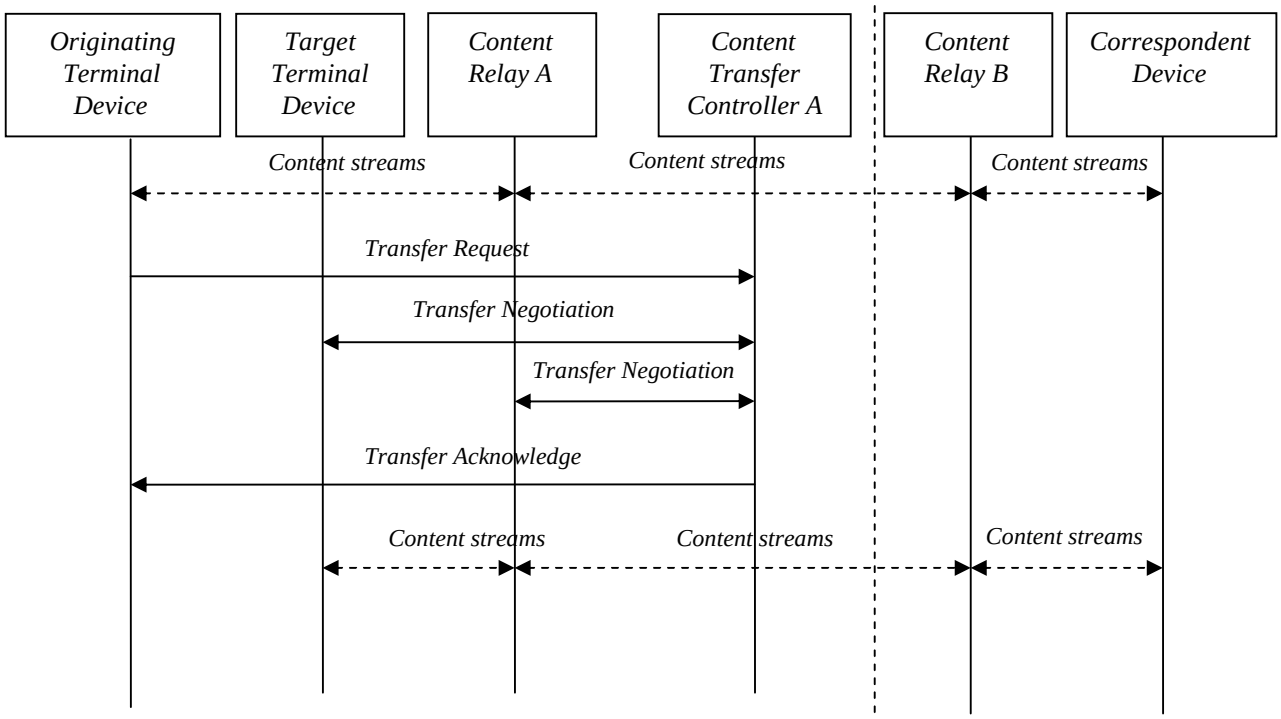


Figure 6-17: Session and Content Transfer for Session Mobility

Content Transfer Controller: A gateway or router which receives content transfer request from terminal devices and exchange session context information and devices capability with content relay. One media transfer controller may control one or several content relays.

Content Relay: A gateway or router which negotiates session context information and device capabilities with content transfer controller and relays content to corresponding device. One content relay may provide content relay functionality to one or several terminal devices.

6.13 Supplementary content

This is defined as video, audio, textual, graphical or other forms of content that can be optionally accessed by the user and rendered by the terminal device. It has the following features:

– It only works in conjunction with the main content.

– It is synchronous with the main content.

Examples of use are:

1) Subtitles and captions

These services can be provided by means of either textual or graphical supplementary content. Subtitles provide a real-time on-screen transcript of dialogue for the purpose of language translation. The subtitles and the dialogue are in different languages. Captions for hearing impaired people provide a real-time on-screen transcript of the dialogue as well as any sound effects. Different speakers are distinguished, usually by different colours. The captions and the dialogue are in the same language. The service is primarily to assist end-users having hearing difficulties. Ideally, end-users may have some control over the position and size of the presentation.

2) Audio description

Primarily intended to assist end-users who are unable to see the video content clearly, this service provides a commentary describing the visual events pertinent to the content. The narrative passages fit between the dialogue and other significant audio content so as not to interfere with it. Ideally the end-user can control the volume and spatial positioning of the audio or derive it from a separate output.

3) Sign language interpretation

This service comes in the form of supplementary video content, usually smaller in image size to that the main video content. The video shows an interpreter who uses hand gestures and facial expression to convey the main audio content to sign language and lip readers. Ideally the end-user can control the position, size and background properties (solid or transparent and the colour, if solid). It is of sufficient temporal and spatial quality to enable sign reading and lip reading.

4) Other services

Feature films on DVD frequently offer an alternative audio track that contains a commentary on the film by the director or actors. IPTV systems could provide the same service by means of supplementary audio content. It would also be possible to optionally show the commentators by means of supplementary video content.

News services often have 'tickers' in vision, of news headlines or financial information. However, different users have different preferences for these information mechanisms so they may best be provided in the form of selectable and customisable supplementary content. If this was provided in the form of supplementary textual content then terminal devices could render it in alternative formats such as speech or Braille.

Commentators for sports events could optionally be seen by means of supplementary video content. In fact, the main audio content could be just the 'natural sound' of the sport, with a choice of commentaries available as supplementary audio content.

7 Payment methods for accessing IPTV services

Payment methods are one of the essential components for accessing IPTV services. Such methods affect the way IPTV services are delivered and accessed by end-users.

There are a number of well-known payment methods that can be also applied to the IPTV services as shown below. The following list of payment methods is not exhaustive. Such payment methods can vary or can be applied concurrently, depending on the IPTV service characteristics, the IPTV service environment and the service provider's policy.

- **Free**

  End user can access the IPTV content without paying for it. In this case, no change for the service scenario related to charging is required.

- **Subscription**

  End-user should pay the predefined amount of money in order to access the IPTV services. In this case, additional procedure for appropriate subscription and for checking whether the end user is properly subscribed or not is required.

- **Pay per view (PPV) or Pay per use (PPU)**

  End-user pays for accessing each individual content of the IPTV service. In this case, additional procedure for proper payment and authorization and/or accounting is required.

- **A La Carte**

  End user can purchase only the channel(s) he/she wants to receive, instead of the entire list of programs proposed by the service provider. In this case, the end-user makes his/her own program. Additional procedure for proper payment and authorization and/or accounting is required.

- **Cash-back Point**

  Cash-back point is a kind of credit which can be used as real money to pay for IPTV services. The end-user can either acquire the cash-back point(s) by using or purchasing IPTV services with real money or use it for payment instead of real money. In this case, additional procedure for managing the cash back point with proper authentication, authorization, and accounting is required.

- **Package**

  The end-user can select and/or purchase a set of channels, contents, applications, or a combination thereof, and which are already organized by the service provider. In this case, additional procedure for proper payment and authorization and/or accounting is required.

Bibliography

[IETF RFC2778] IETF RFC 2778 (2000), A Model for Presence and Instant Messaging.

[3GPP TS 22.141] 3GPP Technical Report 22.141 v7.0.0, Presence Service: Stage1 (Release 7).

II.1.4 Gap analysis

Introduction

A gap analysis is a tool to help determine how well a specification answers a set of requirements and/or use cases. It takes a specification and a set of requirements and/or use cases as inputs. It outputs unaddressed requirements and issues.

For the gap analysis to be complete, it should start from the most complete set of requirements and associated use cases.

The objective of this document is to perform a gap analysis not only over one but over several standards of the IPTV domain.

[EDITOR'S NOTE – Contributions are solicited to clarify if the gap analysis should only be performed over existing standards or whether other, commercial, specifications should be considered upon contribution]

CONTENTS

Page

1 Scope 203

2 References 203

3 Definitions 203

3.1 Terms defined elsewhere 203

3.2 Terms defined in this document 203

4 Abbreviations and acronyms 203

5 Gap identification 204

Bibliography 204

Gap analysis

1 Scope

This document identifies gaps between existing IPTV standards and uses cases or requirements developed in the WG1 requirements subgroup and documented in document [REQ].

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[REQ] ITU-T Focus Group Draft Requirements Document [reference to be updated]

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

For further study.

3.2 Terms defined in this document

This document defines the following terms:

For further study.

4 Abbreviations and acronyms

This working document uses the following abbreviations:

DRM Digital Rights Management

DiffServ Differentiated Services

DVB Digital Video Broadcasting

IP Internet Protocol

IPTV Internet Protocol TeleVision

QoS Quality of Service

STB Set-Top Box

5 Gap identification

Requirement: interworking of existing IPTV systems with NGN

Statement: DVB IP [DVB IPI] has a specified interface for DiffServ for the purpose of supporting Quality of Service. However, there is no specification allowing DVB to benefit from NGN QoS mechanisms.

Action:

[EDITOR'S NOTE – Contributions are solicited for an internal document structure.]

[EDITOR'S NOTE – Contributions are solicited to establish a list of standards to be reviewed. Contribution 69 could be used a list of potential candidates.]

[EDITOR'S NOTE – Contributions are solicited to establish a list of commercial specifications to be reviewed if applicable.]

Bibliography

[DVB IPI] Transport of MPEG2-based DVB services over IP-based networks, ETSI TS 102034 v010101.

II.2 QoS AND PERFORMANCE ASPECTS

II.2.1 Quality of experience requirements for IPTV services

Summary

This document defines user requirements for Quality of Experience for IPTV services. The QoE requirements are defined from an end user perspective and are agnostic to network deployment architectures and transport protocols. The QoE requirements are specified as end-to-end and information is provided on how they influence network transport and application layer behaviour. QoE requirements for video, audio, text, graphics, control functions and meta-data are provided.

Keywords

IPTV, QoE, QoS

Current status

All sections are in good shape, except for the section on accessibility requirements. We have identified the need for specific QoE requirements related to accessibility and therefore included a section as a placeholder in the document. However, this section still requires substantial input.

Dependency on or relationship to other FG IPTV documents

- IPTV service requirements document; defining the basic requirements.
- The document references the application layer error recovery mechanisms for IPTV services document, however it can also be used without this reference.

CONTENTS

		Page
1	Scope	208
2	References	208
3	Definitions	209
	3.1 Terms defined elsewhere	209
	3.2 Terms defined in this document	209
4	Abbreviations and acronyms	209
5	Introduction to QoE	211
6	QoE for video and audio	212
	6.1 Requirements for media compression and synchronization	213
	6.1.1 Standard definition TV (SDTV): General minimum objectives	215
	6.1.2 Standard definition (SD) TV: VoD and Premium Content Objectives	217
	6.1.3 High definition TV (HDTV): Objectives	218
	6.2 Requirements for network transmission	220
	6.2.1 Standard Definition Video: Broadcast TV Transport Layer Performance Objectives	222
	6.2.2 Standard Definition Video: VoD and Premium Content Transport Layer Performance Objectives	224
	6.2.3 High Definition TV: Transport Layer Performance Objectives	224
	6.3 Network Layer Performance Objectives	225
7	QoE for text and graphics	227
	7.1 Media component text	227
	7.1.1 Definition	227
	7.1.2 Description	228
	7.1.3 Quality Aspects	229
	7.1.4 Intercommunication	229
	7.2 Media component graphics	229
	7.2.1 Definition	229
	7.2.2 Description	229
	7.2.3 Quality aspects	229
8	QoE for control functions	230
	8.1 QoE requirements for channel zapping time	230
	8.1.1 Classification of channel zapping time	230
	8.1.2 Requirements for channel zapping time	231
	8.2 QoE requirements VoD trick mode	231
	8.2.1 Trick Latency	231
	8.2.2 Requirements for VoD Trick Features	231

Page

9 QoE for other IPTV services 232
9.1 QoE requirements for Metadata 232
9.1.1 QoE requirements for EPG 232
9.2 QoE requirements for Browser 232
9.3 QoE requirements for Content Navigation 233
9.3.1 Contents navigation by direct channel selection, by up/down button 233
9.3.2 Contents navigation by EPG/ECG 233
9.3.3 Contents navigation by contents recommendation 233
10 Accessibility requirements 234
Appendix I – Network QoS parameters affecting QoE 234
I.1 Transport Impairments 234
I.1.1 IP Packet Transfer Delay 234
I.1.2 IP Packet Loss Ratio (PLR) 235
Bibliography 235

Quality of experience requirements for IPTV services

1 Scope

This document defines user requirements for Quality of Experience (QoE) for IPTV services. The QoE requirements are defined from an end-user perspective and are agnostic to network deployment architectures and transport protocols. The QoE requirements are specified for the end-to-end service and information is provided on how they influence network transport and application layer behaviour.

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 published regularly. The reference to a document here does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.800] ITU-T Recommendation E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*

[ITU-T F.700] ITU-T F.700 (2000), *Framework recommendation for multimedia services*

[ITU-T H.264] ITU-T Recommendation H.264(2005), *Advanced video coding for generic audiovisual services*

[ITU-T P.10/G.100] ITU-T Recommendation P.10/G.100, Amd. 1 (2007), New Appendix I, *Definition of quality of experience (QoE)*

[ITU-T P.800] ITU-T Recommendation P.800 (1996), *Methods for subjective determination of transmission quality*

[ITU-T T.140] ITU-T Recommendation T.140 (1998), *Protocol for multimedia application text conversation*

[ITU-T Y.1541] ITU-T Recommendation Y.1541 (2006), *Network performance objectives for IP-based services*

[ITU-T FG IPTV REQ] FG IPTV-DOC-0147, *Working document: IPTV services requirements*

[ITU-T FG IPTV ALERM] FG IPTV-DOC-0186, *Working document: Application layer error recovery mechanisms for IPTV services*

[ITU-R BT.500-11] ITU-R Recommendation ITU-R BT.500-11 (2003), *Methodology for the subjective assessment of the quality of television pictures*

[ITU-R BT.601-6] ITU-R Recommendation ITU-R BT.601-6 (2007), *Studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios*

[ITU-R BT.1359-1] ITU-R Recommendation ITU-R BT.1359-1 (1998), *Relative timing of sound and vision for broadcasting*

[ETSI TR 101 154] ETSI TR 101 154 V1.4.1 (2000), *Digital Video Broadcasting (DVB); Implementation guidelines for the use of MPEG-2 Systems, Video and Audio in satellite, cable and terrestrial broadcasting applications*

[IETF RFC 3393] IETF RFC 3393 (2002), *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*

[DSLF TR126] DSL Forum TR-126 (2006), *Triple-play Services Quality of Experience (QoE) Requirements*

[SMPTE 421M] SMPTE 421M(2006), *Television – VC-1 Compressed Video Bitstream Format and Decoding Process*

[ISO-10646] ISO/IEC 10646 (2003), *Information technology – Universal Multiple-Octet Coded Character Set (UCS)*

[ISO/IEC 14496-3] ISO/IEC 14496-3 (2005), *Information technology – Coding of audio-visual objects – Part 3: Audio*

[ATIS-0800004] ATIS-0800004 (2006), *A Framework for QoS Metrics and Measurements Supporting IPTV Services*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Quality of experience (QoE) [ITU-T P.10/G.100]: The overall acceptability of an application or service, as perceived subjectively by the end-user.

NOTE 1 – Quality of Experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.).

NOTE 2 – Overall acceptability may be influenced by user expectations and context.

3.2 Terms defined in this document

This document defines the following terms:

3.2.1 Group of Pictures: The Group of Pictures (GOP) is a group of successive pictures within a MPEG-coded film and/or video stream. Each MPEG-coded film and/or video stream consists of successive GOPs. From the MPEG pictures contained in it, the visible frames are generated.

3.2.2 VoD Trick Modes: Download and streaming video on demand (VoD) systems provide the user with a large subset of VCR functionality including pause, fast forward, fast rewind, slow forward, slow rewind, jump to previous/future frame, etc. These functions are usually referred to as "trick modes".

3.2.3 Triple Play Services: Services that include IPTV, VoIP, and Internet Access.

3.2.4 Clean Audio: Audio track of an IPTV Service with background sounds removed.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

AAC Advanced Audio Coding

AC-3 Dolby Digital Audio (Advanced Codec 3)

ARQ Automatic Repeat reQuest

ATIS Alliance for Telecommunications Industry Solutions

ATSC	Advanced Television Systems Committee
A/V	Audio Video
AVC	Advanced Video Codec
AVS	Audio and Video coding Standard (Chinese)
BER	Bit Error Rate
BML	Broadcast Markup Language
CBR	Constant Bit Rate
CPU	Central Processing Unit
DCT	Discrete Cosine Transform
DSCQS	Double Stimulus Continuous Quality Scale
DSL	Digital Subscriber Line
DVB	Digital Video Broadcast
DVD	Digital Video Disk
ECG	Electronic Content Guide
EPG	Electronic Program Guide
FEC	Forward Error Correction
FFW	Fast ForWard
fps	frames per second
GOP	Group of Pictures
GWR	GateWay Router
HDTV	High Definition TeleVision
HG	Home Gateway
HTML	HyperText Markup Language
IETF	The Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interactive Gateway Protocol
IPG	Interactive Program Guide
ITU-R	International Telecommunication Union Radiocommunication Sector
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
MOS	Mean Opinion Score
MP	Measured Point
MP-3	MPEG-1 Audio Layer 3
MPEG	Moving Pictures Expert Group
MPLS	MultiProtocol Label Switching
NICAM	Near Instantaneous Companded Audio Multiplex
NTSC	National Television Standards Committee
PAL	Phase Alternating Line
PC	Personal Computer

PDV	Packet Delay Variation
PHB	Per-Hop Behaviour
PLR	Packet Loss Ratio
PTD	Packet Transfer Delay
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request For Comments
SDH	Synchronous Digital Hierarchy
SDTV	Standard Definition TeleVision
SECAM	SEquentiel Couleur A Mémoire, French for "Sequential Colour with Memory"
SMPTE	Society of Motion Picture and Television Engineers
SONET	Synchronous Optical NETwork
STB	Set-Top Box
VBR	Variable Bit Rate
VoD	Video on Demand
VCR	Video Cassette Recorder

5 Introduction to QoE

QoE is defined in [ITU-T P.10/G.100] in Appendix I as the overall acceptability of an application or service, as perceived subjectively by the end-user. It includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.) and may be influenced by user expectations and context. Hence the QoE is measured subjectively by the end-user and may differ from one user to the other. However it is often estimated using objective measurements.

Contributing to the QoE are objective service performance measures such as information loss and delay. Those objective measures together with human components that may include emotions, linguistic background, attitude, motivation, etc. determine the overall acceptability of the service by the end-user. Figure 5-1 shows factors contributing to QoE. These factors are organized as those related to quality of service and those that can be classified as human components.

QoE for video is often measured via carefully controlled subjective tests [ITU-R BT.500-11], [ITU-T P.800], where video samples are played to viewers, who are asked to rate them on a scale. The rating assigned to each case are averaged together to yield the mean opinion score (MOS).

Quality of service (QoS) is defined in [ITU-T E.800] as the collective effect of performance which determines the degree of satisfaction of a user of the service. In telecommunications, QoS is usually a measure of performance of the network itself. QoS mechanisms include any mechanism that contributes to improvement of the overall performance of the system and hence to improving end-user experience. QoS mechanisms can be implemented at different levels. For example at the network level it includes traffic management mechanisms such as buffering and scheduling employed to differentiate between traffic belonging to different applications. Other QoS mechanisms at levels other than the transport include loss concealment, application forward error correction (FEC), etc.

Related to QoS are the QoS performance parameters. Similar to the QoS mechanisms QoS parameters can be defined for different layers. At the network layer those parameters usually include information loss rate and information delay and delay variations.

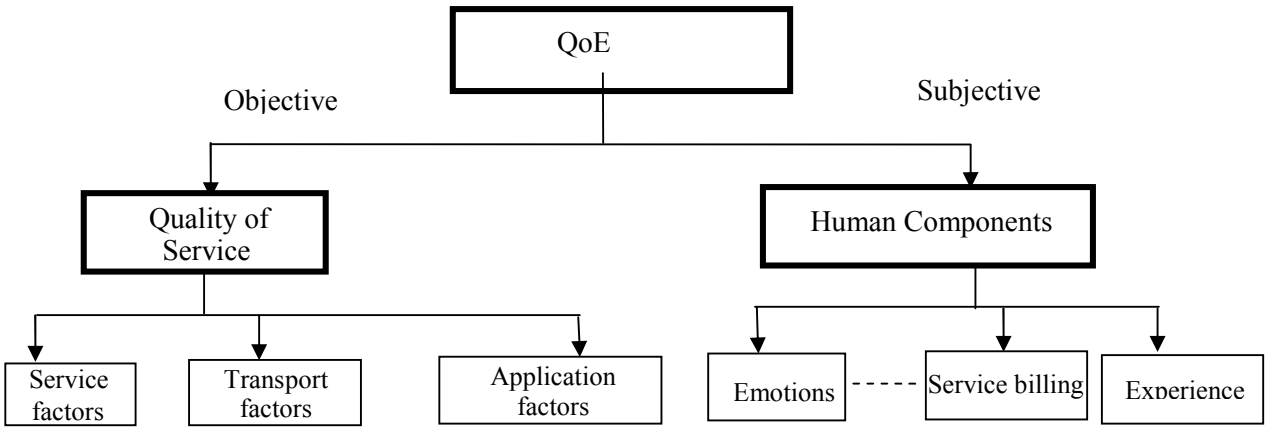


Figure 5-1: QoE Dimensions

In general there is correlation between the subjective QoE as measured by the MOS and various objective parameters of service performance (e.g. encoding bit rate, packet loss, delay, availability, etc.).

Typically there will be multiple service level performance (QoS) metrics that impact overall QoE. The relation between QoE and service performance (QoS) metrics is typically derived empirically. Having identified the QoE/QoS relationship, it can be used in two ways:

a) Given a QoS measurement, one could predict the expected QoE for a user

b) Given a target QoE for a user, one could deduce the net required service layer performance.

To ensure that the appropriate service quality is delivered, QoE targets should be established for each service and be included early on in system design and engineering processes where they are translated into objective service level performance metrics. Quality of Experience will be an important factor in the marketplace success of triple-play services and is expected to be a key differentiator with respect to competing service offerings. Subscribers to network services do not care how service quality is achieved. What matters to them is how well a service meets their expectations for effectiveness, operability, availability, and ease of use.

6 QoE for video and audio[1]

QoE requirements for video and audio may be defined by the subjective QoE scales such as the Mean Opinion Score (MOS) and Double Stimulus Continuous Quality Scale (DSCQS) [ITU-R BT.500-11]. However, conducting subjective tests is difficult for most IPTV service providers because they are time consuming and expensive. Moreover, reliable objective quality assessment methods have not been established for video and audio transmitted. Therefore, this clause provides provisional QoE requirements on the basis of the objective parameters that are correlated to the subjective QoE. QoE targets listed in the Tables in this section should be updated according to the advances in coding technologies.

---

[1] Much of this material comes from [DSLF TR-126]

6.1 Requirements for media compression and synchronization

One of the main components of QoE for video and audio is digitization and compression of video and audio source materials and the various settings and parameters selected. Since video compression schemes such as MPEG are lossy and an identical copy of the original cannot be recovered, there are potentially negative impacts on video picture quality and therefore on viewer QoE. The main factors influencing video QoE at the application layer due to compression are:

- Quality of source material
  - "garbage in = garbage out"
- The baseline quality (no network impairments) of the codec standard used
  - There are a range of video codecs available, but typically television applications will use one of the following: MPEG-2, MPEG-4 AVC (also known as MPEG-4 Part 10 or H.264), SMPTE VC-1 (previously known as VC-9, the standardized version of Windows Media™ 9), and AVS.
- Resolution
  - Some systems reduce the horizontal resolution to achieve the target bit rates, for example in standard definition television (SDTV) the resolution maybe reduced to "Half" or "Three Quarters" which produces a less sharp picture than "Full" resolution.
- Bit rate
  - During periods of high complexity (entropy) compression may leave visible artefacts if the bit rate is not sufficient.
- Application layer video encoding – Constant Bit Rate (CBR) vs. Variable Bit Rate (VBR) at the encoder output
  - Video encoding is naturally variable bit rate but to simplify network engineering for Telco delivery systems, the video encoders are set to provide a constant bit rate (as averaged over some specified time period on the order of seconds).
  - VBR streams such as those used in DVD encoding have constant quality since the bit rate is allowed to vary to accommodate varying complexity of the source material.
  - CBR streams have variable quality since there may be times when the bit rate is insufficient to accommodate the video complexity but CBR steams enable more straightforward traffic engineering and system design.
- Group of Pictures (GOP) structure
  - Shorter GOPs improve quality in terms of performance of random accessibility and error recovery, but reduce the maximum compression ratio.
  - Longer GOPs improve maximum compression ratio, but increase channel change time and the amount of damage a lost packet will cause.
  - Dynamic GOPs can be used to better handle scene changes and other effects but are not always implemented on STBs. In addition, dynamic GOPs can impact the variability of zapping latency and may complicate mechanisms to increase zapping speed considerably.
- Motion vector search range
  - Wider searches provide improved quality but at increased complexity and encoder delay.
  - Large search ranges are required for high motion content such as sports.
- Rate control
  - Mode decisions greatly affect the bit rate.
  - Proprietary schemes are commonly used to gain competitive advantage.

- Pre-processing (such as noise reduction)
  - usually proprietary and non-standard but can improve bit rate/quality trade-off.
- Tandem encoding and rate shaping (e.g. digital turnaround)

Video Compression Artefact Examples

Figure 6-1 illustrates several kinds of compression artefacts that are largely due to insufficient bits allocated resulting in too coarse quantization of DCT coefficients or motion vectors and/or otherwise poor motion estimation. Addition details of compression artefacts may be found in [NTIA264].

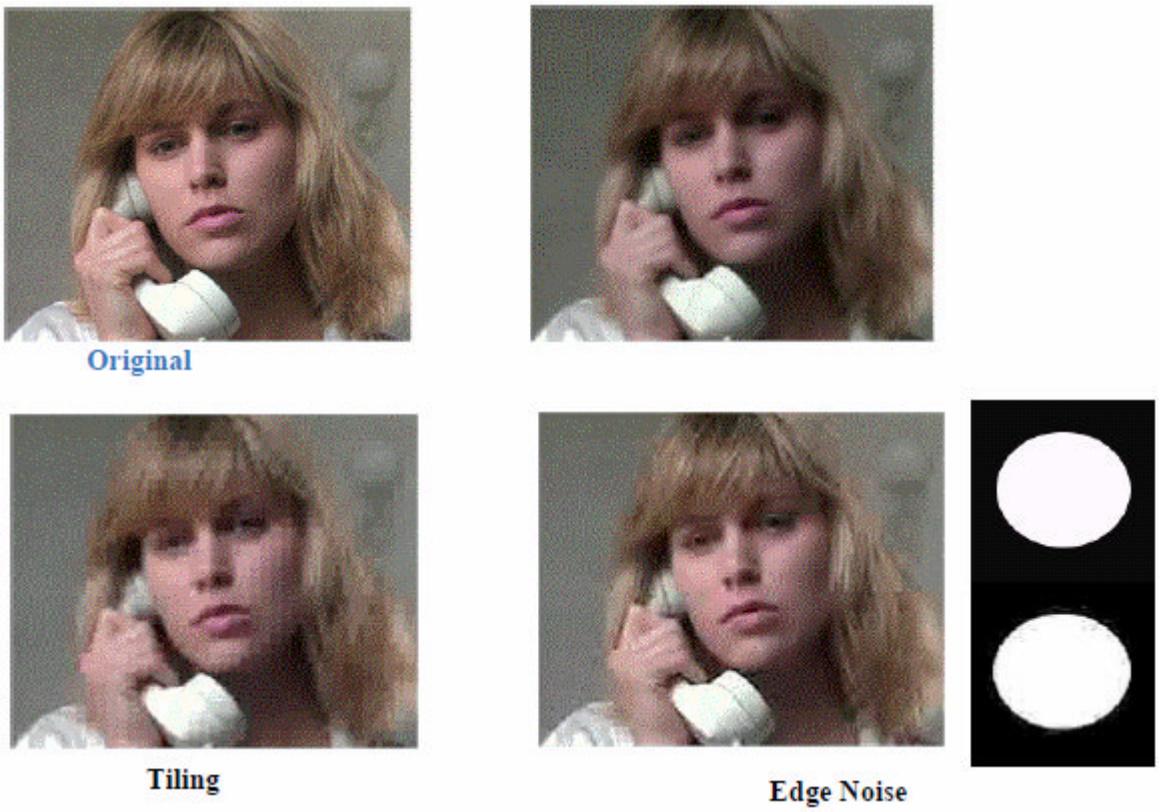


Figure 6-1: Compression Artefacts [ITS Video Quality Research (2003)]

Similarly, there are multiple choices of audio codecs and similar parameter implications on the audio side. Most video service offerings (e.g. those using MPEG Transport Streams or similar) are capable of supporting more than one audio codec along with a single or sometimes multiple video encoding schemes depending on the headend equipment and Set-top box. Commonly used audio formats for television applications include MPEG Layer II (also known as Musicam used in DVB systems, and MPEG-1, Audio Layer 2), Dolby Digital used in ATSC systems (formerly known as AC-3), NICAM 728 (European digital format for PAL), Advance Audio Coding – AAC (either MPEG-2 AAC or MPEG-4 AAC ([ISO/IEC 14496-3], Subpart 4)), and sometimes other formats such as MP-3 (MPEG-1 Audio Layer 3) will be used, particularly for music content.

In addition to the separate audio and video application layer impairments, the synchronization between audio and video components must be maintained to ensure satisfactory QoE. There has been a great deal of research on A/V synchronization requirements in video conferencing and analogue broadcast systems and specifications in such bodies as ITU-R [ITU-R BT.1359-1]. Because audio that appears before video is very unnatural (sound takes longer to propagate than light so sound lagging visual is normal) some bodies specifying television specific A/V synchronization have recommended tighter tolerances than typically used for video conferencing applications.

Recommended minimum engineering objectives for application layer, data plane parameters are presented in the following clauses for various video services. In general these parameters are guided by industry best practices (e.g. CableLabs specifications, encoder vendor guidelines), performance of competitive systems (e.g. cable, satellite benchmarks), telco deployment experiences, and the state of encoding technologies (e.g. MPEG-2, MPEG-4 AVC, VC-1, AVS, etc. commercial offerings) at the time of publication of this document. In the following tables, the Minimum Bit Rate for each codec is the target value for achieving sufficient quality. Not all of the codecs in the tables below may have achieved these targets as of the time of publication of this document.

6.1.1 Standard definition TV (SDTV): General minimum objectives

Table 6-1 lists the recommended minimum video application layer performance objectives at the MPEG level, prior to IP encapsulation for broadcast SDTV (480i/576i). The audio stream bit rates are additional and specified separately below. Assumptions include:

Source material:

- NTSC or PAL/SECAM
- 4:3 aspect ratio
- Source could enter the head end in analogue or digital form

Maximum Viewable Resolution:

- Horizontal × Vertical: 720 pixels × 480 lines (NTSC) [ITU-R BT.601-6] or 720 pixels × 576 lines (PAL)
- Lower resolutions (ex. ¾ Horizontal or ½ Horizontal – so-called ½ D1) could be used to ensure encoding quality is maintained for complex materials

Frame rate:

- 29.97 fps (NTSC) or 25 fps (PAL/SECAM)
- 23.97/24 fps may also be used for film-based materials (with 3:2 pulldown for NTSC conversion to 30 fps)
- Two interlaced fields per frame

Table 6-1: Recommended Minimum Application Layer Performance for Standard Definition Broadcast Program Sources

Video Codec standard	Minimum Bit Rate (video only)	Pre-processing Enabled
MPEG-2 – Main profile at Main level (MP@ML)	2.5 Mbit/s CBR	Yes (if available)
MPEG-4 AVC (Main profile at Level 3.0)	1.75 Mbit/s CBR	Yes (if available)
SMPTE VC-1	1.75 Mbit/s CBR	Yes (if available)
AVS	1.75 Mbit/s CBR	Yes (if available)

Notes on SDTV Video Bit Rate

The bit rates achieved by a particular video encoder undergo continuous improvement over time particularly when first introduced. As is the case with MPEG-2 since its commercialization in the mid-1990s, improvements have typically followed McCann's law that states encoder bit rate improves approximately 15% per year with the same quality [b_McCannLaw]. In most cases the encoder improvements are done within the scope of the existing standards and therefore do not require upgrades to the decoders.

The MPEG-2 bit rates shown in Table 6-1 are nearing the end of the improvement cycle and although one may run at lower bit rates (particularly with proprietary pre-processing), the values indicated are the minimum required to provide adequate quality over a range of broadcast program material complexity. Note that many competing services (e.g. digital cable and satellite) use higher MPEG-2 bit rates and often VBR encoding. Where access link bandwidth permits, service providers are encouraged to use higher bit rates, particularly for broadcast materials with highly complex image content, such as sports.

MPEG-4 AVC, SMPTE VC-1, and AVS codecs are newer (broadcast systems became commercially available in 2005 for SDTV and 2006 for HD) and are similarly expected to improve over time, although perhaps not aggressively as suggested by McCann's law of 15% per year. The recommended minimum bit rate values shown in Table 6-1 represent the state of commercially available encoders at present. Table 6-1 assumes similar quality/bit-rate performance of MPEG-4 AVC, VC-1, and AVS.

Table 6-2 lists the recommended minimum audio application layer performance guidelines for standard definition audio sources. Assumptions include:

Source material:

- NTSC or PAL/SECAM
- Sources could include more than one stereo audio track to support multiple languages or multichannel audio for surround sound effects. Unless indicated in Table 6-2, recommended minimum bit rates are for one stereo pair only

Audio channels:

- Most broadcast content is now in stereo (left/right)
- Many broadcasters are also using Dolby 5.1 (up to 6 channels) for primetime series and special events, particularly concerts and sporting events

Audio Sample Rate:

- 48 kHz sample rate for Dolby digital as per ATSC
- 16 kHz to 44.1 kHz for MP3
- 32 kHz, 44.1 kHz or 48 kHz for DVB source audio as per [ETSI TR 101 154]

Table 6-2: Recommended Minimum Audio Application Layer Performance for Standard Definition Sources

Audio Codec Standard	Number of Channels	Minimum Bit Rate (kbit/s)
MPEG Layer II	Mono or stereo	128 for stereo
Dolby Digital (AC-3)	5.1 if available, else left/right stereo pair	384 for 5.1/128 for stereo
AAC	Stereo	96 for stereo
MP3 (MPEG-1, Layer 3)	Stereo	128

In general, audio codecs chosen should align with industry standards in the geography of deployment to ensure maximum compatibility with consumer receivers. There is a general trend to global support of Dolby Digital 5.1, particularly in North America (ex. ATSC) and this is also an option for DVB-based systems. Bit rates should be aligned with original source material quality and transcoding between formats should be avoided if possible. An MP3 target is provided to support music services.

Table 6-3 lists the recommended audio-video synchronization requirements based on guidelines provide by the ATSC for SDTV program materials. Although these guideline were based on North American digital television they should apply equally well to formats in other geographies. Note the asymmetry in the requirement is due to the unnaturalness of audio leading video since light travels faster than sound.

Table 6-3: SDTV Audio – Video Synchronization Requirements

Audio – Video Synchronization	Audio Lead Video	Audio Lag Video
	15 ms maximum	45 ms maximum

Inconsistent loudness levels between channels can negatively impact QoE. It is recommended that equipment be used in the service provider head-end to ensure similar loudness levels across the range of channels provided to the user. Another audio quality issue beyond the scope of this document is the dynamic range compression for RF links between the STB and TV.

6.1.2 Standard definition (SD) TV: VoD and Premium Content Objectives

Video on demand (VoD) and other premium content such as pay per view in standard definition format will have similar application layer performance factors as regular broadcast materials. However, subscriber expectation may be higher because of additional fees paid to access the content and comparison to alternative delivery options. In the case of VoD, users may compare to VoD materials delivered over digital cable systems or even DVDs.

In North America, VoD application layer parameters are defined by Cable Labs [CLVoD2]. Since a great deal of existing VoD content is aligned with the parameters used by cable providers and consumers will compare the quality levels, it is recommended that telco-based video service providers adopt these as the minimum guidelines. The current guidelines are limited to MPEG-2 encoding. Recommendations for MPEG-4, AVC, VC-1, or AVS encoded VoD materials assume a 1.5x improvement in bit rate, aligned with the state of commercial deployments of these encoders. Table 6-4 lists the recommended video encoding bit rates for standard definition, VoD and other premium content and underlying assumptions below.

Source material:

- NTSC or PAL/SECAM
- 4:3 aspect ratio
- Encoding could be done offline using multipass systems for stored content such as VoD assets

Minimum Viewable Resolution:

- Horizontal × Vertical: 1/2 D1 352 pixels × 480 lines (NTSC) [ITU-R BT.601-6] or 352 pixels × 576 lines (PAL/SECAM) is permitted to ensure encoding quality is maintained for complex materials
- However, it's recommended that ¾ D1 resolution (528x480/528x576) be used where possible to align with the maximum specified for cable systems
- Telco service providers could run VoD assets at full D1 resolutions but would likely not be able to re-use assets pre-encoded for cable deployments

Frame rate:

- 29.97 fps (NTSC) or 25 fps (PAL/SECAM)
- 23.97 fps may also be used for film-based materials (with 3:2 pulldown for NTSC conversion to 30 fps)
- Two interlaced fields per frame

Table 6-4: Recommended Minimum Application Layer Performance for Standard Definition VoD and Premium Program Sources

Video Codec standard	Minimum Bit Rate (video only)	Pre-processing Enabled
MPEG-2 – Main profile at Main level (MP@ML)	3.18 Mbit/s CBR	Yes (if available)
MPEG-4 AVC (Main profile at Level 3)	2.1 Mbit/s CBR	Yes (if available)
SMPTE VC-1	2.1 Mbit/s CBR	Yes (if available)
AVS	2.1 Mbits/s CBR	Yes (if available)

Notes on SDTV Video Bit Rate for VoD and Premium Content

- Bit rates for MPEG-2 is as per Cable Labs® maximum for VoD content and aligns with the majority of VoD assets available
- AVC, VC-1, and AVS bit rates are extrapolated from MPEG-2 using a 1.5x factor
- These guidelines are recommended minimums. Telco service providers are encouraged to use higher resolutions and bit rates where possible/practical for better quality
- Total video plus audio bit rate for most commonly available MPEG-2 encoded VoD assets is 3.75 Mbits/s
- The QoE of a VoD service may also be impacted by the quality of the implementation of trick mode features such as fast forward and rewind. The fast forward and rewind modes should be as smooth as possible and include intelligible audio during trick modes if possible.

Table 6-5 lists the recommended audio codec and bit rates for VoD and premium content. The bit rates assume a sampling rate of 48 kHz.

Table 6-5: Recommended Minimum Audio Application Layer Performance for VoD and Premium Standard Definition Materials

Audio Codec Standard	Number of Channels	Minimum Bit Rate (kbit/s)
Dolby Digital (AC-3)	5.1 if available, else left/right stereo pair	384 for 5.1/192 for stereo

6.1.3 High definition TV (HDTV): Objectives

Table 6-6 lists the recommended minimum video application layer performance objectives for broadcast HDTV (720p/1080i). Assumptions include:

Source material:

- ATSC or DVB
- 16:9 aspect ratio
- Source enters the head end in digital form

Resolution and Frame rate:

- 720p60 (ex. SMPTE 296M) or 720p50 (DVB)
  - Horizontal × Vertical: 1280 pixels × 720 lines
  - 50, 59.94, 60 progressive scan frames per second
- 1080i60 (ex. SMPTE 274M) or 1080i50 (DVB)
  - Horizontal × Vertical: 1920 pixels × 1080 lines
  - 29.97 (59.94i), 30 (60i) interlaced frames per second, two fields per frame

Table 6-6: Recommended Minimum Application Layer Performance for High Definition (HD) Broadcast Program Sources

Video Codec standard	Minimum Bit Rate (video only)	Pre-processing Enabled
MPEG-2 – Main profile at Main level (MP@ML)	15 Mbit/s CBR	Yes (if available)
MPEG-4 AVC (Main profile at Level 4)	10 Mbit/s CBR	Yes (if available)
SMPTE VC-1	10 Mbit/s CBR	Yes (if available)
AVS	10 Mbits/s CBR	Yes (if available)

Notes on HDTV Video Bit Rate

Bit rates for video encoding and corresponding decoders undergo continuous improvement over time particularly when first introduced. As with SDTV, improvements have typically followed McCann's law [b_McCannLaw].

The MPEG-2 bit rates shown in Table 6-6 are nearing the end of the improvement cycle and although one may run at lower bit rates (particularly with proprietary pre-processing), the values indicated are the minimum required to provide adequate quality over a range of broadcast program material complexity. It should be noted that many competing services (ex. digital cable and satellite) use higher MPEG-2 bit rates and often VBR encoding. If access link bandwidth is available, service providers are strongly encouraged to use higher bit rates and/or VBR encoding for HDTV, particularly for complex broadcast materials such as sports.

MPEG-4 AVC, SMPTE VC-1, and AVS codecs are newer (broadcast systems commercially available in 2005) and are expected to improve significantly over time. The recommended minimum bit rate values shown in Table 6-6 represent the state of commercially available encoders at the time of publication but lower bit rates with satisfactory quality are expected as encoder technology improves. MPEG-4 AVC Main Profile is listed in Table 6-6, but as High Profile encoders and compatible STBs become available, service providers may choose to take advantage of superior features available for HDTV encoding in the High Profile. Table 6-6 also assumes similar quality/bit rate performance of MPEG-4 AVC, VC-1, and AVS.

Table 6-7 lists the recommended minimum audio application layer performance guidelines for high definition audio sources, guided by industry best practices, performance of competitive systems (ex. cable, satellite), telco deployment experiences, and the state encoding technologies at the time of publication of this document. Assumptions include:

Source material:

- ATSC or DVB
- Sources could include more than one audio track to support multiple languages
- For HDTV materials multichannel audio for surround sound effects should be provided where possible

Audio channels:

- Many broadcasters are also using Dolby 5.1 for primetime series and special events, particularly concerts and sporting events

Audio Sample Rate:

- 48 kHz sample rate for Dolby digital as per ATSC
- 16 kHz to 44.1 kHz for MP3
- 32 kHz, 44.1 kHz or 48 kHz for DVB source audio as per [ETSI TR 101 154]

Table 6-7: Recommended Minimum Audio Application Layer Performance for High Definition Sources

Audio Codec standard	Number of Channels	Minimum Bit Rate (kbit/s)
MPEG Layer II	Mono or stereo	128 for stereo
Dolby Digital (AC-3)	5.1 if available, else left/right stereo pair	384 for 5.1 / 128 for stereo
AAC	Stereo	96 for stereo
MP3 (MPEG-1, Layer 3)	Stereo	128

Notes on HDTV Audio Bit Rate

In general, audio codecs chosen should align with industry standards in the geography of deployment to ensure maximum compatibility with consumer receivers. There is a general trend to global support of Dolby Digital 5.1, particularly in North America (e.g., ATSC) and this is also an option for DVB-based systems. Bit rates should be aligned with original source material quality and transcoding between formats should be avoided if possible. An MP3 target is included to support music services.

A/V synchronization requirements for HDTV materials is currently under study the ATSC and other bodies, Until additional data is available, the guidelines presented in Table 6-3 for SDTV materials should be followed for HDTV materials as well.

6.2 Requirements for network transmission

Key criteria for network transmission include loss, latency and jitter (see Appendix I). In general, reasonable end-to-end delay and jitter values are not problematic due to STB de-jitter buffers, provided the de-jitter buffer size is provisioned to match network and video element performance. Video streams however are highly sensitive to information loss and the QoE impact is in turn correlated to a number of variables including:

- Highly dependent on type of data lost
  - System information and header losses produce different impairments
  - Lost data from I and P frames produce different impairments than B frame packet losses due to temporal error propagation
- Dependent on codec used
- Dependent on transport stream packetization used
- Loss distance and loss profile
- With high encoding bit rates, the stream is more vulnerable to packet loss impairments
  - For the same packet loss ratio, impairments due to loss on a higher rate video stream occur more frequently (i.e., there are more visible errors per unit time) simply because there are more packets per second transmitted and each one has the same probability to be affected
- Decoder concealment algorithms can mitigate perceptual impact of some losses.

An error or sequence of errors in a video bit stream can cause effects ranging from no noticeable audio or video impact to the user to complete loss of the video or audio signal depending on what was lost and the robustness of the implementation. Figure 6-2 shows an example of the impact of a single lost IP packet (containing seven MPEG-2 packets) on a video frame if the lost information is from a B or an I frame. As indicated, since the I frame is a key frame used in the compression of subsequent P and B frames, the I frame

impairment propagates in time across 14 frames of video or almost a half second (assuming 33 ms per frame). If the lost packet impacted a B frame, the impairment impacted only that frame with duration of 33 ms. Note that no loss concealment algorithms were running at the decoder.

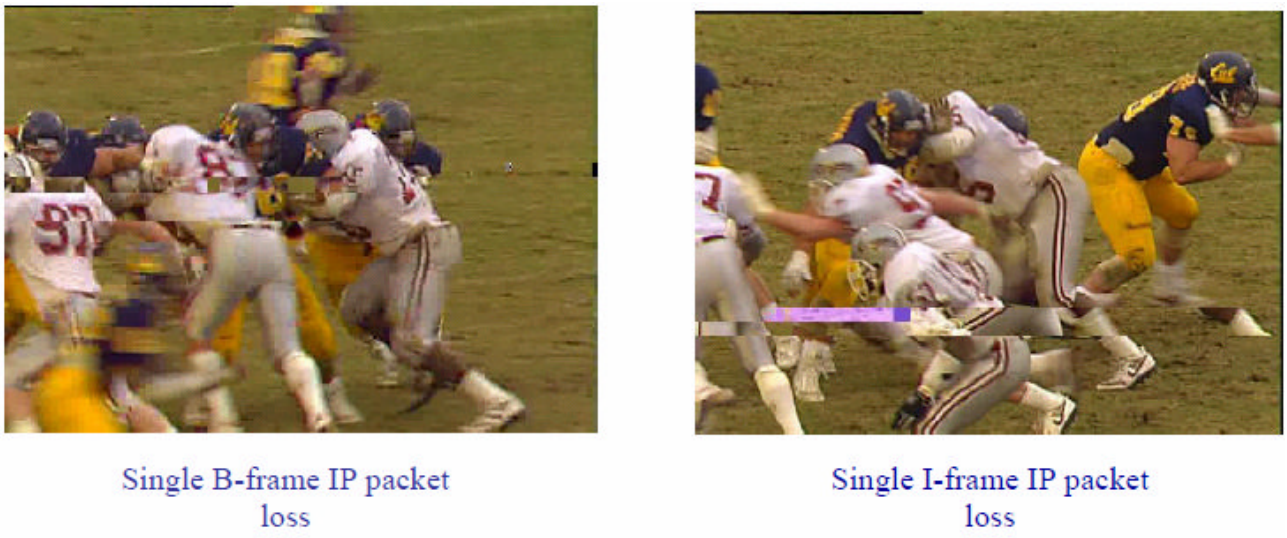


Figure 6-2: Impact of Single IP Packet Loss (B Frame and I Frame)

The following tables show IP packet transport loss and jitter requirements to achieve satisfactory service quality targets.

Network latency and jitter should be engineered to closely align with Set-top box jitter buffer provisioning (wait time and buffer size) and overall network design and therefore may vary from implementation to implementation. Typical Set-top box de-jitter buffers can store 100-500 ms (of SDTV) video, so network jitter must be within these limits and delay variation beyond these limits will manifest itself as loss. Increasing buffering also negatively impacts channel change latency so ideally the de-jitter buffers should be set as small as possible. Objectives outlined for jitter are based on experiences of operators and STB buffering capabilities.

Packet loss objectives are stated in terms of loss period and loss distance as defined in [b_IETF RFC3357] One-way Loss Pattern Sample Metrics. Essentially loss distance is a measure of the spacing between consecutive network packet loss or error events; a loss period is the duration of a loss or error event (e.g. and how many packets are lost in that duration). The loss rates in the tables below are objectives designed to ensure satisfactory end user service level quality assuming no or minimal loss concealment. If the network infrastructure performance is below the required levels, service providers may make use of network level techniques (e.g. interleaving and FEC) and application layer mechanisms (e.g. loss concealment, application layer FEC, Automatic Repeat Request (ARQ)) as outlined in Appendix II to [DSLF TR126] – Error Protection Mechanisms Overview to achieve the required performance levels. In addition, the use of these techniques may provide an improved quality of experience over competing service offers.

Ideally the maximum loss period would correspond to one IP packet since even a single lost packet can result in a very noticeable impairment as shown in Figure 6-2. However, to account for possible use in a xDSL environment, including loop impairment behaviour and FEC techniques available at the xDSL physical layer (RS, interleaving), we consider a loss period greater than a single packet.

Often random bit errors or minor amounts of congestion cause an isolated loss event with a loss period of one packet. DSL errors are different; interleaved Reed Solomon FEC codes are typically used at the DSL physical layer, and when these are overwhelmed by powerful impulse noise it causes an uncorrectable error at the output of the DSL decoder with a loss period greater than a single packet. Uncorrectable DSL errors typically wipe out an entire block of length equal to the interleaver depth.

A common configuration for DSL is an interleaver depth (i.e. FEC block duration) of 8 or 16 milliseconds. The corresponding loss period will therefore be 8 or 16 ms. Depending on the video bit rate this will correspond to a different number of lost video IP packets.

The recommended loss period is specified as less than 16 ms, which provides a balance between interleaver depth protection from impulse noise induced xDSL errors, delay added to other applications and video service QoE requirements to reduce visible impairments to on average one per 60 minutes for SDTV resolution video streams. The loss period will result in different numbers of packets being lost, depending on bit rate of the video stream as shown in the following tables. This maximum loss period objective is provisionally set until further studies allow better tuning of the maximum loss period allowed, in a xDSL environment considering all DSL variants, protection mechanisms, and optimum settings.

For DSL access cases, DSL modem resynchronization events imply a packet loss outage duration on the order of 10-20 seconds. An IPTV system would not be expected to maintain normal service through such an event. Such events might be considered a service outage rather than a quality defect.

The video application should be able to operate normally in the presence of normal operational defects. One such normal operational consideration is the operation of protection switching mechanisms in the network. SONET/SDH protection switching mechanisms may result in a potential packet loss duration on the order of 50 ms. For some other protection mechanisms (e.g. MPLS fast reroute, fast IGP convergence) the potential packet loss duration can be longer, on the order of 250 ms. Service providers are encouraged to add mechanisms to minimize or eliminate the visible effect of such protection mechanisms as these events cascade to a large number of subscribers.

Considering some other protection mechanisms the potential packet loss duration can be longer. For example, a complete reconvergence of the IP (IGP) routing table would imply potential packet loss bursts on the order of 30 sec. An IPTV system would not be expected to maintain normal service through such an event. Such events can be considered a service outage rather than an in service quality defect.

All impairments are specified as end-to-end objectives (from video origin to the video output of set-top box to the television including any loss correction mechanisms that may be applied at network or application layers).

- Loss Distance of error events should be limited to at most one per 60 minutes for SDTV materials and one per 4 hours for HD. Error event is defined as a loss or corruption of a group of a small number of IP packets each containing up to seven MPEG packets of 188 bytes in length.
- There should be sufficient noise margin in the xDSL link to combat line noise and enough FEC interleaver depth to combat impulse noise in order to achieve required BER to achieve the packet loss objectives, without undue degradation for other services.
- Set-top box decoders should employ error concealment techniques to minimize impact of loss or corrupted video packets.
- Appendix II to [DSLF TR126] Error Protection Mechanisms Overview provides additional details on access BER, FEC and ARQ mechanisms.

The goal is to minimize visible artefacts to as few as possible using a combination of network performance requirements, loss recovery mechanisms (e.g. FEC, interleaver) and loss mitigation mechanisms (e.g. decoder loss concealment).

6.2.1 Standard Definition Video: Broadcast TV Transport Layer Performance Objectives

Assumptions for Table 6-8 below:

- MPEG-2 codec
- MPEG-2 transport stream
- seven 188-byte packets per IP packet

- no or minimal loss concealment (tolerable loss rates may be higher depending on degree and quality of STB loss concealment)
- encoder output to after any application layer protection mechanisms at the customer premises
- metrics are for the IP flows containing video streams only, IP streams for other applications may have different performance requirements

Table 6-8: Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-2 encoded SDTV Services

Transport stream bit rate (Mbit/s)	Latency	Jitter	Maximum duration of a single error	Corresponding Loss Period in IP packets	Loss Distance	Corresponding Average IP Video Stream Packet Loss Rate
3.0	<200 ms	<50 ms	<= 16 ms	6 IP packets	1 error event per hour	<= 5.85E-06
3.75	<200 ms	<50 ms	<= 16 ms	7 IP packets	1 error event per hour	<= 5.46E-06
5.0	<200 ms	<50 ms	<= 16 ms	9 IP packets	1 error event per hour	<= 5.26E-06

Table 6-9 lists the QoE performance objectives for MPEG-4 AVC or VC-1 encoded standard definition video materials. Assumptions for Table 6-9:

- MPEG-4 AVC or VC-1 codec
- MPEG-2 transport stream with seven 188-byte packets per IP packet
- no or minimal loss concealment (tolerable loss rates may be higher depending on degree and quality of STB loss concealment)
- metrics are end-to-end from head-end encoder output to after any application layer protection mechanisms at the customer premises
- metrics are for the IP flows containing video streams only, IP streams for other applications may have different performance requirement

Table 6-9: Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded SDTV Services

Transport stream bit rate (Mbit/s)	Latency	Jitter	Maximum duration of a single error	Corresponding Loss Period in IP packets	Loss Distance	Corresponding Average IP Video Stream Packet Loss Rate
1.75	<200 ms	<50 ms	<= 16 ms	4 IP packets	1 error event per hour	<= 6.68E-06
2.0	<200 ms	<50 ms	<= 16 ms	5 IP packets	1 error event per hour	<= 7.31E-06
2.5	<200 ms	<50 ms	<= 16 ms	5 IP packets	1 error event per hour	<= 5.85E-06
3.0	<200 ms	<50 ms	<= 16 ms	6 IP packets	1 error event per hour	<= 5.85E-06

6.2.2 Standard Definition Video: VoD and Premium Content Transport Layer Performance Objectives

The requirements for network performance of broadcast SDTV applications listed above should be followed for VoD and premium content services also.

6.2.3 High Definition TV: Transport Layer Performance Objectives

It is commonly agreed upon that ideally HDTV services meet a criterion of one visible impairment event per 12 hours or better. In the remainder of this section, we propose a value of four hours as the minimum Loss Distance for HDTV services, assuming that not all errors will result in a visible impairment, because:

- loss of B-frame information is sometimes below threshold of notability
- error concealment will be used with HDTV decoders

Table 6-10 below shows the loss period and loss distance for MPEG-2 HDTV under the following assumptions:

- MPEG-2 codec
- MPEG-2 transport stream with seven 188-byte packets per IP packet
- STB has some level of loss concealment
- encoder output to after any application layer protection mechanisms at the customer premises
- metrics are for the IP flows containing video streams only, IP streams for other applications may have different performance requirements

Table 6-10: Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-2 encoded HDTV Services

Transport stream bit rate (Mbit/s)	Latency	Jitter	Maximum duration of a single error	Corresponding Loss Period in IP packets	Loss Distance	Corresponding Average IP Video Stream Packet Loss Rate
15.0	<200 ms	<50 ms	<= 16 ms	24 IP packets	1 error event per 4 hours	<= 1.17E-06
17	<200 ms	<50 ms	<= 16 ms	27 IP packets	1 error event per 4 hours	<= 1.16E-06
18.1	<200 ms	<50 ms	<= 16 ms	29 IP packets	1 error event per 4 hours	<= 1.17E-06

Table 6-11 lists the QoE performance requirements for MPEG-4 AVC or VC-1 encoded high definition video materials.

Assumptions for Table 6-11 below:

- MPEG-4 AVC, VC-1, or AVS codec,
- MPEG-2 transport stream with seven 188-byte packets per IP packet
- STB has some level of loss concealment
- encoder output to after any application layer protection mechanisms at the customer premises
- metrics are for the IP flows containing video streams only, IP streams for other applications may have different performance requirements

Table 6-11: Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services

Transport stream bit rate (Mbit/s)	Latency	Jitter	Maximum duration of a single error	Corresponding Loss Period in IP packets	Loss Distance	Corresponding Average IP Video Stream Packet Loss Rate
8	<200 ms	<50 ms	<= 16 ms	14 IP packets	1 error event per 4 hours	<= 1.28E-06
10	<200 ms	<50 ms	<= 16 ms	17 IP packets	1 error event per 4 hours	<= 1.24E-06
12	<200 ms	<50 ms	<= 16 ms	20 IP packets	1 error event per 4 hours	<= 1.22E-06

The PLR in the range of 10^{-6} recommended for video services may require special error control techniques to achieve the target. Appendix II of [DSLF TR126] and [ITU-T FG IPTV ALERM] provide additional details on network BER, FEC performance and mitigation options.

6.3 Network Layer Performance Objectives

The network layer performance objectives are summarized in the figures below. Figure 6-3 shows packet loss ratios as a function of bit rate and time between uncorrected loss events for isolated packet loss events. Points from Table 6-8 and Table 6-9 are plotted as representative of SDTV video with a loss distance of one hour between packet loss events.

Points from Table 6-10 and Table 6-11 are plotted as representative of HDTV video with a loss distance of 4 hours between packet loss events. The figure assumes that each IP packet carries 7 MPEG data packets, each 188 bytes long. The plots implicitly assume that error statistics are stationary and time invariant.

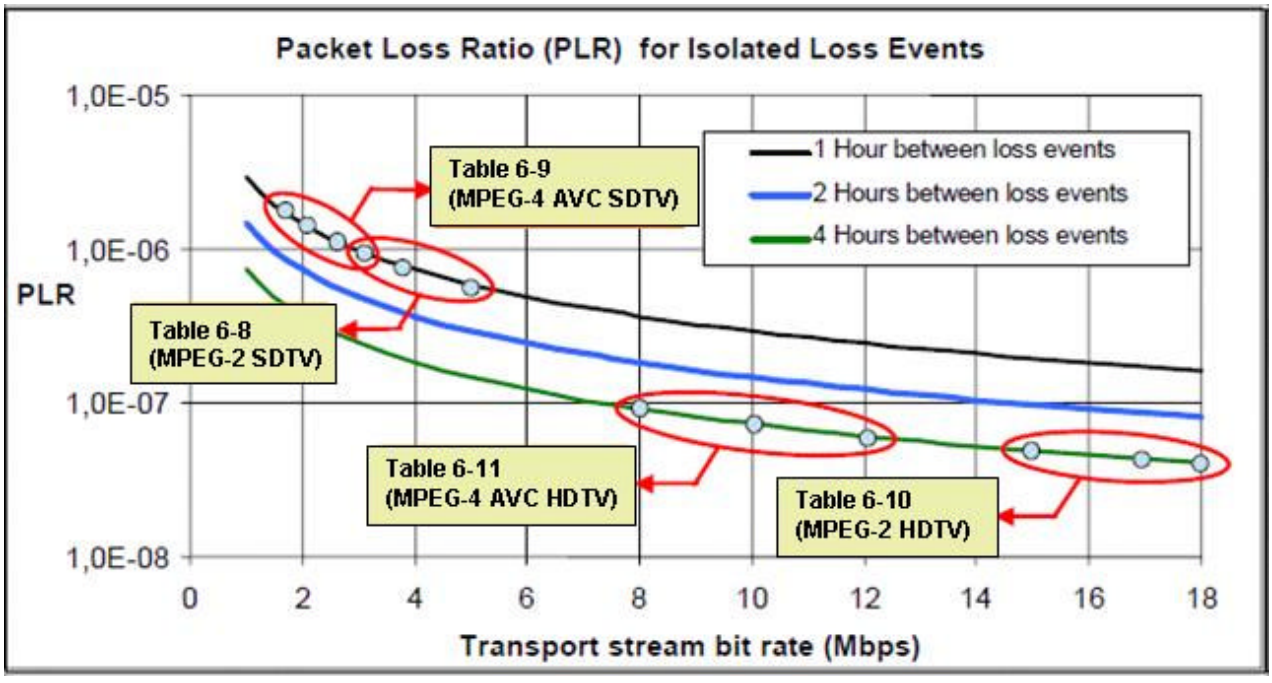


Figure 6-3: PLR required to meet average time between loss events of 1, 2 and 4 hours assuming isolated lost packets

Figure 6-4 and Figure 6-5 show packet loss ratios as a function of bit rate and time between uncorrected loss events for typical DSL burst loss events of 8 ms and 16 ms, respectively. The "ripple effect" in the charts is the result of rounding to an integer number of lost/corrupted IP packets. For example, 8 ms of lost video data in an MPEG-2 transport stream at a bit rate of 3 Mbits/s:

Total MPEG packets per second = 3 Mbit/s/8 bits per byte/188 bytes per MPEG packet

= 1994.7 MPEG packets per second

Total IP packets per second = 1994.7/7 MPEG packets per IP packet

= 285 IP packets per second

A loss of 8 ms corresponds to = 285 IP packets per second * 0.008 seconds

= 2.28 IP packets lost.

Because an entire IP packet is lost if a part of a packet is lost, this is rounded to the next integer = 3 IP packets. And because the lost bytes are not necessarily aligned to IP packet boundaries, this would be further rounded to 4 IP packets.

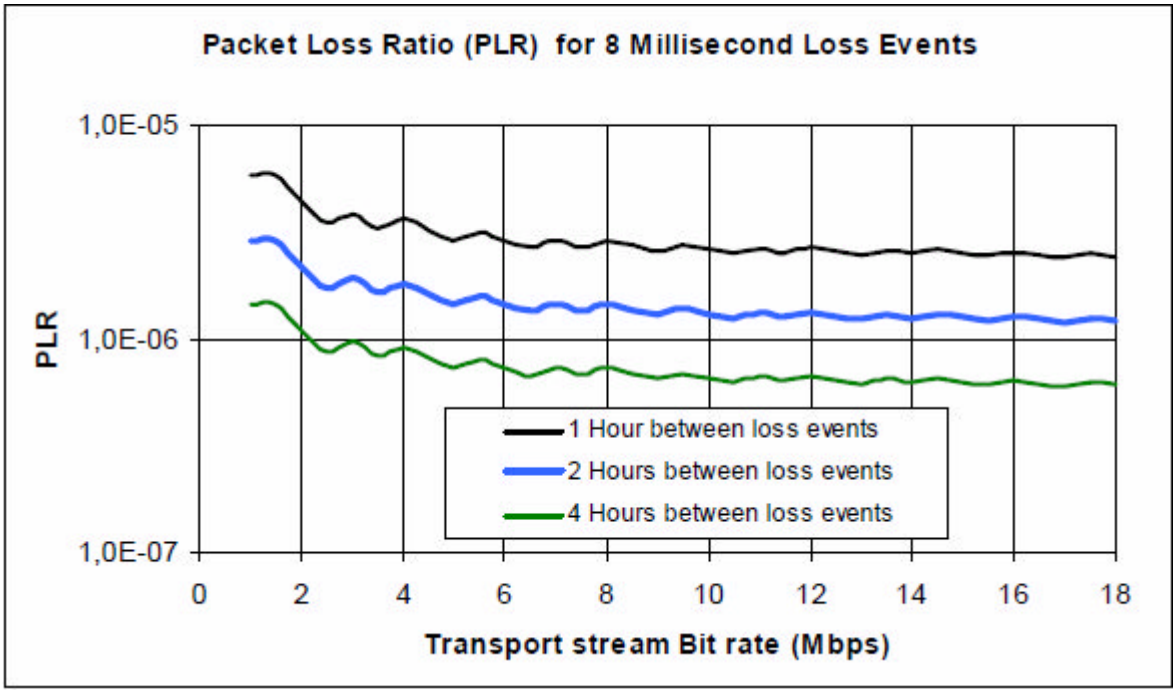


Figure 6-4: PLR required to meet average time between loss events of 1, 2, and 4 hours assuming each event is an uncorrectable DSL error that loses 8 milliseconds of contiguous data

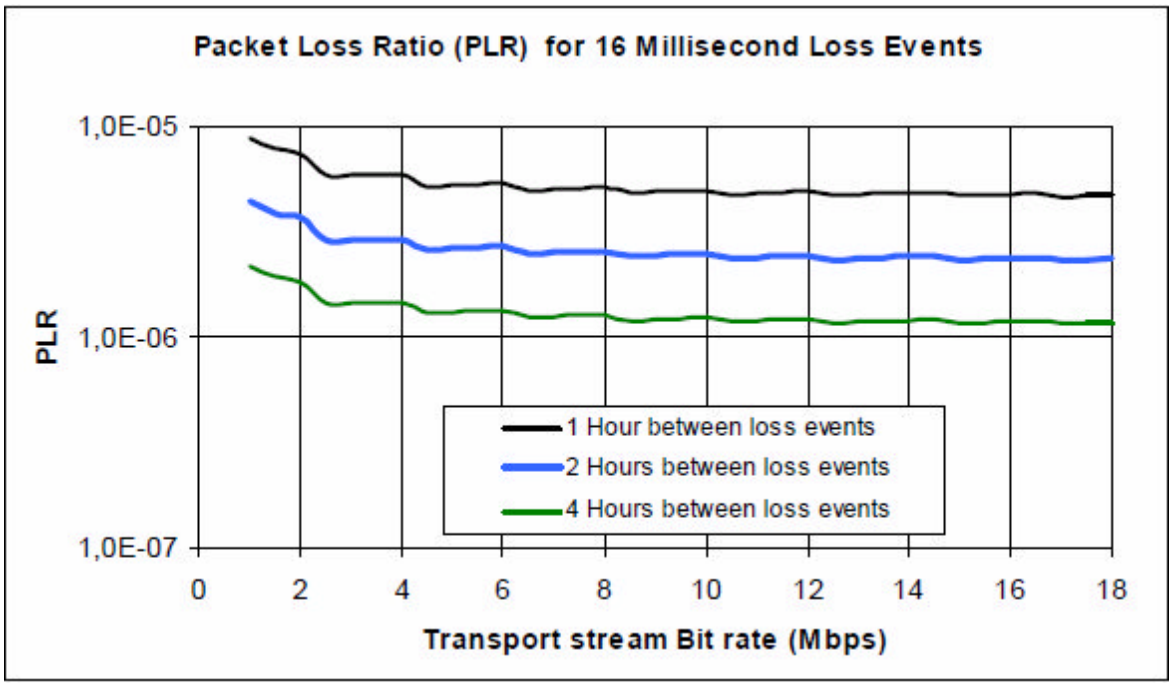


Figure 6-5: PLR required to meet average time between loss events of 1, 2, and 4 hours assuming each event is an uncorrectable DSL error that loses 16 milliseconds of contiguous data

Severe error limits for SDTV and HDTV services

In addition to average packet loss rates impacting picture/audio quality and availability metrics, it may also be advantageous to define a second set of limits on severe impairments. These limits would apply to quality degradations that fall between the impairments generated by the packet loss limits specified above and total service outage (i.e. black screen) metrics specified by the dependability metrics. These gross impairments could include video frame drops, frame repetitions (freeze frames), or short duration loss of intelligible audio or video or control (e.g. due to protection switching). Metrics are TBD based on industry input and could be specified by frequency of the error event per time unit – e.g., a maximum of one severe error per day and the duration of the impairment.

7 QoE for text and graphics

Information in this clause is taken from [ITU-T F.700].

7.1 Media component text

7.1.1 Definition

The media component text allows for the capture and representation of information, its transfer from originating user(s) to destination user(s), its presentation to human user(s), processing, filing and retrieval.

7.1.2 Description

7.1.2.1 General description

Text is a representation medium consisting of formatted characters. It is stored and transmitted as a sequence of codes. Although it may be displayed on the same screen as video and still pictures, it requires decoding into specific fonts for presentation to the user, whether on the screen or on paper. The input is through a keyboard. The output may be a printer or a screen.

The following levels of quality are defined:

T0: minimum quality, basic alphabet and punctuation, no formatting or choice of font;

T0 *bis*: videotex quality, basic alphabet and punctuation, basic graphic character set, no formatting or choice of font;

T1: Usable text conversation quality characterized by:

- Font support for [ISO-10646] Language area Latin-1 plus the target language area for the implementation.
- No more than 1 corrupted, dropped or marked missing character per 100.
- Delay from character input in the transmitter to display in the receiver shorter than 2 s.

T2: Good text conversation quality characterized by:

- Font support for all characters in [ISO-10646].
- No more than 1 corrupted, dropped or marked missing character per 500.
- Delay from character input in the transmitter to display in the receiver shorter than 1 s.

7.1.2.2 Additional facilities

The user may be given control over text through editing and presentation functions. He may also be able to insert graphics, still pictures or animated pictures within the text.

7.1.2.3 Requirements for various audiovisual services

When text is the support for conversational services, the timing aspects of text entry and display are critical. Text may be transmitted and displayed in near real time, as text is entered. It may also be transmitted only after specific end-of-sentence action or on a specific send request. In a conversation between two users, the near real-time conversation is important for optimized benefit of the conversation. For multi-user conferences, a sentence based transmission may be more relevant in an open discussion, while for a subtitled speech, the real-time text transmission is preferred.

For retrieval services, it may be accepted to transmit and display a whole page of text in one operation.

For conversation, editing may be reduced to "new line", "erase last character", while the editing for information retrieval should contain a possibility to replace text anywhere on the page and add various formatting effects to any part of text. Annotations that stand out distinctly are also desirable.

The levels of text quality required for various services are the following (marked by X):

Table 7-1: Levels of Text Requirements

Service	T0	T0 *bis*	T1	T2
Telex	X			
Videotex		X		
Text telephony			X	X
Total Conversation				X
Messaging services			X	X
Retrieval services			X	X

7.1.3 Quality aspects

The quality of text depends mainly upon the capabilities for formatting and using different types of fonts and special characters. When no error correction is made, for instance in conversation, text quality is also measured in terms of corrupted characters, dropped characters and characters replaced by the missing text marker [ITU-T T.140].

7.1.4 Intercommunication

The characters with their formatting may be decoded and assembled into bit maps which can then be handled as still pictures, e.g. as facsimile pages.

7.2 Media component graphics

7.2.1 Definition

The media component graphics allows for the capture and representation of information, its transfer from originating user(s) to destination user(s), its presentation to human user(s), processing, filing and retrieval. This media component allows graphic pictures to be captured and transmitted as geometrical objects whose positions, shapes and colours are coded so that they can be reproduced in a distant terminal.

7.2.2 Description

7.2.2.1 General description

Graphics is a representation medium consisting of geometrical objects featured by their positions, shapes and colours. It is stored and transmitted as a set of codes and parameters. Although it may be displayed on the same screen as video and still pictures, it requires decoding into specific geometrical figures for presentation to the user, whether on a screen or on paper.

The input may be through a graphics tablet, an electronic pencil, some other two-dimensional transducer or dedicated graphic software on a microcomputer or workstation. The output device may be a printer or a screen.

7.2.3 Quality aspects

The intrinsic quality of the graphic depends on the number and the complexity of the objects that can be generated, the precision of their dimensions and positions, the number of possible colours. The overall quality perceived by the user depends also on the resolution of the input and output systems.

7.2.4 Intercommunication

The graphic objects may be decoded and assembled into bit maps which can then be handled as still pictures.

8 QoE for control functions

8.1 QoE requirements for channel zapping time

Channel zapping time (channel switching time) has strong relationship with end user experience of service quality. Generally, it is primarily determined by the time required to have a proper frame at the STB to start decode processing for the new channel. Channel zapping requests can occur when

– Meta data request in EPG or IPG

– Random selecting channel by entering channel number using remote control

– Channel Up/Down button using remote control

– Channel Up/Down button using STB front panel

– Selecting a channel on IPG application menu

– Powering on STB/TV and tuning to initial channel assigned by IPG

As the QoE parameter, channel zapping time can be described by three components: IGMP delay, buffering delay, and decoding delay.

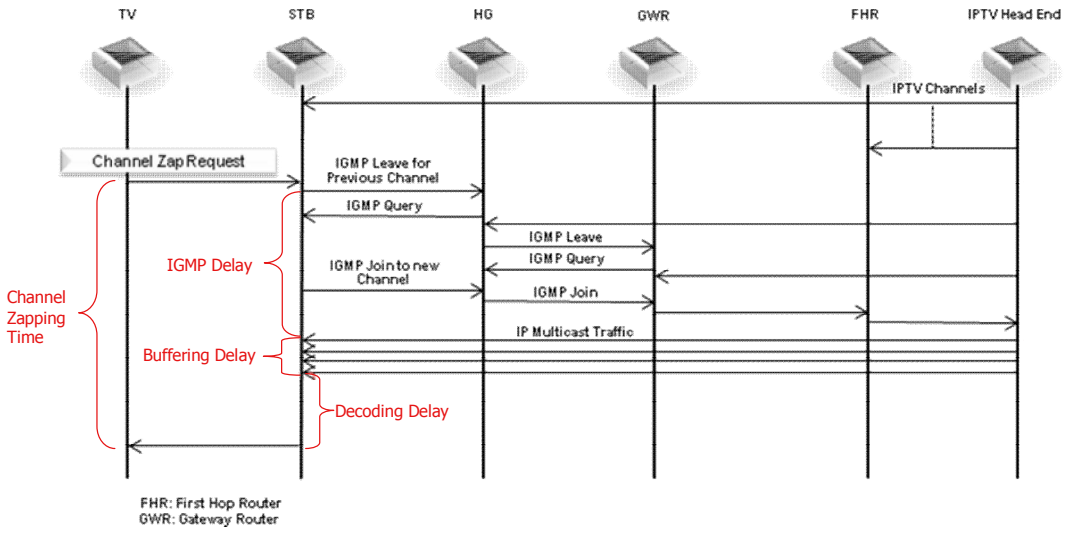


Figure 8-1: Components that contribute to Channel Zapping Time

8.1.1 Classification of channel zapping time

8.1.1.1 IGMP delay

A channel zap request is triggered by a channel change which is mapped by the STB to a multicast group address carried in the IGMP message. The IGMP message, which includes join message, is sent to the homegate (HG). The HG, playing an IGMP proxy role, will process the IGMP message and send an IGMP request to the Gateway Router (GWR). After the IGMP message is sent towards the rendezvous point by the GWR, the corresponding channel data should be delivered to the end point at some point. The time to get the content data after sending the first IGMP message is called the IGMP delay.

8.1.1.2 Buffering delay

While the STB receives IPTV multicast traffic, it stacks the packets in a buffer. Buffering delay is the time between the arrival of the first multicast traffic in the buffer and when the STB has sufficient data for playing to the screen.

8.1.1.3 Decoding delay

After STB starts to receive and buffers multicast stream, decoding delay processes buffered data and render them to TV screen. This type of delay includes both codec decoding delay, which intends to program-specific information frames in order to decide the target channel and I-frame acquisition delay, which is for reduction of bandwidth required for digital video transmission.

8.1.2 Requirements for channel zapping time

The IPTV architecture is recommended to support means to provide channel zapping with sufficient QoE.

The IPTV architecture is recommended to provide means to support flexible channel switching times as a trade off to improve efficiency.

Specific values are for further study.

8.2 QoE requirements VoD trick mode

Video on Demand (VoD) trick mode provides VCR-like features in VoD services. When a subscriber desires a video content through STB, the subscriber accesses the video content from the EPG which supports the contents-search engine to help access of content information. To guarantee VCR-like flexibility, this mode provides the trick ability to handle pause, play, rewind, fast forward, and stop entries for these control features.

8.2.1 Trick Latency

Correspondently, each control function (video selection, play, pause, rewind, FFW, stop) has its own delay. QoE metrics for VoD transaction quality are expressed by the following indicators:

– Video selection process delay: Timing period from the time when the subject is selected to the time when content is displayed.

– Play Delay: Timing period from the time when the Play entry was selected to the time the content is displayed.

– Stop Delay: Timing period from the time when the Stop play video entry was selected to the time the content is stopped playing as indicated by video content display.

– Rewind Delay: Timing period from the time when the Rewind video entry was selected to the time the rewind action is executed as indicated on display device.

– Pause Delay: Timing period from the time when the Pause video entry was selected to the time the pause action is executed as indicated on display device.

– FFW Delay: Timing period from the time when the Fast Forward video entry was selected to the time the FFW action is executed as indicated on display device.

8.2.2 Requirements for VoD Trick Features

From a QoE perspective, trick feature latency is one of the most important issues to guarantee satisfaction of subscribers. As each trick feature latency directly affects QoE, the latency is required to be sufficiently low to meet user's requirement for QoE relating to VoD trick features.

9 QoE for other IPTV services

9.1 QoE requirements for Metadata

Figure 9-1 shows the components of Metadata.

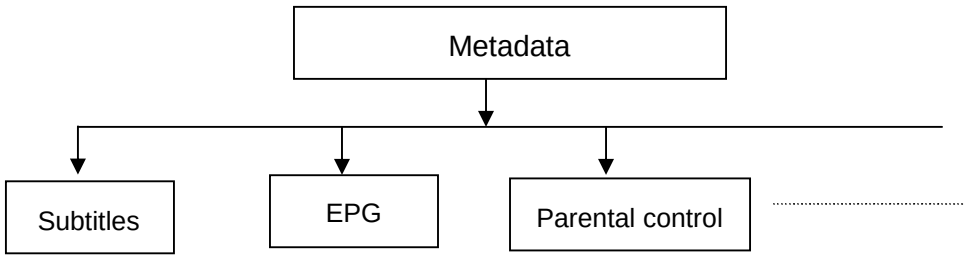


Figure 9-1: Components of Metadata

1) Availability

High availability is recommended to be ensured in transmitting the metadata on network.

2) Data size

Metadata is recommended to be transported in such a way that the size of the transported data would be sufficiently small, relative to such factors as the number of the total services, the number of the contents, and network bandwidth.

3) Correctness

The service provider should ensure the metadata tagged to a particular content is correct.

An example to illustrate the importance of metadata is the correctness of "rating" of content. The correct rating on content is directly related to what the customer expects. An incorrect parental rating e.g. a "family" rating for an adult movie can have serious implications for the customer experience and business of the service provider.

9.1.1 QoE requirements for EPG

The following items are recommended to be considered as part of the definition of QoE for IPTV services.

1) User-friendliness

EPG user interface is recommended to be designed for ease of use.

2) Response time to display EPG page

The response time – the interval from pushing the EPG button of remote control to the display of the EPG page – is recommended to be sufficiently short.

9.2 QoE requirements for Browser

If a browser, such as those for BML or HTML, is used to provide the user an interactive content from the service provider, the following points are recommended to be taken into account.

1) Characteristics of a television set

The IPTV QoE requirements on browsers are recommended to take into account that the behavioural patterns and expectations of television users typically differ from those of PC users.

Moreover the differences in the capacities of typical TVs (and STBs), on one hand, and PCs, on the other, should be taken into account. For example, as the CPU performance of a television set is usually inferior to that of PC, the contents designed for PC-use does not necessarily work in the TV environment, making it necessary to set up QoE measures taking into account the difference in CPU performance between PC and television. It should be stressed that the browser on an IPTV service may not have the same capacity as the browser on a PC has.

2) TV-like display

Some features of TV-like display is recommended to be considered necessary for browser QoE, for such are commonly imposed by content providers. Examples are:

- Overlay function,
- Consistency of displayed pictures across terminals.

3) Character size

The character size is recommended to be sufficiently large.

4) Navigation

The navigation function is recommended to be considered for increasing the level of convenience and operability.

5) Cookie

The use of Cookies is recommended to be done with care because of the possible limitation on the nonvolatile memory capacity of the terminal. The number, the size and the expiration date of cookies may need to be clearly specified.

9.3 QoE requirements for Content Navigation

Content navigation is defined as functions for contents discovery and selection. So, content navigation is provided by various methods such as direct channel selection, EPG, recommendation. QoE requirements according to navigation methods are described in the following sections.

9.3.1 Contents navigation by direct channel selection, by up/down button

Ease of contents selection, especially under numerous contents condition, is recommended to be considered. For that sake, the elapsed time for selecting contents and subjective evaluations of ease of use (e.g. MOS) are recommended to be considered.

9.3.2 Contents navigation by EPG/ECG

EPG/ECG is one of the most useful ways of contents navigation. The elapsed time for discovering and selecting contents, and subjective evaluations of ease of use (e.g. MOS) are recommended to be considered.

9.3.3 Contents navigation by contents recommendation

Effective contents recommendation is useful for users. For example, IPTV service provider recommends contents to the user according to his/her preferences. And, contents recommendation from his/her friends is also effective. The IPTV architecture is recommended to support 3rd parties' metadata for supporting contents recommendation [ITU-T FG IPTV REQ].

For contents recommendation, recommendation accuracy and security of personal information are recommended to be considered. If the recommended contents include many preferring contents, the QoE of recommendation would be high. Obviously, the security of personal information affects QoE. And communication function such as obtaining the 3rd parties' metadata is recommended to be considered.

10 Accessibility requirements

The intent of this section is to capture specific performance requirements for IPTV services related to accessibility. This is for further study, but will encompass the following areas:

- Audio quality (including the provision of clean audio)
- Video quality (including sufficient frame rate and resolution for sign language, lip reading, etc. [b_ITU-T HSup1])
- Audio/video synchronization

Appendix I

Network QoS parameters affecting QoE

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

In general, four main network segments – the content acquisition, encoding and play out, the core network, the access network, and the home network – constitute an IPTV service network.

The core network is an IP network that is usually well engineered to handle different classes of traffic. Well-engineered networks still require the ability to manage traffic belonging to different applications. Packets belong to real-time applications such as IPTV services should be transmitted before those that belong to non-real-time applications such as email and file transfer. This differentiation is usually achieved by employing IP differentiated service and its related traffic conditioning and per-hop behaviour (PHB) mechanisms. The IP network may also implement a subset of the IP performance classes as those defined in [ITU-T Y.1541].

The access network could be based on a range of technologies including Ethernet, WiMax, Wi-Fi, etc. The capacity of the access network is the limiting factor for the decision on how many channels are extended to the end user.

The home network includes a number of consumer electronic products that may be interconnected wirelessly using, for example, Wi-Fi products or via a wired network such as an Ethernet.

I.1 Transport Impairments

Transport impairments are usually characterized in terms of the packet delay and packet loss. This sub-clause defines these two performance parameters. Delay and loss objectives are for further study.

I.1.1 IP Packet Transfer Delay

The measured IP packet transfer delay (PTD) is defined as the elapsed time between a packet exit event at a measured point 1 (MP_1), e.g. at the head end, and the corresponding packet entry event at measurement point 2 (MP_2), e.g. at the Set-top box (STB) for a particular end user.

Two end-to-end delay parameters are considered:

- Packet delay variation (PDV) defined as the difference in the delays encountered by two packets of the same stream selected according to some selection function [IETF RFC 3393]. PDV is usually measure by the worst case delay variation as measured by the difference between the maximum and the minimum transfer delay experienced, i.e.

$$PDV = PTD\ max - PTD\ min$$

Other measurements are also possible [ITU-T Y.1541].

- Maximum Transfer Delay defined according to some quintile of the PTD distribution.

I.1.2 IP Packet Loss Ratio (PLR)

IP packet loss ratio (PLR) is defined as the ratio of the number of packets lost to the number transmitted.

PLR = Number of Packets lost/Number of Packets transmitted

PLR can be defined over a number of time scales. A time scale that is commonly used is over the duration of a session (e.g. a TV program). The long time scale may be useful for engineering purposes but it may not be useful to reflect video artefacts resulting from packet losses at shorter time scale. The time scales at which PLR is measured are for further study.

Packet loss impacts on video quality are related to the packet loss profile. It is recommended that video service packet loss objectives are stated in terms of loss period and loss distance as defined in [IETF RFC 3357] One-way Loss Pattern Sample Metrics. Essentially, loss distance is a measure of the spacing between consecutive network packet loss or error events; a loss period is the duration of a loss or error event (e.g. and how many packets are lost in that duration).

Bibliography

[b_ITU-T Hsup1] ITU-T Series H Supplement 1 (1999), *Application profile-sign language and lip-reading real-time conversation using low-bit rate communications*.

[b_IETF RFC 3357] IETF RFC 3357 (2002), *One-Way Loss Pattern Sample Metric*.

[b_CLVoD2] CableLabs, "CableLabs Headend VoD Metadata Content 2.0 Specification", May 22, 2006

[b_Möller] Sebastian Möller & Alexander Raake, "A taxonomy of quality prediction models recommended by the ITU-T", ITU Workshop on End-to-End QoS/QoE, June 2006, available at: www.itu.int/ITU-T/worksem/qos/200606/index.html.

[b_NTIA264] S. Wolf, "Features for automated quality assessment of digitally transmitted video," NTIA Report 264, June 1990.

[b_McCannLaw] Ken McCann, "McCanns Law on Encoder Technology Improvements", www.zetacast.com , mailto:ken@zetacast.com

II.2.2 Traffic management mechanisms for the support of IPTV services

Summary

The document describes a set of traffic management mechanisms which are aimed to facilitate the efficient support of IPTV services over the network infrastructure. Traffic management mechanisms for the home, access, and core networks are discussed. The network supporting IPTV services will span a number of network domains which may be designed, deployed and operated by different providers and which may differ in their traffic management capabilities. Therefore, it is expected that the network provider(s) will implement a subset of these mechanisms to ensure IPTV service objectives are satisfied efficiently. Furthermore the traffic management mechanisms also depend on the specific network architectures used for IPTV services as defined in the IPTV architecture specification. The document further provides mappings of IPTV service components to the IP network QoS classes defined in ITU-T Y.1541.

Keywords

IPTV, services, Y.1541, home network

Current status

All sections of the document are in good shape.

Dependency on or relationship to other FG IPTV documents

- IPTV services requirements document; providing the basic requirements
- IPTV architecture document; providing the architectural framework for traffic management, however it should be noted that the document doesn't assume a certain architecture
- Application layer error recovery mechanisms for IPTV document; error recovery mechanisms are taken into account for the assignment of IPTV service components to network QoS classes
- The document references the services scenarios for IPTV document, however it can also be used without this reference

CONTENTS

		Page
1	Scope	239
2	References	239
3	Definitions	240
	3.1 Terms defined elsewhere	240
	3.2 Terms defined in this document	240
4	Abbreviations and acronyms	241
5	Traffic management mechanisms	242
	5.1 Control plane	244
	5.1.1 Admission control	244
	5.1.2 QoS routing	245
	5.1.3 QoS routing	245
	5.1.4 Resource management	246
	5.2 Data plane	246
	5.2.1 Traffic conditioning	246
	5.2.2 Transmission schedulers	246
	5.2.3 Buffer management	247
	5.3 Multicast	247
	5.3.1 Multicast replication point	247
6	Mapping of IPTV service components to IP performance classes	248
	6.1 Network QoS classes	248
	6.2 Mapping of IPTV service components to Y.1541 classes	249
7	Cross-layer interaction for IPTV services	250
8	Traffic management capabilities: core networks	250
	8.1 IP network traffic management capabilities	250
	8.2 IP traffic management capabilities applicable to IPTV services	252
9	Traffic management capabilities: access networks	252
	9.1 Overview of access network technologies	252
	9.2 Access traffic management capabilities applicable to IPTV services	252
10	Traffic management capabilities: home networks	253
Appendix I – Admission control example for IMS-based architecture		254
Bibliography		255

Traffic management mechanisms for the support of IPTV services

1 Scope

This document describes a set of traffic management mechanisms which needs to be implemented at the transport network for the efficient support of IPTV services. The network supporting IPTV services will span a number of network segments, with the possibility of being established by different providers and may differ in their traffic management capabilities. Therefore, it is expected that the network provider(s) will implement a subset of these mechanisms to ensure IPTV service objectives are satisfied efficiently.

Traffic management mechanisms will be discussed for the home, access, and core networks.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.264] ITU-T Recommendation H.264 (2005), *Advanced video coding for generic audiovisual services*

[ITU-T Y.1291] ITU-T Recommendation Y.1291(2006), *An architectural framework for support of Quality of Service in packet networks*

[ITU-T Y.1541] ITU-T Recommendation Y.1541 (2006), *Network performance objectives for IP-based services*

[ITU-T FG IPTV.ARCH] FG IPTV-DOC-0181 (2007), *IPTV Architecture*

[ITU-T FG IPTV.SERV] FG IPTV-DOC-0182 (2007), *Service scenarios for IPTV*

[ITU-T FG IPTV.ALERM] FG IPTV-DOC-0186 (2007), *Application Layer Error Recovery Mechanisms for IPTV*

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*

[IETF RFC 2597] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*

[HGI] Home Gateway Initiatives, *Home Gateway Technical Requirements, Release 1*

[ETSI TS 102 034] ETSI TS 102034v1.3.1 (2007), *Digital Video Broadband (DVB) Transport of MPEG-2 TS Based DVB Service over IP Based Networks*

[IEEE 802.1d] IEEE 802.1D (2004), *IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridge*

[IEEE 802.1q] IEEE 802.1Q (2005), *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*

[IEEE 802.3] IEEE 802.3 (2005), *IEEE Standard for Local and Metropolitan Area Networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

[IEEE 802.11] IEEE 802.11 (2007), *IEEE Standard for Local and Metropolitan Area Networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

[IEEE 802.11e] IEEE 802.11e (2005), *IEEE Standard for Local and Metropolitan Area Networks – Specific requirements Part 11: Wireless LAN MAC and PHY specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

None

3.2 Terms defined in this document

This document defines the following terms:

3.2.1 Admission control: The mechanism that controls the traffic to be admitted into the network.

3.2.2 Buffer management: Buffer management deals with which packets, awaiting transmission, to store or drop.

3.2.3 Cross layer interaction: The ability of one layer adapting its performance based on information received from other layers.

3.2.4 Home Gateway (HG): The interface of the home network to provider access network.

3.2.5 IP differentiated model: The model that defines a set of edge functions and a number of per-hop behaviour (PHB).

3.2.6 IP reservation model: The model that is based on the IP Integrated Services (IntServ) and allows the use of RSVP signalling protocol for bandwidth reservation.

3.2.7 QoS routing: The mechanism that is used to control network congestion and improve network utilization by selecting an appropriate path.

3.2.8 Transmission Scheduler: The mechanism that controls which packets to select for transmission on an outgoing link.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

AF Assured Forwarding

AQM Active Queue Management

AR Access Router

BAS Broadband Access Server

BE Best Effort

BRAS Broadband Remote Access Server

BTV Broadcast TV

CAC Connection Admission Control

CLS Controlled Load Service

CoS Class of Service

CS Class Selector

DF Default Forwarding

DSLAM Digital Subscriber Line Access Multiplexer

DSCP Differentiated Services Codepoint

EF Expedited Forwarding

GS Guaranteed Service

HG Home Gateway

IGMP Internet Group Management Protocol

IMS IP Multimedia Subsystem

IP Internet Protocol

IPDV IP packet Delay Variation

IPER IP packet Error Ratio

IPLR IP packet Loss Ratio

IPRR IP Packet Reordering Ratio

IPTD IP Packet Transfer Delay

LAN Local Area Network

LL Low Loss

L2 Layer 2

MAC Media Access Control

MPEG Moving Picture Experts Group

MoD Music on Demand

NAL	Network Adaptation Layer
NALU	Network Adaptation Layer Unit
NVoD	Near Video on Demand
OSPF	Open Shortest Path First
PDU	Protocol Data Unit
PHB	Per-hop Behaviour
PPV	Pay Per View
PVR	Private Video Recorder
QoS	Quality of Service
RED	Random Early Drop
RP	Replication Point
RSVP	Resource Reservation Protocol
RTI	Real-Time Interactive
RTMU	Real-Time Multicast & Unicast
RTP	Real Time Protocol
SLA	Service Level Agreement
TCP	Transport Control Protocol
ToS	Type of Service
VCL	Video Coding Layer
VLAN	Virtual LAN
VoD	Video on Demand
VoIP	Voice over IP
VTC	Video Teleconference
WAN	Wide Area Network
WLAN	Wireless LAN

5 Traffic management mechanisms

This clause provides an overview of the basic traffic management capabilities that are commonly deployed in a managed network. A provider may choose to deploy a subset of these capabilities depending on the performance objectives of applications supported by the network.

Traffic management is a set of generic network mechanisms for controlling the network service response to a service request, which can be specific to a network element, or for signalling between network elements, or for controlling and administering traffic across a network, mainly including bandwidth allocation, admission control, packet classification/marking, congestion management, congestion avoidance, traffic policing, and traffic shaping and line rate constraint, etc. Its basic processing sequence is shown in Figure 5-1.

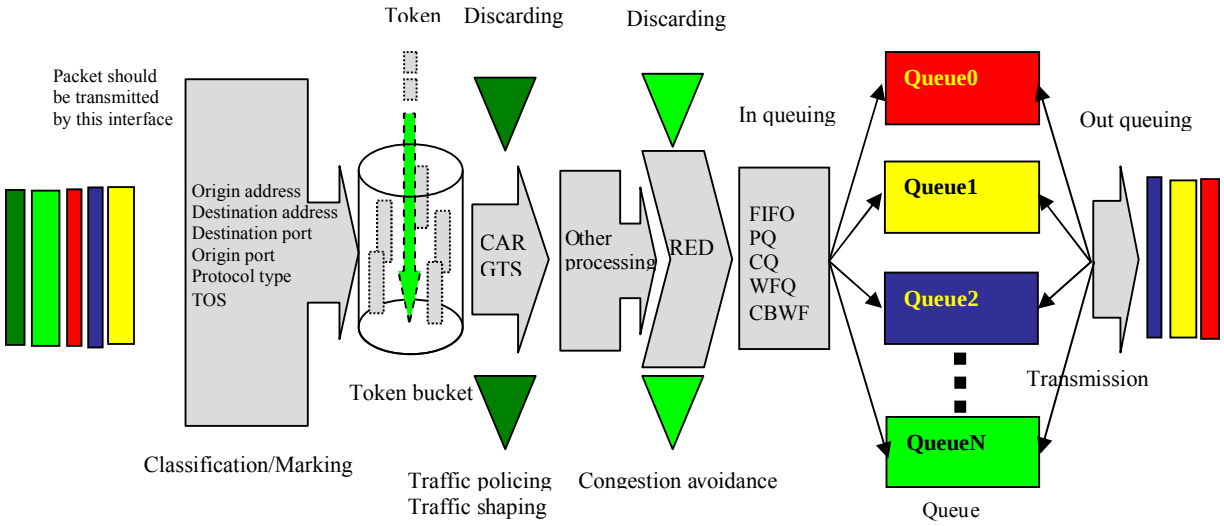


Figure 5-1: The basic processing sequence of traffic management

The traffic management framework contains mechanisms dealing with the user traffic directly, the pathways through which user traffic travels, and the operation, administration and management aspects of the network. As depicted in Figure 5-2, its building blocks are organized into three planes: control plane, data plane, and management plane.

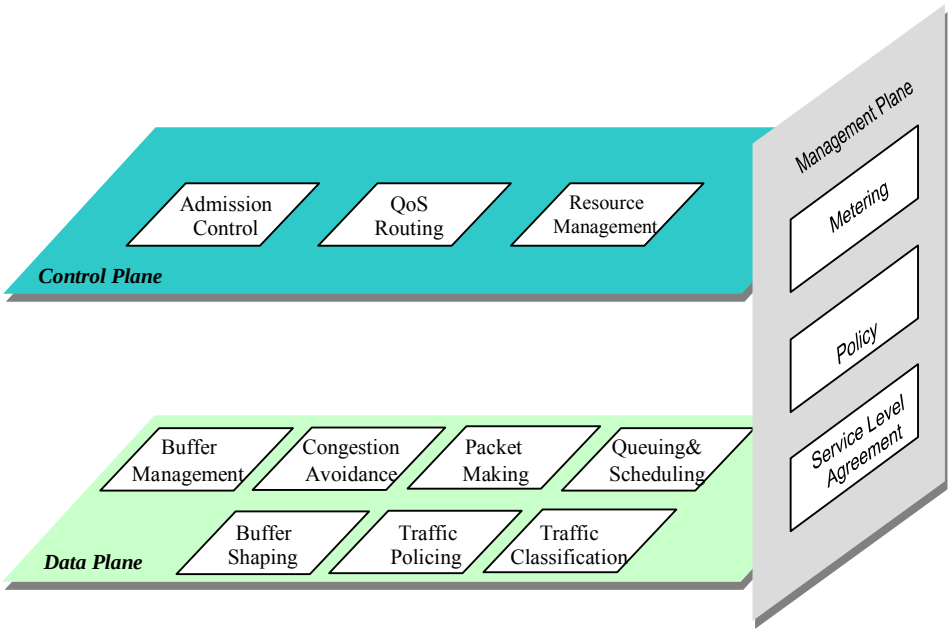


Figure 5-2: Architectural framework for QoS support

5.1 Control plane

5.1.1 Admission control

This mechanism controls the traffic to be admitted into the network. Normally the admission criteria are policy driven [b_IETF RFC 2753]. Whether traffic is admitted depends on an a priori Service Level Agreement (SLA). In addition, the decision can depend on whether adequate network resources are available so that newly admitted traffic does not overload the network and degrade service to ongoing traffic. For a service provider, maximal traffic should be admitted while the same level of Quality of Service (QoS) (including transaction performance as well as service reliability/availability expectations) is maintained for the existing traffic.

Admission control meets requirements for IPTV multicast/unicast services as negotiated in the SLA. Specifically, the desired IPTV services reliability/availability can be requested as a priority level for admission control. Admission control mechanisms can efficiently support QoS assurance for IPTV services on a managed network. IPTV services supported by admission control will meet unicast and multicast service demand for subscribers. Unicast admission control ensures IPTV unicast services, such as Video on Demand (VoD), time shifted TV, etc. Multicast admission control satisfies multicast services, such as Broadcast TV (BTV), Near Video on Demand (NVoD), etc. The policy of multicast admission control is triggered through subscribers joining multicast groups via Internet Protocol (IP) multicast protocols (e.g., Internet Group Management Protocol (IGMP)).

5.1.1.1 Admission control for IPTV services

In the current environment, i.e. cable or satellite TV, support of basic linear TV service is managed on subscription basis. Once subscribed, there is an expectation by the end-user that the linear TV service will continue without interruption with any further need for admission every time the TV set is turned on. This behaviour must be also allowed for IPTV services. Therefore, applying admission control to regular linear TV service is not recommended and management of the service must continue to be on subscription basis. A service provider ensures that the network is properly engineered to accommodate the number of subscribers that match its business model.

There are scenarios where multiple set-top boxes may exist in a single home and reception of multiple video streams may be restricted due to the access bandwidth. These scenarios may require the service provider to limit the number of streams admitted for a single subscriber.

There are other scenarios where reception of some video stream programs may be forbidden due to inappropriate subscription privileges. These scenarios may require the network provider to limit the number of streams admitted for a single subscriber.

Other IPTV services may be subject to admission control. For example a service provider may apply admission control to IPTV services. The request for IPTV services involves the exchange of signalling between user equipment (e.g. set-top box) and the service provider video server. The service provider may reject the IPTV services request based on network resources, user status, or the current use of a specific program across all subscribers. Criteria such as user standing and the current use of a given program are related to policies set by the service provider and do not change very frequently.

As another example, a network provider may apply admission control to IPTV services. Request for IPTV services involves exchanging of signalling between user equipment and network provider, e.g., by means of equipment that maintains subscriber privileges in a local database and may receive IPTV services request. Based on subscriber privileges, equipment may reject this request or forward it to network side transparently and then allow media stream to be transferred from network side to subscriber.

The effect of an IPTV services request on the network resources is a dynamic parameter and it varies based on the program requested. For instance requesting high definition content will impose more demand on the network compared to the demand generated when low definition content is requested. The role of the admission function in this case is to accept or reject the IPTV services request based on the traffic demand of the new request and the current utilization of network resources.

Appendix I shows an example of admission control for on-demand service in an IPTV service scenario using the IP Multimedia Subsystem (IMS)-based architecture as defined in [ITU-T FG IPTV.ARCH].

5.1.2 QoS routing

Text in this sub-clause is based on sub-clause 7.2 of [ITU-T Y.1291] with modifications.

This mechanism is used to control network congestion and improve network utilization by selecting an appropriate path. The path selected is most likely not the traditional shortest path. Depending on the specifics and the number of QoS metrics involved, computation required for path selection can become prohibitively expensive as the network size grows. Hence practical QoS routing schemes consider mainly cases for a single QoS metric (e.g., bandwidth or delay) or for dual QoS metrics (e.g., cost-delay, cost-bandwidth, and bandwidth-delay). To further reduce the complexity of path computation, various routing strategies exist. According to how the state information is maintained and how the search of feasible paths is carried out, there are strategies such as source routing, hierarchical routing, and distributed routing. And according to QoS granularity and model expansibility, there are strategies such as Intserv, Diffserv and class based Intserv in which the network is divided into several QoS autonomous systems (i.e., QoS domains) and each QoS domain may adopt its own resource allocation scheme so that end-to-end QoS can be achieved based on resources allocated in a single QoS domain or multiple QoS domains. In addition, according to how multiple QoS metrics are handled, there are strategies such as metric ordering and sequential filtering, which may trade global optimality with reduced computational complexity [b_IETF RFC 2386].

The path selection process involves the knowledge of the flow's QoS requirements and characteristics and (frequently changing) information on the availability of network resources (expressed in terms of standard metrics such as available bandwidth and delay). The knowledge is typically obtained and distributed with the aid of signalling protocols. For example, Resource Reservation Protocol (RSVP) [IETF RFC 2205] can be used for conveying a flow's requirements and characteristics and Open Shortest Path First (OSPF) extensions as defined in [IETF RFC 2676] for resource availability. Compared with shortest-path routing that selects optimal routes based on a relatively constant metric (i.e., hop count or cost), QoS routing tends to entail more frequent and complex path computation and more signalling traffic.

It is important to note that QoS routing provides a means to determine only a path that can likely accommodate the requested performance. To guarantee performance on a selected path, QoS routing needs to be used in conjunction with resource reservation to reserve necessary network resources along the path.

QoS routing can also be generalized to apply to traffic engineering. (Concerning slowly-changing traffic patterns over a long time scale and a coarse granularity of traffic flows, traffic engineering encompasses traffic management, capacity management, traffic measurement and modelling, network modelling, and performance analysis.) To this end, routing selection often take into account a variety of constraints such as traffic attributes, network constraints, and policy constraints [b_IETF RFC 3272]. Such generalized QoS routing is also called constraint-based routing.

5.1.3 Resource management

The network resource management system acquires network traffic information (e.g. QoS requests) from a network resource manager of a bearer control layer, and carries out network traffic management according to the acquired network information by means of data transmission between the network resource manager and the network nodes (e.g. DSLAM, Broadband Remote Access Server (BRAS), switches, routers, gateways, etc.). A network management interface needs to be configured on the resource manager for exchanging the network information with the network management system, and the network information is acquired from the resource manager via the configured network management interface, and is added, modified and deleted in the network management system. By employing the network resource manager of the bearer control layer, high-quality IPTV services are able to be provided in the IPTV system.

5.2 Data plane

5.2.1 Traffic conditioning

The following are required in access network for supporting multimedia services such as IPTV services:

- QoS provisioning per subscriber and per service
- Traffic classification based on multiple header fields (5-tuple, 6-tuple, etc.)
- Minimum bandwidth guarantee
- Traffic shaping/policing
- Advanced packet queuing and scheduling
- Traffic marking (IP Differentiated Services Codepoint (DSCP), Ethernet priorities [IEEE 802.1q], etc.)

5.2.2 Transmission schedulers

This mechanism controls which packets to select for transmission on an outgoing link. Incoming traffic is held in a queuing system, which is made of, typically, multiple queues and a scheduler. Governing the queuing system is the queuing and scheduling discipline it employs. There are several key approaches:

- First-in, first-out scheduler: Packets are placed into a single queue and served in the same order as they arrive in the queue.
- Round-Robin Scheduler: Packets are classified based on some criteria. One possible criterion is the classification based on flow identity. A less granular and consequently more scalable is to classify packets based on application or forwarding classes. Each class is then assigned a separate queue, and queues are serviced in round-robin fashion.
- Priority scheduler: Packets are first classified and then placed into different priority queues. Packets are scheduled from the head of a given queue only if all queues of higher priority are empty. Within each of the priority queues, packets are scheduled in first-in, first-out order.
- Weighted Round-Robin scheduler: Packets are classified into flows and assigned to queues dedicated to respective flows. A queue is assigned a percentage of output bandwidth according to the bandwidth need of the corresponding flow. By distinguishing variable-length packets, this approach also prevents flows with larger packets from being allocated more bandwidth than those with smaller packets.
- Class-based scheduler: Packets are classified into various service classes and then assigned to queues assigned to the service classes, respectively. Each queue can be assigned a different percentage of the output bandwidth and is serviced in round robin. Empty queues are skipped.

- Hierarchical scheduling: Packets are classified into various service classes and then assigned to queues. Hierarchical scheduling then schedules queues layer by layer based on the queue hierarchy mode. Hierarchical queue can control the bandwidth of each service or the total bandwidth of multiple services to guarantee the QoS on the access side. In contrast to static queue scheduling, the controller for queue scheduling in hierarchical queue can be configured dynamically.

5.2.3 Buffer management

Queue or buffer management deals with which packets, awaiting transmission, to store or drop. An important goal of buffer management is to minimize the steady-state buffer size while not underutilizing link as well as avoiding the monopolization of the available buffer space by a single flow [b_IETF RFC 2309]. Schemes for buffer management differ mainly in the allocation of the buffer space and the criteria for dropping packets.

A common criterion for dropping packets is the buffer reaching its maximum size. Packets are dropped when the buffer is full. Determining which packet to drop depends on the drop disciplines, for example:

- "Tail drop" drops the newly arriving packet. This is the most common strategy since it is easy to implement.
- "Front drop" A buffer space for the newly arriving packet is made available by dropping the packet at the front of the queue, provided that the length of the newly arriving packet is less than or equal to the dropped packet.
- "Random drop" A buffer space for the newly arriving packet is made available by randomly choosing a packet to drop from the queue, provided that the length of the newly arriving packet is less or equal to the dropped packet.

Active queue management (AQM) is a scheme for dropping packet before the buffer reaches its full size. Random Early Drop (RED) is an example of theses schemes. AQM algorithms are developed in the context of Transport Control Protocol (TCP) congestion avoidance scheme with the objective to improve network throughput. AQM may not be applicable to IPTV traffic since TCP is not likely to be used as the transmission protocol for these applications.

5.3 Multicast

IPTV network supports transportation of multicast traffic and multicast admission control policy for QoS of IPTV services. The multicast admission control system based on users' admission control policy allocates, reserves resource and controls IPTV multicast transportation for subscribers. The multicast replication function forwards the IPTV multicast stream to subscribers according to their successful resources allocation in the network control system. So quality of service for IPTV multicast services will be able to be guaranteed by multicast admission control.

5.3.1 Multicast replication point

Replication of video streams is one of the essential functions for multicast and selection of applicable Replication Points (RPs) within the IPTV network is important because it may affect bandwidth utilization and traffic management complexity.

The network equipment serving as the multicast RP is required to have good functionality and processing capability. Network elements including Broadband Access Server (BAS), Access Router (AR) and Layer 2 (L2) equipment can perform multicast replication.

There is a trade-off relationship when we select RPs within the network. The nearer the multicast replication points approach to users, the less bandwidth the network needs, while the management becomes more complex.

When selected as the multicast RP, the BAS/AR implements the user-oriented replication without requiring the access network to support multicast. This solution supports simplicity in management. On the other hand, the BAS/AR poses higher bandwidth requirement for the access network. Moreover, the BAS/AR demands more on its port density and processing capability.

If L2 equipment nearest to the end-user (e.g. DSLAM or WAN switch) is selected as the multicast replication point, then only the bandwidth of the access network can be saved. This solution supports distributed replication, so it has a relatively weak requirement for processing capability at the replication point. Hence, it is applicable for large-scale service deployment. However, the access network must support multicast, and the L2 devices are required to support IGMP functionality. This solution is also complex to manage.

6 Mapping of IPTV service components to IP performance classes

6.1 Network QoS classes

ITU-T Recommendation Y.1541 [ITU-T Y.1541] defines classes of network QoS with objectives for IP performance parameters. Each QoS class defines a specific combination of limits on the performance values. Table 6-1 shows IP network QoS definitions, network performance objectives and guidance for applicability. Classes 6 and 7 are assigned provisionally in [ITU-T Y.1541] and are intended to support the performance requirements of high bit rate user applications that have more stringent loss/error requirements than those supported by classes 0 and 1.

Table 6-1: IP network QoS class definitions and network performance objectives/Applications

QoS class	IPTD	IPDV	IPLR	IPER	IPRR	Applications (examples)
0	100 ms	50 ms	1×10^{-3}	1×10^{-4}	–	Real-time, jitter sensitive, low delay, highly interactive
1	400 ms	50 ms	1×10^{-3}	1×10^{-4}	–	Real-time, jitter sensitive, medium delay, interactive
2	100 ms	U	1×10^{-3}	1×10^{-4}	–	Transaction data, low delay, highly interactive
3	400 ms	U	1×10^{-3}	1×10^{-4}	–	Transaction data, medium delay, interactive
4	1 s	U	1×10^{-3}	1×10^{-4}	–	Low loss
5	U	U	U	U	–	Best effort
6	100 ms	50 ms	1×10^{-5}	1×10^{-6}	1×10^{-6}	High bit rate, strictly low loss, low delay, highly interactive
7	400 ms	50 ms	1×10^{-5}	1×10^{-6}	1×10^{-6}	High bit rate, strictly low loss, medium delay, interactive
NOTES – U: undefined						

6.2 Mapping of IPTV service components to Y.1541 classes

This sub-clause focuses on the mapping of some key service components to the IP QoS classes defined in [ITU-T Y.1541] and listed above in Table 6-1.

IPTV services as listed in [ITU-T FG IPTV SERV] usually consist of several service components which can have different QoS requirements regarding the transport of related data. For example, a VoD service includes selection of a movie from a content guide (which could be downloaded or accessible via web pages), a transaction for renting the movie, streaming control and the actual content streaming. User generated content services can include the upload of the content to a network based server, publishing the availability of the content to the users, selection and streaming to the other users. The QoS requirements for these different service components are usually different.

Table 6-2 provides suggestions (√) of the mapping of service components to QoS classes. For the actual mapping the specific deployment and also the use of application layer error recovery mechanisms as for example defined in [ITU-T FG IPTV ALERM] have to be taken into account.

Table 6-2: Mapping of key IPTV service components to Y.1541 QoS classes

IPTV service components	Example IPTV services	Y.1541 QoS class							
		5	**4**	**3**	**2**	**1**	**0**	**7**	**6**
Streaming of live TV content	Linear TV including Pay per View and Multi-view						√ [1]		√
Streaming of video content	VoD, Network PVR, time-shift TV					√ [1]		√	
Streaming of audio content	Music on Demand					√			
Streaming control	VoD, Network PVR, time-shift TV				√				
Download of video content	Push VoD, Near VoD		√						
Upload of video content	User-generated content		√						
Download of data	Content guides, pictures, applications download	√							
Access to web pages	Portals, information services			√					
Streaming of live speech	Voice call, audio conference						√		
Streaming of live low resolution video content	Video telephony, videoconference						√		
Interactive message exchange	Chatting			√					
Message exchange	Messaging, Email	√							
Payment Transactions	VoD rental			√					

1. Consumer television quality can be achieved using the standard Y.1541 QoS classes 0 and 1 together with the DVB-IP AL-FEC mechanism, low to modest overhead and the enhanced decoder according to [ETSI TS102034], Annex E, sub-clause E.5.1.2.

7 Cross-layer interaction for IPTV services

Figure 7-1 shows a generic layer architecture for offering of video services (not limited to the examples shown). At the application layer video codec generates video elementary streams as a result of the encoding process. Service layer is responsible for packaging video streams into services such as broadcast video, VoD, etc. The function of the transport layer is to transport video streams from source to the destination through different network segments.

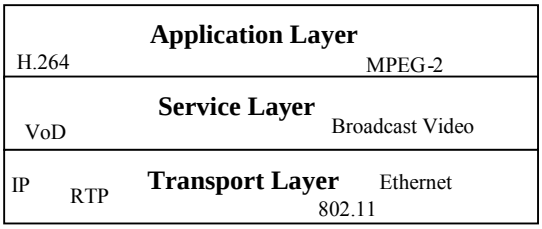


Figure 7-1: Layer Architecture for Video Transport

Cross-layer interaction is the ability of one layer adapting its performance based on information received from other layers. For instance in a wireless transport environment it may be beneficial for the application to adjust its rate based on the status of the rates that can be supported by the transport layer. Cross layer interaction may be implemented in a top-down or down-top fashion.

Of particular interest is the ability to make use of application layer priority to optimize transport layer performance. Video codec generates video elementary streams with different priorities based on the picture type (i.e. I, P or B). Type I pictures are essential for the codec operation and should always be given transport priority over the P and B frames. MPEG-2 transport stream and H.264 Network Adaptation Layer (NAL) generate transport video stream packets with relative priority indication (one bit transport priority in the MPEG-2 transport stream packet and 2 bits NAL Reference ID (NRI) in H.264)

8 Traffic management capabilities: core networks

8.1 IP network traffic management capabilities

This sub-clause describes an overview of the IP traffic management capabilities including those related to integrated services and differentiated service.

IP networks allow both reservation as well as differentiated models for QoS support and traffic management. The IP reservation model is that based on the IP Integrated Services (Intserv) and allows the use of RSVP signalling protocol for bandwidth reservation. Two service classes are defined in the context of IP Intserv:

- Guaranteed Service (GS) defines a service type where all packets belonging to the same session are delivered within a deterministic delay bound. Routers along the path of the session must employ appropriate scheduling algorithm and reserve resources to ensure that the delay bound is always satisfied.
- The Controlled Load Service (CLS) provides a service equivalent to a "lightly" loaded best effort network.

IP networks are also capable of supporting a differentiated model with the IP differentiated service (Diffserv). The IP differentiated model defines a set of edge functions and a number of Per-hop Behaviour (PHB). Edge functions are those related to classification, metering, marking, dropping, and shaping. A PHB defines an externally observable treatment applied at a network node to a Diffserv behaviour aggregate. A number of PHBs are defined by the IETF in the context of IP Diffserv:

- Expedited Forwarding (EF): The intent of the EF behaviour is to provide the building block for the creation of low-loss, low delay, and low delay variation services. The EF PHB definition mandates that the EF packets should ideally be served at a rate R or faster and bounds the deviation of the actual departure time for each packet by the relationship [IETF RFC 3246]:

$$d_j \le f_j + E_a$$

$$f_j = \max\left[a_j, \min\left[d_{j-1}, f_{j-1}\right]\right] + \frac{\ell_j}{R}$$

where:

d_j: actual departure time of the j^{th} packet.

f_j: target departure time of the j^{th} packet.

E_a: error term bounding the deviation of the actual departure time from the target departure time. E_a is a function of the nodal scheduler implementation.

l_j: length of the j^{th} packet.

The above relationship paves the way for the specification of a delay bound as long as the aggregate EF traffic adheres to some traffic pattern (e.g. as specified by a leaky bucket).

- Assured Forwarding (AF): The AF PHB group defines four AF classes. For each class three discard precedence levels are defined (AFij, i = 1, 2, 3 or 4 and j = 1, 2 or 3). No priority order is defined among the four AF classes. [IETF RFC 2597] requires that each node in the networks to allocate certain amount of forwarding resources for each AF class to assure forwarding of the IP packets. However, no delay or loss bounds are defined.

- Class Selector (CS): The CS PHB group is defined for Diffserv to be backward compatible with legacy routers that support the Type of Service (ToS) bits in the IP packet header. CS PHB group defines 8 forward treatments where packets belonging to CSi are served before packets marked with CSj as long as i > j. It effectively defines a straight priority discipline with CS1 being reserved for the Default Forwarding (DF) used for the traditional IP Best Effort (BE) service.

IP DiffServ is scalable compared to IP Intserv since it doesn't require per flow reservation, scheduling, and buffering. In IP Diffserv flow information is available at the network edge while nodal behaviour is applied on an aggregate basis.

IP DiffServ paradigm doesn't include the definition of service classes. However, service classes could be realized by proper specification of edge rules and consistent application of PHB by the different nodes in the network.

8.2 IP traffic management capabilities applicable to IPTV services

The core IP network transporting IPTV services is expected to be well-engineered and shared between a number of applications including data and voice support. Since IP Diffserv allows the core IP network to scale to a large number of flows it is also expected that the network will be equipped with Diffserv capabilities in terms of scheduling implementation that supports all or some of the Diffserv PHBs. It can be shown that if the EF traffic arriving at an interface is bounded by a leaky bucket with parameters (B, R) then the delay of any packet departing the interface is bounded by:

$$D \leq \frac{B}{R} + E_a$$

IPTV services that require stringent loss and delay constraints may be supported using EF PHB. The use of PHB will ensure that IPTV packets are transported within a certain delay bound with almost no loss as long as the aggregate burstiness of the offered EF traffic is within some bound. The EF PHB must be configured with enough resources to satisfy the delay requirements of video packets. Since performance of video application is sensitive to packet loss, sufficient buffer needs to be allocated to ensure that it accommodates a burst size equal to B.

It is also possible to support IPTV services using AF PHB group as long as the AF class or classes designated for IPTV services are configured with the amount of resources needed to assure the service QoS parameters. Unlike the EF PHB there is no delay constraint associated with the definition of the AF PHB. However, the use of the AF offers the added benefit of selectively discard video packets based on their relative importance. This will require the relative importance of video information to be inherited by the IP layer.

An IP node supporting the CS PHB group implies an absolute priority scheduler is in place. IPTV services shall be supported at a priority level high enough to maintain its quality assurances. Starvation of classes supporting IPTV services must always be avoided.

9 Traffic management capabilities: access networks

9.1 Overview of access network technologies

Access networks should have means to control the following functions for traffic management:

- per packet/flow and per class basis Connection Admission Control (CAC)
- per user and per service QoS provisioning
- per packet/flow mapping between IP DSCP markings and Ethernet priorities [IEEE 802.1q]

9.2 Access traffic management capabilities applicable to IPTV services

Generic mechanisms are required for traffic management of upstream and downstream directions in an access network.

(a) Upstream

To support quality of service in access networks including broadcasting traffic, network nodes should have the following requirements in the upstream direction.

- Guarantee of minimum bandwidth
- Guarantee of bandwidth quality per service (e.g. VoIP, Videoconference, and IPTV).

To address the above two requirements, the following functions should be supported:

- 5-tuple based Classification & Policing
- Priority Queuing
- Traffic shaping

(b) Downstream

To support quality of service in access networks including broadcasting traffic, network nodes should have the following requirements in the downstream direction.

- Guarantee of minimum bandwidth per service

To support the above requirement, access networks should have the following functions in downstream side.

- Per packet/flow and per class basis CAC for broadcast channels
- Traffic shaping/policing per subscriber
- Support of Class of Service (CoS) based DSCP
    - 5-tuple classification
    - DSCP marking

Mapping between IP DSCP markings and Ethernet priorities [IEEE 802.1q].

10 Traffic management capabilities: home networks

This clause describes home network environment and the need for traffic management for IPTV applications. A possible architecture for the home network is shown in Figure 10-1 [HGI].

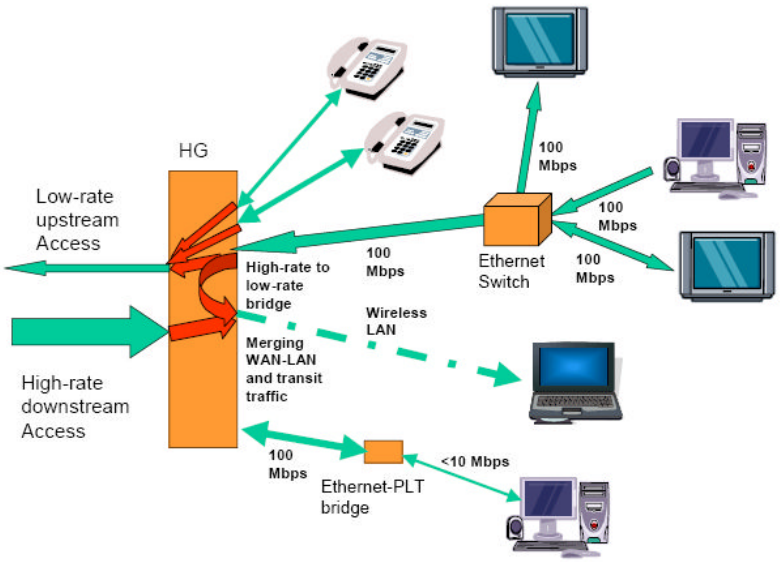


Figure 10-1: Home Network Architecture

As shown in Figure 10-1, home network employs multiple Local Area Network (LAN) technologies. Prominent among those technologies are the Wireless LAN (WLAN) based on [IEEE 802.11] and wireline Ethernet and bridges based on [IEEE 802.3] and [IEEE 802.1d]. The Home Gateway (HG) is the interface of the home network to provider access network. HG receives and sends packets from and to the Wide Area Network (WAN). It also supports transit (LAN-to-LAN) traffic. The main function of the HG is the classification of the packets as they traverse the HG to and from the WAN and setting the appropriate priority level using the IP DSCP or the Ethernet user priority bits. Possible classification criteria include type of LAN, Media Access Control (MAC) addressing, and Virtual LAN (VLAN) Tag. HG requirements include the support of multiple queues managed using strict priority or weighted round robin at the WAN egress ports. It requires the support buffer management mechanisms.

Home Ethernet switches may support the existence of the user priority bits (a.k.a. p-bits). User priority bits define up to 8 priority levels that can be used to identify traffic classes such as voice, video, best effort, etc.

The current IEEE 802.11 standards support rates up to 54 Mbps. Emerging IEEE 802.11 standards are expected to support rates up to 600 Mbps based on [b_IEEE 802.11n]. Traffic management is supported on a WLAN using [IEEE 802.11e] which defines 4 access categories that effectively supports 4 priority levels.

Appendix I

Admission control example for IMS-based architecture

(This Appendix is not an integral part of this document.)

Figure I-1 shows an example of admission control for on-demand service in an IPTV service scenario using the IP Multimedia Subsystem (IMS)-based architecture as defined in [ITU-T FG IPTV ARCH].

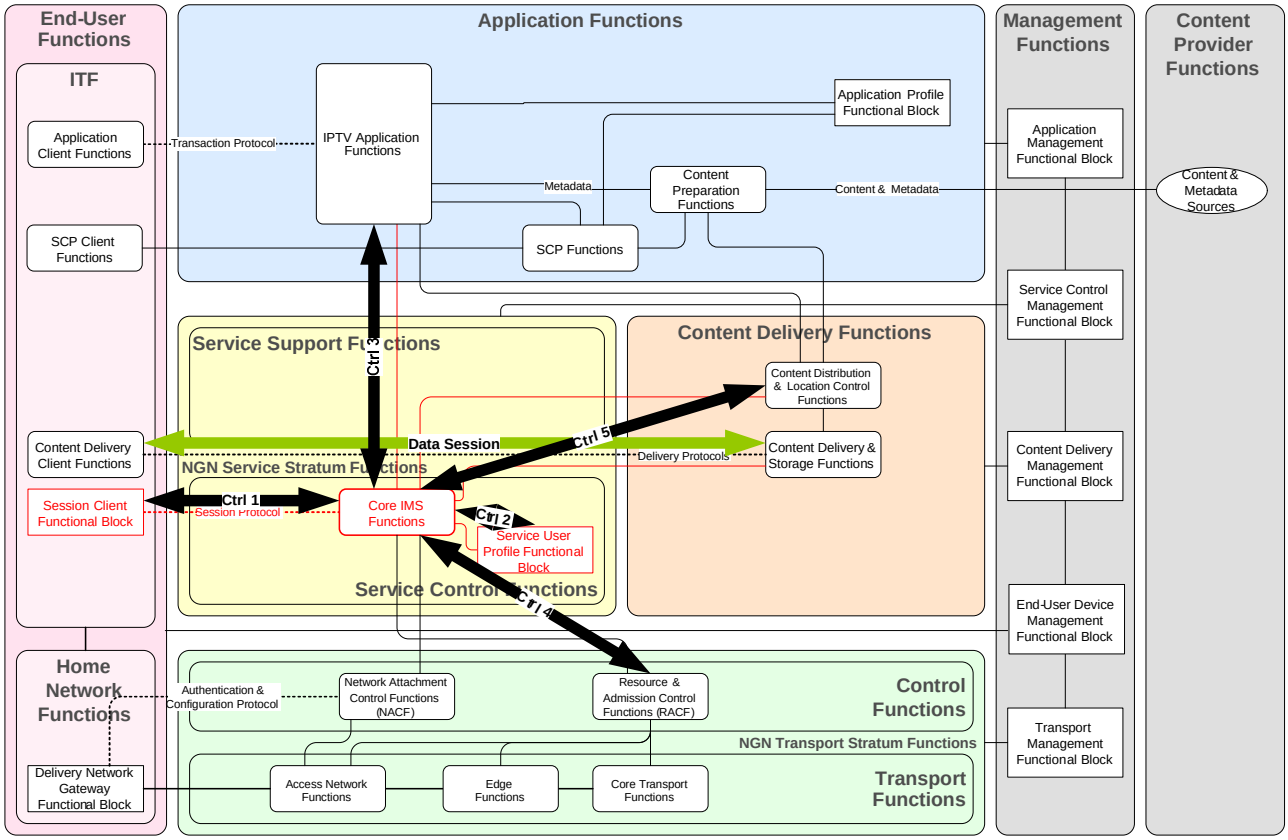


Figure I-1: Admission Control Example for IMS-based architecture

The admission sequence involves the generation of the request by the session client of the IPTV terminal function using a session level protocol (Ctrl 1 flow in Figure I-1). The request is received by the core IMS. The core IMS checks with the Service user profile (Ctrl 2 flow in Figure I-1) and IPTV application (Ctrl 3 in Figure I-1) if the user is allowed to access the specific service and content and checks with the resource & admission control function (Ctrl 4 flow in Figure I-1) if the required resources are available. Based on this information the incoming request may be accepted or rejected and the result of the admission process is reported back to the session client (Ctrl 1 flow in Figure I-1). In case the request is accepted the content delivery control function is notified (Ctrl 5 flow in Figure I-1) and the session is established between the media client IPTV terminal and the content delivery and storage function (data session flow in Figure I-1).

Bibliography

[b_IETF RFC 2309] IETF RFC 2309 (1998), *Recommendations on Queue Management and Congestion Avoidance in the Internet.*

[b_IETF RFC 2386] IETF RFC 2386 (1998), *A Framework for QoS-based Routing in the Internet*.

[b_IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy Based Admission Control.*

[b_IETF RFC 3272] IETF RFC 3272 (2002), *Overview and Principles of Internet Traffic Engineering.*

[b_IEEE 802.11n] IEEE 802.11n (D3.00) Draft, *IEEE Standard for Local and Metropolitan Area Networks – Local* and *metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*

II.2.3 Application layer error recovery mechanisms for IPTV services

Summary

The ability to deliver high levels of service quality to users is an essential aspect of IPTV services, and thus captured in many IPTV-related requirements. IPTV services may be degraded if the media decoders are exposed to impairments such as packet loss. Mechanisms are needed to reliably ensure the quality of experience of the IPTV service in the presence of such defects.

This document describes specific mechanisms and the applicability of these mechanisms to IPTV services and network conditions, and provides recommendations and guidance on their use. It has been determined that with the use of these mechanisms, consumer television quality can be achieved using the standard Y.1541 QoS Classes 0 and 1.

Keywords

Forward error correction, retransmission, IPTV, error recovery, QoS

Introduction

Application layer reliability is an important aspect for IPTV services. Data being delivered over IP networks may suffer from packet losses. In case of the delivery of video and audio data errors being exposed to the media decoder generally degrade the IPTV service quality. Therefore, reliability support for them is essential to IPTV service.

The material in this document is intended to address the requirement that the IPTV architecture provide a mechanism for resiliency in the service provider infrastructure to maintain a high QoE for video services. The document addresses specific realizations of the content delivery error recovery function and the content delivery error recovery client function in the IPTV architecture.

The document provides an overview on application layer error recovery mechanisms and related standards. Usage guidelines for the mechanisms as well as specific recommendations are provided.

Current status

All sections of the document are in good shape.

The document could be extended with additional error recovery mechanism for streaming and download applications (e.g. based on ongoing work in DVB).

Dependency on or relationship to other FG IPTV documents

- IPTV network control aspects document; defining the relevant protocols and configuration information
- IPTV architecture document; defining the architectural support for application layer error recovery mechanisms, however the use of application layer error recovery mechanisms is independent of a specific architecture
- IPTV services requirements document; providing the basic requirements
- IPTV traffic management mechanisms for the support of IPTV services document; considers error recovery mechanisms for the assignment of IPTV service components to network QoS classes

CONTENTS

		Page
1	Scope	259
2	References	259
3	Definitions	260
4	Abbreviations and acronyms	260
5	Conventions	261
6	Introduction	262
7	Overview on error recovery mechanisms and related standards	262
	7.1 Overview	262
	7.2 Retransmission	263
	7.3 Forward Error Correction	264
	7.3.1 FEC for Streaming Applications	264
	7.3.2 FEC for Download Services	265
	7.4 Hybrid Combinations of FEC with Retransmissions and Feedback	267
8	Usage Guidelines	268
	8.1 General Discussion on Retransmission and FEC	268
	8.2 Relation of mechanisms to the QoS classes in Y.1541	269
	8.2.1 Overview	269
	8.2.2 DVB-IP AL-FEC	269
9	Recommendations	271
Bibliography		272

Application layer error recovery mechanisms for IPTV Services

1 Scope

The ability to deliver high levels of service quality to users is an essential aspect of IPTV services, and thus captured in many IPTV-related requirements. As IPTV services can easily be degraded if the media decoders are exposed to impairments such as packet losses, mechanisms are needed to reliably deliver good IPTV service quality in the presence of such defects.

This document describes specific mechanisms and discusses the applicability of the mechanism to IPTV services and network conditions, and provides recommendations and guidance on their use.

2 References

The following ITU-T working text and other references contain provisions, which, through reference in this text, constitute provisions of this working text. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working text 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 working text does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.1541] ITU-T Recommendation Y.1541 (2002) – *Internet protocol aspects – Quality of service and network performance. Network performance objectives for IP-based services*

[ITU-T IPTV-0147] ITU-T FG IPTV-DOC-0147 (2007), *Service scenarios for IPTV*

[ITU-T IPTV-0181] ITU-T FG IPTV-DOC-0181 (2007), *IPTV architecture*

[ITU-T IPTV-0185] ITU-T FG IPTV-DOC-0185 (2007), *Traffic management mechanism for the support of IPTV services*

[ITU-T IPTV-0191] ITU-T FG IPTV-DOC-0191 (2007), *IPTV Related Protocols*

[ATIS-0800005] ATIS-0800005 (2006), *ATIS IPTV Packet Loss Report*

[IETF RFC2733] IETF RFC2733 (1999), *An RTP Payload Format for Generic Forward Error Correction*

[ETSI EN301192] ETSI EN 301 192 (2004), *Digital Video Broadcasting: DVB Specification for Data Broadcasting*

[ETSI TS102034] ETSI TS 102 034v1.3.1 (2007), *Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

[ETSI TS102472] ETSI TS 102 472 (2006), *Digital Video Broadcasting (DVB): IP Datacast over DVB-H: Content Delivery Protocols*

[ETSI TS 126346] ETSI TS 126 346v6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs (3GPP TS 26.346 version 6.2.0 Release 6)*

[SMPTE 2022-1] SMPTE specification 2022-1 (2007), *Forward Error Correction for Real-time Video/Audio Transport Over IP Networks*

[IETF RFC3550] IETF RFC3550 (2003), *Real Time Protocol: A Transport Protocol for Real-Time Applications*

[IETF RFC3556] IETF RFC3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol*

[IETF RFC3605] IETF RFC3605 (2003), *Real Time Control Protocol (RTCP) Attribute in Session Description Protocol (SDP)*

[IETF RFC3611] IETF RFC3611 (2003), *Real Time Protocol Control Protocol Extended Reports (RTCP XR)*

[IETF RFC4585] IETF RFC4585 (2004), *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

[IETF RFC4588] IETF RFC4588 (2005), *RTP Retransmission Payload Format*

[IETF RFC5053] IETF RFC5053 (2007), *Raptor Forward Error Correction Scheme for Object Delivery*

3 Definitions

This section left intentionally blank.

4 Abbreviations and acronyms

This working document uses the following abbreviations and acronyms:

3GPP Third Generation Partnership Project

ALC Asynchronous Layered Coding

AL-FEC Application Layer FEC

ARQ Automatic Repeat request

ATIS IIF Alliance for Telecommunication Industry Solutions – IPTV Interoperability Forum

AVP Audio-Visual Profile

CBR Constant Bit Rate

CDP Content Delivery Protocol

DSL Digital Subscriber Line

DVB Digital Video Broadcasting

DVB-H Digital Video Broadcasting – Handheld

ECG Electronic Content Guide

EPG Electronic Program Guide

FEC Forward Error Correction

FLUTE File Delivery over Unidirectional Transport

IETF Internet Engineering Task Force

IP Internet Protocol

IPDV IP packet Delay Variation

IPER IP packet Error Ratio

IPLR IP packet Loss Ratio

IPTD IP Packet Transfer Delay

IPTV Internet Protocol TeleVision

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

LCT Layered Coding Transport

MBMS Multimedia Broadcast/Multicast Service

MPEG Moving Pictures Experts Group

MTBA Mean Time Between Artefacts

NACK Negative ACKnowledgement

P2P Point-to-Point

QoE Quality of Experience

QoS Quality of Service

RFC Request for Comments

RMT Reliable Multicast Transmission

RTCP Real-Time Control Protocol

RTP Real-Time Protocol

RTT Round Trip Time

TCP Transmission Control Protocol

TS Transport Stream

UDP User Datagram Protocol

VoD Video on Demand

XOR eXclusive OR

5 Conventions

This section left intentionally blank.

6 Introduction

Application layer reliability is an important aspect for IPTV services. Data being delivered over IP networks may suffer from packet losses. In case of the delivery of video and audio data errors such as packet losses or bit errors being exposed to the media decoder generally degrade the IPTV service quality. Moreover, losses in the metadata such as electronic program guide (EPG), electronic content guide (ECG), and interactive user data may cause more severe problem in IPTV service. Therefore, reliability support for them is essential to IPTV service.

Retransmission, forward error correction (FEC), and hybrid combinations of both are known mechanisms for error recovery. When an error recovery scheme and the associated protocol is selected, at least the following aspects should be taken into account:

1) type of IPTV service, e.g., real time streaming video, EPG, application data;

2) type of data delivery mechanisms, e.g., broadcast, multicast, unicast, overlay multicast, and P2P;

3) protocol or processing overhead at senders and receivers;

4) network bandwidth overhead aspects.

The material in this document is intended to address the requirement that the IPTV architecture provide a mechanism for resiliency in the service provider infrastructure to maintain a high QoE for video services [ITU-T IPTV-0147]. The document addresses specific realizations of the content delivery error recovery function and the content delivery error recovery client function in the IPTV architecture [ITU-T IPTV-0181]. Reference point E4 is used to exchange messages for delivering and requesting error recovery information [ITU-T IPTV-0181]. Protocol related aspects to application layer error recovery mechanisms are discussed in [ITU-T IPTV-0191].

The document is structured as follows: Clause 7 provides an overview on application layer error recovery mechanisms and related standards. Clause 8 provides usage guidelines for the mechanisms. Finally, Clause 9 provides conclusions and recommendations.

7 Overview on error recovery mechanisms and related standards

7.1 Overview

This clause introduces retransmission-based error recovery functions, FEC-based error recovery functions, and combinations of the two. Retransmission and FEC are two different techniques to recover packet losses during the delivery of IPTV services. The retransmission approach recovers from packet losses by requesting retransmission from the sender or intermediate retransmission server. The FEC approach operates by adding redundant information to the data at the sender.

An FEC-based error recovery protocol uses redundant information to allow the receiver to correct packet losses. With this redundant information, the receivers can recover from packet losses locally at the receiver. FEC may be used in unicast and multicast delivery.

Retransmission-based error recovery protocols use feedback messages to recover from packet losses, thereby requiring a return feedback path and one or more retransmission servers. On detecting a packet loss, e.g. by noting the gap of packet sequence number, a receiver requests a sender or designated repair servers to retransmit the lost packets. Retransmission may be either unicast or multicast depending on the distribution of clients reporting the errors.

7.2 Retransmission[2]

RTP retransmission is one viable packet loss recovery technique for real-time applications. Retransmitted RTP packets can be sent in a separate stream from the original RTP stream. Like TCP retransmissions, it is assumed that feedback from receivers to senders is available, but, unlike TCP, RTP/UDP does not mandate congestion control by reducing the packet transmission rate, thereby making RTP more appropriate for broadcast-grade video.

The companion protocol to the Real Time Protocol (RTP), the Real Time Control Protocol (RTCP) as specified in [IETF RFC 3550] does not acknowledge single RTP packets but does report statistics on packet loss and jitter. The source node can evaluate the statistics to decide if adaptation is appropriate. Recently, an extension to the RTCP for the Audio-Visual Profile (AVP) enables receivers to provide, statistically, more immediate feedback to senders, allowing for efficient feedback-based repair mechanisms (e.g., retransmission) to be implemented.

More specifically, the RTP Retransmission related specifications from the IETF uses a simple system in which clients request retransmission of specific, lost packets by sending negative acknowledgements (RTCP NACK) to a feedback target/retransmission source over the RTCP flow of the RTP session. A receiver can use a single NACK packet to request transmission for one or multiple lost packets. Then the retransmission source responds with a retransmission of the missing packets over IP unicast or alternatively via IP multicast (for multicast sessions).

References for RTP, RTCP and RTP retransmissions are detailed in Table 7-1.

Table 7-1: IETF RTP and RTCP RFCs status

RFC	Date	Status	Title	Abstract	Reference
3550	07-03	S	Real Time Protocol: A Transport Protocol for Real-Time Applications	The Real Time Protocol provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services.	[IETF RFC3550]
3556	07-03	S	Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol	This document defines an extension to the Session Description Protocol (SDP) to specify two additional modifiers for the bandwidth attribute. These modifiers describe the bandwidth allowed for Real Time Control Protocol (RTCP) packets in a Real-time Transport Protocol (RTP) session.	[IETF RFC3556]
3605	10-03	S	Real Time Control Protocol (RTCP) Attribute in Session Description Protocol (SDP)	When the session crosses a network address translation device that also uses port mapping, the ordering of ports can be destroyed by the translation. To handle this, the document proposes an extension attribute to SDP.	[IETF RFC3605]
3611	11-03	S	Real Time Protocol Control Protocol Extended Reports (RTCP XR)	This document defines the Extended Report (XR) packet type for the Real Time Control Protocol (RTCP) and defines how the use of XR packets can be signaled by an application if it employs the Session Description Protocol (SDP).	[IETF RFC3611]

2 This material has been taken in large part from ATIS-0800005 [ATIS-0800005], clause 3.1.2.

Table 7-1: IETF RTP and RTCP RFCs status (*end*)

RFC	Date	Status	Title	Abstract	Reference
4585	8-04	S	Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)	This document defines an extension to the Audio-visual Profile (AVP) that enables receivers to provide, statistically, more immediate feedback to the senders and thus allow for short-term adaptation and efficient feedback-based repair mechanisms to be implemented.	[IETF RFC4585]
4588	9-05	S	RTP Retransmission Payload Format	This document describes an RTP payload format for performing retransmissions.	[IETF RFC4588]
RFC Editor Queue	3-06		draft-ietf-avt-rtcpssm-13.txt	Extension that specifies how unicast NACK RTCP packets are correlated to the multicast sender for a particular RTP stream.	[b_IETF AVT-RTCPSSM]
Legend: S = Proposed Standard					

7.3 Forward Error Correction

Forward Error Correction (FEC) at the Application/Transport layers generally refers to packet erasure correction techniques. In these techniques, an amount of data is sent which is in total greater than the stream or the object to be communicated, with the property that the stream or the object can be reconstructed from any sufficiently large subset of the transmitted data. The stream or object is thus resilient to a certain amount of loss (at most the difference between the transmitted and the original data size).

7.3.1 FEC for Streaming Applications

In general, for streaming applications, there are considerable advantages in using systematic FEC codes, in which the original packets of the stream source packets are sent accompanied by a certain overhead of "repair" packets. The repair packets can be used to recover source packets which have been lost between sender and receiver.

Many possible application/transport FEC schemes for streaming media exist which could be applied to IPTV. The following are some of the erasure correction schemes for streaming media that have been standardized elsewhere:

– **IETF RFC2733 [IETF RFC2733]**

  - This defines a simple mechanism for applying short block parity codes to RTP streams. The scheme is limited by the small number of packets that can be protected as a block (24 packets). This RFC has not been widely implemented and will likely soon be obsolete by an update which provides slightly longer blocks (48 packets) and the possibility to apply unequal protection to different parts of each packet.

– **ETSI TS 126 346 – Universal Mobile Telecommunications System (UMTS); Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs [ETSI TS 126 346]**

  - This standard defines a generic framework for application of FEC to media streams. The framework is not specific to RTP and operates just above the UDP layer. This framework could be used with many FEC codes, however 3GPP specify and require support of a single specific code (the Digital Fountain Raptor code).

– **ETSI EN 301 192 Digital Video Broadcasting: DVB Specification for Data Broadcasting [ETSI EN 301 192]**

  • This defines how a link layer erasure code is intended to be used with the DVB-H system for transmission to mobile terminals. This FEC scheme operates below the IP layer and is completely independent of applications and is based on a large Reed-Solomon erasure code.

– **SMPTE Specification 2022-1: Forward Error Correction for Real-time Video/Audio Transport Over IP Networks [SMPTE-2022-1]**

  • The Pro-MPEG COP3/SMPTE 2022 [SMPTE-2022-1] standard has been designed to ensure that high quality video that is used by broadcasters for their most valuable live video feeds are able to be transported over these networks. COP#3 FEC is designed to protect a video stream from burst packet losses. The generation of FEC packets in the COP #3 standard is based upon a matrix defined by the parameters *L* and *D*. FEC packets are generated by exclusive OR (XOR) of the media packets. While Pro-MPEG COP #3 FEC may be adequate for private IP links, it is not robust enough to handle the challenges associated with moving video over highly loss IP networks such as the Public Internet.

– **ETSI TS 102 034 version 1.3.1 Transport of MPEG 2 Transport Stream (TS) Based DVB Services over IP Based Networks [ETSI TS 102 034]**

  • DVB has recently completed an evaluation of FEC codes for IPTV applications within the IPI working group [b_DVB A115]. As a result of this activity, DVB has produced an FEC specification for IPTV based on a layered approach with a base layer consisting of a simply parity (XOR) code taken from [SMPTE-2022-1] and an enhancement layer based on the Raptor code as used in the 3GPP specification [ETSI TS 126 346]. The DVB-IP AL-FEC mechanism has been carefully reviewed and assessed in the DVB project to meet the requirements of an FEC mechanism in different IPTV environments with respect to performance, flexibility, and implementation aspects.

The IETF has also initiated a new working group *fecframe* to standardize a framework for application of FEC to media streams; this is along similar lines defined by 3GPP (Multimedia Broadcast/Multicast Service for 3G cellular networks). The framework will not specify a particular FEC code but will use an approach similar to that adopted by the IETF RMT working group, which standardized protocols for reliable file delivery over IP multicast. This approach allows the most powerful FEC codes to be used for streaming mechanisms as opposed to [IETF RFC 2733], which provides a flexible framework that applies to any type of streaming format. The DVB-IP AL-FEC makes use of this concept as well.

The FEC framework is currently in draft status within the IETF.

7.3.2 FEC for Download Services

References for the relevant IETF reliable multicast transport (RMT) documents are provided in Table 7-2. The IETF has defined FEC Building Block, which describes how the specification of protocols, which use FEC, could be separated from specification of the FEC codes themselves. This has resulted in creation of a set of *plug & play* specifications which can be combined according to the needs of a given application.

Table 7-2: IETF RMT RFC status

RFC	Date	Status	Title	Abstract	Reference
2887	08-00	I	The Reliable Multicast Design Space for Bulk Data Transfer	This document provides an overview of the design space and application constraints.	[b_IETF RFC2887]
3048	01-01	I	Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer	This document describes a framework for the standardization of bulk-data reliable multicast transport.	[b_IETF RFC3048]
3269	04-02	I	Author Guidelines for RMT Building Blocks and Protocol Instantiation Documents	This document provides general guidelines to assist the authors of Reliable Multicast Transport (RMT) building block and protocol instantiation definitions.	[b-IETF RFC3269]
3450	12-02	E	Asynchronous Layered Coding Protocol Instantiation	This document describes the Asynchronous Layered Coding (ALC) protocol, a massively scalable reliable content delivery protocol.	[b_IETF RFC3450]
3451	12-02	E	Layered Coding Transport (LCT) Building Block	Layered Coding Transport (LCT) provides transport level support for reliable content delivery and stream delivery protocols. The transport is specifically designed to support protocols using IP multicast, but also provides support to protocols that use unicast.	[b_IETF RFC3451]
3453	12-02	I	The Use of Forward Error Correction in Reliable Multicast	This memo describes the use of Forward Error Correction (FEC) codes to efficiently provide one-to-many reliable data transport. Different classes of FEC codes and some of their basic properties are described.	[b_IETF RFC3453]
3695	02-04	E	Compact Forward Error Correction (FEC) Schemes	This document introduces some Forward Error Correction (FEC) schemes with a more compact FEC payload. The schemes can deliver blocks of an object of indeterminate length.	[b_IETF RFC3695]
3926	10-04	E	FLUTE – File Delivery over Unidirectional Transport	This document defines a protocol for the unidirectional delivery of files that is suited to multicast networks. The specification builds on Asynchronous Layered Coding, the base protocol for massively scalable multicast.	[b_IETF RFC3926]
5052	09-07	E	Forward Error Correction Building Block	This document describes how to use Forward Error Correction (FEC) codes to efficiently provide and/or augment reliability for data transport.	[b_IETF RFC5052]
5053	09-07	S	Raptor Forward Error Correction Scheme for Object Delivery	This document describes a Fully-Specified Forward Error Correction (FEC) scheme, corresponding to FEC Encoding ID 1, for the Raptor forward error correction code and its application to reliable delivery of data objects.	[IETF RFC5053]
Legend: I = Informative, E = Experimental, S = Proposed Standard					

FEC in download delivery services, which could be applied to IPTV services, has been standardized elsewhere. All of them rely on the IETF RMT RFCs in Table 7-2, especially on FLUTE, LCT and ALC.

– **ETSI TS 126 346 – Universal Mobile Telecommunications System (UMTS); Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs [ETSI TS 126 346]**

  • For the download delivery service of this standard File Delivery over Unidirectional Transport (FLUTE) as specified in [b_IETF RFC3926] is applied. FLUTE provides mechanisms to signal and map the properties of a file to the Asynchronous Layered Coding (ALC) protocol [b_IETF RFC3451] such that receivers can assign these parameters to the received files. The object to be transmitted is partitioned in one or several source blocks. For each source block, additional repair symbols can be generated by applying an FEC code. FLUTE could be used with different FEC codes, however 3GPP specifies and requires support of a single specific code (the Raptor code [IETF RFC5053]). FLUTE with Raptor allows the support of very efficient scheduled multicasting as well as carousel services. The latter is efficiently supported by the fountain property of the Raptor code.

– **ETSI TS 102 472 Digital Video Broadcasting: IP Datacast over DVB-H: Content Delivery Protocols [ETSI TS 102 472]**

  • The Content Delivery Protocol (CDP) for file delivery in DVB-H re-uses the technology of 3GPP MBMS [ETSI TS 126 346] download delivery. The use of Raptor codes is strongly recommended, especially for files with size larger than 32 kByte.

7.4 Hybrid Combinations of FEC with Retransmissions and Feedback

FEC and retransmission technologies for error recovery are not necessary competing technologies, but they may be used combined and complementary. By applying such combinations, some interesting benefits may be obtained. The significance of the benefits depends, among others, on the considered service, the considered distribution mean, i.e. multicast or unicast, and/or the number of available retransmission servers. This clause provides a high-level overview of possible combinations.

For retransmission-based mechanisms when combined with an FEC repair mechanism, negative acknowledgements (NACKs) of packets may result in the transmission of repair packets instead of original data packets. This may be beneficial especially for the case of multicast transmission as the repair packets may serve the retransmission request of several receivers, which may have observed the loss of different data packets. Such a scheme may allow to reduce the average transmit bandwidth.

For FEC-based mechanisms, the introduction of feedback messages may be used to influence the sender strategy. For example, if receivers are aware that the sender will transmit some small amount of initial repair data for the current source block, retransmission requests need only to be sent in case this initial repair information is not sufficient. If the loss exceeds what can be repaired by the initial repair data, retransmission requests can be made and in response the sender can send additional repair data for the source block that is independent of the initial repair data. Such a scheme may reduce the amount of necessary feedback messages and therefore may allow reducing the amount of necessary retransmission servers when compared to conventional retransmission mechanisms. In an alternative setup, a default level of AL-FEC protection is provided which is capable of correcting all anticipated errors (i.e. the same level of AL-FEC protection as for an AL-FEC-only mechanism). For each FEC source block, the receiver may send an acknowledgement packet requesting that sending of FEC data for that source block should be terminated early, because the receiver has received enough data to recover the block. Such scheme may allow reducing the average bandwidth when compared to an AL-FEC-only mechanism.

8 Usage Guidelines

8.1 General Discussion on Retransmission and FEC

This clause discusses general usage guidelines for Retransmission and FEC.

The main advantage of FEC is that there is no need for a back channel to request retransmission from the sender. It therefore very suitable for uni-directional communications, but can obviously also be used on any (bidirectional) network. FEC introduces a fixed delay due to the generation and processing of the redundant information and as data must be buffered before the error recovery can take place. The delay depends, among others, on service bitrates, FEC block size, and sending arrangements.

In case of retransmission-based error recovery, since the error recovery is handled by requesting and receiving a retransmitted packet from a server with a copy of the original stream, the time needed to receive a repair packet is composed of the Round Trip Time (RTT) between the receiver and the recovery retransmission server plus any jitter imposed in the packet repair process.

Jitter could be caused by variations in time for detecting lost packet and for generating the repair packet due to server loads. Buffering at the receiver is needed to provide time to receive repair packets before the data stream is sent to the decoder. There are trade-offs among buffer size, latency through the buffers, server load based on the number of users on the server, and quality of the video delivery.

In terms of bandwidth consumption in case of FEC, since the redundant information should be always be sent along with the original packets, it generally consumes more average bandwidth than retransmission. Since a retransmission is done on demand, the additionally required average bandwidth for error recovery can be lowered. However, note that to serve the retransmission request fast enough, a certain peak bandwidth higher than the average bandwidth needs to be reserved for retransmission. Therefore, for the case of retransmission, the bandwidth being saved compared relative to FEC may generally only be used for lower priority traffic on the shared access.

The complexity in encoding and decoding FEC data may provide some computational overhead at both the sender and receiver. Retransmission approaches do not require extra decoder computing resources because the entire lost packet is retransmitted to the receiver.

In the retransmission-based approach, an intermediate retransmission server may receive many feedback messages from multiple receivers who experience packet losses. This may lead to the phenomenon of feedback implosion, the concept of receiving many feedback messages for common errors.

To reduce the problem of feedback implosion for retransmission-based mechanisms, a careful architectural design is necessary. When retransmission is used in multicast delivery, proper attention must be paid to the ratio of clients to retransmission servers to avoid any scalability issues. A distributed retransmission approach can be introduced to resolve the issues of timeliness, scalability, and feedback implosion. A local retransmission server placed in the vicinity of the receiver can be used to recover the losses across the access and consumer environment and a core retransmission server located near the head end can be used to recover losses in the core and common losses requested via the local retransmission server. However, such architecture may require additional network equipment to serve retransmission requests or the function may reside in servers already present for other purposes. Due to the different architectural design, feedback implosion is not existent for FEC-based approaches.

Any application layer recovery scheme has a non-zero probability that a complete recovery from packet loss cannot be done. Lowering the probability for missing packets is a balance between complexity of design and quality of the received video. In case of FEC, if the packet loss exceeds the repair capabilities of the FEC scheme, recovery will not be possible. In case of retransmission, recovery may be deficient due to non-persistent Automatic Repeat reQuest (ARQ) protocols or late arrival of packets.

In these unlikely cases of failures, media post-decoder remediation schemes may need to be used.

8.2 Relation of mechanisms to the QoS classes in Y.1541

8.2.1 Overview

[ITU-T Y.1541] describes a number of QoS classes for IP networks. Specifically, Table 1/Y.1541 defines six IP network QoS classes and the respective network performance objectives. In addition, Table 3/Y.1541 proposes two additional provisional QoS classes mainly for the purpose to support sufficient QoS for digital television transmission. The difference to those in Table 1/Y.1541 is that these values need not to be met by networks until they are revised (up or down) based on operational experience.

Appendix VIII of [ITU-T Y.1541] considers digital television transmission on IP networks and concludes that, by the use of specific application layer error recovery mechanism digital television quality requirements can be met using the new provisional QoS classes.

However, as stated in the document additional experience on application layer error recovery mechanisms may allow revising the considerations on QoS classes 6 and 7. Error recovery mechanisms being considered in the ITU-T IPTV architecture are related to the QoS classes in Y.1541 and appropriate parameter settings should be applied.

For this relation, suitable performance metrics shall be applied. Table VIII.1/Y.1541 proposes some loss/error considerations. DVB and the ATIS IIF [ATIS-0800005] propose to measure the performance of mechanisms in terms of the *Mean Time Between Artefacts* (MTBA) in the video playout. Both have used a quality target of 4 hours MTBA, which also fits into the loss ratio recommendations of Table VIII.1/Y.1541.

Y.1541 QoS classes specify an upper bound on the packet loss ratio (Class 0-4: 10^{-3}, provisional classes 6 and 7: 10^{-5}), but do not specify packet loss patterns. However, suitable parameter settings to meet the requirements may be affected not only by the loss rate, but also by loss patterns. In order to present application layer reliability performance with different loss patterns, different packet loss models may be considered, e.g. independent random loss model or burst loss models.

Y.1541 also specifies limits on the IP Packet Transfer Delay (IPTD), IP Packet Delay Variation (IPDV), and IP Packet Error Rate (IPER). The effect of these parameters in relation to the error recovery mechanism is also of interest.

The performance and parameter settings for a certain mechanism may also depend on the service bit rate. This effect should also be considered when relating mechanisms to QoS classes.

8.2.2 DVB-IP AL-FEC

8.2.2.1 Parameters

The DVB AL-FEC code according to [ETSI TS 102 034], Annex E, is a block erasure code, meaning that it applies erasure protection to blocks of packets of the original stream. The code is basically fully determined by two parameters:

1) The size of each of these blocks is usually expressed in terms of the *protection period*, which is the interval of time taken to send the packets of a block.

2) For each block, the AL-FEC code provides a number of additional "repair" packets that can then be sent immediately after the original packets of the block (the "source" packets). The number of repair packets sent for each block is another parameter of the code, usually expressed as the *FEC overhead* – the ratio of repair packets to source packets.

There is a trade-off between these two parameters of the code, protection period and FEC overhead: in general if the protection period is increased then the FEC overhead required will decrease and vice versa, all other factors remaining equal. The "other factors" are the packet loss rate and pattern and the quality target. This feature allows service operators to trade efficiency vs. channel switching times.

Note that the channel switching times correlate to the latency added by the AL-FEC. However, there are also many other things which contribute to channel change time, for example IGMP latency, the need to wait for an IDR frame, RTP buffering, video decoding buffer, etc. These factors have already led to the development of a number of channel change acceleration techniques. A good survey is available in [b_ISMA TD00096] and some of the techniques described there are already deployed. These techniques can be used to mitigate the additional delay caused by the use of FEC, making it practical to consider relatively long protection periods without significantly impacting channel change time.

8.2.2.2 Relation to Network Performance Parameters

By some representative investigations, the AL-FEC mechanism is related to the different network parameters.

For the IP packet loss ratio (*IPLR)* two models are considered:

- An independent random loss model assumes that each packet is lost with independent probability. Although in practice IP packet losses are not independent, this channel provides some kind of baseline from which other cases can be assessed.
- A short burst loss model considers burst outages of fixed duration, occurring at independent random intervals (Poisson distribution). This is intended to simulate a DSL access line subject to electrical impulse noise. In this case each impulse causes an outage equal in length to the DSL inter-leaving depth, which we take to be 8ms.

For a streaming service such as IPTV the absolute *IPTD* is only important insofar as it affects channel change time and so need not be considered further here for the simulations. The IPTD is additive to the latency introduced by the AL-FEC mechanism.

The *IP packet delay variation (IPDV)* may affect performance if it results in packets arriving too late to be rendered to the user. The use of FEC mitigates this problem, since as long as each packet arrives before the appointed time to decode its FEC block there will be no problem. Packets at the beginning of a block could arrive extremely late and still arrive in time. On the other hand if packets at the end of the block arrive too late then cannot be used, but these packets may be considered lost and recovered by the FEC.

In general, as long as the IPDV is in the range of the protection period, or the protection period is greater than the IPDV as defined in Y.1541, then for QoS classes 0-4 the IPDV does not have any influence on the performance. Therefore, for QoS classes 0 and 1 and protection periods of at least 50ms, the IPDV does not influence the performance. Furthermore, it should be noted that with the addition of modest IPDV requirements, then Y.1541 Classes 2-4 would also be suitable for IPTV applications, especially if the protection period is relaxed.

It is expected that erroneous packets are detected by the UDP checksum and therefore are converted to packet losses. As the *IPER* for QoS classes 0-4 is a magnitude less than the IPLR, this effect is negligible.

8.2.2.3 Recommended Parameter Settings

The recommended parameter settings for the DVB-AL-FEC mechanism for QoS classes 0-4 are provided in the following. The influence of IPTD, IPDV, and IPER has been discussed in clause 8.3.2.2. Therefore, the benchmarking and recommended parameter setting are provided for IPLR of 10^{-3} for two channel models, namely independent random packet losses (random) and the short burst model (burst) with 8ms independent burst losses.

Results are obtained for Standard Definition (2.1Mbit/s) and High Definition (9.4Mbit/s) video streams. The streams are assumed to be CBR MPEG-2 Transport Streams (TS) encapsulated within RTP packets with 7 MPEG-2 TS packets per RTP packet to achieve a MTBA of at least 4 hours. Table 8-1 shows the required overhead for different bit rates, different channel models at IPLR 10^{-3}, and different protection periods.

Table 8-1: Required Overhead for DVB-IP AL-FEC for different bit rates, different channel models at IPLR of 10e-3, and different protection periods

Protection Period	Random, 2.1 Mbit/s	Random, 9.4 MBit/s	Burst, 2.1 Mbit/s	Burst, 9.4 Mbit/s
100 ms	16%	5%	20%	12%
200 ms	8%	3.5%	10%	6%
400 ms	5%	3%	7%	4%
600 ms	4%	2%	4%	2.5%
800 ms	3.5%	2%	4%	2.5%
1000 ms	3%	2%	4%	2%

The results show that with modest additional delay and low to modest FEC overhead, a consumer television quality target of a MTBA of 4 hours can be achieved using the standard Y.1541 QoS Classes 0 and 1. The provisional QoS classes 6 and 7 are not required by the use of the DVB-IP AL-FEC mechanism. Note that in all cases the enhanced decoder according to, Annex E, sub-clause E.5.1.2 of [ETSI TS102 034], was applied as the minimum decoder could not fulfil the service requirements.

In addition, note that if the FEC source block structure is chosen with proper alignment, for example with the random access points of the video stream, then the FEC latency can be absorbed into the video decoding buffer latency. This would mean that the protection period is in general not additive to the end-2-end latency, but generally lower. With encoding parameters and alignment strategies, even no difference in the latency may be observed when FEC is used and when it is not.

9 Recommendations

The support of an application layer error recovery mechanism is not required for all networks, in particular for networks that can fulfil the desired IPTV service requirements.

In the case that a network cannot fulfil the packet loss requirements necessary to achieve the IPTV service requirements, the use of an application layer error recovery mechanism is recommended.

For an application layer error recovery mechanism based on FEC, the DVB-IP AL-FEC in Annex E of [ETSI TS 102 034] is recommended.

- The relation of this AL-FEC mechanism to the QoS classes in Y.1541 [ITU-T Y.1541], especially recommended parameters settings for different QoS classes and different services is discussed in clause 8.2.2, specifically in Table 8-1. Consumer television quality can be achieved using the standard Y.1541 QoS Classes 0 and 1 together with the DVB-IP AL-FEC mechanism, low to modest overhead and the enhanced decoder according to [ETSI TS 102 034], Annex E, sub-clause E.5.1.2.

NOTE – An application layer error recovery mechanism based on retransmission may also be recommended.

Bibliography

[b_DVB A115] DVB A115, *Blue Book on AL-FEC Evaluations.*

[b_IETF RFC2887] IETF RFC2887 (2000) – The Reliable Multicast Design Space for Bulk Data Transfer.

[b_IETF RFC3048] IETF RFC3048 (2001) – Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer.

[b_IETF RFC3269] IETF RFC3269 (2002) – Author Guidelines for RMT Building Blocks and Protocol Instantiation Documents.

[b_IETF RFC3450] IETF RFC3450 (2002) – Asynchronous Layered Coding Protocol Instantiation.

[b_IETF RFC3451] IETF RFC3451 (2002) – Layered Coding Transport (LCT) Building Block.

[b_IETF RFC3453] IETF RFC3453 (2002) – The Use of Forward Error Correction in Reliable Multicast.

[b_IETF RFC3695] IETF RFC3695 (2004) – Compact Forward Error Correction (FEC) Schemes.

[b_IETF RFC3962] IETF RFC3962 (2004) – FLUTE – File Delivery over Unidirectional Transport.

[b_IETF RFC5052] IETF RFC5052 (2007) – Forward Error Correction (FEC) Building Block.

[b_IETF AVT-RTCPSSM] IETF AVT draft-ietf-avt-rtcpssm-13.txt (2007), RTCP Extensions for Single-Source Multicast Sessions with Unicast Feedback.

[b_ISMA TD00096] Internet Streaming Media Alliance (ISMA) TD00096 (2007), "Fast channel changing in RTP" Internet Streaming Media Alliance.

II.2.4 Performance monitoring for IPTV

Summary

Successful deployment of IPTV services requires performance to be monitored at the customer premises, key aggregation points and at interconnect points between disparate network domains. The document defines monitoring points, monitoring parameters and monitoring methods for IPTV services. It covers both network and service related performance monitoring parameters from the physical up to the application layers.

Keywords

IPTV, performance, QoS, QoE, monitoring

Current status

The document contains an extensive list of monitoring parameters relevant for IPTV services. However, definitions of the monitoring methods for many of these parameters are still required.

Dependency on or relationship to other FG IPTV documents

- IPTV services requirements document; providing the basic requirements

CONTENTS

		Page
1	Scope	278
2	References	278
3	Definitions	279
4	Abbreviations and acronyms	279
5	Conventions	281
6	Monitor points	281
	6.1 Monitoring Point Definitions	282
	6.1.1 Point 1 – PT1	282
	6.1.2 Point 2 – PT2	283
	6.1.3 Point 3 – PT3	283
	6.1.4 Point 4 – PT4	283
	6.1.5 Point 5 – PT5	283
7	Monitoring parameters	283
	7.1 Physical Layer Parameters	285
	7.1.1 RF Integrity	285
	7.2 IP Layer/Network Parameters	286
	7.2.1 Link IP Layer Used Bandwidth	286
	7.2.2 Link IP Layer Available Bandwidth	286
	7.2.3 End-to-End IP Layer Bandwidth	286
	7.2.4 End-to-End IP Layer Available Bandwidth	286
	7.2.5 Loss run length distribution	286
	7.2.6 Error-free interval distribution	287
	7.2.7 Packet Loss Metrics & Models	287
	7.2.8 Streaming Jitter (SJ)	287
	7.2.9 Packet Loss Rate	287
	7.2.10 Out of Order Packet Rate	287
	7.2.11 Burst Loss Rate	288
	7.2.12 Gap Loss Rate	288
	7.2.13 Mean Gap Length	288
	7.2.14 Mean RTP Burst Length	288
	7.2.15 Loss Period Count	288
	7.2.16 IP Maximum Loss Period	288
	7.2.17 Retransmissions	288
	7.2.18 IGMP Join/Leave Time	288
	7.2.19 IP Flow List	289

Page

7.3 Transport Stream parameters 289
7.4 Service Line-Up parameters 290
7.4.1 Channel line up 290
7.4.2 Service metadata 290
7.4.3 Channel zap time 291
7.4.4 Correctness Rate (CR) 291
7.5 Channel Attribute parameters 291
7.5.1 Channel attributes 292
7.5.2 Video quality 292
7.5.3 Audio quality 292
7.5.4 Blackout Detection 293
7.5.5 Freeze Frame Detection 293
7.5.6 Ancillary channel associated attributes 293
7.6 Content on Demand Parameters 294
7.6.1 Content on Demand request performance 294
7.7 Other Parameters 294
7.7.1 AAA Success Rate (AAASR) 294
7.7.2 STB Booting Time 294

8 Monitoring methods 294
8.1 Generalized monitoring method for multi-media data based on transmission packet loss 295
8.2 RF Integrity Monitoring 296
8.3 Network performance monitoring 297
8.3.1 Network Performance Monitoring Procedure 297
8.4 Service Attribute Monitoring 297
8.4.1 Channel line up validation 297
8.4.2 Service metadata validation 298
8.4.3 Channel zap time 298
8.4.4 Channel Attribute Monitoring 298
8.5 Video quality monitoring 298
8.5.1 Subjective quality monitoring 299
8.5.2 Objective quality monitoring 299
8.6 Audio quality monitoring 307
8.6.1 Subjective quality monitoring 307
8.6.2 Objective quality monitoring 308
8.7 Ancillary attribute monitoring 308
8.7.1 Subtitles 308
8.7.2 Closed captions 308
8.7.3 Descriptive audio 308

Page

Annex A – Considerations for Network Performance Monitoring when using Overlay Networks 309

1 Overlay Measurement 308

2 Measurement Unit 309

Bibliography 309

List of Figures

Figure 6-1: IPTV Domains 281

Figure 6-2: Monitoring Points 282

Figure 7-1: IPTV Service Hierarchy 283

Figure 8-1: Performance Monitoring Point Deployment 295

Figure 8-2: Typical Index Structure 295

Figure 8-3: Direct Observation Monitoring Model for Domain E 297

Figure 8-4: A Full-Reference Model 300

Figure 8-5: A Reduced-Reference Model 300

Figure 8-6: Back Channel for Quality Reporting 301

Figure 8-7: A streaming server which optimizes codec parameters based on the perceptual quality .. 301

Figure 8-8: A network provider which uses perceptual quality information 301

Figure 8-9: A block diagram of video quality monitoring using an RR model 302

Figure 8-10: A method for a transmitter to monitor video quality at a receiver using transmission 303

Figure 8-11: Relationship between packet-layer model and bit stream layer model hybrid perceptual/bit-stream models 304

Figure 8-12: Input requirements for FR hybrid perceptual/bit-stream models 304

Figure 8-13: Input requirements for RR hybrid perceptual/bit-stream models 304

Figure 8-14: Input requirements for NR hybrid perceptual/bit-stream models 305

Figure 8-15: Generating and transmitting video quality scores of compressed data 305

Figure 8-16: Input requirements for a FR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data 306

Figure 8-17: Input requirements for a RR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data 306

Figure 8-18: Input requirements for a NR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data 306

List of Tables

Page

Table 7-1: Monitoring points and parameters 284

Table 7-2: RF standards and their essential measurements 287

Table 7-3: Transport Stream Monitoring Parameters 290

Table 8-1: Video Quality Measurements in Various Domains 300

Table 8-2: Message Descriptions 303

Table 8-3: Audio Quality and Impairment Scales 307

Table 8-4: Audio Comparison Scale 307

Performance monitoring for IPTV

1 Scope

This document defines performance monitoring for IPTV. Monitoring parameters, monitoring points and monitoring methods are defined that allow the service provider/network operator to monitor the performance of the service delivery to the end user.

Successful deployment of IPTV services requires performance to be monitored at the customer premise (e.g. set-top-box), key aggregation points such as DSL Access Multiplexer DSLAM) or cable modem termination system (CMTS) and at interconnect points between disparate network domains. Performance monitoring can help:

- Find errors in an end-to-end system (system debugging)
- Check the resource utilization and the work load of system components
- Compare values (metrics) regarding performance of different system deployments
- Provide a base for modelling the system
- Find system bottlenecks
- Optimize IPTV network deployment
- Ensure that system performance does not degrade with time.

The goal of performance monitoring for IPTV is to provide higher QoS/QoE to customers by identifying, localizing and quantifying service and network issues.

IPTV performance monitoring can be software based, hardware based, or a hybrid of software and hardware based.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T O.211] ITU-T Recommendation O.211 (2006), *Test and measurement equipment to perform tests at the IP layer*

[ITU-T P.800] ITU-T Recommendation P.800 (1996), *Methods for subjective determination of transmission quality*

[ITU-T P.862] ITU-T Recommendation P.862 (2001), *Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs*

[ITU-T P.910] ITU-T Recommendation P.910 (1999), *Subjective video quality assessment methods for multimedia applications*

[ITU-T Y.1540] ITU-T Recommendation Y.1540 (2002), *Internet protocol data communication service – IP packet transfer and availability performance parameters*

[ITU-T Y.1543] ITU-T Recommendation Y.1543 (2007), *Measurements in IP networks for inter-domain performance assessment*

[ITU-R BS. 1283-1] ITU-R Recommendation ITU-R BS.1283-1 (2003), *A guide to ITU-R Recommendations for subjective assessment of sound quality*

[ITU-R BS.1387] ITU-R Recommendation BS.1387 (2001), *Method for objective measurements of perceived audio quality*

[ITU-R BT.500-11] ITU-R Recommendation ITU-R BT.500-11 (2002), *Methodology for the subjective assessment of the quality of television pictures*

[ETSI EN 302 307] ETSI EN 302 307 V1.1.2 (2006-06), *Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications*

[ETSI EN 300 429] ETSI EN 300 429 V1.2.1 (1998-04), *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for cable systems*

[ETSI EN 300 421] Digital Video Broadcasting (DVB); *Framing structure, channel coding and modulation for 11/12 GHz satellite services*

[ETSI EN 300 743] ETSI EN 300 743 V1.2.1 (2002-10) *Digital Video Broadcasting (DVB); Subtitling systems*

[ETSI EN 300 744] ETSI EN 300 744. Digital Video Broadcasting (DVB); *Framing structure, channel coding and modulation for digital terrestrial television*

[ETSI TR 101-290] ETSI Technical Report 101-290 (2000), *Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems*

[IETF RFC3611] IETF RFC3611 *RTP Control Protocol Extended Reports (RTCP XR)*

3 Definitions

This working document uses or defines the following terms:

TBD

4 Abbreviations and acronyms

This working document uses the following abbreviations and acronyms:

AAA Authentication, Authorization, and Accounting

AAASR AAA Success Rate

ACR-HRR Absolute Category Rating with Hidden Reference Removal

BER Bit Error Rate

CAT	Conditional Access Table
CMTS	Cable Modem Termination System
CR	Correctness Rate
CSR	Connection Success Rate
CT	Connect Time
DSCS	Double Stimulus Comparison Scale
DSLAM	DSL Access Multiplexer
DSCQS	Double Stimulus Continuous Quality Scale
EPG	Electronic Program Guide
FR	Full Reference
HTML	HyperText Markup Language
HTTP	Hyper Text Transfer Protocol
IGMP	Internet Group Management Protocol
IPDV	IP Packet Delay Variation
IPER	IP Error Rate
IPLR	IP Packet Loss Rate
IPRR	IP Reordering Ratio
IPTD	IP Packet Transfer Delay
KoD	Karaoke On Demand
MAE	Mean Absolute Error
MER	Modulation Error Ratio
MI	Metadata Integrity
MOS	Mean Opinion Score
MPTS	Multi-Program Transport Stream
MSE	Mean Square Error
MV	Metadata Validity
NMS	Network Management System
MOS	Mean Opinion Score
NR	No Reference
OSS	Operations Support System
PEAQ	Perceptual Estimation Audio Quality
PESQ	Perceptual Estimation of Speech Quality
PID	Program Identifier
PSNR	Peak Signal to Noise Ratio
PVS	Processed Video Sequence
QoE	Quality of Experience
QoS	Quality of Service
RED	Random Early Discard

RF	Radio Frequency
RR	Reduced Reference
RTCP	RTP Control Protocol
RTP	Real Time Protocol
SI	System Information
SJ	Streaming Jitter
SPTS	Single Program Transport Stream
SRC	Source Video Sequence
SSCQE	Single Stimulus Continuous Quality Evaluation
STB	Set-Top Box
TS	Transport Stream
VOD	Video on Demand
VoIP	Voice over IP
XML	Extensible Markup Language
XR	Extended Report

5 Conventions

TBD

6 Monitor points

The entire content delivery chain can be divided into multiple *domains.* Operators at domain borders have the option to perform monitoring which, when taken together, forms an end-to-end monitoring topology.

This domain approach is independent of any specific monitoring method (e.g. RR).

Monitored performance characteristics, across a single domain or multiple domains, can be integrated with existing or new operations support systems (OSS) and/or network management system (NMS) systems.

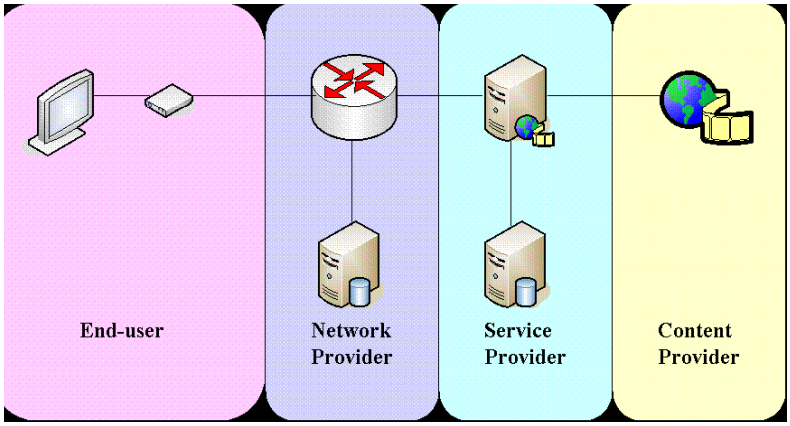


Figure 6-1: IPTV Domains

The exact topology and domains will vary from one operator to another; however, monitoring can be applied at each domain boundary. An example topology with generalized domain boundaries is shown in Figure 6-1. These domains are further divided into specific monitoring domains in Figure 6-2. Within each domain, different aspects can be monitored at each domain boundary as outlined below.

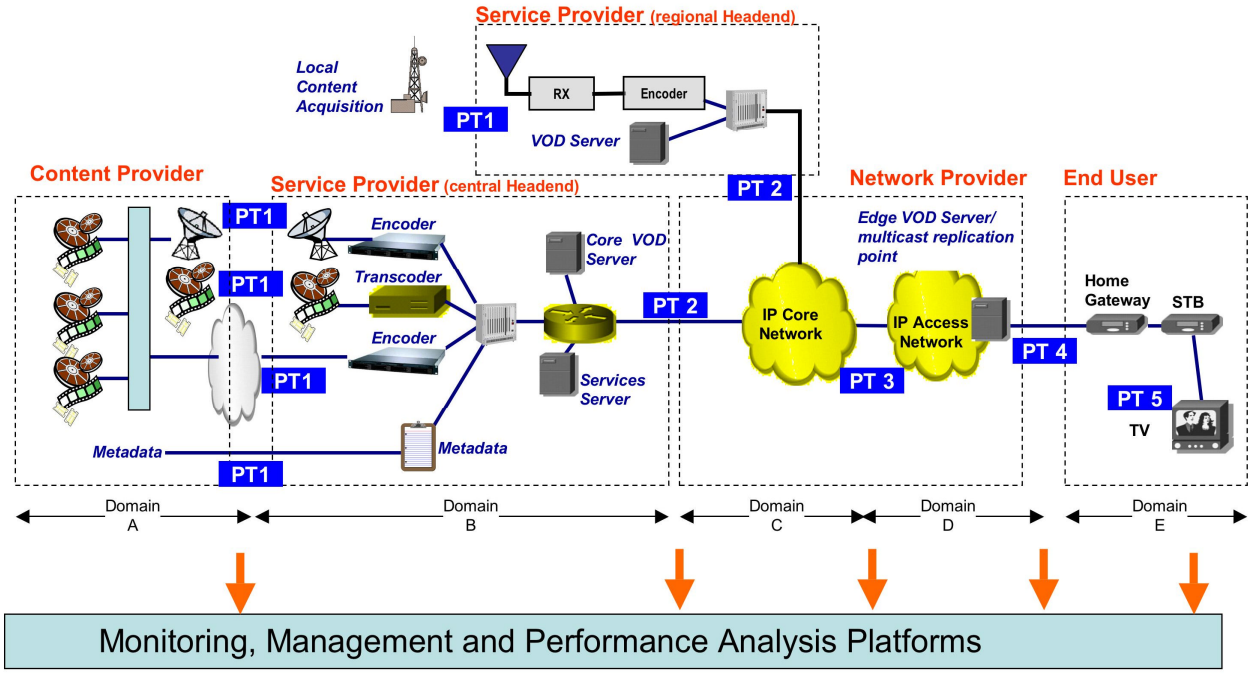


Figure 6-2: Monitoring Points

A whole performance monitoring system is recommended to include a performance monitoring management platform.

The interfaces between the performance monitoring management platform(s) and the monitoring points should be further defined in the future.

The management platform entities manage individual or some domains and collect parameters from monitoring points, perform performance analysis, and generate reports. The range of the management platform(s) may cover all domains as shown in Figure 6-2.

6.1 Monitoring Point Definitions

6.1.1 Point 1 – PT1

This point demarcates the domain border between content provision and IPTV control. It should aim for source video quality monitoring, source audio quality monitoring, and metadata verification.

6.1.2 Point 2 – PT2

This point demarcates the domain border between Service Provider and Network Provider. It should aim for original streaming quality monitoring, such as audio-visual quality monitoring, IPTV Service Attribute Monitoring, and metadata verification.

6.1.3 Point 3 – PT3

This point demarcates the IP Core and IP Edge networks where monitoring of IP-related performance parameters, such as Network Monitoring, Network Performance Monitoring are important.

6.1.4 Point 4 – PT4

This point is closest to the user where monitoring the quality of streaming, audio-visual quality, and IPTV service attribute monitoring are important.

6.1.5 Point 5 – PT5

This point is at the final end-point and directly relates to end-user QoE. Monitoring audiovisual quality and IPTV service attribute monitoring are important.

7 Monitoring parameters

This clause describes the parameters which need to be monitored at different stages of an end-to-end IPTV delivery chain. With reference to Figure 6-2 which identifies monitoring points and domains, specific parameters are applicable to only few domains, but all parameters listed are equally significant for monitoring the true performance of IPTV delivery.

There is a hierarchical relationship within an IP television service, where a physical interface (e.g. Ethernet) can carry one or many IP flows, these IP flows in turn carry single or multiple program transport streams, each channel/program within, having multiple attributes defining the content, as shown in Figure 7-1.

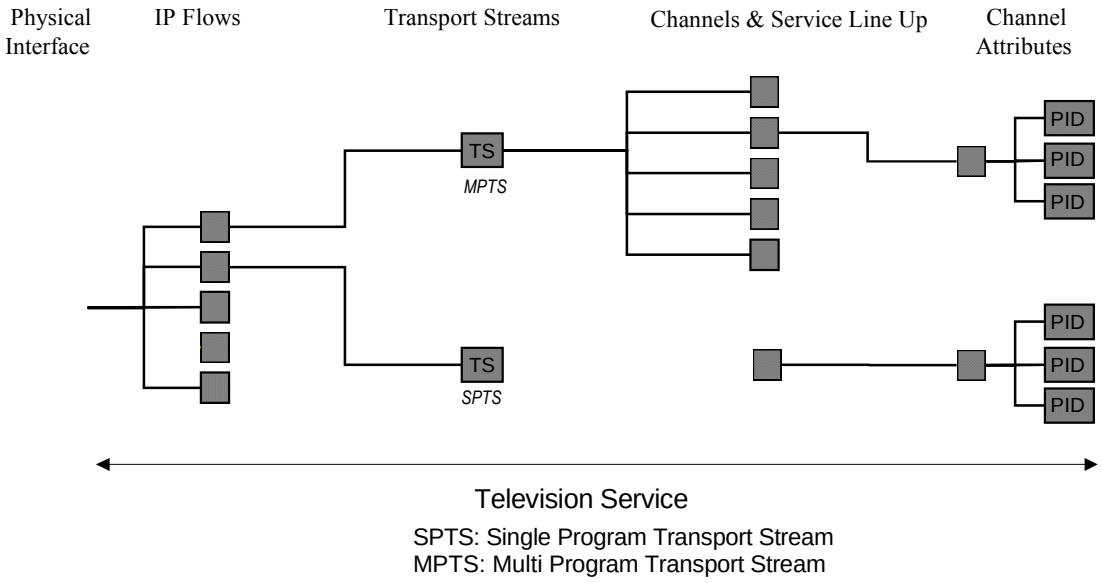


Figure 7-1: IPTV Service Hierarchy

Table 7-1 identifies the monitoring points which are shown in Figure 6-2. A checkmark in each cell of Table 7-1 indicates applicability of a monitoring parameter. These monitoring parameters are defined in this clause.

Table 7-1: Monitoring points and parameters

Monitoring Parameters	PT1	PT2	PT3	PT4	PT5
Physical Layer Parameters					
RF Integrity	✓				
IP Layer/Network Parameters					
Packet Loss	✓		✓	✓	
Packet Jitter	✓		✓	✓	
IGMP Join/Leave				✓	
IP Flow List	✓	✓	✓	✓	
Link IP Layer Used Bandwidth	✓	✓	✓	✓	
Link IP Layer Avail Bandwidth	✓	✓	✓	✓	
End-to-End IP Layer Bandwidth	✓	✓	✓	✓	
End-to-End IP Layer Avail Bandwidth	✓	✓	✓	✓	
Loss Run Length Distribution	✓	✓	✓	✓	
Error Free Interval Distribution	✓	✓	✓	✓	
Other Packet Loss Metrics & Models	✓	✓	✓	✓	
Streaming Jitter	✓	✓	✓	✓	
Packet Loss Rate	✓	✓	✓	✓	
Out of Order Packet Rate	✓	✓	✓	✓	
Burst Loss Rate	✓	✓	✓	✓	
Gap Loss Rate	✓	✓	✓	✓	
Mean Gap Length	✓	✓	✓	✓	
Mean RTP Burst Length	✓	✓	✓	✓	
Loss Period Count	✓	✓	✓	✓	
IP Maximum Loss Period	✓	✓	✓	✓	
Retransmissions	✓	✓	✓	✓	
Transport Layer Parameters					
ETSI TR 101 290 P1	✓	✓	✓	✓	
ETSI TR 101 290 P2	✓	✓			
ETSI TR 101 290 P3	✓				
Service Line-Up Parameters					
Channel Line-Up		✓			✓
Service Metadata	✓	✓			✓
Channel Zap Time					✓
Correctness Rate					✓
Connection Success Rate					✓
Connection Time					✓

Table 7-1 *(end)*

Monitoring Parameters	PT1	PT2	PT3	PT4	PT5
Channel Attributes Parameters					
Channel Attributes	✓	✓			✓
Video Quality	✓	✓	✓	✓	✓
Audio Quality	✓	✓	✓	✓	✓
Video Blackout	✓	✓			✓
Video Freeze Frame	✓	✓			✓
Audio Tone/Silence	✓	✓			✓
Ancillary Channel Associated Attributes	✓	✓			✓
VOD Parameters					
VOD Request Performance					✓
Other Parameters					
AAA Success Rate		✓			✓
STB Booting Time					✓

7.1 Physical Layer Parameters

7.1.1 RF Integrity

Table 7-2 presents a list of some commonly used radio frequency (RF) standards for the delivery of broadcast content over terrestrial, satellite and cable mediums. While this list is not exhaustive and other standards or vendor proprietary solutions may exist, the measurements below can be used to characterize the state of the RF signal. An unacceptable result in any of the measurements can result in the delivery of poor service down the transmission chain and throughout the rest of the Domains.

Table 7-2: RF standards and their essential measurements

Monitoring Parameters	Terrestrial		Satellite		Cable
RF Signal Level Signal to Noise Ratio (SNR) Modulation Error Ratio (MER) Bit Error Rate (BER)	DVB-T [ETSI EN 300 744]	8VSB [ATSC A/53B]	DVB-S [ETSI EN 300 421]	DVB-S2 [ETSI EN 302 307]	DVB-C [ETSI EN 300 429]

7.2 IP Layer/Network Parameters

[ITU-T Y.1540] defines parameters for network performance and [b_RFC 3357] defines loss distance, loss period, loss noticeable rate, loss period length, and inter loss period length.

In addition, impairments may occur in a number of burst patterns. Sparse bursts are periods of high packet loss, analogous to severely errored seconds, and is a period that begins and ends with a lost (or discarded) packet during which some constraint is satisfied. Sparse burst are often due to network congestion, Random Early Discard (RED) and related effects.

Continuous bursts are periods during which every packet is lost. Contiguous losses may occur due to packetization (i.e. packing several transport packets within an IP packet), to link failures within an IP network or other phenomena.

Finally, isolated lost packets are also possible and typically occur due to bit errors in transmission or excessive collisions on local area networks.

7.2.1 Link IP Layer Used Bandwidth

The link IP layer used bandwidth is defined as the sum of the IP layer bandwidth for all IP packet flows within in a link.

7.2.2 Link IP Layer Available Bandwidth

The link IP layer available bandwidth is defined as the maximum IP layer bandwidth which the link can provide without influencing other existing flows (background flows) in the link.

NOTE 1 – For a given link, the "Link IP Layer Available Bandwidth" plus the "Link IP Layer Used Bandwidth" is equal to the "Link IP Layer Bandwidth".

NOTE 2 – With the knowledge of the values of the above two parameters the network providers can determine the bandwidth utilization ratio of a link.

7.2.3 End-to-End IP Layer Bandwidth

The end-to-end IP layer bandwidth is defined as the maximum IP layer bandwidth an end-to-end path can provide given no background flows exist along that end-to-end path. It can be also understood as equal to the lowest Link IP Layer Bandwidth along that end-to-end path, and hence the bottleneck along that path.

7.2.4 End-to-End IP Layer Available Bandwidth

End-to-end IP layer available bandwidth is defined as the maximum IP layer bandwidth which an end-to-end path can provide without influencing other existing flows (background flows) along that path.

7.2.5 Loss run length distribution

Loss run length distribution describes the distribution of run lengths of consecutive lost IP packets.

Let l_i, $i = 1, 2, \ldots, n\text{-}1$ denote the number of loss bursts of length i, where n-1 is the longest loss burst. L denotes the number of total lost packets ($L > 0$). The loss run length distribution can be calculated as l_i/L, $i = 1, 2, \ldots, n\text{-}1$.

7.2.6 Error-free interval distribution

Error-free interval distribution describes the distribution of run lengths of consecutive correctly received IP packets.

Let f_i, $i = 1, 2, \ldots, n\text{-}1$ denote the number of error-free intervals having length i, where n-1 is the longest error-free interval. F denotes the number of total received packets ($F > 0$). The error-free interval distribution can be calculated as f_i/F, $i = 1, 2, \ldots, n\text{-}1$.

7.2.7 Packet Loss Metrics & Models

(i) Sparse bursts

Sparse bursts and extended report (XR) packet type for the RTP control protocol (RTCP) [IETF RFC3611] are periods of high packet loss, analogous to severely errored seconds. These may be modelled using multi-state Markov Models or Gilbert-Elliott models (see [b_BSTJ Elliot] and [b_BSTJ Gilbert]). A sparse burst is a period that begins and ends with a lost (or discarded) packet during which some constraint is satisfied. In [IETF RFC3611] the defined constraint is that within a burst there must be less than Gmin consecutively received packets. Gmin is selected such that the minimum effective loss rate within a burst corresponds to the lowest packet loss rate at which some noticeable distortion occurs within the decoded media stream. Sparse burst are often due to network congestion, Random Early Discard (RED) and related effects.

(ii) Continuous bursts

Continuous bursts are periods during which every packet is lost. Contiguous losses may occur due to packetization (i.e. packing several transport packets within an IP packet), to link failures within an IP network or other phenomena.

(iii) Isolated losses

Isolated lost packets typically occur due to bit errors in transmission or excessive collisions on local area networks.

7.2.8 Streaming Jitter (SJ)

Streaming Jitter (SJ) represents the maximum and minimum bit rate of the streaming server output. SJ is from the network's viewpoint and it is a vital metric when monitoring the performance.

7.2.9 Packet Loss Rate

Proportion of IP or RTP packets lost in the network or discarded by Layer 1 or 2, or lost after correction by FEC or retransmission, expressed as a binary fraction of the Total Packets Lost divided by Total Packets Expected for a given Measurement Interval.

7.2.10 Out of Order Packet Rate

Out of order packet rate indicates the proportion of (IP or RTP) packets arriving out of order, expressed as a binary fraction of the Total Packets Out of Order divided by the Total Packets Expected for a given Measurement Interval.

This indicates the proportion of packets that arrive out of order. It also indicates network condition and some video decoders discard out of order packets.

7.2.11 Burst Loss Rate

Burst loss rate indicates the proportion of IP or RTP packets lost within a (sparse) burst expressed as a binary fraction represented by the Burst Loss divided by Burst Length.

This indicates the severity of transient problems affecting video quality which is useful for configuration of FEC and retransmission.

7.2.12 Gap Loss Rate

Proportion of IP or RTP packets lost within gap periods represented by the Gap Loss divided by Total Packets Expected in the gap period.

Loss distribution before error correction. Indicates loss conditions during good quality periods.

7.2.13 Mean Gap Length

The mean gap length indicates the mean length of gaps between bursts of IP or RTP packets.

It indicates loss conditions during good quality periods.

7.2.14 Mean RTP Burst Length

The mean RTP burst length is the mean length of (sparse) burst periods or IP or RTP packets.

It indicates the severity of transient problems affecting video quality.

7.2.15 Loss Period Count

The loss period count is the count of the number of times the loss period exceeded the Loss Period Threshold.

It indicates the frequency of very severe loss conditions where the video screen will go blank.

7.2.16 IP Maximum Loss Period

Maximum number of IP packets in an excess loss event. It reports the maximum time a screen will freeze or go blank.

Useful for setting error correction or retransmission parameters.

7.2.17 Retransmissions

Retransmission shows the number of retransmitted RTP/UDP packets in a Measurement Interval.

This metric will help viewing reliability where retransmissions indicate a lost packet(s). Indicates error conditions and bandwidth usage.

7.2.18 IGMP Join/Leave Time

The time difference between the IGMP join command and the reception of the first video packet by the decoder or STB. It takes into account network latency.

The IGMP latency plus the time it takes to fill the decoder's input buffer, decode and render the content constitutes the total channel change time.

7.2.19 IP Flow List

The flow list refers to the collection of IP streams that are expected between two points in the network. This is critical in ensuring that proper delivery of IP streams occurs throughout the network.

7.3 Transport Stream parameters

The MPEG-2 Transport Stream (TS) protocol facilitates the exchange of audio/video services with associated System Information tables between compatible equipment. This mechanism is commonly used in broadcast environments.

IPTV operators might plan to deploy networks that do not use the Transport Stream protocol. This approach compromises the interoperability between networks and equipment. Such deployments have to rely on proprietary equipment. This also ties the operator with a particular equipment vendor or product family.

The following paragraphs assume that the Transport Stream packet headers are not encrypted. Some encryption schemes might involve the scrambling of all data after the IP header. In such cases, no monitoring of Transport Stream parameters is possible. Only IP related statistics would be relevant.

[ETSI TR 101-290] defines the essential TS parameters to be monitored. These are categorized according to severity and are listed as Priorities 1, 2 and 3.

- Priority 1 is defined as those "necessary for de-codability (basic monitoring)",
- Priority 2 is "recommended for continuous or periodic monitoring", and
- Priority 3 is defined as "application dependant monitoring".

Scenario 1: DVB Compliant MPEG-2 Transport streams delivery of IPTV

Monitoring all the parameters listed in Priorities 1, 2 and 3 of the [ETSI TR 101 290] specification are essential in this scenario.

Scenario 2: IPTV MPEG-2 Transport Streams without DVB System Information Tables

Operators adopt multiple approaches to deliver IPTV. The use of DVB System Information (SI) tables is optional, as operators might utilize other mechanisms to describe events and associated data. In the absence of DVB SI, certain Transport Stream tests described in the [ETSI TR 101 290] specification are still applicable.

All the tests in Priority 1 are relevant. These tests relate to basic MPEG-2 Transport Stream parameters, regardless of whether DVB SI is used.

Monitoring the Conditional Access Table (CAT) in Priority 2 is not required. The encryption algorithms used in IPTV systems might not conform to conditional access signalling protocol. All other Priority 2 parameters should be monitored.

Tests in Priority 3 are specific to DVB SI and are thus not required. IPTV operators typically utilize proprietary means to specify EPG and other data services.

Transport stream parameters – End to End IPTV monitoring

With reference to the monitoring points identified in Figure 1, the applicable transport stream parameters across different domains are marked as "Yes" in Table 2, below.

Table 7-3: Transport Stream Monitoring Parameters

ETSI TR 101 290	Domain A	Domain B (PT1 to PT2)	Domain C (PT2 to PT3)	Domain D (PT3-PT4)	Domain E (PT4- PT5)
Priority 1	Yes	Yes	Yes	Yes	Yes
Priority 2	Yes (excluding CAT_error test)	Yes (excluding CAT_error test)			
Priority 3	Yes				

7.4 Service Line-Up parameters

7.4.1 Channel line-up

It is essential to monitor the parameters applicable to the entire channels/programs offering of the IPTV Service. Monitoring these parameters is essential as it details the presence and correctness of channels intended to be delivered over the service.

Some of the parameters that need to be monitored are:

- Number of channels on the service
- Channel ID
- The names of the services
- Source of content for the services (content provider/ aggregator)
- Number of interactive channels
- Number of free to air/pay channels
- Genre of channel content and number in each genre

7.4.2 Service metadata

Service metadata carries additional information aside from the video, audio, and subtitles comprising the main components of the television service. Incorrect or non-existent metadata might severely affect overall service quality or result in legal liabilities for the operator.

A non-exhaustive list of metadata parameters includes:

- Parental or age rating
- Source provider of metadata
- Language sets correctness
- EPG correlation to actual content
- Correctness of subtitling
- Size of metadata
- Availability of metadata

Metadata Validity (MV)

Metadata Validity is for checking whether the metadata files from content provision meet or comply with the language used, syntax and semantics which has been specified in advance. For example, the IPTV control domain should check if the file used XML as the description language if XML is the normative description language for IPTV metadata file.

Metadata Integrity (MI)

Metadata Integrity is for checking whether the metadata files from content provision has contain all the necessary information and comply with the metadata specification. For example, the IPTV control domain should check all the attributes such as information about director, actor and so on when it received a metadata file of a movie for VOD purpose.

7.4.3 Channel zap time

The measure of channel zap time is the time it takes for the channel to change from the moment the subscriber presses the button on the remote until the video leaves the display.

Channel zap time is typically measured in milliseconds (ms).

7.4.4 Correctness Rate (CR)

The correctness rate is the number of times the "correct" content expected by the user is played as a percentage of total number of requests attempted by users in a pre-defined time interval. The CR can be treated as an important parameter to measure the overall users' experience of the IPTV service.

7.4.4.1 Connection Success Rate (CSR)

The Connection Success Rate is the number of connections which were successfully established with the streaming server as a percentage of total attempted connections in a unit time. The CSR is a good viewpoint from users' experience when using IPTV service.

7.4.4.2 Connection Time (CT)

Connection time measures the amount of time elapsed between the initial request by the media player or STB and the start of buffering. This time may include Domain Name System (DNS) lookup and resolution, metafile actions, RTSP handshakes and the transport of the first byte of data to the player. The CT is also a good viewpoint from IPTV users' experience.

7.5 Channel Attribute parameters

As described in Figure 7-1, each channel has specific attributes attached to it. They are embedded as part of the transport stream carrying the channels. The program ID (PID) defines the identity of the program being carried by the transport stream (TS).

7.5.1 Channel attributes

Multiple attributes of each channel have to be monitored to ensure the performance of the service.

General Parameters:

- Program ID (PID)
- Channel Name
- Number of components in the channel
- Type: Video / Audio / Data
- Conditional access: Enabled / Disabled
- Age rating
- Bit rate of the channel

Video Parameters:

- Aspect ratio
- Bit rate of the Video
- Encoding format of video content
- Resolution of Video content
- Chroma format
- Frame rate
- GOP (Group Of Pictures) size

Audio Parameters:

- Bit rate of each audio channel
- Number of Audio channels in the service
- Encoding format of the audio channels
    - Mode
    - Sampling frequency
    - Layer
- Language

7.5.2 Video quality

Video quality assessment represents the video quality grade by assessing according to the quality assessment parameter sets, subjective assessment, or objective assessment.

The user perception of video quality can only be approximated by using objective estimation models and represented as a Mean Opinion Score (MOS).

7.5.3 Audio quality

Audio quality assessment represents the audio quality grade by assessing according to the quality assessment parameter sets, subjective assessment, or objective assessment.

The user perception of audio quality can only be approximated by using objective estimation model and represented as an MOS.

7.5.4 Blackout Detection

Blackout is defined as the loss of video for a particular service. The detection is done by analysing the spatial variation in the picture after decoding the elementary stream. If the spatial variation is less than a certain threshold for a period of time, a blackout is considered to have occurred.

7.5.5 Freeze Frame Detection

A freeze frame is defined as a still picture. This condition is detected by analysing the temporal variation of the decoded pictures. If the temporal variation is less than a certain threshold for a period of time, a freeze frame condition is deemed to have occurred.

7.5.6 Ancillary channel associated attributes

7.5.6.1 Subtitles

Subtitles (also known as Closed Captions) can be defined as textual versions of the dialog in films and television programs, usually displayed at the bottom of the screen. Subtitling information can be "burned in" to the video itself, known as "hard subtitles" or passed as metadata to the program content and superimposed on the video within the set top box.

Subtitles passed as metadata within the transmission stream are sent using either proprietary formats, or according standard methods such as those defined in [CEA CEA-608D], [CEA CEA-708C], and [ETSI EN 300 743].

The parameters to be monitored for subtitling are:

- **Language**: The language of subtitling.
- **Type**: Type and formatting such as plain text, HTML or XML
- **Timing Precision**: How accurate is the timing precision of the inserted subtitles. The metric is milliseconds. Timing precision is also dependent on bit stream and frame encoding.

7.5.6.2 Descriptive audio

7.5.6.3 Conditional access/scrambling considerations

The MPEG-2 transport stream packet contains the MPEG-2 payload along with the header information. This section assumes the transport stream is in the clear and the conditional access section can be accessed.

The parameters that need to be monitored are part of the conditional access section of the MPEG-2 payload.

The monitoring sub-system must be able to decode the conditional access tables in the MPEG-2 transport stream. The presence/ absence of the conditional access can also be derived from the table decode of the MPEG-2 Transport stream.

Multiple proprietary flavours of conditional access are available, each applying the encryption services at different layers of the protocol stack.

7.6 Content on Demand Parameters

7.6.1 Content on Demand request performance

Similar to channel zap time the performance of on-demand content can be measured as the time elapsed between the user pressing the remote control button to request content until the time the video first arrives on the screen.

7.7 Other Parameters

7.7.1 AAA Success Rate (AAASR)

The success rate about service-related requests from end-users reflects the users' experience. So authentication, authorization, and accounting success rate should be monitored.

7.7.2 STB Booting Time

Turning on the STB includes the process of a user clicking on an "on" button. The time it takes for the STB to start up and be ready for service consumption (i.e. STB boot up time) is of interest to the consumer.

8 Monitoring methods

Network performance monitoring can be performed by either a network element device or a dedicated measurement device. Methods of network performance monitoring are divided largely into three categories: active monitoring, passive monitoring and active and passive hybrid monitoring.

In active monitoring, a measurement device injects test packets into the network, and the same device or a separate device at other points within the network measures test packets. This method makes the network suffer extra traffic during active monitoring time. On the other hand, it provides control of traffic generation based on various scenarios.

In passive monitoring, a measurement device just observes characteristics of packets on a network link. The observed characteristics can be used for flow analysis. This method does not generate any extra traffic, so it can measure real network status. However, there are limitations in observing characteristics of all packets and in estimating trouble scenarios.

In active and passive hybrid monitoring, passive devices can recognize the sent active probe packets and measure network level metrics such as delay and jitter from the customer's terminal to the passive measurement point. For this method to be possible, IP Performance Measurement Specification (IPPMS) which is defined in [ITU-T O.211] to uniquely identify the active probe packet across multiple administration domains is used. [ITU-T O.211] defines controller ID and flow ID to make absolute identification across multiple administration domains. The passive measurement with IPPMS capability captures the desired packets for various measurement operations. The main advantage of this method is to reduce a large number of active probes in the middle of managed networks.

8.1 Generalized monitoring method for multi-media data based on transmission packet loss

In this method, monitoring points are composed of some sampling points and a reference point. At the reference point, the whole copies of data sent by the sender must be obtained, and the sampling points can be located wherever service monitoring is requested. A bidirectional channel between the reference point and the sampling points is essential, see Figure 8-1.

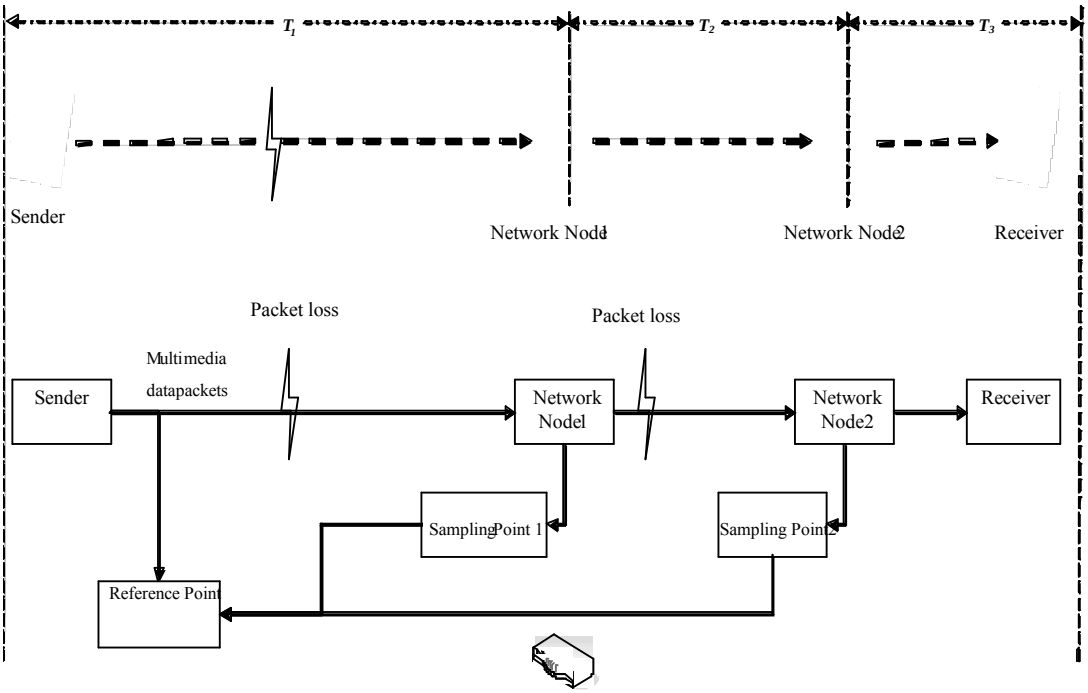


Figure 8-1: Performance Monitoring Point Deployment

There are three steps required to execute this method:

Step 1: After the reference point gets the whole copies of sender's data, the relations between transmission packet number and the characteristics are established and saved.

One typical index structure is shown in Figure 8-2.

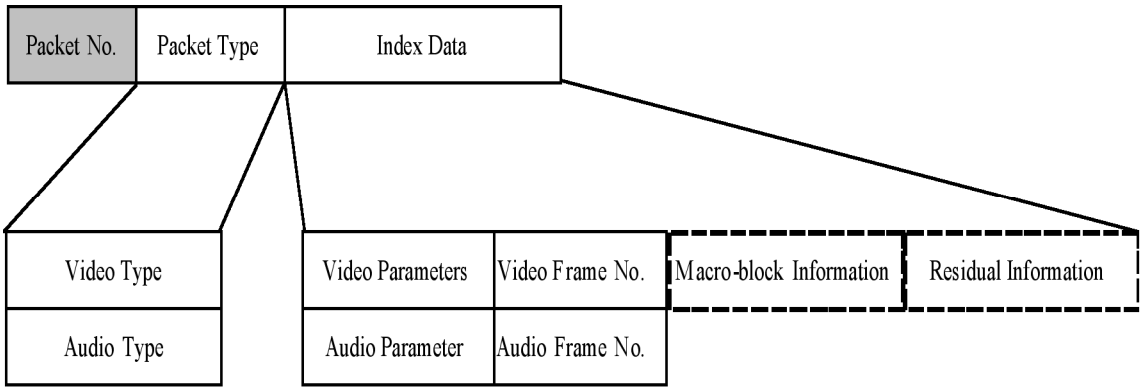


Figure 8-2: Typical Index Structure

A typical index structure includes three parts: Packet No., Packet Type, and Index Data.

Packet No.: specifies the received multi-media packet number, which is used to retrieve the multi-media data.

Packet Type: specifies the type of current multi-media packet, which can be video type or audio type.

Index Data: specifies the multi-media characteristics corresponding to the packet number.

For video type, the index data should include Video Parameters, Video Frame number, Macro-block Information and Residual Information, where Macro-block Information and Residual Information are optional multi-media characteristics for index construction.

Video Parameters: specifies the parameters of video sequences, such as image width, image height, video frame rate, video format, etc.

Video Frame number: specifies the video frame index corresponding to the multi-media video packet.

Macro-block Information: specifies the feature data that is used to reconstruct damaged video frames, including block type, block address, motion vector, reference picture index, etc.

Residual Information: specifies the difference between a prediction of a sample and its decoded value for each pixel.

For audio type, the index data should include Audio Parameters, Audio Frame No.

Audio Parameters: specifies the parameters of audio.

Audio Frame No.: specifies the video frame index corresponding to the multi-media audio packet.

Step 2: At the sampling point, received packets are sorted according to packet numbers. We can find out which packets are lost by checking the integrity of packets then feed back to the reference point.

Step 3: At the reference point, according to loss packet numbers from the sampling points, we can retrieve loss characteristics according to the stored relationship between the transmitted packet number and their characteristics. Consequently, we can judge which grade the current service belongs to.

8.2 RF Integrity Monitoring

Several processes are involved in the demodulation of RF signals. Generally, they are tuning and demodulation. Demodulation comprises of the following major blocks: analog to digital converter, frequency control and forward error correction.

The RF signal level can be extracted from the tuning stage, while the rest of the measurements can be taken from the demodulator module. The unit of measure for RF signal level is dBm.

The Signal to Noise Ratio (SNR) and the Modulation Error Ratio (MER) can be derived from the constellation of the RF signal, or by other means. The unit of measure for both the SNR and BER is decibel (dB).

The Bit Error Rate (BER) can be derived from the forward error correction stage. Depending on the RF modulation, different forward error correction schemes are used.

8.3 Network performance monitoring

Network resource and operational status monitoring shall be conducted during network operation and should include link and bandwidth characteristics, flow direction, inter-node time delay, jitter, and packet loss rate. When a monitored network parameter exceeds a threshold value defined by the operator the network operator should be notified.

8.3.1 Network Performance Monitoring Procedure

8.4 Service Attribute Monitoring

A direct observation approach to monitoring via the use of a dedicated measurement device or functionality built into a device deployed at appropriate monitoring points in the IPTV delivery network presents a true metric of service performance.

Figure 8-3 shows a deployment scenario that involves monitoring the direct user experience before and after the STB. This setup is applicable for Domain E and monitoring points 4 and 5.

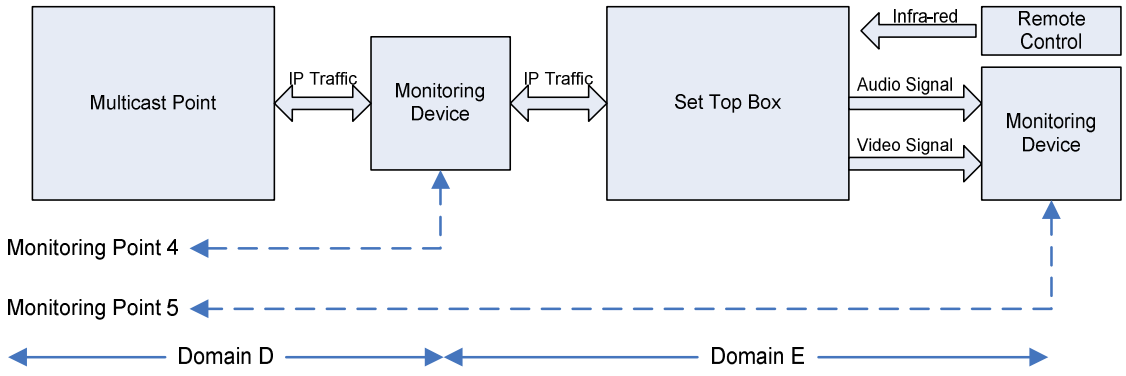


Figure 8-3: Direct Observation Monitoring Model for Domain E

8.4.1 Channel line up validation

All the channels in the service should be tested. This has to take into account the various service plans and also region-specific channels.

8.4.1.1 Channel Line Up Validation for Domain B

Channel line up validation at Domain B involves checking the various unicast and multicast IP flows prior to delivery from the headend. All the outgoing IP flows should be checked. Their unicast and multicast addresses should be correlated with the channel line up. This will ensure that the IP flows' addresses are configured correctly.

8.4.1.2 Channel Line Up Validation for Domain E

Channel line up validation at Domain E involves examining the IP traffic entering the STB as well as the audio/video output of the STB.

Examining the STB's incoming IP traffic requires checking the unicast or multicast address. Each channel is typically assigned a multicast address. A remote control should be used to invoke channel change on the STB. A correlation should be made between the remote control's channel change parameter and the multicast address of the IP traffic. This channel – multicast address correspondence is specific to an operator's service.

This test also ascertains whether an STB has received the correct channel – multicast address mapping information.

The presence and status of the audio/video output of the STB should be checked whenever a new channel change command is issued by the remote control. Presence indicates whether any audio/video content is produced. Status indicates whether the video is frozen or is in the blackout condition. For the case of audio, silence and tone should be checked. This test is applicable to all the available audio/video outputs of the STB.

8.4.2 Service metadata validation

Metadata is typically delivered via tables in the Transport Stream, or by other means, which might comprise of XML tables, HTTP traffic, encrypted data and out-of-band channel delivery. The method in which metadata is represented and delivered is usually operator and STB specific. This implies a potentially proprietary approach to decoding and examining the metadata.

8.4.2.1 Service Metadata Validation at Domains A and B

Metadata that are generated and subsequently embedded in the IP flows or delivered by other means should be decoded and validated against the operator's service offering. Multiple metadata sets can be checked simultaneously.

8.4.2.2 Service Metadata Validation at Domain E

Metadata is usually presented to the user in the form of an Electronic Program Guide. The STB's incoming IP traffic should be decoded appropriately at monitoring point 4, according to the method of delivering the metadata. This metadata should be checked against the operator's service offering. Only one metadata set can be checked at any one time.

8.4.3 Channel zap time

Channel zap time can be measured by taking the time difference between the channel change commands from the remote control and the time the new channel's video and audio are presented on the display. This measurement method takes into account the STB's internal data buffering and also the audio/video decoding time.

A device can be used to detect the presence of the new channel's video and audio content. This entails connecting the audio/video outputs of the STB to a display device. An appropriate method must be employed to determine whether audio/video content relating to the new channel is actually received.

8.4.4 Channel Attribute Monitoring

Measurement methods for this parameter are for further study.

8.5 Video quality monitoring

Video quality assessment can be carried out in two ways:

- Subjective assessment
- Objective assessment

Objective assessment can be further subdivided into the following:

- Methods based on perceptual models of the human visual system, and
- Methods based on parametric models

Subjective and objective assessment may be used appropriately. Since the performance monitoring for IPTV should be performed automatically at the monitoring points in Figure 6-2, objective assessment may be used in real IPTV services. Subjective assessment is still useful for verifying the performance of objective assessment methods.

8.5.1 Subjective quality monitoring

There are a number of subjective video quality measurement methods suggested in [ITU-R BT.500-11]. Depending on the impairment being evaluated, the selection of a method requires careful considerations of sequence duration, transmission condition, ecological environment and other factors. The output of the subjective tests is often an average of the quality ratings called Mean Opinion Score (MOS).

[ITU-R BT.500-7] recommends a five-grade impairment scale:

5 – imperceptible

4 – perceptible, but not annoying

3 – slightly annoying

2 – annoying

1 – very annoying

The grading of video quality can also be expressed as a percent from 0 to 100, with 0 indicating no distortion. The higher the value is, the greater the distortion occurs.

ITU-R BT.500-11 includes specifications on how to perform different types of subjective test. The double stimulus continuous quality scale (DSCQS) and double stimulus comparison scale (DSCS) are both double stimulus where viewers rate the quality or change in quality of two video streams (reference and impaired). The single stimulus continuous quality evaluation (SSCQE) assesses only one impaired video stream. The DSCQS is claimed to be less sensitive to the context, while SSCQE is claimed to produce more representative estimates for quality monitoring.

In addition, ITU-T P.910 includes specifications on how to perform a type of subjective test for video. The absolute category rating with hidden reference removal (ACR-HRR) is a single stimulus continuous quality evaluation.

8.5.2 Objective quality monitoring

Many advances have been made in objective video quality monitoring techniques. Although not as accurate as subjective quality measurement, objective assessment can provide quick support to fine-tuning network variables. Due to the complexity and time consuming nature of subjective video monitoring, there has been significant development of perceptual video quality measurement (PVQM) algorithms in recent years in an attempt to replicate the scores given by subjects in an objective tool. Objective quality monitoring can be classified into following categories:

- Techniques based on models of human video perception
- Techniques based on video signal parameters

Human video perception models attempt to emulate the characteristics of the human visual system to obtain video quality scores. A good model should yield high correlation to the ratings the actual viewers would provide. Three popular approaches can be used:

- Full reference (FR) – both the original transmitted and received video are available to determine the video quality (Figure 8-4).
- Reduced reference (RR) – partial information about transmitted video and full information about received video are available to determine the video quality (Figure 8-5).
- No reference (NR) – only the received video is available to determine the video quality.

By comparison between the transmitted and received video, various parameters can be obtained which are valuable in quality monitoring. Mean square error (MSE) and mean absolute error (MAE) calculate the frame difference between corresponding streams. The difference can also be assessed by the peak signal to noise ratio (PSNR) which is the log of the ratio of the peak signal squared to the MSE in a similar fashion to analogue system.

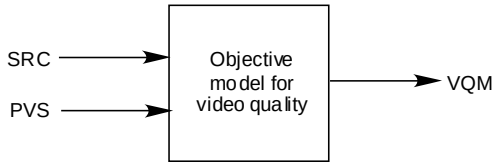


Figure 8-4: A Full-Reference Model

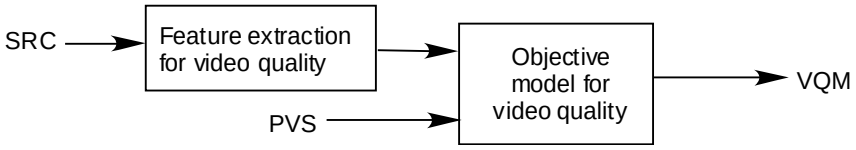


Figure 8-5: A Reduced-Reference Model

The three objective models of measuring video quality can be applied to different parts of the IPTV delivery chain. Cells marked "Yes" in Table 8-1 are relevant in their corresponding domains. Blank cells are not relevant.

Table 8-1: Video Quality Measurements in Various Domains

	PT 1	PT 2	PT 3	PT 4	PT 5
Full Reference	Yes	Yes			
Reduced Reference	Yes	Yes	Yes	Yes	Yes
No Reference	Yes	Yes	Yes	Yes	Yes

8.5.2.1 Back channel requirements

IPTV terminals may have a video quality evaluation function and a reporting function of the video quality scores to IPTV servers (or service managing servers) in order to gather video quality reports from all or some of IPTV terminals.

When this approach is employed, an appropriate transmission protocol to send video quality scores and other information related with end-user quality is required. Furthermore, an appropriate transmission protocol to send feature information is required, when a reduced reference method is employed for video quality evaluation.

This approach is shown in Figure 8-6.

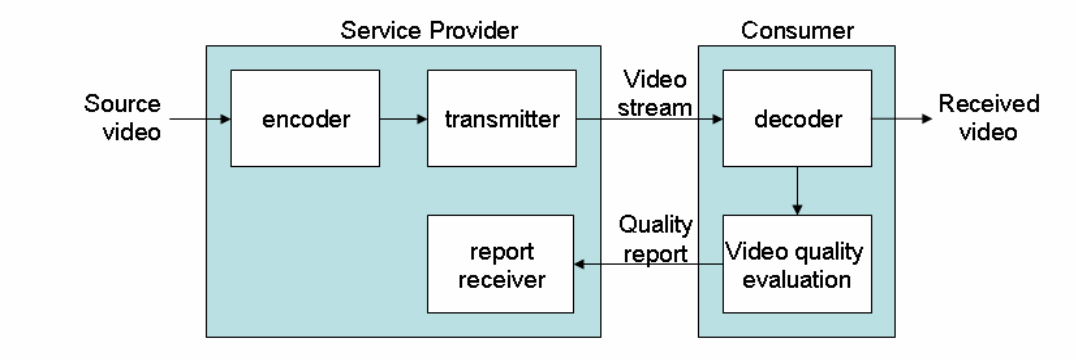


Figure 8-6: Back Channel for Quality Reporting

Quality measurements can be made at various measuring points including a number of reference points and terminals and can be used for various purposes. For example, they can be used for quality-based billing. Quality monitoring can be also used to optimize codec parameters at streaming servers. Furthermore, it can be used for network management. Therefore, depending on applications, the unit in which quality measurements are performed should send the quality scores to the corresponding destination. If the quality scores are used for quality-based billing, the measuring unit should send the information to the service provider (Figure 7). When quality scores are used to optimize the codec parameters, the measuring unit needs to send the information to a streaming server (Figure 8-7). If they are to be used for network management, the measurement results need to be sent to the network provider (Figure 8-8).

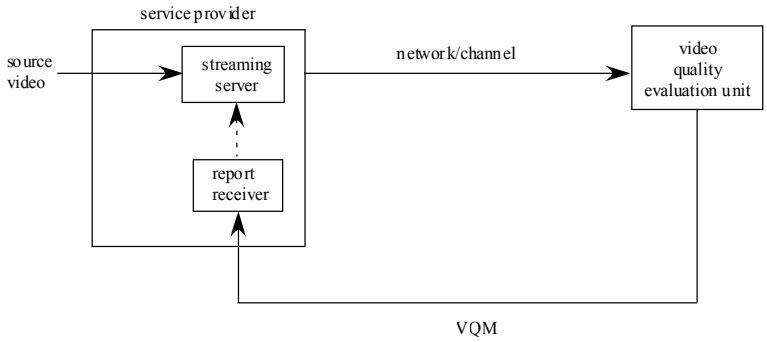


Figure 8-7: A streaming server which optimizes codec parameters based on the perceptual quality

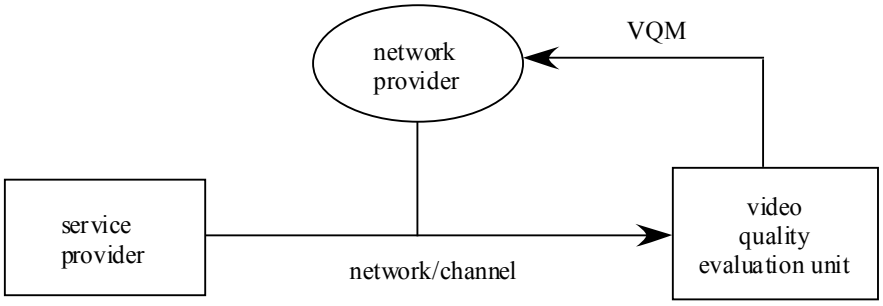


Figure 8-8: A network provider which uses perceptual quality information

8.5.2.2 Full-Reference Models

A full-reference model requires that both source video sequences and processed video sequences should be available at the measurement point.

ITU-T J.144 specifies different types of objective test methods for monitoring objective video quality as a full reference model. They are based on human video perception.

8.5.2.3 Reduced-Reference Models

A reduced-reference method can be employed to monitor the perceptual video quality at a measurement point. If a reduced-reference method is used at the receiver, the transmitter needs to transmit feature data in addition to video data (Figure 8-9). When a reduced-reference is to be employed in IPTV applications, a transmission protocol to send the feature data should be specified. It is desirable that the feature data should be available at the receiver in a timely manner. It is preferred that the feature data is sent with a time advance. Furthermore, some error handling mechanisms should be employed for sending the feature data.

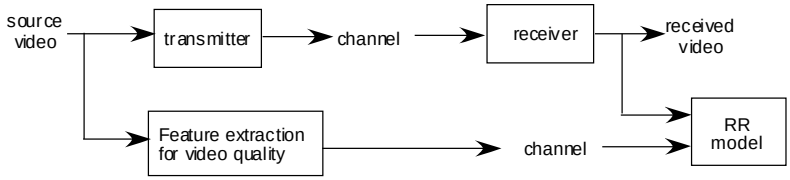


Figure 8-9: A block diagram of video quality monitoring using an RR model

8.5.2.4 No-Reference Models

When a no-reference method is used, there may be no special requirements for the system.

Although the performance of no-reference methods is inferior to that of full-reference and reduced-reference methods, it can be improved by developing NR methods which also use video stream data.

8.5.2.5 Reconstructing the received video using transmission error information

In digital communications, transmission errors include packet loss and packet delay and their effects can be exactly identified when video data is transmitted using packets. Furthermore, if there is no transmission error, the video quality at the receiver will be identical to the video quality of the video sent by the transmitter. Therefore, if the receiver sends transmission error information which includes information on packet loss and delay in packetized video transmission, the service provider can exactly reconstruct the received video seen at the receiver (Figure 8-10). Finally, the service provide may use a FR or RR method to evaluate the video quality of the received video seen at the receiver. Table 8-2 describes messages for sending transmission error information to the service provider.

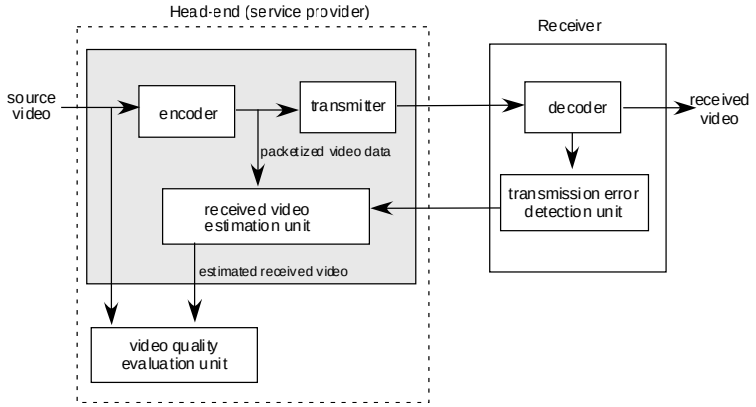


Figure 8-10: A method for a transmitter to monitor video quality at a receiver using transmission

Table 8-2: Message Descriptions

Type of transmission error	Message description
Information on the receiver	Message identifying the model
Source Identifier	Message identifying the source
Information on a lost packet	Lost packet index
Information on lost packets	Starting packet index and an ending packet index of the lost packets
Information on a delayed frame	Delayed frame index and the amount of delayed time
Information on a skipped frame	Skipped frame index
Information on skipped frames	Starting frame index and an ending frame index of the skipped frames

8.5.2.6 Packet-layer model

The packet-layer model can estimate video quality using IP information that excludes video-related payload information, as shown in Figure 8-11. This model cannot take into account the effects of video content on the subjective quality. Its computational load is very light because it does not use video-related payload information.

8.5.2.7 Bit stream layer model

It is possible that an objective model may have access to bit stream data from which the model can obtain additional information on transmission errors (e.g., delay, packet loss), codec parameters (e.g., type, bit-rates, frame rates, codec parameters), etc. This kind of information is easily available from bit-stream data at the receiver. It is expected that such models may provide improved performance in terms of accuracy and speed compared to objective video quality models which use only processed video sequences.

The bit stream layer model can estimate the quality of each video sequence using IP information that includes video-related payload information, as shown in Figure 8-11. That is, it can take into account the effects of video contents.

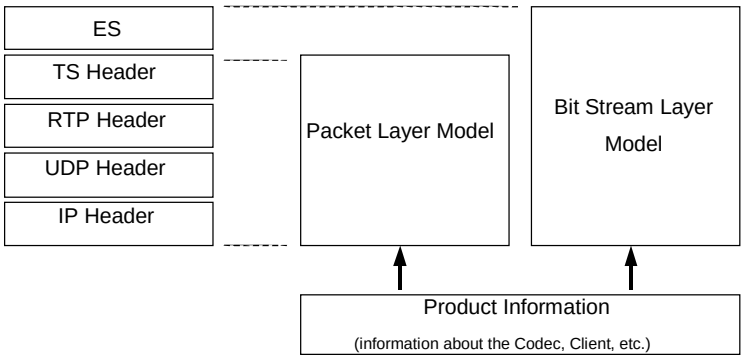


Figure 8-11: Relationship between packet-layer model and bit stream layer model hybrid perceptual/bit-stream models

If an IPTV terminal or monitoring equipment is to use such a hybrid perceptual/bit-stream model for quality monitoring, it should provide bit-stream data to the model. The input requirements for hybrid perceptual/bit-stream models are shown in Figure 8-12, Figure 8-13 and Figure 8-14.

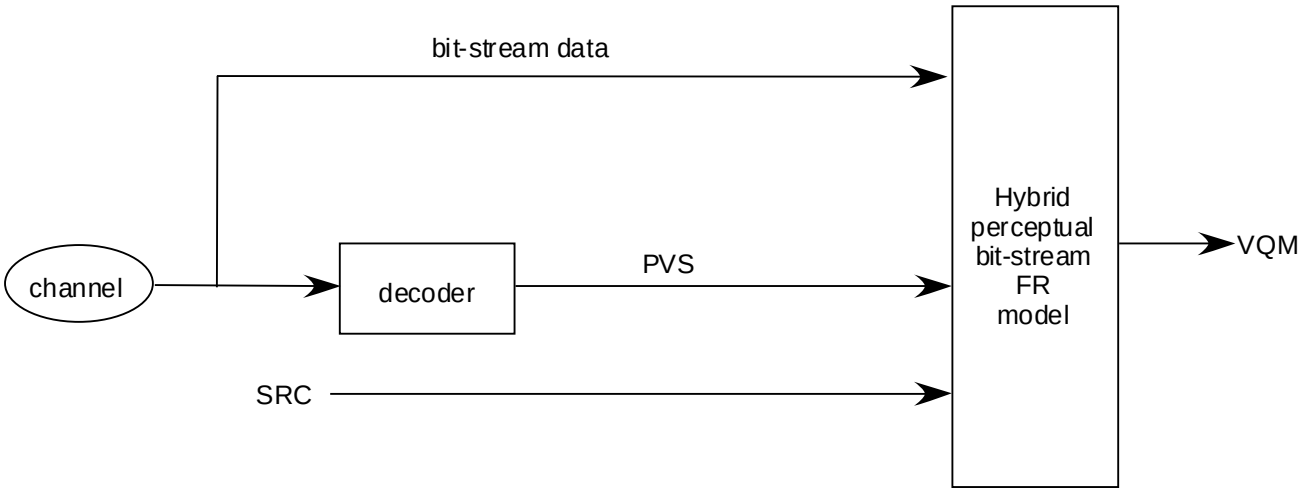


Figure 8-12: Input requirements for FR hybrid perceptual/bit-stream models

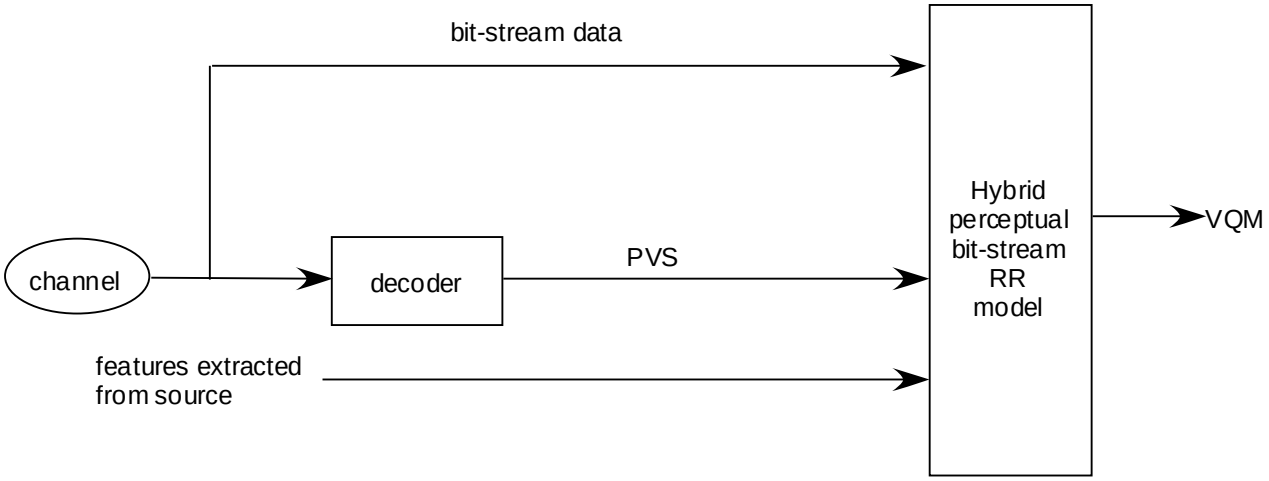


Figure 8-13: Input requirements for RR hybrid perceptual/bit-stream models

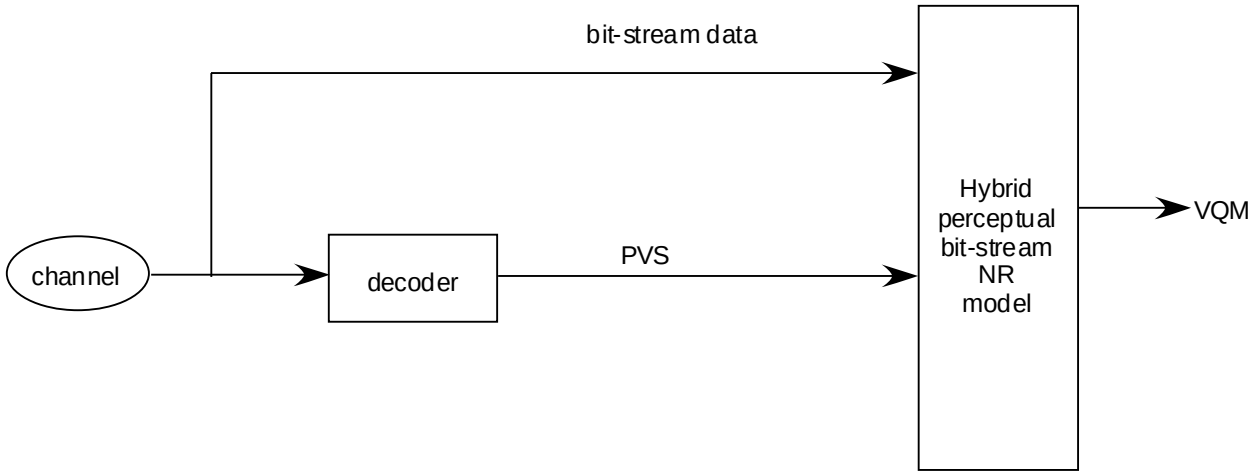


Figure 8-14: Input requirements for NR hybrid perceptual/bit-stream models

In order to improve the accuracy of objective models, it is also possible to transmit video quality scores of the compressed video data which are transmitted (Figure 8-1). Periodic video quality measurements should be made such that sufficient information is available on the video quality of the processed video quality sequence. If there are no transmission errors, the video quality at the receiver would be the same as that of the transmitted video sequence. If transmission errors occur, the received video sequence suffers from both compression impairments and transmission error impairments. With video quality scores available, an objective model which measures the video quality of the received video sequence may be improved, particularly for NR models. The video quality scores can be transmitted as metadata. Alternatively, they can be transmitted using watermark techniques.

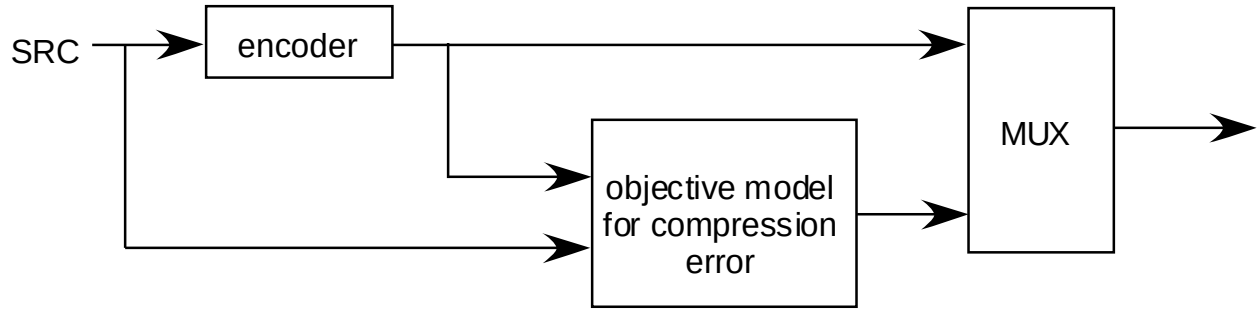


Figure 8-15: Generating and transmitting video quality scores of compressed data

If an IPTV terminal or monitoring equipment are to use these objective models for quality monitoring, the input requirements are shown in Figure 8-16 through Figure 8-18.

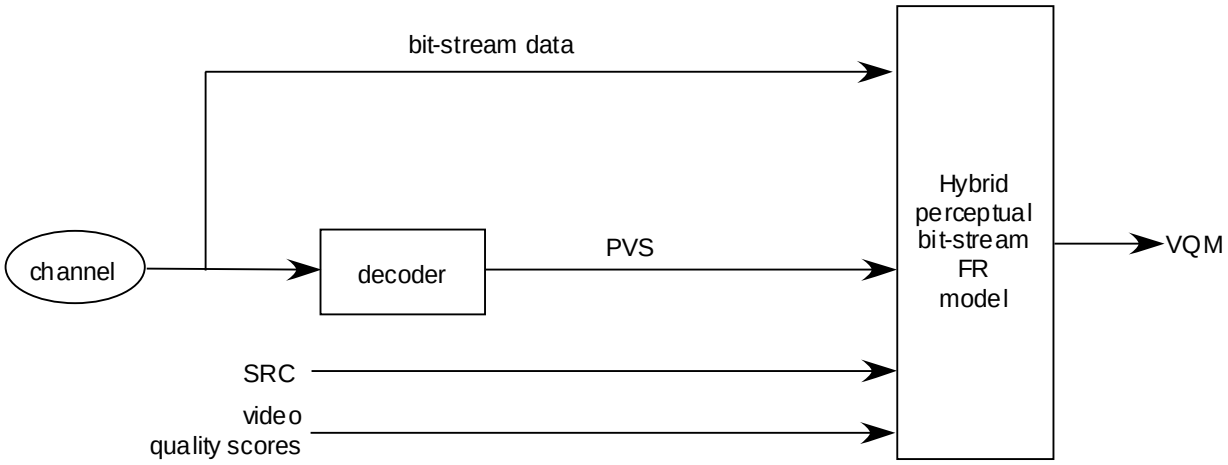


Figure 8-16: Input requirements for a FR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data

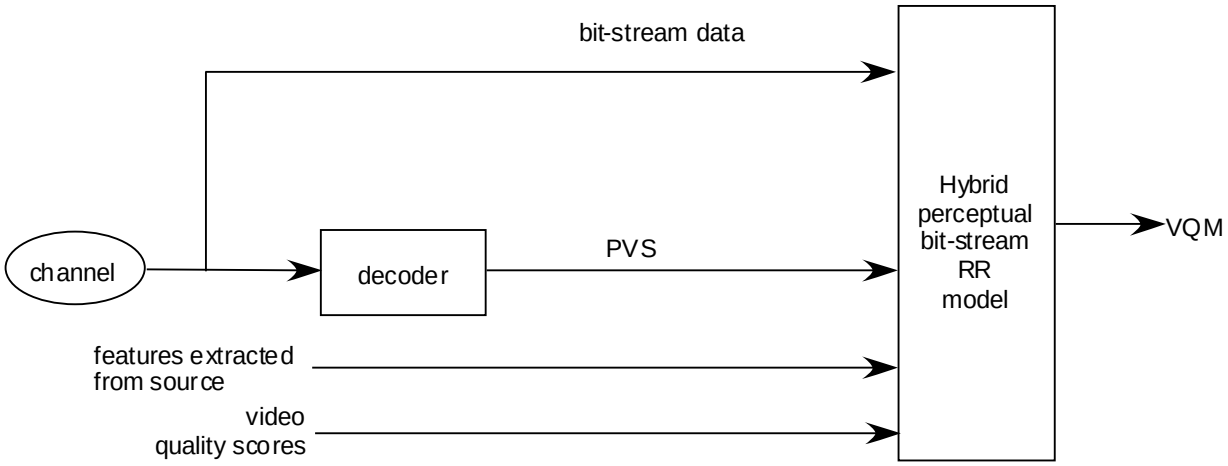


Figure 8-17: Input requirements for a RR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data

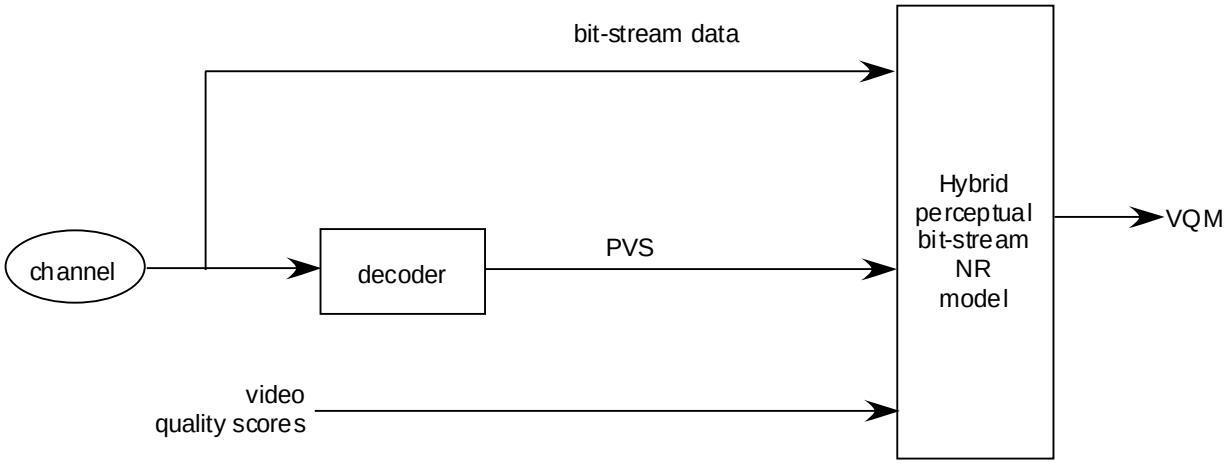


Figure 8-18: Input requirements for a NR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data

8.6 Audio quality monitoring

Audio quality can be carried out in two ways:

- Subjective assessment
- Objective assessment

8.6.1 Subjective quality monitoring

There are a number of subjective audio quality measurement methods suggested in ITU-R BS.1283-1 and ITU-T Recommendation [ITU-T P.800]. The methods used for the subjective assessment of sound quality itself and of the performance of audio systems depend to some extent on the intended purpose of the assessment. The output of the subjective tests is often an average of the quality ratings, called Mean Opinion Score (MOS).

The following five-grade scales may be used for the subjective assessment of sound quality or impairment as shown in Table 8-3.

Table 8-3: Audio Quality and Impairment Scales

Quality		Impairment	
5	Excellent	5	Imperceptible
4	Good	4	Perceptible, but not annoying
3	Fair	3	Slightly annoying
2	Poor	2	Annoying
1	Bad	1	Very annoying

For comparison tests, either a method based on the seven-grade comparison scale shown in Table 8-4 or one based on numerical differences using the above five-grade scales may be used. In general, these are not equivalent and may not give the same results. It is essential that the intended direction of the comparison be clearly indicated.

Table 8-4: Audio Comparison Scale

Comparison	
3	Much better
2	Better
1	Slightly better
0	The same
–1	Slightly worse
–2	Worse
–3	Much worse

ITU-R BS.1283-1 shows the list of Recommendations on subjective methods for audio quality assessment. Clearly, some areas of application overlap. The applicability of one or more of the Recommendations should be decided, based on the purpose of the tests, before the tests are designed.

8.6.2 Objective quality monitoring

Since subjective quality assessments are both time consuming and expensive, it is desirable to develop an objective measurement method in order to produce an estimate of the audio quality. A number of methods for making objective perceptual measurements of perceived audio quality have been introduced during the last decade, including Perceptual Estimation Audio Quality (PEAQ), the full reference audio quality estimation method in the [ITU-R BS.1387] and Perceptual Estimation of Speech Quality (PESQ) as defined in [ITU-T P.862].

One must, however, keep in mind that objective measurement methods are not generally a substitute for formal subjective listening tests.

8.7 Ancillary attribute monitoring

Measurement methods for this parameter are for further study.

8.7.1 Subtitles

Measurement methods for this parameter are for further study.

8.7.2 Closed captions

Measurement methods for this parameter are for further study.

8.7.3 Descriptive audio

Measurement methods for this parameter are for further study.

Annex A

Considerations for Network Performance Monitoring when using Overlay Networks

(This annex forms an integral part of this document.)

1 Overlay Measurement

In applications such as IPTV overlay multicast, the overlay path is constructed between overlay nodes in the application layer to perform overlay functions. In order to ensure high performance of the overlay network, overlay measurement needs to be carried out to measure the IP network performance, e.g. bandwidth, packet loss between overlay nodes such that the appropriate overlay path is selected.

On the other hand, overlay measurement can also be used by the service providers to monitor the IP network performance of the delivered applications to help ensure QoS to the end users. For example, if the IP network performance of an overlay path is poor, another overlay path may be constructed to guarantee good service quality to the end users.

2 Measurement Unit

A network measurement unit for overlay measurement is recommended to be deployed in the IP network layer. The reason is that the network measurement unit could reside on, or correspond with one or more existing network monitoring points (defined in Section 6 – "Monitor Points" in WD – "Performance Monitoring for IPTV") to utilize the capability of performance monitoring of these monitoring points.

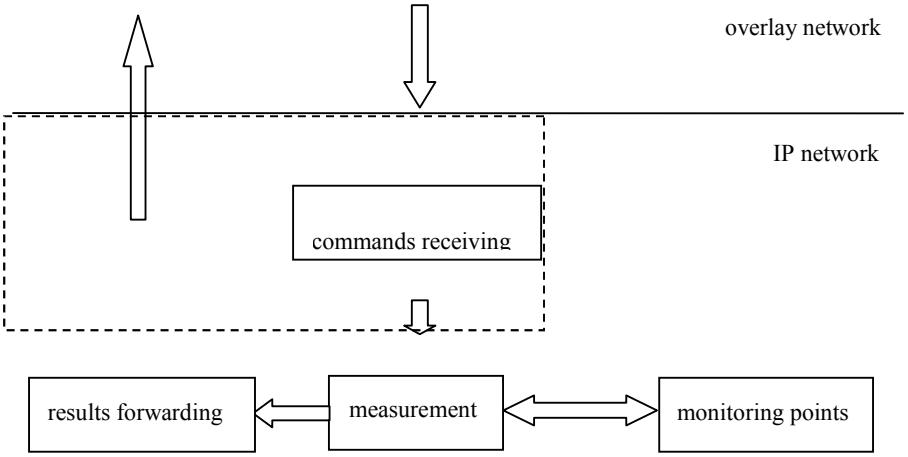


Figure A.1: Network Measurement Unit

Hence, a network measurement unit could include a receiving function, measurement function and forwarding function, as shown in Figure A.1. The receiving function receives overlay measurement commands from the overlay network and forwards the commands to the measurement function. The measurement function calls the network monitoring points to measure the performance between network devices and forwards the results to the forwarding function. The forwarding function sends the network measurement results to the overlay network.

Bibliography

[b_ATSC A/53B] Advanced Television Systems Committee (June 2005), Digital Audio Compression (AC-3) (E-AC-3) Standard, Rev. B.

[b_IETF RFC3357] IETF RFC 3357 (August 2002), *One-way Loss Pattern Sample Metrics*.

[b_BSTJ Elliot] E. O. Elliot. *Estimates of error rates for codes on burst-noise channels*. Bell System Technical Journal, 42:1977-1997, September 1963.

[b_BSTJ Gilbert] E. N. Gilbert, *Capacity of a burst-noise channel*. Bell System Technical Journal, 39:1253-1265, September 1960.

II.3 SERVICE SECURITY AND CONTENT PROTECTION

II.3.1 IPTV security aspects

Summary

This document addresses threats, requirements, architecture, and mechanisms that pertain to security and protection aspects of IPTV content, services, networks, terminal devices, and subscriber (end-users).

Keywords

Authentication, Authorization, Content Protection, Encryption, Privacy Protection, Rights Management, Scrambling, Security, Service Protection, Threat Analysis.

Introduction

IPTV services, content delivered through such services, terminal devices used in the processing and presentation of such services require consideration of many security aspects. This document develops requirements, architectural models, functional entities, interfaces, mechanisms, and additional informative background material that describes and addresses these security aspects.

Current Status

The current output work document is complete.

Future work may focus on refinement of security related functional entities, specification of security interfaces, and elaboration of detailed aspects of security mechanisms. Additional refinement of the distinction(s) between service protection aspects and content protection aspects would be beneficial.

Dependency on or relationship to other FG IPTV Documents

- IPTV Service Requirements document
- IPTV Architecture document

CONTENTS

		Page
1	Scope	314
2	References	314
3	Definitions	314
3.1	Terms defined elsewhere	314
3.2	Terms defined in this Recommendation	315
4	Abbreviations and acronyms	317
5	Conventions	317
6	Security Requirements	318
6.1	General Security Requirements	318
6.2	Content Security Requirements	318
6.3	Service Security Requirements	320
6.4	Network Security Requirements	322
6.5	Terminal Security Requirements	322
6.6	Subscriber Security Requirements	323
7	Security Architecture	324
7.1	General Security Architecture	324
7.2	Content Protection Architecture	325
7.3	Service Protection Architecture	327
7.4	Security Functional Entities	328
7.4.1	General Architecture Entities	328
7.4.2	Content Protection Architecture Entities	329
7.4.3	Service Protection Architecture Entities	330
7.5	Security Interfaces	330
8	Security Mechanisms	330
8.1	Security Mechanisms that pertain to Content or Content Protection	331
8.1.1	Content Tracing	331
8.1.2	Watermarking	331
8.1.3	Content Labelling	331
8.2	Security Mechanisms that pertain to Services or Service Protection	331
8.2.1	Service Authentication	331
8.2.2	Service Authorization	332
8.2.2	Service Access Control	332
8.3	Security Mechanisms that pertain to Networks	332
8.4	Security Mechanisms that pertain to Terminal Devices	332
8.5	Security Mechanisms that pertain to Subscribers or End-Users	332
8.6	Security Mechanisms that pertain to Multiple or Unspecified Functional Areas	333
8.6.1	Programmatic Content	333
Annex A – Service Authorization for Linear TV Service (Informative)		333
Annex B – Subscriber Security Protection (Informative)		335

Page

Appendix I – Security Threats 337
I.1 Security Attack Points 338
I.2 Security Threats Model 340
I.2.1 Content Security Threat 341
I.2.2 Service Security Threat 341
I.2.3 Network Security Threat 342
I.2.4 Terminal Device Security Threat 343
I.2.5 Subscriber Security Threat 345
Appendix II – Discussion of Interoperability of SCP 346
Appendix III – An example of IPTV Service and Content Protection Process 352
Appendix IV – Usage Rights 354
Appendix V – Downloadable Application Protection 355
V.1 Authorization and authentication before the software downloading 355
V.2 Authorization and authentication during the software program running 356
V.3 The encryption of the software programs when the programs are stored in STB, and decryption before running/duplicating the software programs 357
Appendix VI – DVB Content Protection & Copy Management 358
VI.1 Introduction 358
VI.2 Definitions 358
VI.3 Abreviations and acronyms 359
VI.4 CPCM Architecture 360
VI.5 CPCM Reference Model & Functional Entities 361
VI.6 CPCM Authorized Domain 361
VI.7 CPCM Content Usage Rules 361
VI.8 Usage State Information Metadata 362
VI.9 CPCM Content 362
VI.10 CPCM Device 362
VI.11 Usage Rule & Usage State Information 362

IPTV Service security and content protection aspects

1 Scope

This document addresses threats, requirements, architecture, and mechanisms that pertain to security and protection aspects of IPTV content, services, networks, terminal devices, and subscribers.

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 document 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 published regularly.

A reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

[FG IPTV-DOC-0147] ITU-T IPTV Focus Group, *IPTV Service Requirements*

[FG IPTV-DOC-0181] ITU-T IPTV Focus Group, *IPTV Architecture*

[ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems*

[ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Access Control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 Authentication [ITU-T X.800]: See Data Origin Authentication and Peer-Entity Authentication.

3.1.3 Authorization [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 Accessibility [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 Confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.6 Data Origin Authentication [ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.7 Denial of Service [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.8 Digital Signature [ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

3.1.9 Integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.10 Key [ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.11 Key Management [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.12 Masquerade [ITU-T X.800]: The pretence by an entity to be a different entity.

3.1.13 Peer-Entity Authentication [ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.1.14 Privacy [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.15 Repudiation [ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.16 Security label [ITU-T X.800]: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

NOTE – The marking and/or binding may be explicit or implicit.

3.1.17 Security policy [ITU-T X.800]: The set of criteria for the provision of security services.

3.1.18 Threat [ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This document defines the following terms:

3.2.1 Acquisition: The process of obtaining content by the end-user.

NOTE – For content with accessibility features this means that the content will be available in a form that can be used by the end-user.

3.2.2 Conditional Access: The function served by a Conditional Access System; often used as an abbreviation for Conditional Access System.

3.2.3 Conditional Access System: A component of a Service and Content Protection system the purpose of which is to prevent unauthorized (unentitled) access to a service or to content.

3.2.4 Content Protection: Ensuring that an end-user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder.

3.2.5 Content Tracing: A process to enable the identification of the (arbitrary) origin of content, and/or the responsible party (e.g. the end-user), to facilitate subsequent investigation in the event of unauthorized use of content, for example, content copying or redistribution.

NOTE – Content tracing information may be attached to content either as metadata, or as a forensic watermark.

3.2.6 **Digital Rights Management:** A synonym for Service and Content Protection or Content Protection, depending upon the context of use.

NOTE – In this document, the term Service and Content Protection is used instead of Digital Rights Management.

3.2.7 **Phishing:** Act of acquiring sensitive or personal information such as usernames, date of birth, passwords or credit card details, by masquerading as a trustworthy entity.

3.2.8 **Rights:** One or more legal or business entitlements to Use or employ Content, e.g., to view, record, redistribute Content.

3.2.9 **Rights Expression:** The syntactic embodiment of Rights in a concrete form.

3.2.10 **Scrambling Algorithm:** An algorithm used in a scrambling (encryption) or descrambling (decryption) process.

3.2.11 **SCP End-to-End:** Using a single Service and Content Protection system, two or more devices exchange and access content according to granted rights. This mode should be the simplest mode to implement since only a single Service and Content Protection system.

3.2.12 **SCP Bridge:** On a single device, two or more Service and Content Protection systems are operative. Content acquired via one Service and Content Protection system can be accessed via another Service and Content Protection system resident on the same device according to granted rights.

3.2.13 **SCP Interchange:** This case is characterized by two or more devices, each device having one or more operative Service and Content Protection systems. The content acquired by one device through one of its Service and Content Protection systems can be securely transferred to and accessed on another device through a different Service and Content Protection system according to granted rights.

3.2.14 **Service:** A set of functionality enabled by a provider for end users; for example, providing IP connectivity with managed quality of service, providing an IPTV Service, providing a content on demand service, etc.

3.2.15 **Service Protection:** Ensuring that an end-user can only acquire a service, and, by extension, the content contained therein, that they are entitled to receive.

3.2.16 **Service and Content Protection:** A combination of Service Protection and Content Protection, or a system or implementation thereof.

3.2.17 **Spoofing:** An activity in which a forged (spoofed) source (e.g. a person or computer program) successfully masquerades as a legitimate source by falsifying data and for the purpose of obtaining information and/or obscuring the true source to prevent non- repudiation for spreading computer viruses.

3.2.18 **Terminal Device Protection:** Ensuring that a terminal device employed by an end-user in the reception of a Service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters (e.g., saved keys) not otherwise protected.

3.2.19 **User Privacy Protection:** Ensuring that information considered to be private (or confidential) by an end-user be maintained in confidence, while remaining subject to mandatory disclosure due to legal processes.

3.2.20 **Use:** The purpose(s) for which acquired content is employed

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, and Accounting
CAS	Conditional Access System
CDN	Content Delivery Network
CP	Content Protection; Content Provider
CPE	Customer Premises Equipment
DoS	Denial of Service
DRM	Digital Rights Management
DVI-D	Digital Visual Interface – Digital Only
HDD	Hard Disk Drive
HDMI	High Definition Multimedia Interface
IPTV	Internet Protocol Television
PC	Personal Computer
PKI	Public Key Infrastructure
PVR	Personal Video Recorder
REL	Rights Expression Language
SCP	Service and Content Protection
SCP-B	SCP Bridge
SCP-EE	SCP End-to-End
SCP-IX	SCP Interchange
SP	Service Protection; Service Provider
WM	Watermark(ing)
VoD	Video on Demand

5 Conventions

In this document:

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

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/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 Security Requirements

The following requirements are duplicates of those identified in *IPTV Service Requirements* [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

6.1 General Security Requirements

- The IPTV architecture is recommended to take into account the influence/impact on performance, quality of service, usability, scalability and cost constraints on deployment of security.
- The IPTV architecture can optionally support SCP of end-user shared content.

6.2 Content Security Requirements

This clause specifies requirements that pertain, individually or collectively, to Content and Content Protection.

Architecture Requirements

- The IPTV architecture is required to support content protection as defined in Clause 3.
- The IPTV architecture is required to support associating content with protection and content management metadata in order to permit the expression of its rights of usage.
- The IPTV architecture is required to support the secure delivery of content protection and content management metadata, including usage rights metadata.
- The IPTV architecture is required to support content usage rights metadata that distinguishes between rights of use including rendering (viewing), storage, (re)distribution, and combinations thereof.
- The IPTV architecture is required to support protection of content that is distributed simultaneously to a very high number of subscribers (scalability).
- The IPTV architecture is required to support protection of content that is transferred over multicast and/or over unicast streams.
- The IPTV architecture is required to apply possible rights specifications and protect content for multiple common existing content formats (e.g., MP-3, MPEG-4).
- The IPTV architecture is required to support the securing of stored content according to granted usage.
- The IPTV architecture is required to support robust content tracing to content in an offline manner (e.g., VoD content).
- The IPTV architecture is required to support a means for conveyance of content tracing information (e.g. Watermark facilitation metadata).

  NOTE – Such provision may be made by the selection of appropriate standards profiles or by extensions to the existing standards.

- The IPTV architecture is required to support the application of content tracing technology within the output of an IPTV terminal device for the purpose of uniquely identifying a session (e.g., channel, time/date), IPTV terminal device and/or network operator. Examples of such content tracing technology can optionally include visible and invisible information.
- The IPTV architecture is required to allow the retrieval of all the content tracing information from the content.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability where only authorized user(s) or device(s) are allowed to use the IPTV content, even after content is transferred to another security system.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to keep identification information to identify IPTV content consistently, no matter which identification schemes are used and no matter to which security system the content is transferred to.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to not reduce the level of security when content is transferred to another security system.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to allow only trusted devices.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to provide a secure environment for exchanging service and content protection interoperability data (e.g. authentication information, metadata, key information, etc.).
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability such that interoperability is not dependent on specific software or hardware.
- The IPTV architecture is prohibited from requiring a service and content protection mechanism of either side to be openly specified to achieve interoperability.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability which is flexible and extensible to support various business models
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability among multiple security systems which use different security mechanisms, respectively, where the purpose is to support the seamless time-shifting service (subscribers can store the content and retrieve it later) and place-shifting service (subscribers can see the content anywhere) although the security mechanisms are different.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to maintain transparency to users.
- The IPTV architecture is prohibited from precluding support for multiple content and service protection mechanisms regardless of specific hardware or software requirements.

Architecture Recommendations

- If IPTV content employs a content tracing technology, then it is recommended that the tracing technology be imperceptible.
- The IPTV architecture is recommended to support robust content tracing to content in real-time (e.g., broadcast content).
- The IPTV architecture is recommended to support the capability for authenticating and authorizing end-users for content sharing services (e.g. content export and content redistribution).

Architecture Options

- The IPTV architecture can optionally support the inclusion of content tracing information. This content tracing information can optionally contain the operator ID, content owner ID, IPTV terminal device ID, and other information.

Scrambling Algorithm Requirements

- Scrambling algorithms for IPTV are required to have sufficiently large key entropy to protect the content fully from plausible threats (e.g., at least 128 bits for the AES symmetric algorithms).
- Scrambling algorithms for IPTV are required to be built using publicly-available and standardized cryptographic algorithms
- Scrambling algorithms for IPTV are required to not preclude support for either Simulcrypt or Multicrypt approaches. The purpose is to support multiple SCP vendors within a single network platform when required by the content distributor.
- Scrambling algorithms for IPTV are required to:
  - be designed with suitable, variable key lengths defined by the appropriate experts;
  - be an adaptable, technical solution which allows configurable, variable parameters (such as key length, crypto periods, etc.) for scalable and future proof levels of security in the same stream;
  - be designed by appropriate experts and is not broken within a reasonable amount of time, using "brute force" attacks;
  - be designed by appropriate experts and whose rationale is a cost/benefit analysis
- Scrambling algorithms for IPTV are required to be efficiently implementable for both hardware and software implementations.

Scrambling Algorithm Options

- Scrambling algorithms for IPTV can optionally apply cryptographic algorithms of different strength to different content types.

6.3 Service Security Requirements

This clause specifies requirements that pertain, individually or collectively, to Services and Service Protection.

Architecture Requirements

- The IPTV architecture is required to support Service Protection, as defined in Clause 3.
- The IPTV architecture is required to support authorization and authentication capabilities for the end-user.

  NOTE – This can optionally include the capability of a service provider to authenticate and authorize a subscriber (subscriber's IPTV terminal device) and a different service provider.
- The IPTV architecture is required to support a mechanism to signal the IPTV terminal device to utilize a specified scrambling algorithm based on a standardized framework.
- The IPTV architecture is required to have the ability to use standard key management systems (e.g., MIKE, EMM/ECM), to the extent that this is required for interoperability.
- The IPTV architecture is required to support the capability to the server side SCP interfaces to update and query the SCP System concerning scrambling algorithms for IPTV and any other operator-selected scrambling algorithms.
- The IPTV architecture is required to support rights management that is independent of specific content formats or specifications.

- The IPTV architecture is required to support a mechanism for secure delivery of entitlements to the IPTV terminal devices.
- The IPTV architecture is required to support content usage control (e.g. re-play entitlements).
- The IPTV architecture is required to support different modes of re-play entitlements, e.g., limit on number of plays, time limit on plays, restriction of fast forward or rewind.
- The IPTV architecture is required to support a mechanism for transmitting signalling messages securely between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to allow for the confidentiality of signalling messages between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to allow for the authenticity of signalling messages between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to allow for the integrity of signalling messages between the SCP server and the IPTV terminal device SCP client.
- The IPTV architecture is required to support a mechanism to securely retrieve the SCP parameters (e.g. configuration, status) from IPTV terminal device.
- The IPTV architecture is required to support a mechanism to securely update the SCP parameters (e.g. configuration) of the IPTV terminal device.
- The IPTV architecture is required to support the capability to turn on and off content tracing function with flexibility (e.g., based on time, an event, content, or channel).
- The IPTV architecture is recommended to support the capability for authenticating and authorizing end-users for content sharing services (e.g. content export and content redistribution).
- If the IPTV architecture employs a Key Management System, then it is required to be designed for scalability, reliability, and interoperability.
- If the IPTV architecture employs a Key Management System, then a hierarchical key management scheme is recommended to be considered to support scalability.
- If the IPTV architecture employs a Key Management System that uses a Group Key Management Protocol, then a hierarchical key management and key management algorithm alternative is recommended to be considered to support scalability.
- If the IPTV architecture employs a Key Management System that uses Short Term Keys, it is recommended that the media path is provisioned in such a way that NAT traversal and bandwidth constraints do not limit the key exchange.
- The IPTV architecture is recommended to support the joint transmission of content and content tracing information such that the content and its respective content tracing information remain synchronized during transport.
- The IPTV architecture is recommended to support at least the same degree of protection (for purposes of controlling unauthorized access) to content tracing information as is applied to the corresponding traced content.

Architecture Recommendations

- The IPTV architecture is recommended to enable content confidentiality, i.e. support a capability to the head-end to support multiple scrambling algorithms.
- The IPTV architecture is recommended to support a "blackout mechanism": a mechanism for limiting viewing-rights of certain programs to certain groups of subscribers (e.g. block viewing by residents of a specific area (for example, this can optionally be useful for sporting events)).

- The IPTV architecture is prohibited from precluding support for the installation and operation of multiple service protection solutions without hardware replacements except removable devices (such as USB dongle and SIM cards).
- The IPTV architecture is prohibited from precluding support for an identification mechanism for available service protection solutions which are capable to satisfy the requirement that is specified for related content protection.
- The IPTV architecture is prohibited from precluding support for a SCP system discovery mechanism, such that whenever specific content requires a specific service protection system, the IPTV architecture may support a discovery method and adapt to it.
- The IPTV architecture is prohibited from precluding support a mechanism for the selection of a SCP system from the available SCP systems without any hardware replacement except removable devices.
- The IPTV architecture is prohibited from precluding support a secure downloading for a SCP system. The downloaded SCP system can optionally depend on specific service protection requirements.
- The IPTV architecture is prohibited from precluding support the verification and authentication of the downloaded SCP system mechanisms.

6.4 Network Security Requirements

This clause specifies requirements that pertain, individually or collectively, to Networks or the protection thereof.

Architecture Requirements

- The IPTV architecture is required to support the capability of preventing the DoS attack to network.
- The IPTV architecture is required to support the provision of security measures to block illegal or unwanted traffic.
- The IPTV architecture is required to support network operators to prevent that the network topology and its resources are visible to unauthorized entities.
- The IPTV architecture is required to be capable of supporting a network which uses content label information in order to control access to content.
- The IPTV architecture is required to be hardened against attacks on multicast capabilities.
- The multicast architecture is required to support the capability of multicast protocol adjacency authentication in order to establish a reliable peer.

Architecture Recommendations

- To protect the home network from malicious or unauthorized access, the IPTV architecture is recommended to support the ability for the DNGF to establish a firewall, with multiple levels of security and appropriate application level gateways.

6.5 Terminal Security Requirements

This clause specifies requirements that pertain, individually or collectively, to Terminal Devices or the protection thereof.

Architecture Requirements

- The IPTV architecture is required to support terminal device protection, as defined in Section 3.
- The IPTV architecture is required to support a method to authenticate IPTV terminal devices.

- The IPTV architecture is required to support physical tamper-resistance for terminal device.
- The IPTV architecture is required to support a means to detect when physical tampering has occurred for terminal device.
- The IPTV architecture is required to support secure download and installation of the SCP operating code to IPTV terminal devices.
- The IPTV architecture is required to support a secure means for performing security critical processes in IPTV terminal device, such as key management and media serialization, to abort playback of content in the event of a security related malfunction, detection of tampering, or other indication of misuse.
- The IPTV architecture is required to provide physical protection of sensitive security enabling processes and components involved in the processing transmission and storage of valued content in IPTV terminal device in case no logical protection (such as encryption or serialization watermarks) is present. These processes include descrambling and media serialization (content tracing).
- The IPTV architecture is required to recognize the need for physical protection of sensitive security enabling processes in IPTV terminal device, including descrambling and media serialization (content tracing), critical data supporting those processes, as well as for all components involved in the processing, transmission, and storage of any valued content lacking logical protections such as encryption or content tracing watermarks.
- The IPTV architecture is prohibited from precluding to support the interchange of content between an IPTV terminal device and other (physical or logical) devices provided that the uses granted for this content includes such an interchange.

6.6 Subscriber Security Requirements

This clause specifies requirements that pertain, individually or collectively, to Subscribers, End-Users or the protection thereof.

Architecture Requirements

- The IPTV architecture is required to support User Privacy Protection, as defined in Section 3.
- The IPTV architecture is required to support a mechanism to allow an IPTV terminal device SCP component to authenticate the SCP servers.
- The IPTV architecture is required to allow a Subscriber to set an access control mechanism (e.g. a password) in order to restrict access to content and/or services.
- The IPTV architecture is required to support a mechanism for parental rating i.e., facilities for rating programs according to content.
- The IPTV architecture is required to be capable of indicating why access to content has been denied to the user.
- The IPTV architecture is required to allow for a mechanism for a Subscriber to request extensions (e.g. more plays, more play-time) to digital rights associated with specific content instances.

Architecture Recommendations

- The IPTV architecture is recommended to allow the end user (as rights allow) to change, i.e. replace, an IPTV terminal device without inherently affecting its rights to consume content.

7 Security Architecture

This clause defines an IPTV security architecture in terms of a general security architecture, a content protection architecture, a service protection architecture, security functional entities and security interfaces.

The IPTV security architecture described below assumes and is intended to be used in the context of the IPTV Functional Domains and IPTV Functional Architecture Framework as defined by Sections 6 and 8 of [FG IPTV-DOC-0181], respectively.

7.1 General Security Architecture

A general security architecture for IPTV is depicted in Figure 7-1 below. This general architecture is divided into two primary areas: one considered in-scope for the purpose of considering interoperability based on this document, and another considered to be out-of-scope, where the first encompasses End-User, Network Provider, and Service Provider domains, and where the second encompasses the Content Provider domain.

All security aspects within the Content Provider domain, and between Content Providers and Service Providers is considered to be out-of-scope, and, instead, subject to private agreements between the stakeholders operating in these domains.

Although the Content Provider and the interconnect between the Content and Service Provider domains are considered out-of-scope in the present context, for the purpose of completeness, the Content Provider domain is nevertheless included in the figures and descriptions that follow. As a consequence, any statement made herein concerning these domains should be considered informative or explanatory in nature.

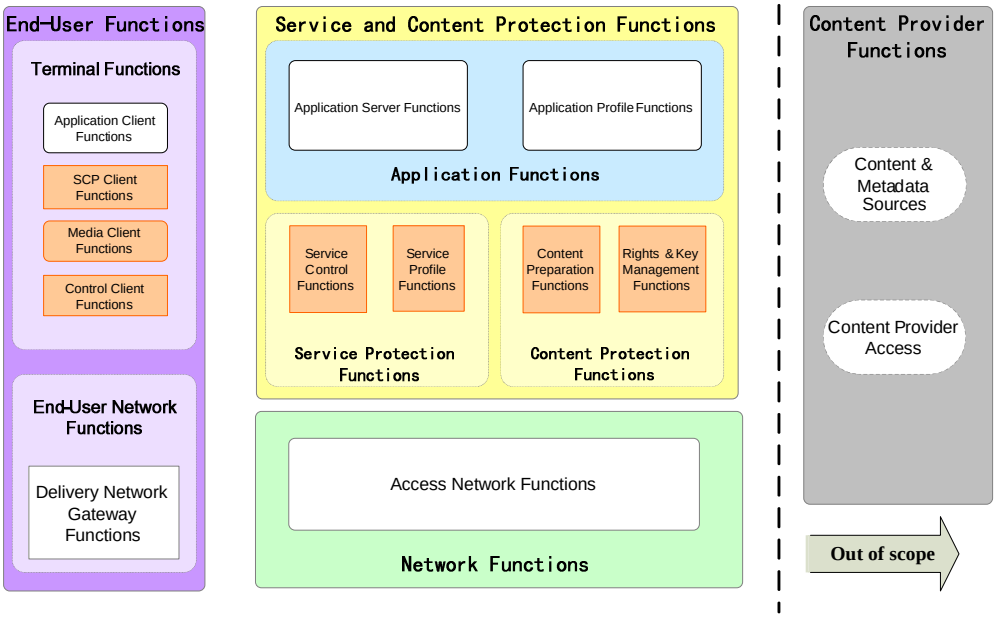


Figure 7-1: IPTV General Security Architecture

The general security architecture is divided roughly into four areas of functionality as follows:

- Content Provider Functions

  Although technically out-of-scope, it is assumed that content provider(s) will provision access to content for those service providers that have established relationship(s) with the content provider(s). In some cases, a content provider may themselves serve as a service provider, in which case this relationship is considered to be internal.

In providing access to content for service providers, a content provider may use standard or private mechanisms to control and enable access to content; however, such mechanisms are considered to be out-of-scope for this document and subject solely to private agreement.

- Service and Content Protection Functions

  The role of service and content protection functions play a central role in the IPTV general security architecture. In particular, service protection functions enable protection of the service infrastructure as well as controlling access to services and the content contained therein, while content protection functions enable controlling the use of services and content according to licensed uses.

  In general, a service provider is obligated by licence(s) with content providers to make content available only under certain conditions of use, such as for one-time viewing but no recording, one-time recording with multiple viewing, one-time recording with transferral of recording rights, etc. The primary purpose of the service and content protection function is to provide technical mechanisms to allow a service provider to satisfy such obligations in an objectively verifiable manner.

  The primary purpose of service protection is to prevent unauthorized access to information considered to be confidential by entities in various domains: service, network, terminal device, and end-user (subscriber).

  A secondary purpose of the service protection aspects of the service and content protection function is to protect the service infrastructure from damage due to both intentional and accidental misuse or access.

- Network Functions

  Security functions that pertain to the network domain are focused on authenticating and authorizing access to the network(s) through which IPTV services are or will be delivered. A secondary function is to protect the integrity of the network itself: physically, electronically, and operationally (e.g., by detecting and thwarting denial of service attacks on the access or bearer network).

- End-User Functions

  Aspects of security that apply to the end-user (subscriber) include protection of the integrity of the IPTV terminal device operating on subscriber premises as well as protection of end-user privacy.

  In some circumstances, a gateway between an IPTV terminal device and a delivery network may be considered to be in the end-user domain and subject to end-user security measures.

  Finally, in those cases where content is received by an IPTV terminal device and subsequently redistributed to other devices, the maintenance and integrity of content protection rules may apply, which results in overlap between end-user security aspects and content security aspects.

More details of the IPTV general security architecture described above are worked out below. Furthermore, more detailed descriptions of the architectural blocks shown in Figure 7-1 are elaborated in Clause 7.4 *Security Functional Entities*.

7.2 Content Protection Architecture

A content protection architecture for IPTV is depicted in Figure 7-2 below.

The primary function of the content protection architecture is to delineate the flow and processing of information pertaining to content usage rights and information required to manage and facilitate such rights.

Ultimately, rights of content use originate with content provider(s); however, such rights may be modified (e.g., narrowed, or perhaps even widened) by service provider(s) according to their agreements with content providers and their operational and business policies. From an operational, and typical legal perspective, an end-user's access and use of content is with the service provider, and not a content provider.

NOTE – An end-user may not, in fact, perceive their access to content is a through a relationship with a service provider; rather, they may misperceive this relationship as one with a content provider. This is not an unlikely circumstance, particularly since content is more often branded by the content provider than by the service provider. At any given time, a service provider may or may not include some type of branding mark that effectively notifies the end-user of their role, for example, a station mark ("bug") or logo superimposed into a video stream. Notwithstanding the presence of such a mark, an end-user may fail to notice or realize that their legal relationship (if one exists) is with the service provider.

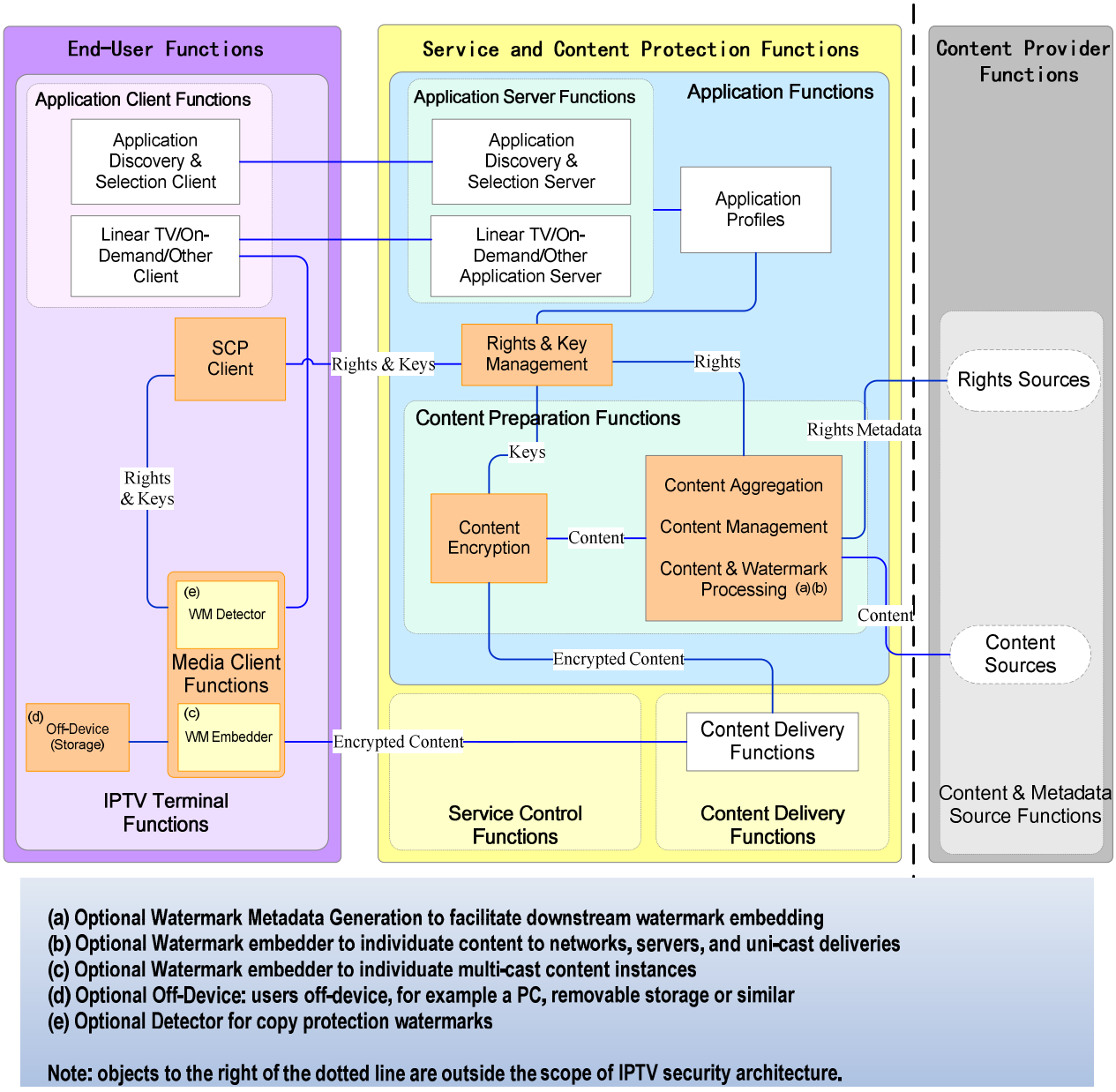


Figure 7-2: IPTV Content Protection Architecture

The content protection architecture shown here focuses primarily on two functional areas:

- Service and Content Protection Functions

  Content and its associated rights are collected from content providers, aggregated, and processed for delivery to the end-user, where the overall process is managed by an IPTV Application Server using stored Application Profile data that describes an end-user's rights and related conditions.

  Content, rights, and keys (used to grant access to and use of content) are organized into a form appropriate for the specific IPTV application, for example, linear television viewing. Rights and key

information are delivered to an *SCP Client* functional entity in the terminal device, content is then processed to (optionally) insert content tracing (e.g., watermarking) metadata and then is then encrypted prior to delivery.

In the context of the IPTV Content Protection Architecture (as opposed to the subsequently described IPTV Service Protection Architecture), the focus is primarily on the management, processing, and delivery of rights and key information as opposed to the encryption of this information or the content subject to these rights.

- End-User Functions

  The IPTV Terminal Device, operating in the End-User domain, is responsible for enforcing content usage rules ascribed to rights information (also known as content protection metadata). An *SCP Client* functional entity interprets content rights and keys obtained from the IPTV Application Server and then acts on the interpretation to control how the content is processed and exposed to the end-user, either through integrated presentation devices (such as a display or audio rendering system) or through physical interconnects to external devices.

  In those cases where the IPTV Terminal Device transmits protected content to an external device (such as a display or another device), the content usage rules may be translated in form, and the content to which such usage rules apply may be further processed to insert client-side content tracing information (e.g., watermarks) or re-encrypt content to effect downstream access control.

More detailed descriptions of the architectural blocks shown in Figure 7-2 are elaborated in clause 7.4.

7.3 Service Protection Architecture

A service protection architecture for IPTV is depicted in Figure 7-3 below.

The primary functions of the service protection architecture include:

- Authentication and Authorization

  For managed services involving protected content, it is typically the case that the end-user (subscriber) must be authenticated and, subsequent to successful authentication, authorized to access service(s) and the content contained therein.

  Depending upon circumstances, authentication and authorization functions may be performed separately on the IPTV terminal device and the end-user(s). In other cases, additional devices in end-user premises, such as a delivery network gateway and other end-user devices may require authentication before service access is authorized.

  The combination of authentication and authorization can be considered to effect positive access control on the terminal device and end-user for purposes of service and content acquisition prior to use.

- Control Signalling and Content Interchange Encryption

  In order to limit acquisition and access of services and content, both control message information and content itself is encrypted (scrambled). Different (strength) levels of encryption may be applied to the various control signalling and content interchange paths in accordance with the requirements of a concrete IPTV system or service providers.

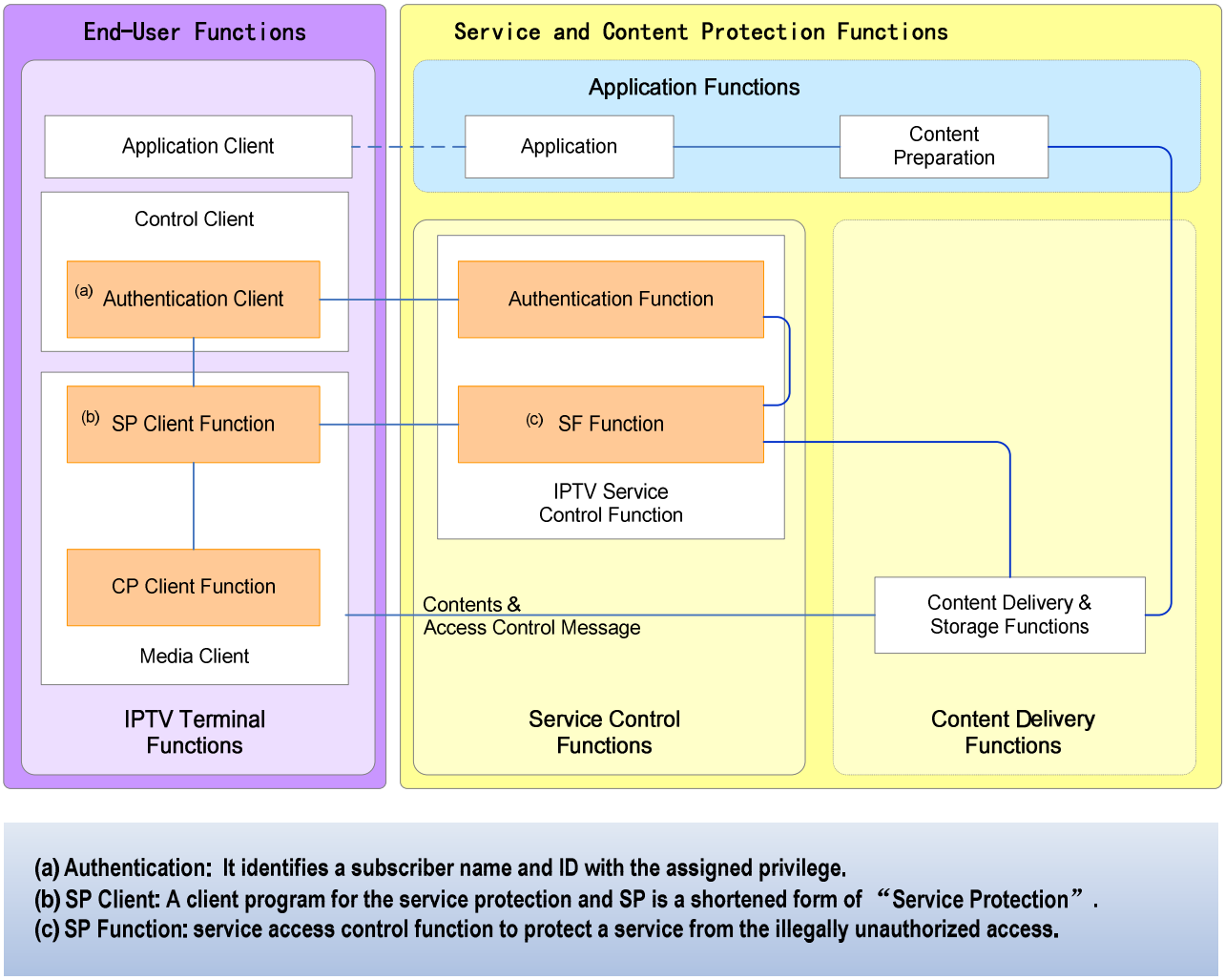


Figure 7-3: IPTV Service Protection Architecture

More detailed descriptions of the architectural blocks shown in Figure 7-3 are elaborated in clause 7.4.

7.4 Security Functional Entities

This clause provides further descriptive details of the functional entities depicted in the architectural models found in clause 7.1, *IPTV General Security Architecture*, clause 7.2, *IPTV Content Protection Architecture*, and clause 7.3, *IPTV Service Protection Architecture*, above. These functional entities are defined only in general, descriptive terms, and are divided into three parts corresponding with each of these three clauses, respectively.

7.4.1 General Architecture Entities

Access Network Functions: Provide for collection and aggregation of control and data traffic originating in core network(s), enabling quality of service, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, and traffic shaping.

Application Functions: Divided between server (service provider) side and client (end-user premises) side, consist of functional components that prepare, originate, receive, and process service level IPTV Applications such as linear television, video on demand services, and related content, for example, accessibility information, interactive applications, etc.

Content Protection Functions: Provide mechanisms that enable enforcement of service and content usage policies, including aggregation, distribution, and management of rights and keys, generation and insertion (embedding) of content tracing information (e.g., watermarks), and content encryption (under control of service protection functions).

Content Provider Functions: Deliver content and content rights and key metadata to service providers.

Delivery Network Gateway Functions: Provide for connectivity between terminal device and delivery network, managing local (end-user premises) IP connectivity, obtaining IP address(s), and IP configuration for the IPTV terminal device.

Service Protection Functions: Provide mechanisms for performing authentication and authorization for and controlling access to IPTV services and content contained therein, including control of and direct implementation of control signal and content interchange encryption either independently of or in conjunction with content protection functions.

Terminal Functions: Provide service protection and content protection clients for decrypting and enforcing service and content usage policies according to usage rights metadata, performing link layer encryption and SCP translation (interchange) as required for further downstream content output or redistribution and internal (or external) content storage, including support for secure (tamper resistant) media processing pipelines, local secret (key) storage, security software renewability, authentication and verification of downloaded software assets, and protection of locally stored and interchanged user data subject to end-user privacy considerations.

7.4.2 Content Protection Architecture Entities

Application Client: Primary point of coordination and control of interaction between end-user and service(s) provided by Application Server. For standard applications, such as Linear-TV viewing, provides for primary user interface and operating paradigm by means of which end-user obtains a service.

Application Discovery and Selection Client: Permits end-user and/or terminal device to discover existence of and selection of applications and application services available from service provider(s).

Application Discovery and Selection Server: Enables end-user and/or terminal device to discover existence and selection of applications and application services.

Application Profile: Stores and manages configuration information about applications and services, both of a global nature and of an end-user (subscriber) specific nature; typically used to permit application server(s) to customize services and content for the end-user, and will frequently interact with or implement (internally) various accounting systems.

Application Server: Logical entity that embodies the point of origination for some IPTV service, such as Linear-TV, Video on Demand, etc. Responsible for orchestrating all service provider facilities to operationally enable the existence of some service(s).

Content Aggregation: Responsible for collecting and packaging content for delivery to IPTV terminal device.

Content Delivery: Performs actual sourcing of content and all related metadata and signalling necessary for content interpretation except for essential content rights and encryption keys, which are interchanged through other (logical or possibly even physical) communication paths.

Content Encryption: Performs encryption of (scrambles) protected content to facilitate access control and confidentiality of that content during the content delivery process.

Content Management: Controls and performs management functions on content storage, processing, and interchange.

Content Sources: Originates content to be aggregated, processed, and subsequently delivered to end-users by means of service applications, such as Linear-TV, Video on Demand, etc.

Content Preparation: Performs various types of content pre-processing prior to delivery, such as content tracing (e.g., watermark) analysis and metadata generation, content and content metadata multiplexing, and content encryption.

Content Watermark Processing: Optional processing step(s) that analyse content in order to produce content tracing (e.g., watermark) metadata for use in subsequent downstream processing, in particular, a process of individuating (associating source identity information with) such metadata.

Off-Device Storage: Post-reception content storage mechanisms that are physically external to an IPTV terminal device *and* whose storage and content use is not managed by IPTV terminal device.

> NOTE – If external storage exists and its use is under control of the IPTV terminal device at all times, then, depending upon applicable terminal device compliance and robustness rules, it may be considered to be On-Device Storage via an Authorized, Protected Interface.

Media Client: Performs content media decryption, demultiplexing, decoding, and subsequent presentation and storage processing on content.

Rights Sources: Originates content metadata pertaining to content usage rights.

Rights and Key Management: Correlates rights and keys with content and manages their distribution to the SCP client in the terminal device.

Service and Content Protection (SCP) Client: Obtains or receives rights and keys, using this information to control content decryption and usage rules.

Watermark Embedder: If present, performs individuation of content instance for presentation and subsequent storage or redistribution.

Watermark Detector: If present, detects use of watermark(s) in content received from service provider(s) in order to verify or effect desired content usage rules in the terminal device or downstream interfaces from the terminal device.

7.4.3 Service Protection Architecture Entities

The functional entities depicted in clause 7.3, *IPTV Service Protection Architecture*, are not described in this version of this document, but are expected to be elaborated in a future version.

7.5 Security Interfaces

This document does not formally define any interfaces between functional entities of the security related architectural elements and functional blocks therein. It is expected that future revisions of this document or companion documents will formally define such interfaces.

8 Security Mechanisms

This document does not define any specific security mechanisms or solutions; however, it does describe, in general terms, certain security mechanisms which may be considered for the purposes of defining or implementing mechanisms that address security requirements, security architectural functional entities and security threats.

The set of security mechanisms described below does not exhaustively address all security requirements documented above.

8.1 Security Mechanisms that pertain to Content or Content Protection

Content security mechanisms include a set of functions that operate between content sources and IPTV terminal devices to ensure the content can be distributed (or transmitted) securely by a network, and can be acquired, consumed, exported, stored, redistributed (or retransmitted) securely by an end-user.

The content security mechanisms can consist of content distribution, content acquisition, content consumption, content storage, content export and content redistribution.

8.1.1 Content Tracing

Content tracing serves to identify and trace the origin (source) of the content, and/or the responsible party (e.g. the end-user), to facilitate subsequent investigation in the event of unauthorized content copying or redistribution.

Content tracing information may be attached to content either as metadata, or as a forensic watermark. Content tracing watermarks are typically designed to be robust and imperceptible, to protect against their intentional or inadvertent removal.

8.1.2 Watermarking

Watermarking refers to a process of adding information to content through alteration of certain content features, a field of study known as *steganography*.

Watermarking is preferable for many applications due to the difficulty of removing this information from content. In an IPTV service, watermarking may refer to the inclusion of hidden information directly in a video or audio stream of multiplexed content. Ideally, watermarks are invisible and/or inaudible to human perception, but will successfully survive conversion among media formats.

8.1.3 Content Labelling

Content labelling is a process of inserting or associating metadata with content that describes the nature of the content as well as other aspects and characteristics of the content. Content which has been labelled with such metadata may be more easily sorted, filtered, or categorized by intermediate devices in the content delivery chain.

Some regions, administrations, or specific deployments of IPTV may require the presence of certain types of content labels, such as rating information in order to permit some degree of end-user (subscriber) control over access of content considered to be inappropriate or harmful.

8.2 Security Mechanisms that pertain to Services or Service Protection

Service security mechanisms include authentication, authorization, and may include implementations of specific access mechanisms such as encryption and decryption systems.

8.2.1 Service Authentication

In the case of managed services for which an end-user (subscriber) has a direct relationship with some service provider, the service provider will typically require the terminal device and/or the end-user (subscriber) to be authenticated in a secure manner, in which case authentication means the produce of presenting some identity information in a secure manner that can be correlated with the service provider's subscriber database.

8.2.2 Service Authorization

Subsequent to end-user (subscriber) and/or terminal device authentication, a service authorization mechanism is used to authorize and grant access to specific services and content contained therein according to service and subscriber provisioning.

An example of authorizing a Linear-TV service is shown in Annex A.

8.2.2 Service Access Control

A service protection system will in most if not all cases contain mechanisms that can or do perform encryption (scrambling) and decryption (descrambling) of both service control signalling traffic and content traffic. Typically, two-way service control traffic will be encrypted in both directions, both from server to client, and from client to server. On the other hand, content streams will typically be encrypted only from server (service provider) to client (terminal device). Nevertheless, there are usage scenarios where a content stream may be uploaded from a client to server, in which case such content may be encrypted on a terminal device for uploading purposes (to ensure, for example, that only an authenticated and authorized service provider may access the uploaded content).

8.3 Security Mechanisms that pertain to Networks

This document does not define or describe any mechanisms that pertain to network security. In general, it is expected that implementations of core, access, bearer, and delivery networks will implement whatever mechanisms are believed to be required to protect the operational integrity of the network, including, for example, denial of service detection and intervention. Generally speaking, security mechanisms employed by IPTV service providers and IPTV terminal devices will be opaque to these networks, provided that these security mechanisms operate at or above the payload data elements provided by network layers.

8.4 Security Mechanisms that pertain to Terminal Devices

Terminal device security mechanisms include a wide range of functionality, including secure and tamper resistant secrets storage, service authentication, service authorization, control signal encryption and decryption, content decryption, content rights metadata decoding, content usage enforcement, watermark detection and embedding, programmatic content authentication and verification, service and content protection bridging and interchange, digital output port (interface) encryption, media path tamper resistance, pluggable and renewable security processors and components, both hardware and software based, and others.

This document does not, at present, define or further describe this wide range of mechanisms. It is expected that future work on this document will elaborate these topics.

8.5 Security Mechanisms that pertain to Subscribers or End-Users

Subscriber or end-user security mechanisms are primarily related to the collection, storage, and transmission of information that may be subject to privacy considerations or end-user confidentiality. As such, these mechanisms may be divided between the point of collection, the terminal device, and the service provider, who may harvest, maintain and re-use this information. Consequently, descriptions and definitions of these mechanisms are expected to be placed in clauses describing service and terminal device security.

This document does not, at present, define subscriber or end-user security mechanisms. It is expected that future work on this document will elaborate these topics.

Additional information on subscriber security is contained in Annex B.

8.6 Security Mechanisms that pertain to Multiple or Unspecified Functional Areas

This clause provides information on certain mechanisms that pertain to overlapping or non-specific areas of functionality.

8.6.1 Programmatic Content

Some types of content may include or take the form of application programs or programmatic components, whether interpreted or directly executed by a terminal device. Examples of such content include (without limitation) ECMAScript program fragments, Java Class Files, and, potentially, native applications or libraries, such as used to augment, update or replace firmware components in a terminal device.

Some types of programmatic content may be utilized or active only when accompanied by related audio/video or audio only programming. Other types of programmatic content may be active independently of any audio or video content. Furthermore, in some cases, programmatic content may be preloaded (by pull or push mechanisms) into a terminal device or may be delivered concurrently with related content. In both cases, such programmatic content may (or may not) be stored and/or cached on a terminal device.

When downloading, storing, caching, activating, and executing (interpreting) programmatic content, a service provider may include and a terminal device may interpret and act on special content authentication and integrity messages as well as metadata used to perform run-time verification or validation of certain content constraints prior to use of such programmatic content.

This document does not, at present, define or further describe mechanisms that may perform authentication and verification of programmatic content. It is expected that future work on this document will elaborate these topics.

Annex A

Service Authorization for Linear TV Service (Informative)

(This annex forms an integral part of this document.)

One possible mechanism to authorize the Linear TV services is described as follows:

(1) The Linear TV application sends the rights information related to a particular end-user (subscriber) to the transport functions to which terminal is connected. The transport functions store the received rights information.

(2) When receiving a user request, the transport functions perform the service authorization procedures according to the stored rights to determine whether to grant access to the user.

The procedure is depicted below in Figure A-1 and described as follows:

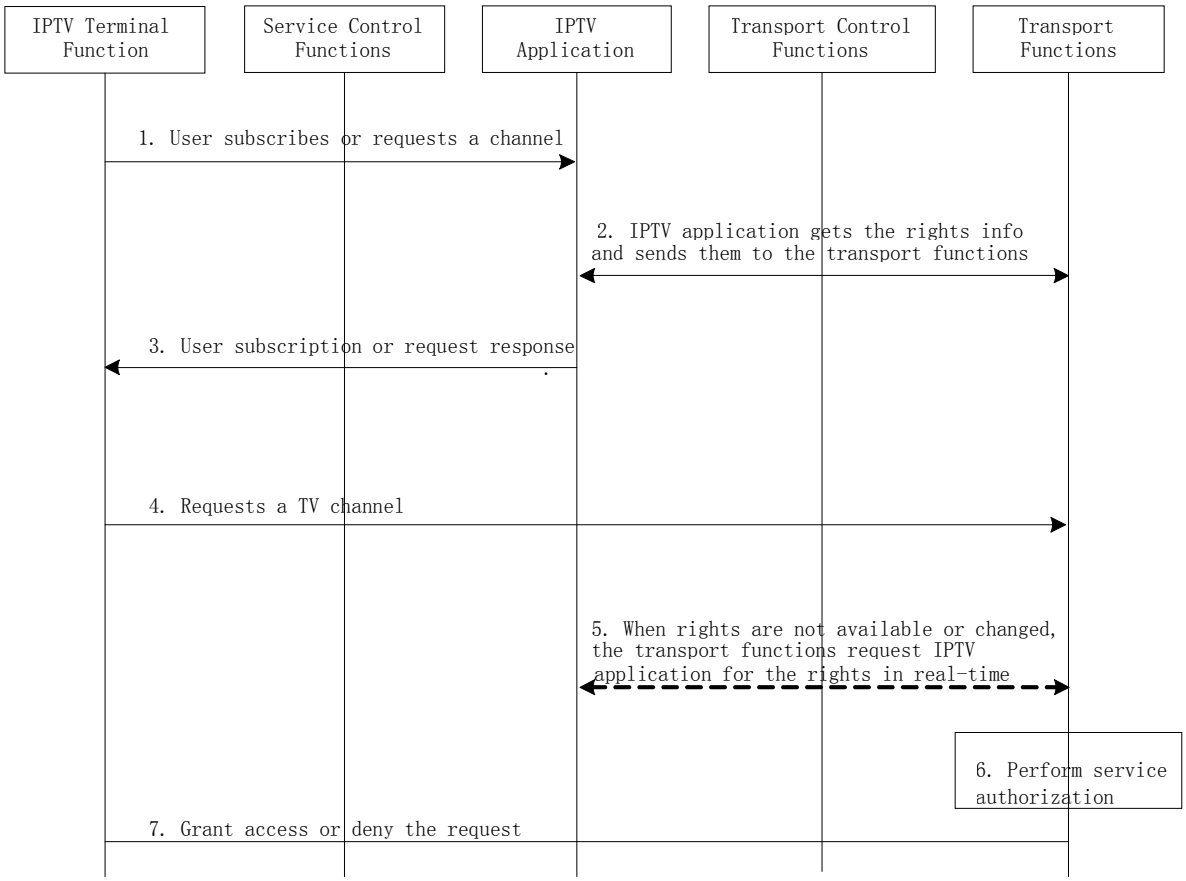


Figure A-1: Service Authorization Information Flow

1. User subscribes to or requests a Linear TV channel via service control functions.

2. The Linear TV application obtains the rights related to the subscribed channel from the application profile function, and sends the rights information to the transport functions via transport control functions. The transport functions store the rights information.

3. The Linear TV application sends a response back to the terminal device.

4. The user requests a TV channel by sending a message, e.g. IGMP Join, to the transport functions.

5. When rights are not available or changed, the transport functions make a request to the Linear TV application via IPTV service control functions for the rights in real-time, and may store them locally. This step is not needed in a case where the rights are available, shown here as dotted lines.

6. The transport functions perform service authorization according to the rights information.

7. Based on the authorization, the transport functions grant access or deny the request.

Annex B

Subscriber Security Protection (Informative)

(This annex forms an integral part of this document.)

B.1 Subscriber Personal Data

When implementing IPTV services to general users, it is necessary to give sufficient consideration to the subscriber's personal data. This subscriber personal data includes basic data such as address, name, age, occupation, and telephone number, and possibly other kinds of information, such as family composition, hobbies, and household income.

The subscriber's personal data may also include tracked data information such as channel number before and after channel change, time of change and user information for EPG service, and package identification, time of play, etc.

(1) The IPTV service can optionally handle the minimum subscriber's personal data necessary for delivering the IPTV services.

(2) The IPTV service can optionally explain the intended use of the subscriber's personal data and obtain the consent for this from the subscriber before collecting the information necessary to deliver the IPTV services.

(3) The IPTV service can optionally destroy subscriber's personal data that becomes unnecessary for the continuation of IPTV services.

(4) When the service provider administers the subscriber's personal data, the IPTV service can optionally store the collected data under strict security.

There are three possible routes by which a subscriber's personal data can leak. These are leaking from the service company, leaking from the network, and leaking from the home, e.g. through terminal devices. Here we present methods for protecting the subscriber's personal data for each of these leakage routes.

B.1.1 Subscriber Personal Data Leakage from Service Provider

In order to prevent leakage of subscriber's personal data, the IPTV service provider should pay careful attention to the points below.

(1) Classifying subscriber's personal data into that which needs to be controlled and that which does not;

(2) Securely administering the subscriber's personal data that needs to be controlled;

(3) Ensuring that subscriber's personal data that needs to be controlled is not used for any purpose other than that intended.

B.1.2 Subscriber Personal Data Leakage from Network Provider

IPTV service providers should pay careful attention to the points below in relation to services and transactions that involve handling of subscriber's personal data.

(1) Classifying subscriber's personal data into that which needs to be controlled and that which does not;

(2) Using encrypted communication channels for transmission of subscriber's personal data that needs to be controlled.

B.1.3 Subscriber Personal Data Leakage from Terminal Device

IPTV service providers sometime store subscriber's personal data in terminal devices, in order to enhance service efficiency. In such cases, they should pay careful attention to the points below. Furthermore, it is necessary to consider security when exchanging terminal devices.

(1) Ensuring that no third party can easily read out subscriber's personal data stored inside terminal device;

(2) The IPTV service provider can optionally control access to subscriber's personal data stored in terminal device;

(3) Ensuring that subscriber's personal data stored in terminal devices can be completely deleted by subscriber or service provider;

(4) It is desirable that terminal devices are protected against infection by computer viruses in the near future.

B.2 Protection of Legal Minors

In the IPTV platform, a Protection of Legal Minors mechanism can be used to restrict the IPTV content that legal minors can access. In a typical usage pattern, a terminal device for IPTV services is shared in a home by multiple people of a wide age range. Terminal devices can be categorized into inside terminal devices and outside terminal devices. Inside terminal device is one type of terminal device used at home. Outside terminal device is one type of terminal device used in the outside of home, e.g., mobile terminal device, fixed terminal device. For terminal devices, the IPTV service provider should:

(1) Ensure that parental ratings can be set for content as necessary;

(2) Ensure that terminal devices can be operated in accordance to parental ratings;

(3) Ensure that terminal devices are capable of changing parental rating settings;

(4) Ensure that terminal devices are capable of password-based controls, so that only the guardians of legal minors can change parental ratings;

(5) Ensure that content ratings can be set for different age groups;

(6) Ensure that subscriber privileges can be allocated for different age groups;

(7) Ensure that authorization can be made in terminal devices for legal minors viewing a particular channel or content, e.g., using a PIN challenge;

(8) Ensure that guardians far from legal minors can use outside terminal device to monitor and receive content for legal minors from network copy storage.

Note that it is may be necessary to consider the conditions of each administration or region in relation to third-party organizations for eliminating harmful content, since this is related to control of content flow and access. When considering simultaneous retransmission of broadcasting, one may assume that the original content creator gives sufficient consideration to this at the time of producing the content, so it is necessary to give sufficient consideration to transmission delays and distribution cost increases.

Appendix I

Security Threats

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

This clause describes a set of identified security threats addressed by some requirement or mechanism of this document.

The security threat model and other fundamental materials have been addressed in the following ITU-T Recommendations:

- [ITU-T X.800] defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required.
- [ITU-T X.805] defines network security architecture for providing end-to-end network security.

Parties interested in security considerations related to IPTV are invited to read these base security documents, as it is assumed the reader of this document is aware of the information presented in those Recommendations.

[ITU-T X.800] and [ITU-T X.805] identify the following security threats to the networks, and which are also security threats to service and content application that are applicable to IPTV:

- Destruction of information and/or other resources;
- Corruption or modification of information;
- Theft, removal or loss of information and/or other resources;
- Disclosure of information; and
- Interruption of services.

Table I-1, which is copied from Table 1 of [ITU-T X.805], lists the Security Dimensions and describes mapping of Security Dimensions to security threats: the letter "Y" in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table I-1: Mapping of security dimensions to security threats

Security dimension	Security threat				
	Destruction of information or other resources	**Corruption or modification of information**	**Theft, removal or loss of information and other resources**	**Disclosure of information**	**Interruption of services**
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Confidentiality			Y	Y	
Communication Security			Y	Y	
Data Integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Figure I-1 depicts the concept of protecting a network by security dimensions at each security plane of each security layer in order to provide a comprehensive security solution. It should be noted that, depending on a given network's security requirements, it might not be necessary to have all architectural elements implemented (that is, to have a complete set of the security dimensions, security layers and security planes).

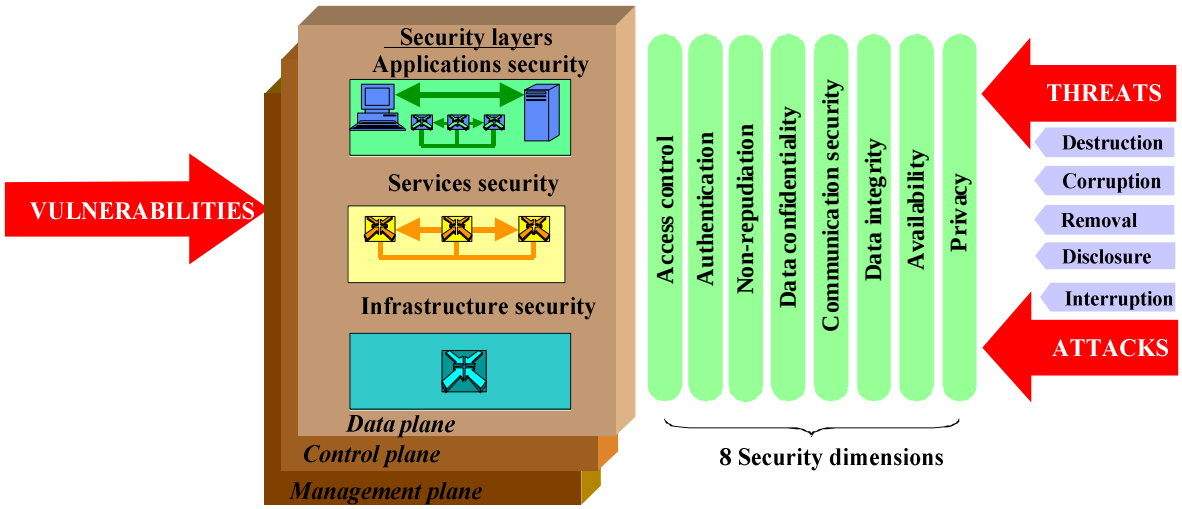


Figure I-1: End-to-End Security

I.1 Security Attack Points

Content security threats are expected to come mainly from the network and from terminal devices, as depicted in Figure I-2.

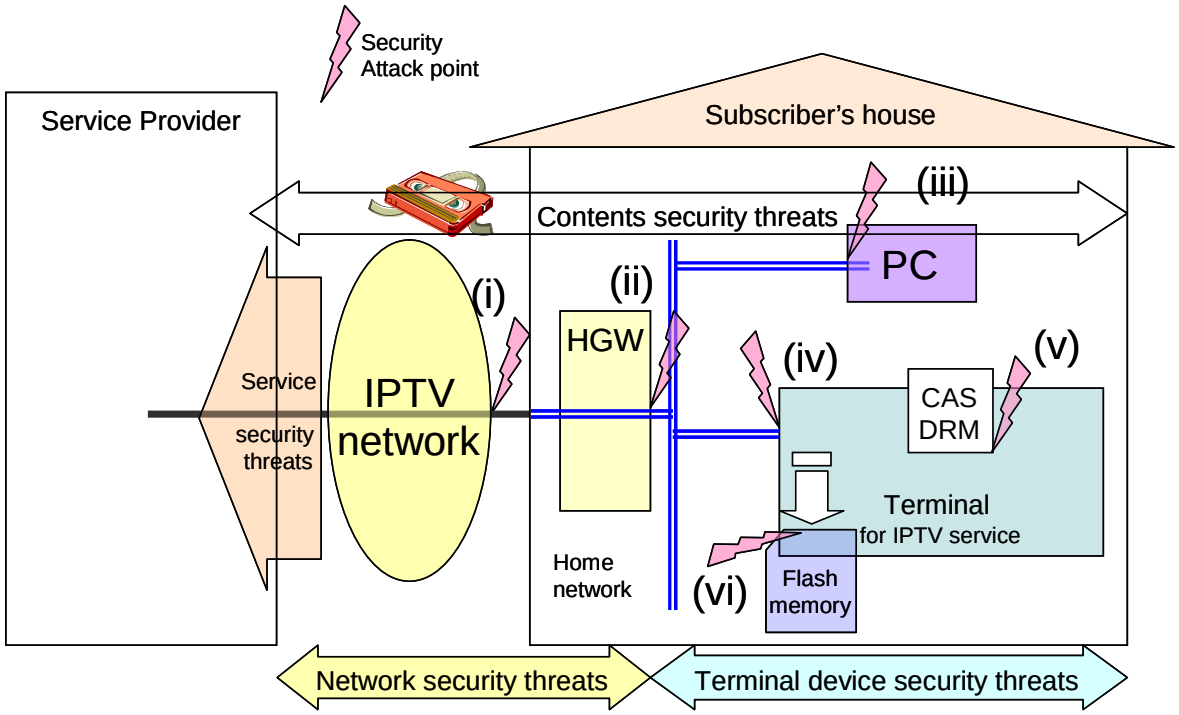


Figure I-2: Security Attack Points

a) Content security threats from Network

The main content security threats from the network are wiretapping, modification, and spoofing. These threats can be prevented by considering the points below in relation to content distribution.

i) Wiretapping: content encryption

ii) Modification and spoofing: digital signature

b) Content security threats from Terminal Devices

Content security threats from home networks can be broadly divided into three two kinds-threats that exploit vulnerabilities of the interfaces between individual devices, passive eavesdropping or probing of accessible connections or components inside the device, and methods that destroy a part of the inside of a device. Security design guidelines to protect against the former kind of threats can be established easily, since the attack points are clear. However, it is difficult to analyse the latter two kinds of security threats because the technical sophistication of attackers, the attack methods, and the attack points all vary widely.

i) Home gateway – terminal (equipment on premises of users)

As a typical example, we can consider an attempt to discover a vulnerability in the SCP/CAS protocol in order to obtain the key information necessary to decode the encrypted content captured from the home network (e.g. Ethernet).

ii) Terminal – CAS

Threats can occur in cases where the hardware configuration of the CAS is detachable from the terminal. In the case of video distribution by multicast, the same kind of threats as those of ordinary broadcasting can be expected. Since CAS is widely used in broadcasting, its technical maturity is high. One advantage is that when a vulnerability is found in the CAS itself, the CAS can be replaced relatively easily.

iii) Terminal – PCs

It is conceivable that content inside a terminal is wiretapped or unauthorized accessed via the home network. A particular danger is the risk of unauthorized access to content by spoofing as a terminal in the case when content or licences can be transferred between terminal devices.

iv) Terminal – monitor display

This threat is conceivable when the TV monitor and terminal are separate. It is extremely difficult to eliminate this threat completely when output is passed through an analogue output. Analogue video coping is not serious problem because the image is deteriorated. There is no degradation of video when using digital outputs, such as HDMI and DVI-D; it is necessary to prevent this threat totally.

v) Terminal – removable media (memory device)

Writing content to highly portable devices such as removable media is extremely appealing, since it allows users to use content anytime and anywhere. To enable this, it is necessary to copy or move the encrypted content and encryption keys securely from the terminal to the removable media, but this can present a security vulnerability.

Note that a fundamental issue here is: even assuming perfect protection against security threats while the device is connected to the system, if there is no user identification function included with the device it is impossible to prevent the sharing by users of items such as books and rental videos. Thus, it is difficult to estimate the level of security threat presented by removable media.

vi) SCP/CAS in the Terminal

This threat needs to be considered particularly when the CAS and the terminal are integrated in the terminal. If implemented in software, it is impossible to make the SCP/CAS completely tamper-resistant, so it is necessary to determine the expected security attack level, and consider an implementation method that can stand up to such attacks. Also, if the SCP/CAS is integrated in the terminal, it is necessary to take into account the fact that it is extremely difficult to replace the SCP/CAS in the event of piracy.

vii) HDD in the Terminal

It is necessary to ensure that content cannot be read irregularly from a terminal containing a built-in hard disk. In particular, when reading from a terminal connected to a network is allowed, careful attention must be paid to preventing unauthorized reading of content.

viii) Memory device

In the case of highly portable media, many of the devices themselves have content protection mechanisms. When using such media, it is essentially impossible to share the media itself, so this should be taken into account to achieve a security balance.

I.2 Security Threats Model

The security threats can be classified into the following types: content security threats, service security threats, network security threats, terminal device security threats, and subscriber security threats.

The security threats model illustrated as Figure I-3, which shows the relationships among each of these threats.

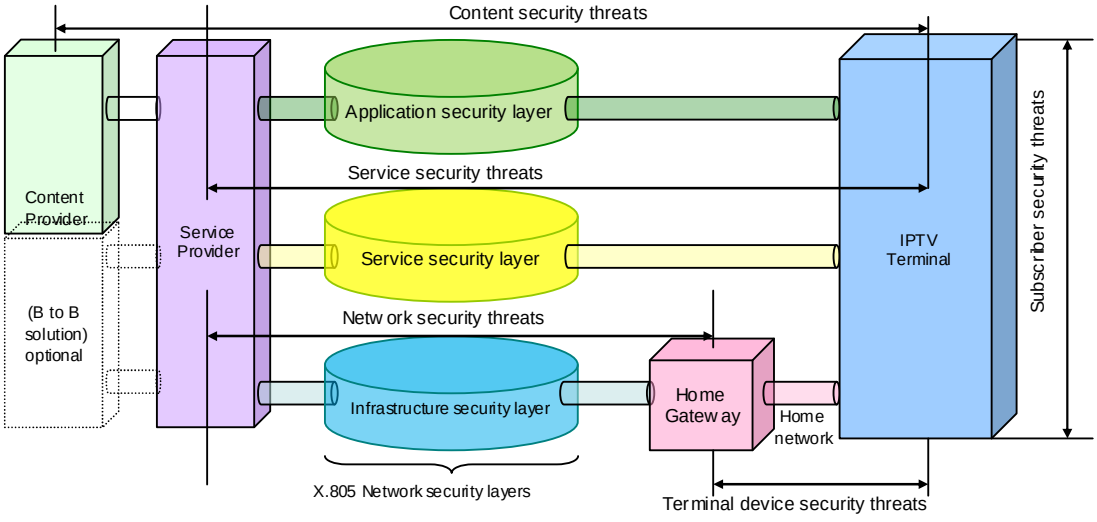


Figure I-3: Security Threats Model

I.2.1 Content Security Threat

Content asset: The assets which belong to Content provider and/or Service provider, and can be consumed by the end-user via IPTV terminal device.

The content assets which need to be protected are as follows:

Linear TV content, VoD content, Push VoD content, PVR content and downloaded applications.

The content threats are listed as below:

- Interception: a breach of confidentiality of the digit content by illegal monitoring the service networks.
- Unauthorized viewing.
- Unauthorized reproduction or redistribution.
- The relationship of content assets, risks and threats are illustrated as following table (see Table I-2).

Table I-2: Content Assets, Risks, and Threats

ASSET	RISK	SEVERITY	THREAT SOURCE	LIKELIHOOD
Compressed, plaintext content asset	Unauthorized copy obtained from network, network device or end system	High if the work is within the release window or deemed highly valuable by the provider. Otherwise Medium to Low	Cracker	High
			Professional	
			Insider	
		Low if end-user does not distribute, or if content is traceable to the end-user, moderate to high otherwise	End-user	High[1]
Compressed, encrypted content asset	Unauthorized access	None, unless the key is obtained, high otherwise	Cracker	N/A
			Professional	
			Insider	
			End-user	Low
Any content asset	Denial of service attack	High	Cracker	Moderate
			Professional	Low
			Insider	Low
			End-user	Low

[1] NOTE – End-users are highly likely to attempt to capture or copy content for their use or limited distribution. The means and motivation are, however, likely to be insufficient for a successful attack on a well secured implementation.

I.2.2 Service Security Threat

The service assets which need to be protected are as follows:

Service assets: The assets belonging to Service Provider, including media servers, AAA servers, SCP servers, CDN servers, and operational information such as service logs and billing information.

Service threats are listed as below:

- Impingement copyrights of the programs which IPTV service platform provided to the subscribers.
- Masquerading/spoofing IPTV service provider.
- Malicious threats aimed at the IPTV servers (AAA servers, media servers, etc.): may include the hacking aiming at security leaks in application software or communication protocol, denial of service attack, etc.
- Theft (often use malicious programs, such as Trojan horse) of the subscribers' information (e.g. identity information, billing information, subscription information).

The relationship of service assets, risks and threats are illustrated as following table (see Table I-3).

Table I-3: Service Assets, Risks, and Threats

ASSET	RISK	SEVERITY	THREAT SOURCE	LIKELIHOOD
Domain Name Server	Denial of service attack	Medium	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized access	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
Electronic Program Guide	Denial of service attack	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized access	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
Media Servers and multiplexers	Denial of service attack	High	Cracker	High
			Professional	Low
			Insider	Low
			Consumer	Low
	Unauthorized access	High	Cracker	High
			Professional	Low
			Insider	Low
			Consumer	Low
CAS and Subscriber Management	Denial of service attack	High	Cracker	High
			Professional	Low
			Insider	Low
			Consumer	Low
	Unauthorized use	High	Cracker	High
			Professional	Low
			Insider	Low
			Consumer	Low

I.2.3 Network Security Threat

The network assets which need to be protected are as follows:

Network assets: The assets belong to Network Provider, and which could include physical equipments (e.g. routers, switches) and network resources (e.g. bandwidth, multicast services, etc).

And the network threats are listed as below:

- Intentional threats aiming at the network equipments or resources (bandwidth): malicious attacks such as denial of service to the bearer network.
- Security threats to multicast technical used in IPTV bearer network: such as masquerading / spoofing multicast TV sources, or illegitimate multicast group members.
- Malicious attacks (like DoS, hacking) on nodes in Content Distribution Network.

The relationship of network assets, risks and threats are illustrated as following table (see Table I-4).

Table I-4: Network Assets, Risks, and Threats

ASSET	RISK	SEVERITY	THREAT SOURCE	LIKELIHOOD
Network bandwidth	Denial of service attack	Medium	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized access or use	High	Cracker	Medium
			Professional	High
			Insider	Low
			Consumer	Low
Network Messages	Unauthorized access	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized modification	High	Cracker	High
			Professional	Medium
			Insider	High
			Consumer	Low
	Replay	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
Routers, intermediate systems, access servers and system hosts	Denial of service attack	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized use	High	Cracker	High
			Professional	Medium
			Insider	Low
			Consumer	Low

I.2.4 Terminal Device Security Threat

The terminal assets which need to be protected are as follows:

Terminal assets: The assets belong to terminal device, by which the end user can use to process and store content and other relevant information for the IPTV service.

And the terminal threats are listed as below:

- Illegally accessing clear content by tampering device hardware or software. For example, clear contents can be copied by bus data interception or SCP software cracking.
- Illegally accessing keys or other secret information in devices using software cracking or hardware tampering. Attackers can tamper the device memory or analyse the data flow to obtain the keys and other secrets. Content key exposure results in content leakage and device key leakage leads to device impersonation.
- Device malfunctioning by hardware methods, such as control of the device clock system to disable the functions of the SCP/CAS systems, or by software methods, such as installation of viruses to exhaust the device resources.
- The unauthorized applications (such as software programs) were downloaded, run and stored in terminal devices.
- The failure of the terminal equipments (hardware and software) caused by malicious codes/viruses from the network.
- The unauthenticated terminal devices connecting to the home network.
- The unauthorized use by subscribers

The relationship of terminal assets, risks and threats are illustrated as following table (see Table I-5).

Table I-5: Terminal Device Assets, Risks, and Threats

ASSET	RISK	SEVERITY	THREAT SOURCE	LIKELIHOOD
Locality	Fixed-location device that is outside residence is given service	Medium	Cracker	Low
			Professional	Low
			Insider	Low
			Consumer	Medium
	Mobile device owned by non-subscriber is given service	Medium	Cracker	Low
			Professional	Low
			Insider	Low
			Consumer	Medium
Processor and Disk	Infection by malicious software	High	Cracker	Low unless executables downloaded from the network
			Professional	Low
			Insider	Low
			Consumer	Low
	Unauthorized use	High	Cracker	Low
			Professional	Low
			Insider	Low
			Consumer	Low
Interface	Subversion of content protection controls (e.g. HDCP, HDMI)	Medium	Cracker	Low
			Professional	Low
			Insider	Low
			Consumer	Low

I.2.5 Subscriber Security Threat

The subscriber assets which need to be protected are as follows:

Subscriber assets: The assets belong to subscriber, which can consist of information about the subscriber, the subscriber household, and their IPTV transactions, etc.

Table I-6: Subscriber Security Categories

	Subscriber Security		
	Example of service	**Example Threats**	**Example of protection mechanism**
Content security	TV, VoD service	Illegal copy	terminal/device identification (Service Protection, Content Protection)
Service security	Bi-directional service	Phishing	personal identification (Protection of personal data, PIN/Password)
	Parental	Spoofing	personal identification (PIN/Password, authentication)
Network Security	Not specify	Eavesdropping	subscriber line identification encryption data, multicast join control
Terminal device security	P2P service	illegal copy	Content Protection (P2P)

Subscriber security requires that a mechanism which realizes Content security and a mechanism which realizes Service security have to work in cooperation each other because IPTV service has a service in which Content security and Service security works in cooperation each other.

And the subscriber threats are listed as below:

- Theft of the subscribers' important information (e.g. login ID and password) and end user's privacy by malicious programs, such as Trojan horse.

The relationship of subscriber assets, risks and threats are illustrated as following table (see Table I-7).

Table I-7: Subscriber Assets, Risks, and Threats

ASSET	RISK	SEVERITY	THREAT SOURCE	LIKELIHOOD
Subscriber information	Unauthorized access: Disclosure to unauthorized party	High	Cracker	Medium
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized access: Modification by unauthorized party	High	Cracker	Medium
			Professional	Medium
			Insider	Low
			Consumer	Low
Transaction information Credit card info	Unauthorized access: Disclosure to unauthorized party	High	Cracker	Medium
			Professional	Medium
			Insider	Low
			Consumer	Low
	Unauthorized access: Modification by unauthorized party	High	Cracker	Medium
			Professional	Medium
			Insider	High
			Consumer	Low

Appendix II

Discussion of Interoperability of SCP

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

II.1 Overview of Interoperability of SCP

The scope of interoperability of SCP will focus on IPTV terminal device and other device, and not involved in SCP server in head-end.

II.2 SCP interoperability scenarios

The SCP interoperability scenarios are classified into at least three modes: SCP End to End (SCP-EE), SCP Bridging (SCP-B) and SCP Interchange (SCP-IX).

(1) SCP End-to-End (SCP-EE)

SCP-EE: Using a single SCP, two or more devices exchange and access content according to granted rights. This mode should be the simplest mode to implement since only a single SCP.

(2) SCP Bridging (SCP-B)

SCP-B: On a single device, two or more SCPs are deployed. Content acquired via one SCP system (from a network for example) can be accessed via another SCP resident on the same device according to granted rights.

(3) SCP Interchange (SCP-IX)

SCP-IX: This case is characterized by two or more devices, each device having one or more deployed SCPs. Content acquired by one device through one of its SCPs can be securely transferred to and accessed on another device through a different SCP according to granted rights.

The following figure II-1 illustrates a model of the case described above.

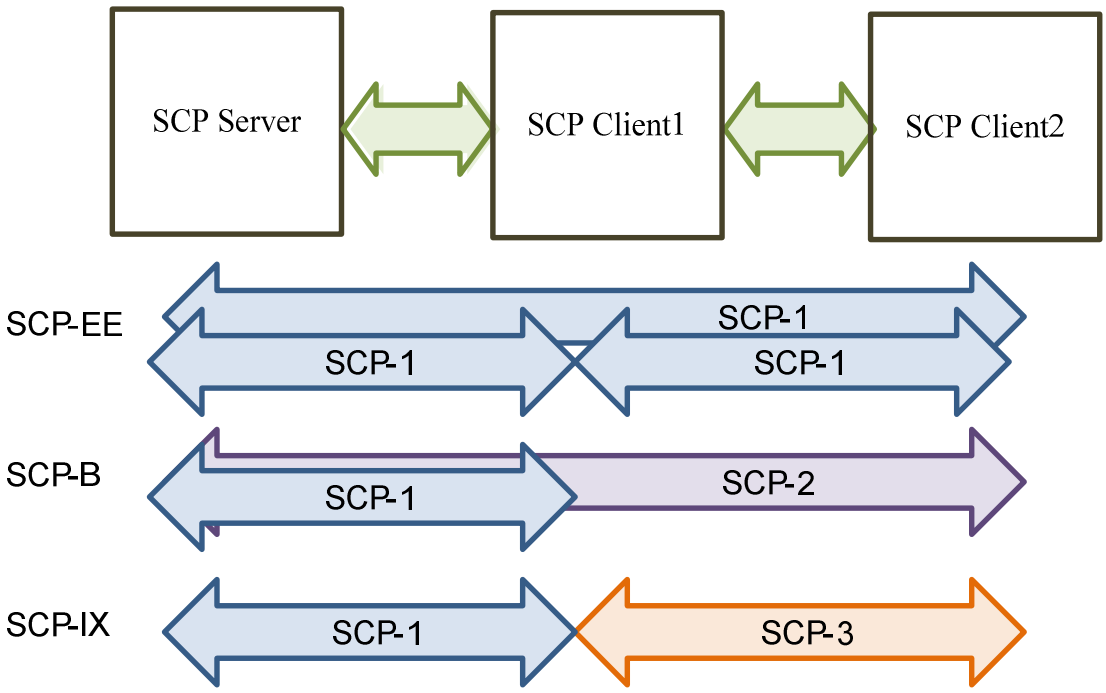


Figure II-1: SCP interoperability mode

II.3 Technical areas of SCP Interoperability

The following areas represent key interoperability elements that are required in the SCP-EE, SCP-B and SCP-IX modes.

(1) Authentication of devices, users and SCPs

Before content can be exchanged between entities, the identity of the terminal device and possibly its user(s) must be confidently established. Also, since content providers may not trust specific *SCPs*, it is important that it be possible to authenticate the receiving *SCP*(s) or implementation levels before exchanging content. This authentication should have a sound cryptographic basis and may employ various well-known digital signature techniques. Public Key cryptography in particular provides a sound mechanism for digital signatures in authentication protocols.

(2) Rights Expression Exchange

Different *SCPs* use different rights expression languages or licence formats. For *SCP*-B and *SCP*-IX modes to function, some means for a common rights expression is required. This could take the form of a common rights expression language (REL) or a rights expression translator. Another possible rights expression exchange mechanism is licence negotiation.

(3) Common encryption algorithms for content exchange

For content to pass securely from the control of one *SCPs* to another or within the same *SCPs* but on different physical devices, content encryption is required. This renders the content unusable except for entities that possess the appropriate key or keys necessary for decryption to occur. There are many different types of encryption algorithms (e.g. block ciphers, stream ciphers, public-key-based, etc.) but generally those that use symmetric keys tend to be best suited for high-speed content exchange. For interoperability purposes, some small number of commonly agreed algorithms must be chosen. Ideally, one default algorithm would also be specified.

(4) Key management and/or exchange for the common encryption algorithms

Before secure content exchange can take place, keys to be used in specific instances need to be exchanged or commonly generated by the authenticated entities. Key management is usually the most difficult part of a security system to implement. Techniques such as Public Key cryptography have simplified device key distribution but require a public key infrastructure (PKI) to establish and maintain the validity of these keys. Such an infrastructure could be sanctioned and maintained by a licence authority which has responsibility for content protection (as opposed to general network security).

(5) Secure download of SCP client

Ideally, any IPTV terminal device would be able to exchange content obtained (legitimately) through other devices and/or using any *SCP* according to the granted rights (i.e., the *SCP*-IX mode). However, it is not practical to pre-load at manufacture time every IPTV terminal device with every *SCP* system that market forces will demand. Thus, a secure mechanism for downloading and executing a selected *SCP* system onto a terminal device is needed. Elements such as secure boot-loaders and secure download protocols play a part in this area of interoperability.

NOTE – When SCP interoperability is deployed in the devices and end systems, IPTV devices should have a trusted architecture to support interoperability of content security.

(6) Secure right exportation

In order to securely export digital rights, IPTV SCP client should check whether usage rights is permitted to export to target SCP system. Digital rights may have rights expressions which enable target SCP system to export rights. In this case, IPTV SCP client should check these rights expressions and authorize proper target SCP systems to export digital rights.

II.4 SCP Interoperable Architectures

Two kinds of possible SCP interoperable architectures are considerable. One is based on mediator-based interoperability architecture. This interoperability architecture uses a mediator system, which is located in the middle of two SCP systems, to process interoperable transmission. The other one is a standard protocol-based architecture. It uses standard interfaces and protocols to transform protected digital content and associate information between two different SCP systems.

The two possible architectures are shown in the following two figures.

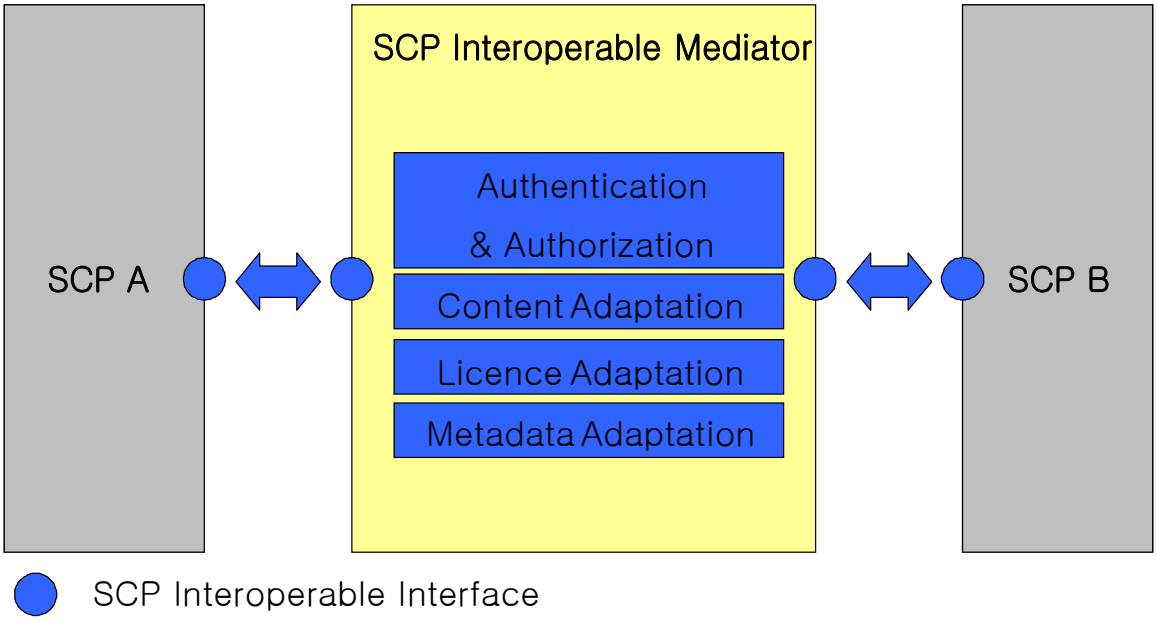


Figure II-2: Mediator based SCP Interoperable Architecture

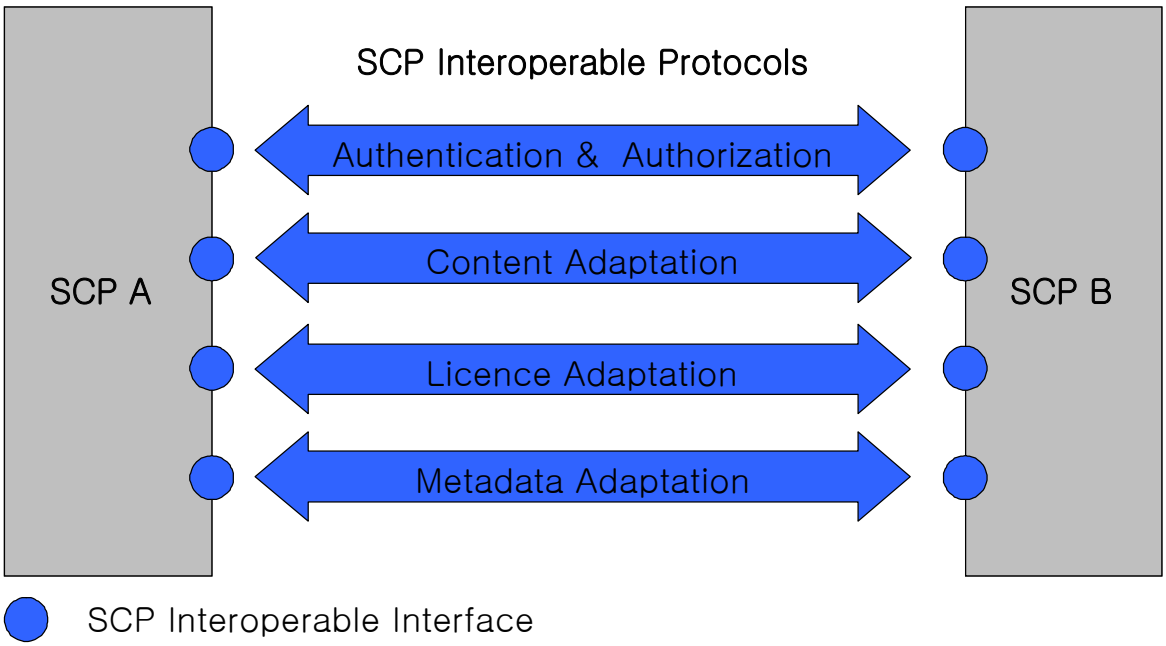


Figure II-3: Standard Protocol based SCP Interoperable Architecture

Function Block Description:

Content Adaptation*:* Content Adaptation is responsible for converting cryptographic algorithm. Given several pre-defined standard encryption algorithms will facilitate these processes.

Licence Adaptation: Licence Adaptation is responsible for converting licence. Any temporal or standard licence, which is known by both parties, should maintain almost same permission behaviours (media assets & consumption permission pair) as the original licence defined. A set of right mapping (rights expression mapping and semantic mapping) may be included in the Licence Adaptation. Also, Licence Adaptation may be responsible for repackaging right information and securely delivering it to native SCP clients.

Metadata Adaptation: Metadata Adaptation is responsible for converting metadata information. The temporal or standard metadata, which is known by both parties, should maintain the same information as the original metadata had. A set of metadata mapping (syntax and semantic mapping) may be included in the Metadata Adaptation. Also, Metadata Adaptation may be responsible for repackaging metadata information and securely delivering it to the other SCP party.

Authentication & Authorization: Each SCP party should judge whether the other party is proper target to achieve SCP interoperability. It is usually accompanied with mutual authentication process as a preliminary step between two SCP parties.

Exceptional Case: If SCP A and SCP B are located within the same device or there is a dedicated secure communication channel between two SCPs, the Content Adaptation process may not need interoperable processing.

II.5 Scenarios of SCP-B or SCP-IX deployed in IPTV terminal device

This clause describes three possible scenarios which need SCP Interchange between Service Security and Content Security.

II.5.1 Definition of terms used in the diagram

- SCP_IN: An input port from which IPTV content protected by SCP comes in.
- SCP_OUT: An output port to which IPTV content protected by SCP goes out.

II.5.2 Scenario 1: SCP with SCP_IX

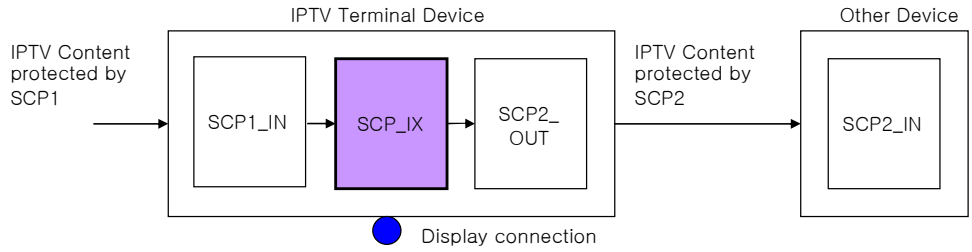


Figure II-4: SCP with SCP_IX

An IPTV TD (Terminal Device) in this case has the SCP with SCP_IX to support interoperability between the IPTV TD without storage which adopts only specific service security, and external device with storage which has only specific content protection.

In order to support secure and flexible connectivity to any kind of external devices which adopts various content protection mechanisms, the IPTV TD should have SCP_IX better than case-by-case implementation for the security connection between two devices.

II.5.3 Scenario 2: SCP with optional SCP-B and storage

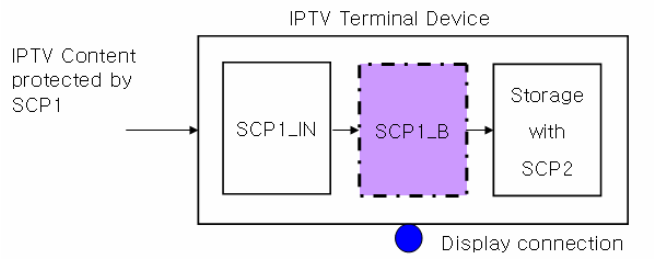


Figure II-5: SCP with optional SCP-B and storage

An IPTV TD in this case has the SCP with SCP-B to support interoperability between service protection and content protection on a single device.

Manufacturer of the IPTV TD may adopt the proprietary content protection mechanism for internal storage. In that case SCP_B is not necessary and the storage may use SCP1

In order to support flexible connectivity to any kind of internal storage which adopts various content protection mechanisms, the IPTV TD is recommended to have SCP_B, better than case-by-case implementation for the security connection between service protection and content protection.

II.5.4 Scenario 3: SCP with storage and SCP_IX

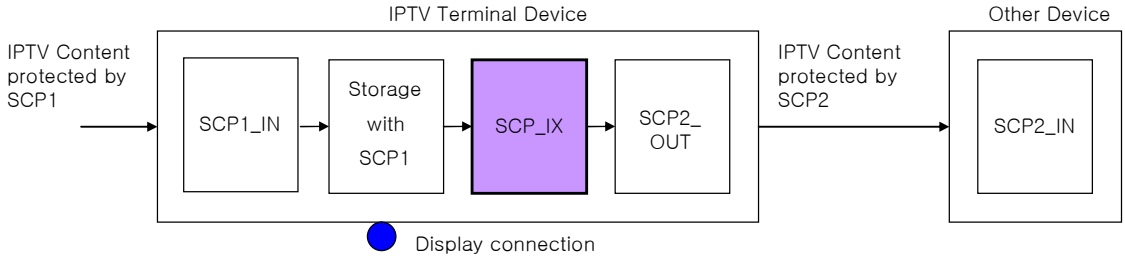


Figure II-6: SCP with storage and SCP_IX

An IPTV TD in this case has the SCP with storage and SCP_IX to support interoperability between internal content protection mechanism and external one.

In order to support flexible connectivity to any kind of external storage which adopts various content protection mechanisms, the IPTV TD is recommended to have SCP_IX, better than case-by-case implementation for the security connection between internal content protection mechanism and external one.

Appendix III

An Example of IPTV Service and Content Protection Process

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

III.1 Example of Content Protection Process

An example process of the IPTV content protection is described as follows:

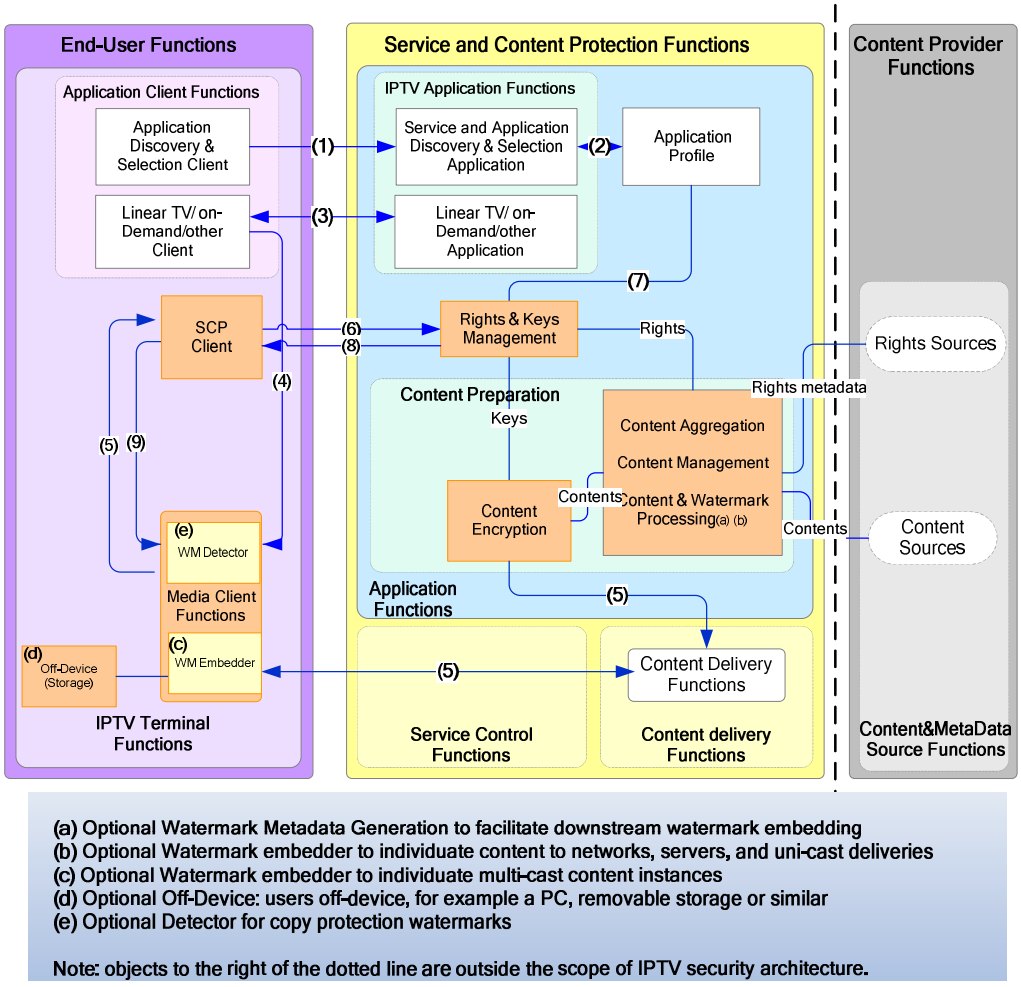


Figure III-1: An example process of the IPTV content protection

(1) Subscriber selects an application (e.g. Linear-TV or On-Demand application) provided by IPTV service provider.

(2) Application Selection Server will send the request to "Application AAA" to verify the subscriber. If success, the associated authorization information will be cached in the "Application AAA" component for inquiry.

(3) Then the subscriber can select the specific media content from the EPG, and the "Linear-TV/VoD Application" will deliver the selected content's URL.

(4) "Linear-TV/VoD client" receives the URL, and gives it to "Media client" component.

(5) "Media client" applies for the media content (encrypted) from the network according to the URL, as well as inquires the "SCP Client" for the rights and keys associated with this content.

(6) If "SCP Client" hasn't the rights and keys, it will request them from the "Rights & Keys management" component.

(7) "Rights & Keys management" component will validate the request by inquiring the "Application AAA" for the authorization information associated with this subscriber.

(8) If successful, the right and key for the selected media contents will be delivered to the "SCP client".

(9) "SCP client" will transfer the key and right to "Media Client" to decrypt and control the usage of the media contents.

III.2 Example of Service Security Protection Process

An example process of the IPTV service security is described as follows:

- Subscriber sections linear TV application, which is provided by the IPTV service provider.
- Service provider verifies the identity via IPTV Service Control Function (Subscriber/Service Authentication Functions) and Control Clients (Subscriber/Service Authentication Client).
- Control Clients gets service key from the above authentication procedure or smart card, off-line and pre-distribution key.
- In case of service key distribution, the subscriber/service authentication function inquires subscriber's information from the subscriber/service management functions.
- Subscriber selects a channel for the live-stream TV, content delivery function determines requested contents are protected or not. If it is protected, contents are scrambled. Otherwise deliver it to the multicast network.
- During the scrambling, the encrypted scramble key or its derived information also delivered via content delivery function in form of multicast stream.
- Multicast Content Client Function, Receive the content and descrambling it with the Scrambling Key, which is delivered via multicast stream and it is encrypted with service key.
- Sometimes, service security functions are replaced with new one. The service security client download functions would like to download new one from the service security client delivery function via unicast network.

The service security client maybe includes its code authentication data, which can verify the integrity and authority.

Appendix IV

Usage Rights

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

Usage Rights can include the information (but not limited to): Payment Information, Copy Restrictions, Storage Restrictions, Thumbnail Display Restrictions, Printing Restrictions, Viewing Period Restrictions, Zone Restrictions, Age Restrictions, Gender Restrictions, Number of Plays, Play Restrictions, Consumer Metadata Usage Restrictions, Type of Content Delivery, Encryption, Types of Authentication Method, Distribution Media, Playback Device, Restriction on Number of Distributions, Usage Report.

Multiple terms or phrases are sometimes used to refer to *usage rights*, including, without limitation:

- rights
- content rights
- content rights metadata
- content usage rules
- content usage information

This document (including its annexes and appendices) does not attempt to unify these expressions into one normative representation.

Appendix V

Downloadable Application Protection

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

V.1 Authorization and authentication before the software downloading

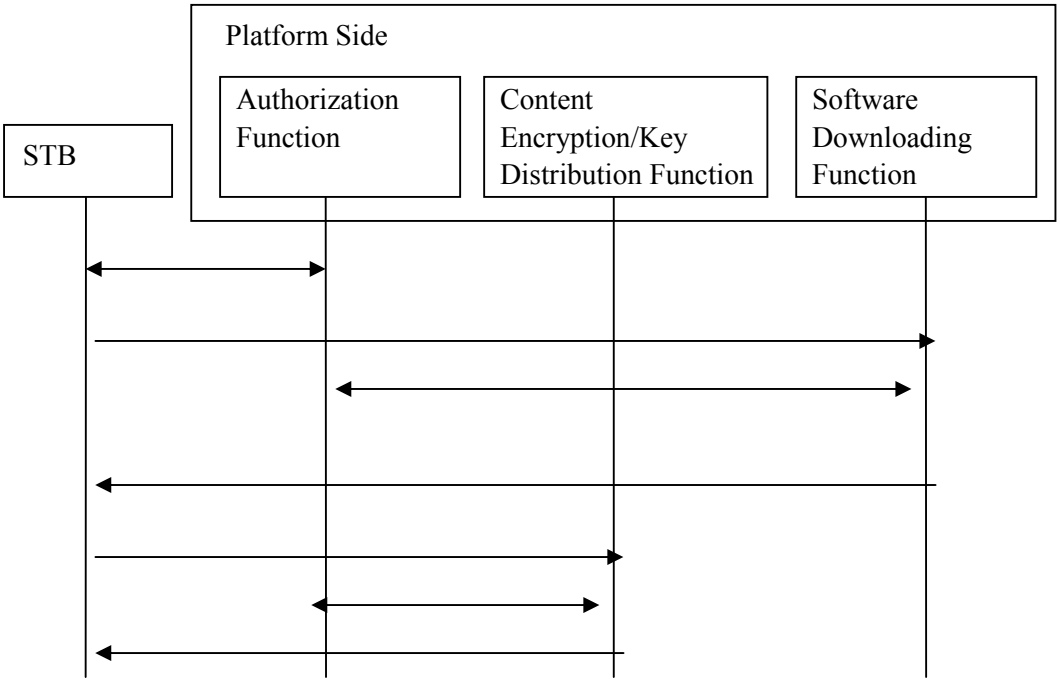


Figure V-1: Authorization before Software Download

1. The user selects a software program to download. Before downloading, the STB communicates with the authorization function to get the permission;
2. After the user passes the authorization, the STB accesses the software downloading function to request the downloading;
3. The software downloading function check the permission info with the authorization function;
4. After the checking work, the software downloading function allows the STB to download the software;
5. After the downloading, STB communicates with the Content Encryption/Key Distribution Function to get the key to decrypt the software package;
6. The Content Encryption/Key Distribution Function request the permission info from Authorization Function;
7. With the permission, the Content Encryption/Key Distribution Function responses the STB with the key. The STB decrypts the software package.

V.2 Authorization and authentication during the software program running

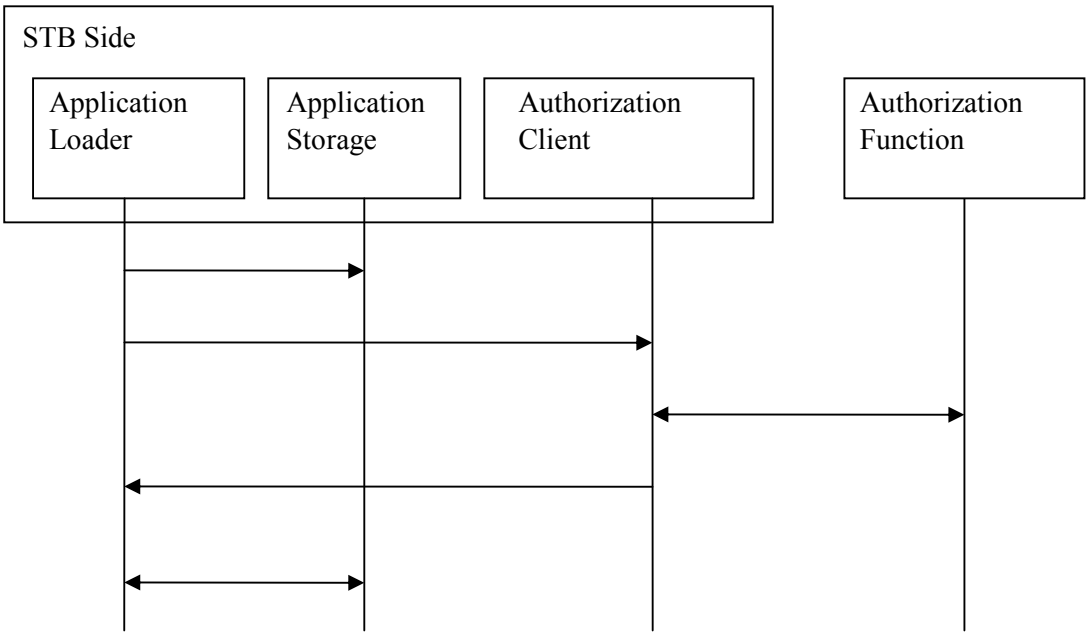


Figure V-2: Authorization after Software Download

The user selects a software program to execute. And the Application Loader request the Application Storage function to read the software program;

1. The Application Loader finds that the software program request an authorization to execute, and it request the Authorization Client to get the info;

2. The Authorization Client communicates with the Authorization Function in platform side to get the Authorization info;

3. The Authorization Client sends the Authorization info to the Application Loader;

4. With the permission, The Application Loader reads and loads the software program from the Application Storage function to execute the software program.

V.3 The encryption of the software programs when the programs are stored in STB, and decryption before running/duplicating the software programs

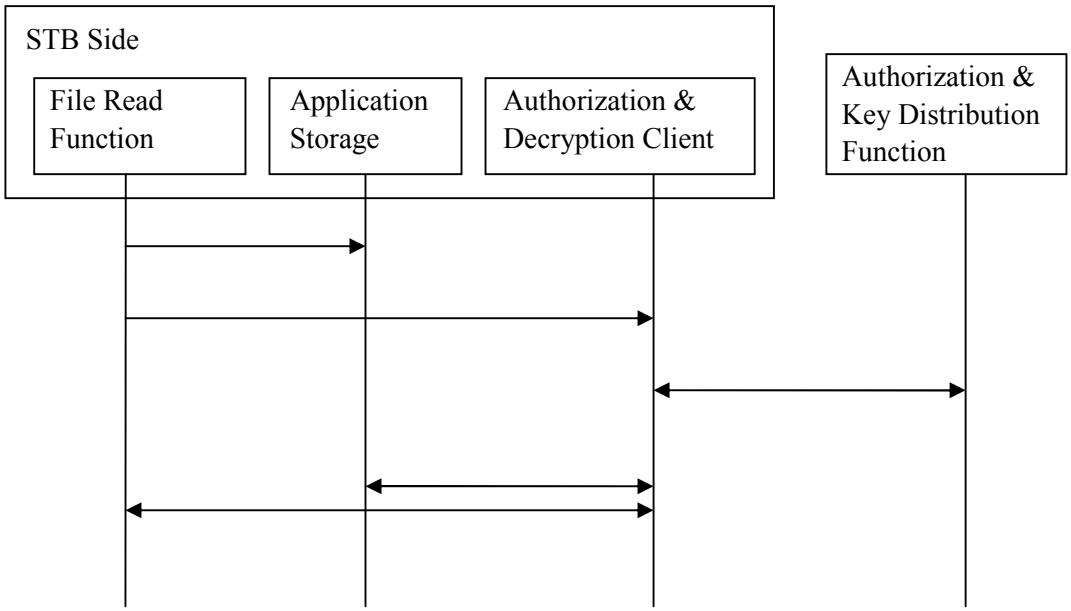


Figure V-3: Encryption at Storage

1. The user selects a software program to run/duplicate. And the File Read Function request the Application Storage function to read the software program;

2. The File Read Function finds that the software program request an authorization or decryption keys to read, and it request the Authorization & Decryption Client to get the info;

3. The Authorization & Decryption Client communicates with the Authorization & Key Distribution Function in platform side to get the authorization info and decryption keys;

4. With the permission, The Authorization & Decryption Client reads and decrypts the software program from the Application Storage function and sends it to the File Read Function.

Appendix VI

DVB Content Protection & Copy Management

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

VI.1 Introduction

The DVB CPCM is a system for Content Protection & Copy Management of commercial and free-to-air digital content delivered to consumer products and home networks. CPCM manages content usage from acquisition into the CPCM system until final consumption, or export from the CPCM system, in accordance with the particular usage rules of that content. CPCM is intended for use in protecting all types of content – audio, video and associated applications and data. CPCM provides specifications to facilitate interoperability of such content after acquisition into CPCM by networked consumer devices for both home networking and remote access. The specification is made up of parts, some of which specify signalling and actions required for technical compliance, and other parts which explain the rational behind the specification, including Implementation Guidelines. A Reference Model provides the framework for the CPCM System and is the foundation upon which the remaining specification elements build.

VI.2 Definitions

Acquire: Receive and ingest content from outside the CPCM System into the CPCM System.

Acquisition Point (AP): Abstract CPCM Functional Entity where content Acquisition takes place.

Acquisition: Receipt and ingestion of content that was outside the CPCM System into the CPCM System.

Authorized Domain (AD): A distinguishable set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household. A household is considered to be the social unit consisting of all individuals who live together, as occupants of the same domicile. This makes no assumptions about the physical locations of the devices owned, rented or otherwise controlled by the members of the household.

Authorized Usage: The permitted usage of CPCM Content, consisting of the set of Usage Rules assertions applied to that Content.

Consume: Tangibly render Content, or output Content constrained to inhibit any other usage.

Consumption Point (CP): Abstract CPCM Functional Entity where Consumption is performed.

Consumption: Tangible rendition of Content, or a Device Output containing a transformation or signal that is intended to inhibit any usage other than the immediate conversion of the Content to sound and vision

Content Item: A discrete instance of Content of finite duration, e.g., a program/event or an incomplete segment thereof.

Content Licence: A securely maintained and communicated data structure containing the information necessary to manage the security of a CPCM Content Item.

Content: Data that is to be protected by the CPCM System. This is generally audio-visual content plus optional accompanying data, such as subtitles, images/graphics, animations, web pages, text, games, software (both source code and object code), scripts or any other information which is intended to be delivered to and consumed by a user.

Copy: A CPCM-managed process whereby a new stored Content Item is created from Acquired Content or from an existing stored Content Item.

CPCM Device: Device that hosts one or more CPCM Instances.

CPCM System: The set of all compliant CPCM Devices.

Device Application: Any non-CPCM functionality within a CPCM Device.

Export Point (EP): Abstract CPCM Functional Entity where CPCM Content leaves the CPCM System.

Export: Release of CPCM Content from explicit protection and management by the CPCM System to a Controlled CPS, a Trusted CPS or an Untrusted Space.

Move: The process of making a Copy wherein the original is then removed, erased or made no longer accessible.

Output: Device interface or CPS used to transmit CPCM Content, Consumed Content, or Exported Content.

Processing Entity (PE): Abstract CPCM Functional Entity where CPCM Content is Processed.

Processing: A CPCM compliant operation upon encrypted or unencrypted Content other than for Consumption or Export. For example, where CPCM Content undergoes a permitted transformation from its original form to create new transformed CPCM Content, or where information is extracted from the Content such as audio volume levels or still images.

Usage State Information (USI): CPCM Content metadata that signals the Authorized Usage for each CPCM Content Item.

View: Consume. NOTE – This also includes listen for audio only content.

Viewing: Consumption. NOTE – This also includes listening for audio only content.

VI.3 Abbreviations and acronyms

AD Authorized Domain

AP Acquisition Point

APECS Acquisition, Processing, Export, Consumption, Storage

CL Content Licence

CP Consumption Point

CPCM Content Protection and Copy Management

CPE Customer Premise Equipment

CPS Content Protection System

DVB Digital Video Broadcasting

EP Export Point

HN Home Network

PE Processing Entity

SE Storage Entity

USI Usage State Information

VI.4 CPCM Architecture

At the heart of CPCM is the "Authorized Domain", a collection of devices belonging to a household, even when they are away from home. The AD concept recognizes that tying content to a single set-top box (IPTV Terminal Device) and an attached TV display is not enough in an age of networked entertainment. CPCM takes content from a trusted source, such as an IPTV SCP system, as embodied as part of an IPTV Terminal Device and protects the received content stream or file, managing how it can be viewed, moved, and copied. The basic CPCM content management model is that Input Content enters the CPCM System to become CPCM Content. CPCM Content is managed and protected within the CPCM System. CPCM Content leaves the CPCM System when it is consumed by the user, or when Exported to another system.

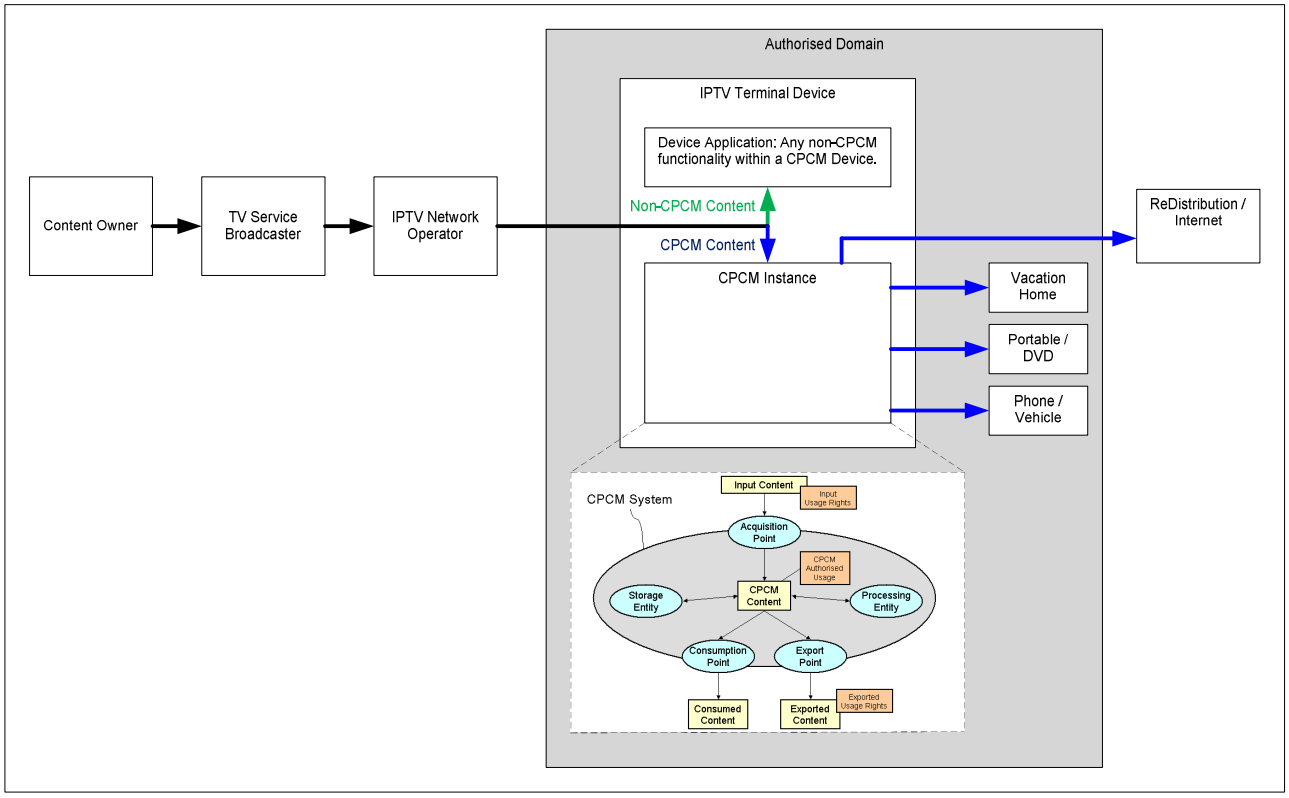


Figure VI-1: Content Flow in a CPCM Environment

CPCM supports a variety of uses of content on a Home Network, and can also manage access to content from remote locations such as a laptop on a broadband internet connection. By using CPCM, service providers can signal to device manufacturers the permissible scenarios for each type of content. This extends many of today's protection methods such as those embodied in IPTV SCP technologies, whereby content is typically constrained to a single point-to-point interconnect cable between the content source device (such as a Set Top Box) and the digital display device.

CPCM goes beyond this localized protection, giving broadcasters, network operators and content owners the option to allow access by a household member from a remote location such as a hotel during a business trip or a vacation.

CPCM can also enable users to copy content to portable devices and removable storage such as a DVD. As long as the playback device belongs to the same Authorized Domain, the device will be able to play back the content even when disconnected from the home and the original service provider. CPCM content does not require any online authorization from a service provider to add or remove devices to/from the Authorized Domain.

The CPCM content protection system doesn't stand alone; it is incorporated / overlayed into the overall end to end IPTV SCP distribution system. As such it does not replace an IPTV SCP system, it co-exists with it. In any IPTV Terminal Device the CPCM Instance is optional, however if it is not present it will not be permitted access to any CPCM protected content. However an IPTV Terminal Device need not implement all CPCM elements, only those that are useful to it to perform the functionality it needs. For example a simple device might only implement CPCM Acquisition and Consumption functionalities, if it has no CPCM storage or export requirements.

VI.5 CPCM Reference Model & Functional Entities

The CPCM Reference Model defines the set of five abstract content management functions – Acquisition, Storage, Processing, Consumption, and Export – which cover all relevant content usage scenarios in the consumer environment. These functions map to the five CPCM Functional Entities – Acquisition Point, Storage Entity, Processing Entity, Consumption Point, and Export Point. Figure VI-1 above shows the view of the CPCM System in terms of the set of abstract Functional Entities.

Thus Input Content that enters the CPCM System does so by being Acquired at an Acquisition Point, by a CPCM Device that implements that Acquisition Point, to become CPCM content. CPCM Content can be Stored or Processed by the corresponding Functional Entities (Storage Entity, Processing Entity), implemented on a CPCM Device. CPCM Content leaves the CPCM System when it is Consumed, at a Consumption Point, or Exported, at an Export Point. Again, these Functional Entities can be implemented inside any CPCM Device.

VI.6 CPCM Authorized Domain

CPCM Devices can be logically grouped into Authorized Domains. If all those devices belong to one household, then they would constitute that household's Authorized Domain (AD). Thus the Authorized Domain provides a destination for content that maps to the bounds of a single household. In general terms the AD can be seen as the logical grouping of all the CPCM Devices belonging to one household, be those devices located in the main domicile, devices located at another domicile (e.g. holiday home), portable handheld devices that are only intermittently connected with the aforementioned stationary devices, or devices fitted in the vehicles(s) belonging to that household. The AD is intended to be an autonomous logical group of devices, not requiring any external administration. However, there may be cases where the AD is linked to a particular service provider, who may offer to administer the AD as part of their service provision to the consumer.

VI.7 CPCM Content Usage Rules

The Authorized Usage for any item of CPCM Content is the set of usage assertions expressed in the CPCM Usage Rules tied to the content. The CPCM Usage Rules may be set by the content or service provider, or may be mapped from the form of delivery (e.g. free-to-air broadcast). The extent to which Storage, Consumption and Export operations might be able to be performed may be subject to the content's Authorized Usage. CPCM defines a common set of Usage Rules that are available for any content provider to select from and accordingly derive the desired Authorized Usage for the content within the CPCM System. The set of CPCM Usage Rules is intended to be flexible enough to cover all applicable content protection and management models, but is also concise enough to maintain clear and relatively simple content usage models for the consumer.

VI.8 Usage State Information Metadata

The Authorized Usage of a Content Item is coded as CPCM Content metadata called Usage State Information (USI). CPCM Content is managed and protected according to the USI applied to each Content Item. Apart from the compliant USI state transitions that are carried out implicitly by the CPCM System, entities holding legitimate authorization over content within the CPCM System can perform other changes to a Content Item's USI state after Acquisition in the CPCM System.

VI.9 CPCM Content

"Content" is generally audio-visual content plus optional accompanying data, such as subtitles, images/graphics, animations, web pages, text, games, software (both source code and object code), scripts or any other information which is intended to be delivered to and consumed by a user. CPCM Content is Content that is protected and managed by, and in conformance with, the CPCM System. A Content Item is a discrete instance of Content of finite duration. Each CPCM Content Item is accompanied by a Content Licence carrying the associated USI together with further CPCM metadata. The CPCM System can handle the Content Licence and the Content Item itself in different ways depending on the target functionality and/or usage rules enforcement required by the USI.

VI.10 CPCM Device

A CPCM Device is a device that implements any CPCM functionality in a compliant manner. The implementation of CPCM functionality is referred to as a CPCM Instance. A CPCM Device is a device that hosts one or more CPCM Instances. A CPCM Device can also contain some other non-CPCM compliant function in addition to its CPCM functionality. CPCM Content handling is performed only by the CPCM Instance inside the device. The non-CPCM part of the device has no access to CPCM Content. The CPCM Device can also host non-CPCM secure functionality, for the secure Acquisition of Content from other protection systems, or the secure Export (or possibly Consumption) of CPCM Content.

VI.11 Usage Rule & Usage State Information

A Usage Rule in CPCM is a particular operation upon, or behaviour of Content to be controlled within the scope of the CPCM System. A complete set of Usage Rules assertions for a particular CPCM Content Item is referred to as the Authorized Usage of that CPCM Content Item. A Content Item's Authorized Usage is expressed by its coding in Usage State Information (USI), which is thus CPCM Content metadata that signals the Authorized Usage for that particular Content.

II.4 IPTV NETWORK CONTROL

II.4.1 IPTV network control aspects

Summary

This document describes various aspects of IPTV network control. It provides a list of detailed requirements to address control and signalling matters related to authentication and authorization, content delivery, consumer domain attachment and initialization, quality of service (QoS), quality of experience (QoE) and security.

Keywords

IPTV, overlay service, overlay network, QoS, QoE

Current status

After carefully reviewing and extensive editing works, this document contains consensus of information from all the contributions addressed to the working group. It mainly addresses the detailed functional requirements and implementation guidelines of the following network control aspects:

- Network control and signalling
- Content delivery network
- IPTV consumer domain attachment and initialization
- Identification
- IPTV inter-working
- Overlay networks

In terms of IPTV network control and signalling inter-working, this document provides a list of items for further study. The list serves as a starting point and is not complete. Further study is needed in the following areas:

- Identifying the complete list of inter-working aspects in the context of IPTV network control
- Providing detailed guidelines for inter-working aspects related to IPTV network control

Dependency on or relationship to other FG IPTV documents:

- IPTV services requirements
- IPTV architecture
- IPTV multicast frameworks
- Aspects of IPTV end system – terminal device
- Aspects of home network supporting IPTV services
- IPTV Middleware, Applications, and Content Platforms

CONTENTS

		Page
1	Scope	366
2	References	366
3	Definitions	367
3.1	Terms defined elsewhere	367
3.2	Terms defined in this document	367
4	Abbreviations and acronyms	367
5	Conventions	368
6	Framework of IPTV Network Control Aspects	368
7	Control and Signalling Aspects	369
7.1	Network Control	369
7.1.1	Unicast Network Control	369
7.1.2	Multicast Network Control	369
7.1.2.1	Multicast IP Address Management	370
7.1.2.2	Multicast User Management	370
7.1.2.3	Multicast Session Identifier Management	370
7.1.2.4	Source Specific Multicast	370
7.1.3	Connection Admission Control	370
7.2	IPTV Network High Availability	371
7.2.1	IPTV Network Service Failure Recovery	371
7.2.1.1	Redundant System Architecture and Topology	371
7.2.1.2	Robust Network against Attacks	371
7.3	Linear TV Control	371
7.4	Parental Control	372
7.5	Network Traffic Identification	372
7.6	Session Control	372
7.7	Stream Control	372
8	Content Delivery Network Aspects	372
8.1	Content Delivery Network Topology	373
8.2	CDN-based IPTV Media Delivery Mechanism	373
8.3	Distributed Content Storage/Cache and Content Serving	374
8.4	Centralized Content Location Management	374
8.5	Distributed Content Delivery	374
8.5.1	Distributed Edge Server Networks	375
8.6	Content Segmentation	375
8.7	Statistical Performance of Content Delivery Network	375
8.8	Content Delivery Protocols	376

Page

9 IPTV Consumer Domain Attachment and Initialization 376

10 Identification Aspects 377

11 IPTV Inter-working 378

12 Overlay Network Aspects 378

12.1 Control Function in IPTV Overlay Network 378

12.2 Multicast Function in IPTV Overlay Network 379

12.3 Session Manager in IPTV Overlay Network 379

12.4 Manageable Overlay Network 379

13 Other Aspects 379

I.1 IPTV Device Initialization and Attachment Flow 380

I.1.1 Network Attachment 381

I.1.1.1 Delivery Network Gateway (DNG) 381

I.1.1.1.1 DHCP Approach1 381

I.1.1.2 IPTV Terminal Device (TD) 385

I.1.2 Service Provider Discovery 389

II.1 Requirement on Multicast VPN in IPTV Network Control Aspect 389

II.2 IPTV Multicast VPN Group Management 390

IPTV network control aspects

1 Scope

This document describes various aspects of IPTV network control. It provides a list of detailed requirements to address control and signalling matters related to authentication and authorization, content delivery, consumer domain attachment and initialization, quality of service (QoS), quality of experience (QoE) and security.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[FG IPTV-DOC-0147] ITU-T FG IPTV document *IPTV services requirements*

[FG IPTV-DOC-0181] ITU-T FG IPTV document *IPTV architecture*

[FG IPTV-DOC-0190] ITU-T FG IPTV document *IPTV multicast frameworks*

[ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in next generation networks*

[IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*

[IETF RFC 2710] IETF RFC 2710 (1999), *Multicast Listener Discovery (MLD) for IPv6*

[IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3*

[IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for Ipv6*

[IETF RFC 4541] IETF RFC 4541 (2006), *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

[IETF RFC 4601] IETF RFC 4601 (2006), *Protocol Independent Multicast – Sparse Mode (PIM-SM)*

[IETF RFC 4604] IETF RFC 4604 (2006), *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

[IETF RFC 4605] IETF RFC 4605 (2006), *Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Channel zapping: The act of fast changing from one channel to another.

3.1.2 Connection admission control

The mechanism that controls the traffic to be admitted into the network.

3.1.3 Electronic program guide: A structured set of data, intended to provide information on available content that may be accessed by end-users.

3.1.4 End-user [ITU-T J.112]: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network

3.1.5 IPTV terminal function: The functionality that is responsible for processing the content conveyed by the IP transport.

3.1.6 Linear TV: A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed.

3.1.7 Video on demand: A service in which the subscriber can view video content whenever desired. The operating assumption is that the content is stored on the provider's VoD server. Subscriber accesses the movie from a library directory which may include search engine that accesses movie description and rating. Subscribers typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time when using this service.

3.2 Terms defined in this document

This document defines the following terms:

3.2.1 Overlay network: A virtual network of nodes and logical links that is built on top of the underlying network infrastructure with the purpose of implement a network service that is not available in the underlying network infrastructure.

3.2.2 Overlay multicast network: One type of overlay network that provides multicast services to end users on top of the general network infrastructure.

3.2.3 Parental control: Parental Control provides a mechanism for deciding the suitability of particular content for a minor on his/her age.

4 Abbreviations and acronyms

This document uses the following abbreviations.

ASM Any Source Multicast

CAC Connection Admission Control

CDN Content delivery network

CRID Content Reference Identifier

DHT Distributed Hash Table

DoS Denial of Service

EPG Electronic Program Guide

IGMP Internet Group Management Protocol

ISP Internet Service Provider

ITF IPTV Terminating Function

P2P Peer-to-Peer

QoE Quality of Experience

QoS Quality of Service

SNI Service Node Interface

SSM Source Specific Multicast

VoD Video on Demand

VPN Virtual Private Network

5 Conventions

In this document:

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

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document 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/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Framework of IPTV Network Control Aspects

NOTE – The terminology and the architecture assumed in this document needs to be checked for alignment with IPTV architecture document.

This clause provides a general overview of IPTV network control aspects, as shown in Figure 6-1. There are many views of addressing control aspects of IPTV networks. This overall framework contains functional components, such as Service Control Functions, Content Delivery Functions and Network Functions, related to IPTV network control aspects and is aligned with IPTV Functional Architecture Framework.

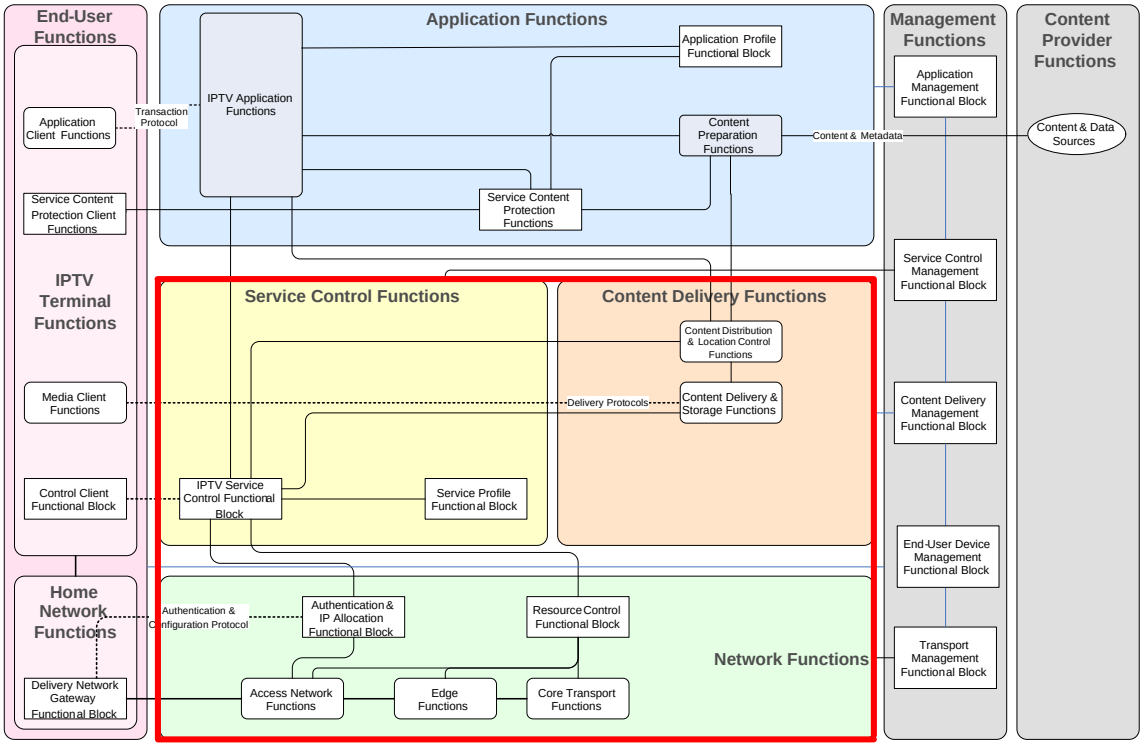


Figure 6-1: Overview of IPTV network control

7 Control and Signalling Aspects

7.1 Network Control

7.1.1 Unicast Network Control

For further study

7.1.2 Multicast Network Control

Multicast network transport is one of the major drivers to promote IPTV service in telecommunications networks. IP multicast communication can improve the efficiency of data transmission and make efficient use of network bandwidth resources when delivering broadcast content. Therefore, multicast technology and its control functions are important in the network to deliver IPTV service.

The IPTV architecture is recommended to support alternative multicast schemes such as content delivery network (CDN), overlay multicast, peer-to-peer (P2P), etc., with control of each multicast scheme. It is required to have a compatible capability of managing different multicast schemes.

The IPTV architecture is recommended to support static configuration of the IP multicast distribution tree, and to support well designed dynamic IP multicast protocol to reduce traffic for IPTV service.

IPTV multicast network control is required to support the multicast control function and multicast replication function which provide IPTV multicast services for users. Multicast control function builds a privilege table for multicast users according to the multicast group address, so that when users receive IPTV multicast services, multicast network control deals with IPTV multicast services according to users' multicast

privilege. The multicast replication function forwards multicast media content to users which have the privilege of IPTV multicast services. That is to say, IPTV multicast network control will forward the IPTV service contents to a user only if the user has multicast privilege.

The IPTV architecture is recommended to support multicast in access network and multicast protocol proxy in access nodes or other network nodes where multicast traffic is replicated to users.

7.1.2.1 Multicast IP Address Management

- The IPTV architecture is recommended to support mechanisms to manage multicast IP address to ensure the deployment of IPTV service successfully.
- The IPTV architecture is recommended to support Multicast IP Address Transition for Cross-domain IPTV Service.
- The IPTV architecture is recommended to support the control of end-users' multicast address for user multicasting.

7.1.2.2 Multicast User Management

- The IPTV architecture is recommended to support multicast user authentication function for multicast services of IPTV.
- The IPTV architecture is recommended to support configuring users' corresponding multicast privileges according to the multicast group address.
- The IPTV architecture is recommended to support configuring the relationship between users and their multicast privilege.

7.1.2.3 Multicast Session Identifier Management

Because there can be various multicast schemes, it is required to describe multicast session uniquely. For example, a multicast session using pure IP multicast can be described by IP multicast address but a multicast session using CDN can be described by URL. IPTV is recommended to manage identifier to describe a specific multicast session uniquely.

7.1.2.4 Source Specific Multicast

Source Specific Multicast (SSM) reduces the overall complexity within IPTV. SSM is also optimized for One-to-Many deployment scenarios which are typically used within IPTV. Any Source Multicast (ASM) and SSM can be used in parallel (deploying different address ranges) if necessary. The use of SSM eases the deployment of IPTV and reduces the complexity, allowing more flexible IPTV services.

7.1.3 Connection Admission Control

It is required that Connection Admission Control (CAC) is supported in the access network based on available resources. When the end user subscribes to a multicast stream, the access network will perform CAC to check if the current available resources are enough for the new service subscription. The resources can be bandwidth, connection number and user service privilege profile.

For the reason that some IPTV service streams are mixed in the access network,

- The IPTV architecture is recommended to support the QoS class queues for each IPTV service stream.
- The IPTV architecture is recommended to support queue control functions to guarantee quality for IPTV service streams in the access network.

- The IPTV architecture is recommended to support bandwidth allocation function for each IPTV service stream in the access network. For reference, bandwidth allocation function can be operated based on the User ID, Service Stream ID, and Bandwidth which includes the whole bandwidth of the access line, minimum guaranteed bandwidth and maximum guaranteed bandwidth.

7.2 IPTV Network High Availability

For general network high availability service requirements, please refer to [FG IPTV-DOC-0147] sub-clause 6.4.

7.2.1 IPTV Network Service Failure Recovery

The IPTV network is recommended to provide the capability for ensuring sufficient availability of IPTV services.

7.2.1.1 Redundant System Architecture and Topology

The IPTV network is recommended to be a fully redundant system architecture and topology such that a single point of failure is recommended to not affect the whole network.

7.2.1.2 Robust Network against Attacks

The IPTV network is recommended to be designed to be robust such that it can tolerate unexpected attacks such as denial of service (DoS) attack.

7.3 Linear TV Control

Channel zapping protocol is the interactions for and between the Service Stratum and the Transport Stratum in terms of channel selection.

Multicast control of Linear TV is recommended to include but not limit to the followings:

- Channel Access Control: Channel Access Control of Linear TV is recommended to support some access right statuses of the entitlement to each of the broadcast channels for each user, such as fully allowed, preview allowed, not allowed.
- Channel Preview Capability: Channel Preview Capability of Linear TV is recommended to support some preview control functions of the Linear TV channel, such as Maximum duration for each preview, Maximum times of previews, Blackout duration after each preview, Reset period of channel preview, Recognition Time of channel preview, etc.
- Call Detail Record: Call Detail Record is recommended to report the entitlement status of the channel being access, and records the channel access activities of each customer should be generated automatically.
- Priority of Linear and other traffic: Linear TV is recommended to support capabilities for classifying channel priorities such as based on bandwidth and multicast resource reserved for programmes, etc. Channel audience rating statistics could be obtained by policy server based on end-user multicast behaviour information collected from access nodes and used to determine and provision subscriber channels priority in the access node for channels difference disposal. The end-user multicast behaviour information can be optionally to include programme item number, start viewing time, stop viewing time. In order to guarantee Linear TV's quality and service provisioning, Linear TV is recommended to be of strict priority than other traffic and no impact from data traffic during the transmission.

- Service Management System: Service management system is recommended to support some service related management functions of Linear TV channel, including user management, policy management, SP/CP management, accounting management, service customization management, security management, performance management, portal management, STB management.

7.4 Parental Control

Parental controls have been typically included in digital television services, video games, etc. that allow parents to monitor or limit what their children can see or do. For the IPTV architecture, parental control mechanism can be used to restrict IPTV contents that children can receive. Policy control and management for parental control is recommended to support the network capability to store and forward the requested IPTV services and its rating to specified terminals (e.g., monitoring terminal for parent) based on preconfigured control policy and user profiles. The policies are varieties include time limiting, content rating, etc.

7.5 Network Traffic Identification

Identification mechanism of Network traffic can optionally be required over the transport network to check traffic status when necessary. Traffic flow traversing IPTV transport network could be satisfied the demand of IPTV services. The use of identification mechanism makes it possible to manage properly according to operating policies. It can also be used to prevent the network intrusion so that to protect IPTV services.

7.6 Session Control

The stream session control protocol is recommended to support carrying authentication/authorization token, carrying message signature and cross server session.

7.7 Stream Control

The stream transport protocol is recommended to support representation of position in frame, frame awareness, frame awareness for trick modes, physical server aware client.

8 Content Delivery Network Aspects

IPTV content delivery networks are required to support non-real time and real-time IPTV services such as Linear TV, Video on Demand (VoD) and Electronic Program Guide (EPG) content delivery, system information, ad-insertion (e.g. SCTE 35); to provide IPTV capabilities such as content protection, closed captioning, content transport leveraging and content segmentation; and to define CDN components to record and provide performance statistic. Content Delivery Network related functions are indicated in Figure 8-1 and aligned with IPTV Functional Architecture Framework.

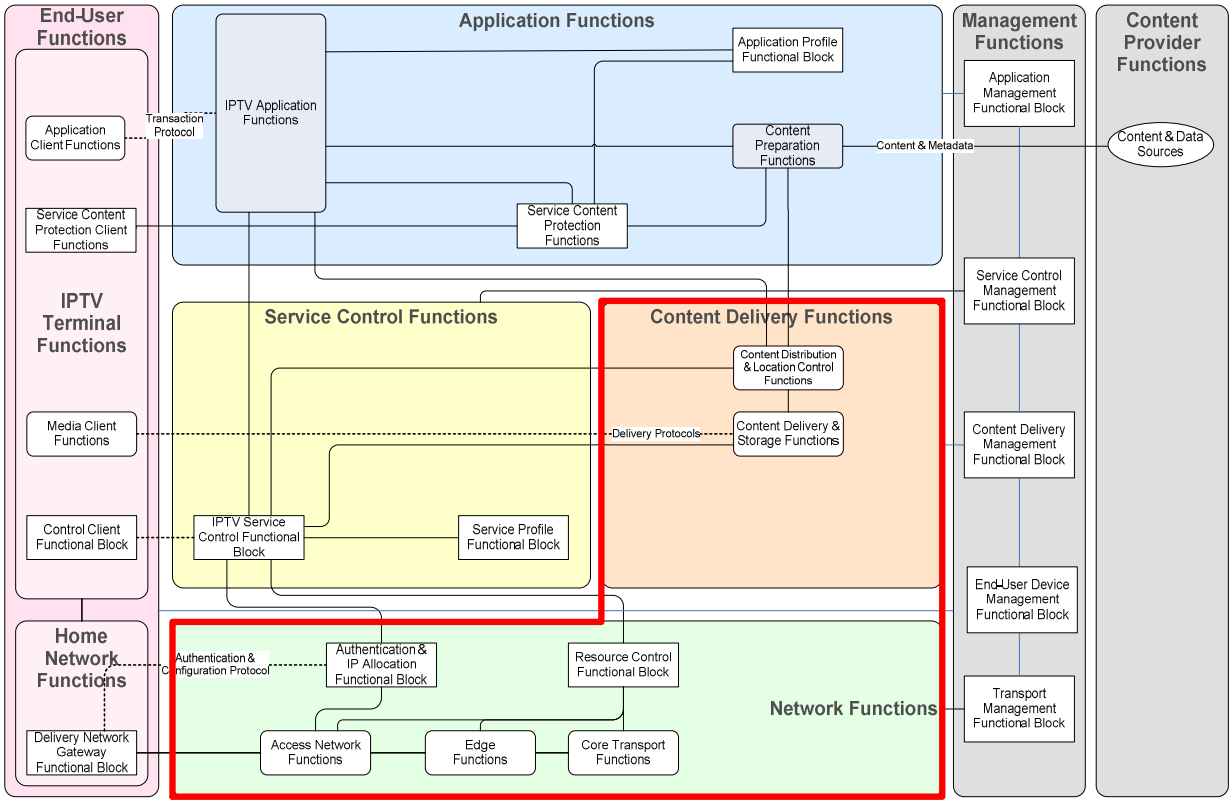


Figure 8-1: IPTV Content Delivery Functions

8.1 Content Delivery Network Topology

The IPTV content delivery network is recommended to be layered. Each layer may have several serving nodes that flexibly construct a content delivery network. The serving node may be constructed by a node controller and several streaming servers. The node controller provides the load balancing among the streaming servers in the serving node, and adjusts the deployment of the contents between serving nodes. The streaming server is required to provide streaming service in real-time to users under the control of the node controller.

A distributed structure is recommended to be adopted in the content delivery network layer. The serving nodes in the content delivery network layer are optionally required to communicate with each other to exchange the contents.

8.2 CDN-based IPTV Media Delivery Mechanism

In order to ensure manageability and interoperability of CDN-based IPTV content delivery network, the CDN-based IPTV media delivery mechanism is recommended to include: Media Delivery Manager, Media Delivery Agent and Streaming media server.

The Media Delivery Manager, which is responsible for global load balancing and interfacing with other subsystems, supports serving control function, content control function and operation maintenance function.

The Media Delivery Agent, which is responsible for local load balancing, is attached to every streaming media node and supports serving control function, content control function and operation maintenance function for the corresponding node.

The Streaming Media Server, which is responsible for storing content and streaming media, supports streaming function, content storage function, content delivery function, and operation maintenance function.

Server-based IPTV media delivery mechanism and CDN-based IPTV media delivery mechanism are described in [FG IPTV-DOC-0190]. In server-based IPTV media delivery mechanism, ISP puts a media server or server pool somewhere; each member connects media server or server pool; then the media server sends data to every receiver. In CDN-based IPTV media delivery mechanism, ISP pre-installs CDN servers in an appropriate place; each receiver finds and then connects the nearest CDN server. Then multimedia streams from source are distributed to each receiver along the data delivery path of CDN servers.

8.3 Distributed Content Storage/Cache and Content Serving

- **Distributed Content Storage/Cache**

  The content delivery network can store, cache, distribute and deliver IPTV media contents according to a distributed content delivery mechanism. The distributed content delivery mechanism enables service providers to store IPTV media contents on storage/cache nodes. The content storage/cache nodes are optionally required to be deployed according to their physical network location and their subscriber coverage. The distributed content storage/cache network enables service providers to dynamically distribute IPTV media contents according to pre-defined delivery policies.

- **Distributed Content Serving**

  Content serving in distributed content delivery network is implemented by independent content serving nodes. The content delivery control node can arrange an appropriate content serving node to provide IPTV streaming service for each end user according to the load of each content serving node and the state of content distributed in each content storage/cache node.

8.4 Centralized Content Location Management

A centralized content location management module is recommended to be responsible for keeping track of the locations of all the content in the IPTV network. It maintains a record of network topology, a content location, and a content delivery session.

The network topology describes the topology of the media servers and the network topology of the media servers. Media content is copied from one location to another by creating content delivery sessions between two media servers in the both locations. These sessions are created and deleted as the copy process starts and finishes respectively. This information is used by the content location management module to keep track of the bandwidth usage among the media servers and the central site.

The characteristics of the centralized content location management are as follows.

- Tracking each content program location in a distributed media servers.
- Tracking the delivery sessions among media servers.
- Keeping statistical and historic data of content delivery and copy sessions.

8.5 Distributed Content Delivery

The IPTV architecture is recommended to support a distributed architecture among content edge servers.

Co-located edge media servers are recommended to have the ability to be organized in a distributed structure to share the load, to improve the reliability and to reduce the total cost of the edge servers.

According to the method of the distributed structure, original files or content can be stored evenly on the edge servers. User's requests can be redirected to the most suitable edge server automatically without the help of a central device.

8.5.1 Distributed Edge Server Networks

Distributed architecture is used to organize all local edge server networks to form distributed edge server networks. That is, distributed architecture among all local edge server networks is recommended to be supportable such that the burden of both serving users and content storage can be evenly distributed on all local edge server networks.

- **Content Locating**

  Some automatic content locating approach is used in the local edge server network to find a suitable edge server for the user. If not found, the user's request will be routed among all local edge server networks (by using automatic content locating method again) to locate a suitable local edge server network containing edge server with desired content.

- **Server functions**

  Each edge server in local edge server network is recommended to support automatic content locating methods for distributed structure. Each local edge server network is recommended to support automatic content locating methods for distributed structure. Automatic content locating capability is recommended to be supported by some agent server in each local edge server network, i.e. the agent server acts as the content locating agent of the corresponding local edge server network.

In Distributed Hash Table (DHT), edge server calculates and distributes content ID and content information to edge server in its local edge server network. Agent server calculates and distributes content ID and content information to another agent server which directly distributes content ID and content information to edge server in that edge server network. Content information is searched among edge servers in requestor's local network. If not found, some agent server is found to be responsible for the content information. That agent server directly searches content information in that edge server network by locating some edge server storing the required content information.

8.6 Content Segmentation

Content Segmentation can optionally be required in some IPTV deployments. IPTV Content Segmentation functions are recommended to generate segment at codec frame boundaries; to realize codec format (e.g. MPEG-2, MPEG-4, AVS, H.264 and VC-1); to apply to both clear-text and encrypted contents; and to support the quick identification of any frame within the segment and the entire program file.

8.7 Statistical Performance of Content Delivery Network

Statistical performance of Content Delivery network mainly includes the content storage server, the content serving server and the content delivery control function.

- **The content storage server** – manages content stored in both memory and persistent storage according to policy, i.e. content swapping, content deletion, etc.

  The content storage server records the number of requests satisfied by pushed contents, requests satisfied by pulled contents, requests satisfied by pulling remote contents, and requests satisfied by local contents. The content storage also records requests for remote contents, content push sessions and content pull sessions. The ratio between number of requests satisfied by pushed contents and the number of content push sessions indicates the effectiveness of content push. The ratio between number of requests satisfied by pulled contents and the number of content push sessions indicates the effectiveness of content pull.

- **The content serving server** – transmits requested content to end system in designated forms, or redirect request to other functionalities.

  The content serving server records the number of received requests for contents, served bytes and unsatisfied requests. The number of received requests for contents indicates the amount of load on the node. The number of served bytes indicates the number of bytes actually consumed by users – the effective bytes. Sum of bytes for pushed contents and bytes for pulled contents indicates the number of bytes made available to users. The ratio between the effective bytes and the available bytes indicates effectiveness of content push and pull.

- **Content delivery control function** – triggers and controls content transmission among content storage server, designate content, source, destination, speed of the transmission.

8.8 Content Delivery Protocols

The typical initial content delivery is through content pushing. The content is pushed from central media server to edge media servers according to the policy, schedule and delivery topology provided by centralized content location management.

The content delivery protocols are recommended to support the following.

- Flexible policies for content delivery
- Scheduled pushing of content to delivery servers
- Quickly identifying a source of the content and starting to copy
- The dynamic pulling of content by the delivery servers
- Multiple sources for content pulling.

9 IPTV Consumer Domain Attachment and Initialization

The IPTV device attachment and initialization process can be broken down into the following steps: Setup & Configuration, Network Attachment, Service Provider Discovery, and Services discovery & Service attachment.

- **Setup & Configuration**

  Setup & Configuration activities relate to acquiring and configuring a physical IPTV Terminating Function (ITF) device. This step establishes the identity and authentication credentials for the ITF, and service provider identity and any additional information for one or more service providers.

- **Network Attachment**

  Network Attachment refers to the activities associated with the ITF establishing Layer-3 connectivity to an IP-network and potentially obtaining additional network configuration data. During the network attachment phase, some information, such as IPv4 address, network mask, default route, DNS, local network domain name, SIP proxies, others …, may be obtained.

- **Service Provider Discovery**

  Service Provider discovery is the process by which an ITF becomes aware of the available IPTV Service Providers, learns the location of their Service Discovery (SD) Servers, and learns the means for attaching to each SD server. As a result, by contacting the discovered SD Server(s), an ITF can perform the subsequent Services Discovery and Service Attachment procedures.

- **Service Discovery & Service Attachment**

  Services Discovery is the process by which an ITF receives the necessary signalling information which prepares it to learn about and access the available IPTV Services. The ITF interacts with one or more Service Provider Servers (discovered earlier) in order to acquire information about specific services.

  The Services Discovery function includes both the "services discovery authorization" means and the "services description". After authorized by a Service Provider SD Server, the consumer needs to be able to navigate through the variety of service offerings and then attach to a specific service.

  For implementation examples, please refer to Appendix I.

10 Identification Aspects

It is necessary to provide identification mechanism to identify IPTV users, customers and subscribers to support IPTV services, which could be used in various players such as customer, service providers, network providers and content providers.

The IPTV network controls, manages and makes provision to optimize the service for various types of resources. In order to realize service optimization, the IPTV network can optionally utilize IPTV Identifiers such as Content ID, Content Provider ID, Service Provider ID, Network provider ID and User ID.

- Content ID (CID) – unique identifier of Content.
- Content Provider ID (CPID) – unique identifier of Content Provider.
- Service Provider ID (SPID) – unique identifier of Service Provider.
- Network Provider ID (NPID) – unique identifier of Network Provider.
- User ID (UID) – unique identifier of User or Subscriber.

The IPTV network uses content identifier to specify content with different granularity, and some locators to locate content among CDN to optimize the storage and serving. The IPTV network can optionally utilize the following IDs and Locators to specify content.

- Persistent Content ID – specifies content with persistent and globally interoperable identifier. It is used for transaction between service provider and content provider, or between service providers.
- Content Referencing ID – specifies content which is provisioned for service, and it is issued by a service provider. It may be not persistent and may be valid only in the service provider domain. It is used for transaction between a service provider and a user/subscriber.
- Logical Locator – specifies content in the context of service, time, place and resource. It is used for requesting a service to the IPTV network. It may include the protocol and service specific information.
- Physical Locator – specifies content in the context of physical IP network resource. It is used for establishing and routing of a delivery connection to the IPTV network. It may include the protocol, IP address and port number.
- Internal Locator – specifies content in the context of internal delivery platform resource of a service provider. It is used for allocation and management of internal server resources of delivery platform. Especially, when servers share a single IP address, it is used for load balancing.

11 IPTV Inter-working

NOTE – The following IPTV inter-working aspects need further study. Identified aspects are based on the contributions to this working group. The complete list of IPTV inter-working items needs further study also.

Inter-working among Non-NGN, NGN, IMS-based NGN

- Network level inter-working and service-level inter-working
- Inter-working between homogeneous IPTV service providers or between heterogeneous IPTV service providers, etc. with views of administrative domain.

More technically even though all these aspects are in question,

- Inter-working between unicast channel and multicast channel
- Inter-working among protocol, signalling, routing, QoS, addressing, naming, etc.
- Inter-working between different routing algorithms for IPTV services

12 Overlay Network Aspects

IPTV overlay network is responsible for forwarding and handling of IPTV application data in ways that are different form. And overlay network is operated in organized and coherent way by the third party service provider or network provider to provide IPTV services.

IPTV overlay network consists of virtual network topologies on top of the physical network, as shown in figure 16-1, which directly interfaces to users. With the rapid advancement of internet and computing technology, much more aggregate information and computing resources are available from clients or peers than from a limited number of centralized servers.

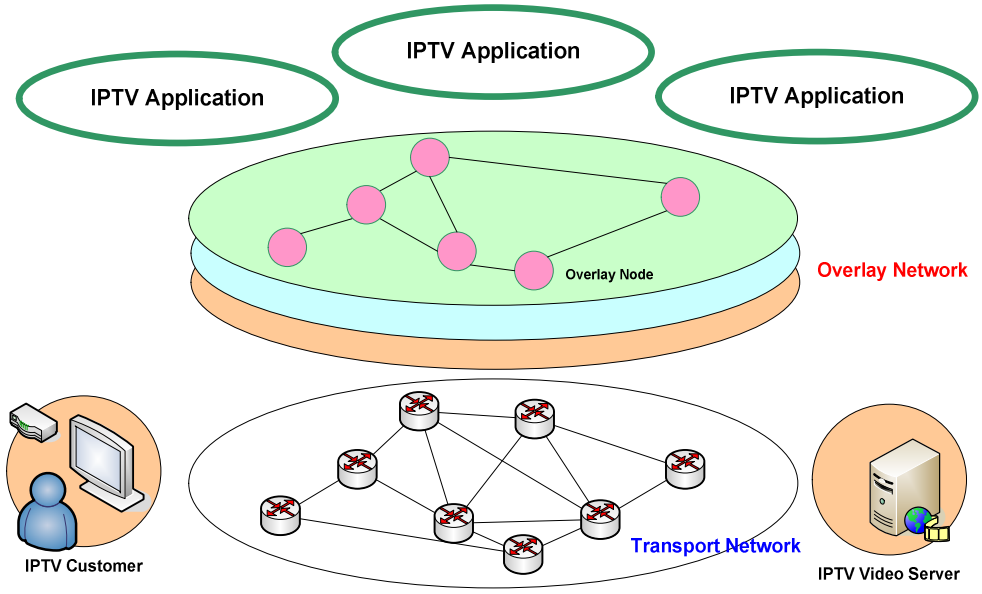


Figure 12-1: Overlay Service and Network for IPTV

12.1 Control Function in IPTV Overlay Network

In order to provide overlay session control in overlay networks for IPTV service, IPTV service control function is necessary to perform session control and management for IPTV overlay network, to establish and to maintain the network and system resources.

12.2 Multicast Function in IPTV Overlay Network

The overlay IPTV multicast can use diverse mechanisms for constructing different multicast trees depending on IPTV application parameters or application classes. The overlay IPTV multicast supports efficient routing and resource usage by overlay multicast control.

In order to provide scalability for multicast function, hierarchical structure for overlay multicast will be introduced in IPTV overlay networks.

12.3 Session Manager in IPTV Overlay Network

In the IPTV Overlay Network, session manager is the process of keeping track of session configuration and maintenance for IPTV service, and provide session initiation, release and management.

12.4 Manageable Overlay Network

In P2P-based IPTV service delivery scheme, each peer can be both a media producer as well as a media consumer. Although peer can exchange media between themselves and the size of peers group is not logically bounded, P2P model does not want to have ISP's censorship.

In order to achieve manageable P2P network, ISP is recommended to involve in some management functions of P2P. With these management functions, ISP can tightly manage the P2P network.

The advantages of manageable P2P model are:

– ISP can tightly manage content delivery network by involving in the management of P2P.

– The number of peers is not bounded by the capability of media server.

Manageable P2P network architecture principles:

• Peers can be classified into some groups.

• Each group has a Management Node (MN) deployed by ISP to manage peers in this group.

• Peers exchange IPTV media contents under the management of MN.

• Group information (e.g. meta-data of media) could be exchanged among groups.

Please refer to Appendix IV for manageable P2P examples.

NOTE – Mapping manageable overlay network to IPTV functional architecture needs for further study.

13 Other Aspects

Multicast VPN

IPTV multicast VPN service may accelerate IPTV applications as the worldwide demand for VPN services grows. In the meantime, IPTV multicast VPN also may enrich IPTV applications, such as classified IPTV service features according to geographical groups and customers' demand, differentiated IPTV service features in security and QoS for communities or groups, classified IPTV group service features, and personalized IPTV service capabilities on IPTV service provider's network.

Please refer to Appendix II for Multicast VPN examples.

Various home, access and core transport scenarios for multicasting

The DSL technology is one of the access networks as the underlying transport network to support IPTV services. The DSL technology is concerned with the networking architecture(s) superimposed over DSL transport to provide IPTV services.

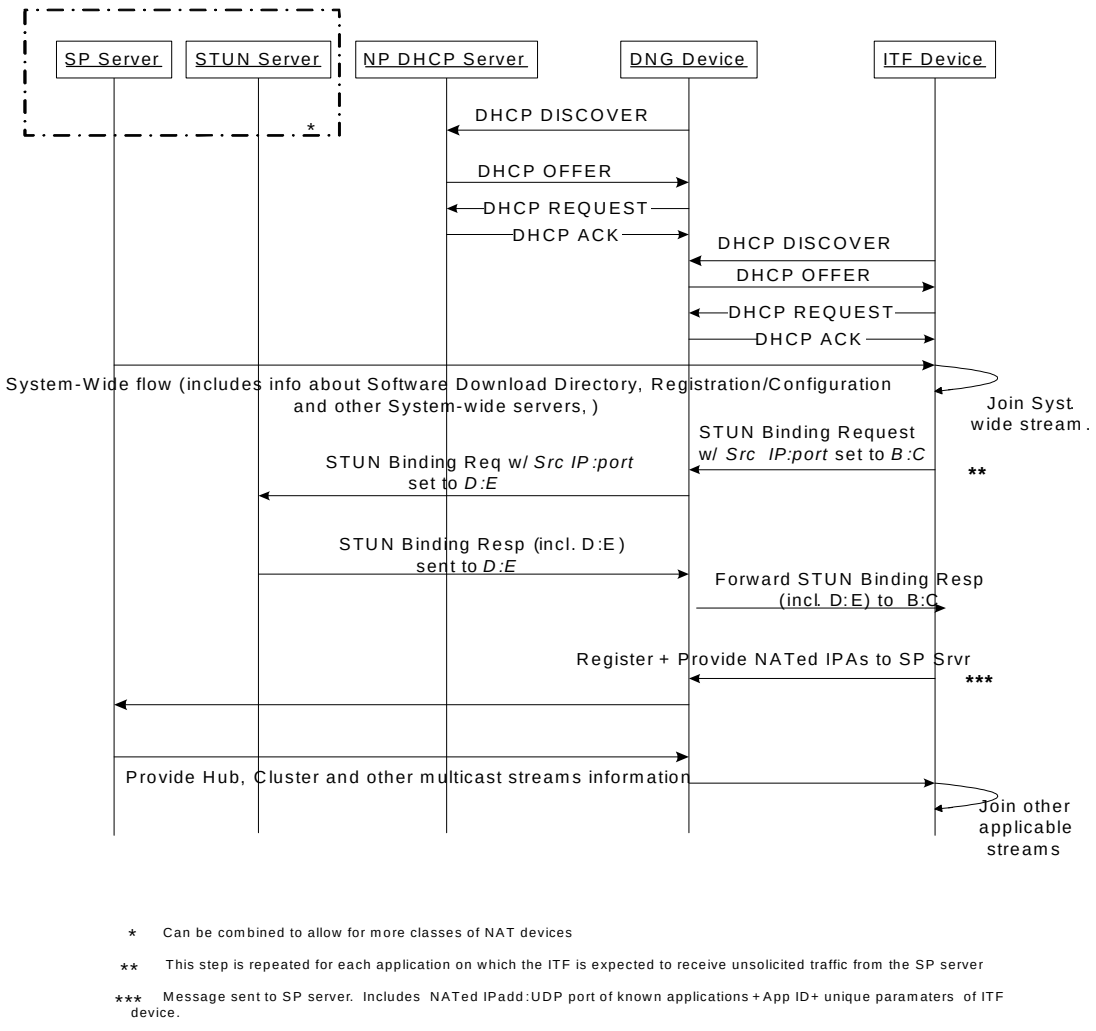
Appendix I

Example of IPTV Consumer Domain Attachment and Initialization

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

I.1 IPTV Device Initialization and Attachment Flow

Figure I-1 is an example of an IPTV device Initialization and Attachment based on DHCP.



* Can be combined to allow for more classes of NAT devices

** This step is repeated for each application on which the ITF is expected to receive unsolicited traffic from the SP server

*** Message sent to SP server. Includes NATed IPadd:UDP port of known applications + App ID+ unique paramaters of ITF device.

Figure I-1: IPTV Device Initialization and Attachment flow based on DHCP

Figure I-2 is an example of an IPTV device Initialization and Attachment based on PPPOE.

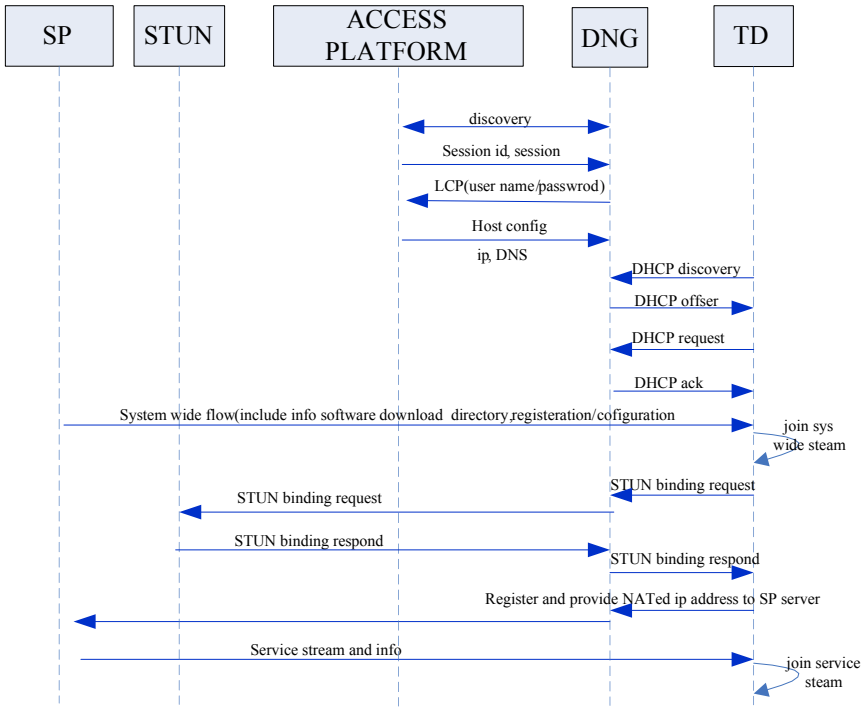


Figure I-2: IPTV Device Initialization and Attachment flow based on PPPOE

The following two sub-sections attached here only for reference purpose.

I.1.1 Network Attachment

I.1.1.1 Delivery Network Gateway (DNG)

The term "Network Attachment" refers to the activities associated with the DNG establishing Layer-3 connectivity to an IP-network. Once the network attachment activities have been completed, the DNG will be capable of transmitting and receiving IP packets, and establishing a management session with a remote configuration server. Subsequently the remote configuration server, such as an auto-configuration server (ACS) defined in TR-69, can be used to provision the DNG with access-network specific parameters.

I.1.1.1.1 DHCP Approach1

The most prevalent automatic method currently used to attach to the network is the DHCP protocol. Using this protocol, the DNG acquires its WAN IP address, and can also learn the address of the remote configuration server.

Figure I-3 below shows the sequence of events that take place when the DNG is powered up or initialized.

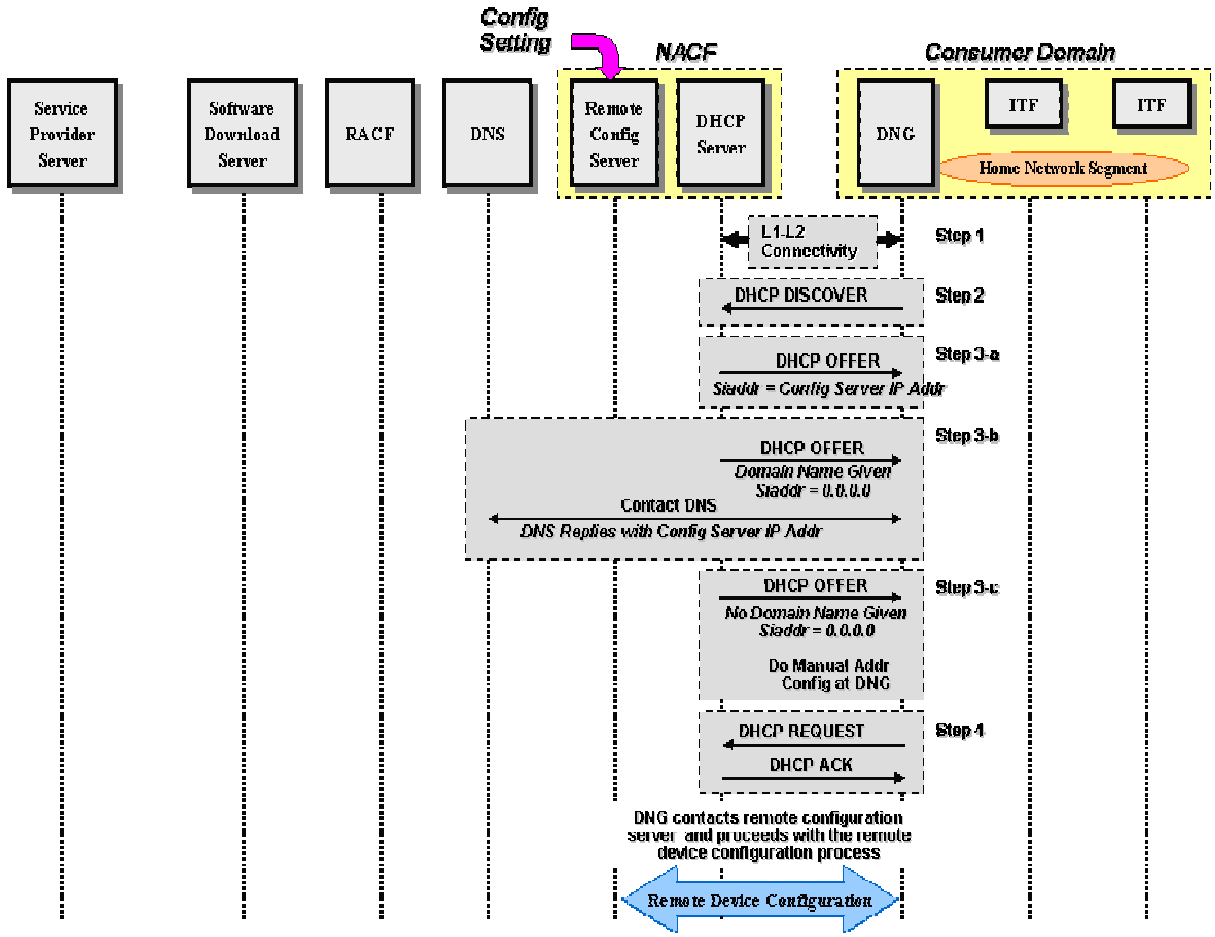


Figure I-3: DNG Network Attachment Approach 1

Specifically, the following procedure takes place:

1) The DNG establishes L1 and L2 connectivity with the network. The specific steps depend on the type of the access network (DSL, PON, HFC, Wireless, etc.) and are beyond the scope of this document.

2) The DNG issues a DHCP DISCOVER message toward the network that must include all the mandatory DHCP options, per RFC 2131. If the DNG device were to support the Container option, it would request it in option 55 (parameter request list). This would be performed in step 2 in the figure above.

   DHCP DISCOVERY message can optionally include Rapid Commit Option per RFC4039 to obtain IP address and configuration information using a 2-message exchange rather than the usual 4-message exchange, expediting the TD configuration.

3) The network provider DHCP server replies to the DNG with a DHCP OFFER message that must include all the DHCP mandatory options, per RFC 2131. The DHCP server must provide the following information to the DNG:

   a) DNG WAN IP address

   b) DNG network mask

   c) DNS Server IP address (es)

d) The Container option requested in step 2 above, if configured, to convey other options to the TD.

e) The remote configuration server addressing information (see possibilities below), if configured.

f) If the DHCP DISCOVERY message contains a Rapid Commit Option, the DHCP server responds with a DHCP ACK message including IP address and configuration information not sending DHCP OFFER.

There are three possibilities related to the siaddr at this point, reflected in the content of the DHCP OFFER message:

i) If the DHCP server is provisioned with the remote configuration server IP address, then it must include it in the siaddr field of the OFFER message. This is shown as step 3-a in the figure above.

ii) If the DHCP server is provisioned with the remote configuration server domain name but not its IP address, then it must set siaddr = 0.0.0.0 and provide the remote configuration server domain name to the DNG. The DNG must interact with the DNS to resolve the remote configuration server IP address. This is shown as step 3-b in the figure above,

iii) If the DHCP server is not provisioned with the remote configuration server addressing information (IP address or domain name) and therefore does not provide the remote configuration server IP address or its domain name, then there must be a mechanism in place to allow the end user to manually configure the DNG. This is shown as step 3-c in the figure above.

4) The DHCP protocol sequence completes with the standard DHCP REQUEST and DHCP ACK messages.

After acquiring the IP address of the remote configuration server, the DNG interacts with the remote configuration server to acquire needed configuration parameters.

I.1.1.1.2 DHCP Approach2

Another approach of network attachment is supported by DHCP as shown in Figure I-4.

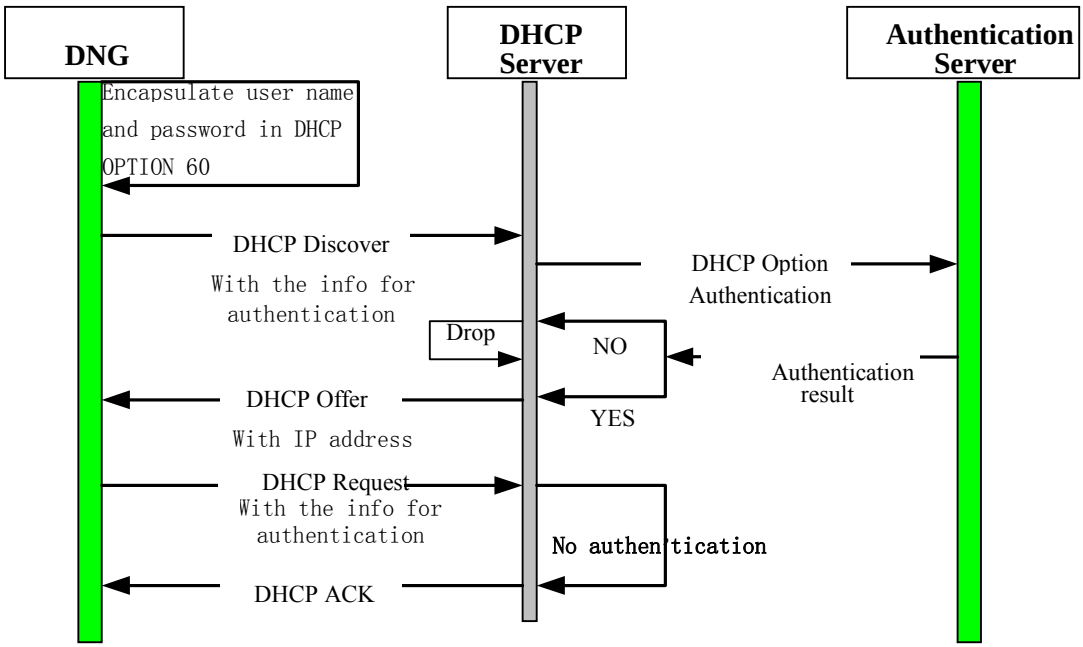


Figure I-4: DNG Network Attachment Approach 2

The flow for IPTV DNG using DHCP to attach the network is following:

(1) When DNG is powered on, DNG check whether are there user name and password for application layer in its store device, and the user name and password are wanted if they are not stored in its store device.

(2) DNG encapsulates the user name and password in options 60 of DHCP request and broadcasts the request message.

(3) The DCHP server platform including DHCP server and authentication server authenticate the validity of the user name and password when the DHCP request message with options 60 received. If the authentication passes, then the DHCP OFFER message with IP address assigned by the DHCP server is delivered to DNG; and if the authentication fails, then the DCHP request message will be dropped.

(4) After receiving the DCHP OFFER message, DNG issues a DHCP request message (including the random number R for encryption, the time tamp TS created recently) again with encapsulation the user name and password to the DCHP server using the IP address assigned in (3).

(5) The DCHP platform echo ACK to DNG. Then the process of DNG acquire IP address finishes.

I.1.1.1.3 PPPOE

PPPoE is a prevalent method to attach the access network. The DNG can attach the access network using the PPPoE. After the process of the PPPoE is complete, the DNG can get the IP address assigned by the ACCESS PLATFORM, and also can acquire the IP address of the remote management server.

Figure I-5 below shows the sequence of events that take place when the DNG is powered up or initialized.

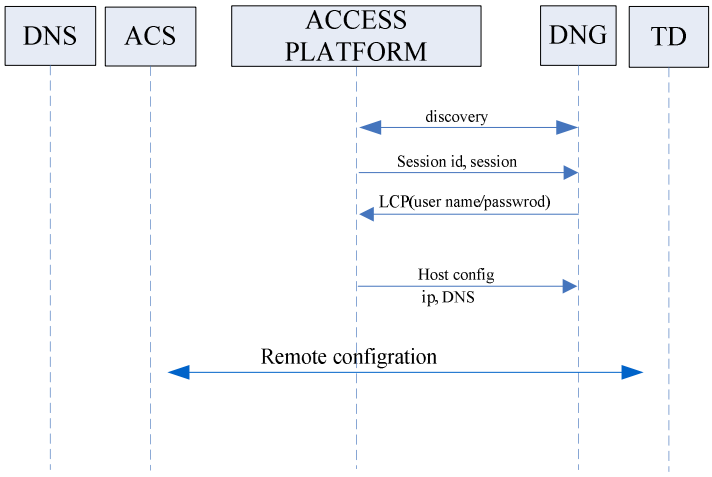


Figure I-5: DNG Network Attachment through PPPoE

The flow for DNG using PPPoE to attach the network is following:

1) The DNG establishes L1 and L2 connectivity with the network. The specific steps depend on the type of the access network (DSL, PON, HFC, Wireless, etc.) and are beyond the scope of this document.

2) The DNG broadcasts a PADI message toward the network.

3) The network ACCESS PLATFORM replies to the DNG with a PADO message.

Above is the discovery part of the PPPoE;

1) The DNG issues a PADR message with the user name and the password to a ACCESS PLATFORM to get the PPP session, this is the LCP process;

2) The ACCESS PLATFORM authenticates the user's validity;

3) The ACCESS PLATFORM echoes the DNG with the assigned IP address and DNS address if the authentication successful.

After acquiring the IP address of the remote configuration server, the DNG interacts with the remote configuration server to acquire needed configuration parameters.

I.1.1.2 IPTV Terminal Device (TD)

During the network attachment phase the following information may be obtained or otherwise established by the TD:

1) IPv4 address, network mask, default route

2) DNS, local network domain name, SIP proxies, others …

Once network attachment activities have been completed, the TD will be capable of transmitting and receiving IP packets and establishing a management session with a remote configuration server. Among existing mechanisms for implementing the Network Attachment function and relevant are:

1) The Dynamic Host Configuration Protocol (DHCP)

2) NGN NACF

The profiles and the details for each of the mechanisms as applicable for various IPTV use cases are described in the following sections.

I.1.1.2.1 DHCP

There are two cases to consider. The first case is when the DNG supports DHCP server capability and thus acts as the network DHCP server for the TDs on the home network. The second case is when the DNG passes DHCP messages through as a DHCP relay agent.

Note that while the second case can still be found in today's deployments, home networks are moving towards self-contained IP domains, with the network DHCP server located in the DNG.

I.1.1.2.1.1 Local DHCP Server on the DNG

In this case it is assumed that the DNG has already attached to the network and acquired its L3 networking information. The following sequence takes place when an TD device is powered up or initialized:

1) The TD establishes L1 and L2 connectivity with the DNG across the home network, which could be over a copper network, a coaxial network, fibre/plastic network, or wireless network.

2) The TD issues a DHCP DISCOVER message toward the DNG that must include all the mandatory DHCP options, per RFC 2131. The TD must include option 60 to allow it to identify itself to the DNG. If the TD were to support the option(s) carried in the Container option, it would request those options in option 55 (parameter request list).

3) The DNG, as a DHCP server, replies to the TD with a DHCP OFFER message that must include all the DHCP mandatory options, per RFC 2131. The DNG must provide the following information to the TD:

   a) TD device local IP address;

   b) TD device local network mask;

   c) DNS Server IP address(es);

   d) The remote configuration server IP address (same as the one assigned to the DNG);

   e) Default gateway IP address;

   f) If configured, the option(s) requested in step 2 above (carried in the Container option) to convey specific information to the ITF, such as Service Provider Discovery information.

4) The TD continues the DHCP message exchange with the standard DHCP REQUEST message.

5) The DNG completes the DHCP message exchange with the standard DHCP ACK message.

The flow is shown in Figure I-6 below:

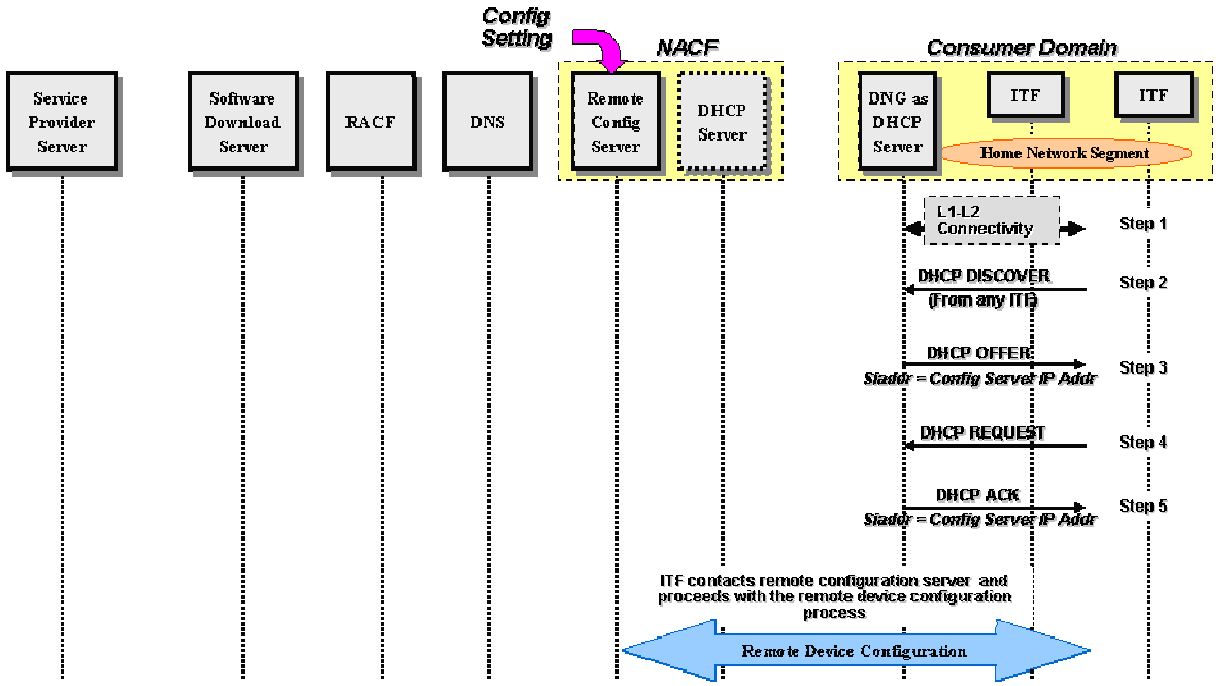


Figure I-6: TD Network Attachment with a Local DHCP Server in the DNG

After acquiring the IP address of the remote configuration server, the TD interacts with the remote configuration server to acquire needed configuration parameters.

I.1.1.2.1.2 Remote DHCP Server across the network

In this case the DNG passes all DHCP messages transparently to the network. Figure I-7 shows the sequence of events that take place when the TD is powered up or initialized.

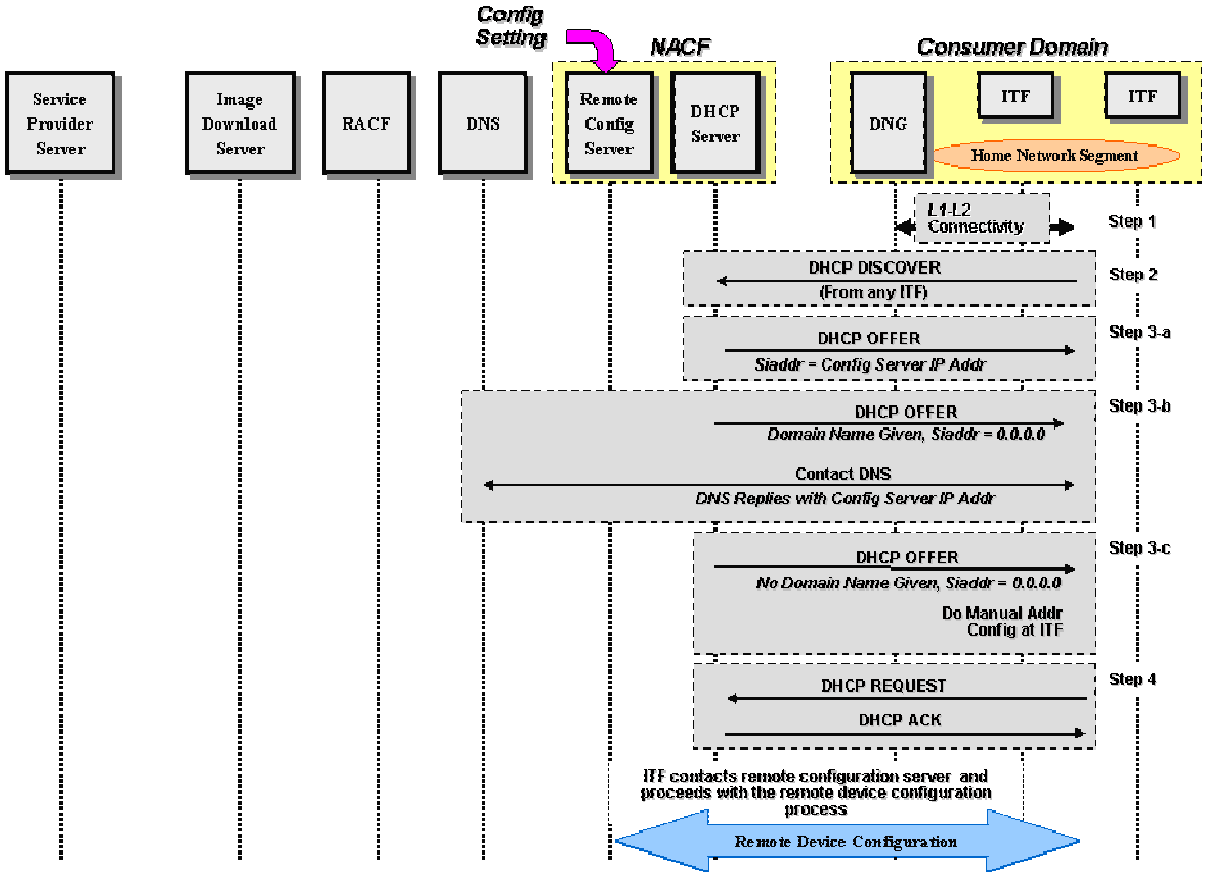


Figure I-7: TD Network Attachment with a Remote DHCP Server

Specifically, the following takes place:

1) The TD establishes L1 and L2 connectivity with the DNG across the home network, which could be a copper network, a coaxial network, fibre/plastic network, or wireless network (not shown in the figure above).

2) The TD issues a DHCP DISCOVER message toward the DNG that must include all the mandatory DHCP options, per RFC 2131. The TD must also include option 60 to allow it to identify itself to the network. The DNG passes this DISCOVER message to the WAN network transparently.

   The network provider DHCP server replies to the TD with a DHCP OFFER message (or DHCP ACK with the Rapid Commit option) that must include all the DHCP mandatory options, per RFC 2131.

3) The network provider DHCP server replies to the TD with a DHCP OFFER message that must include all the DHCP mandatory options, per RFC 2131. The DHCP server must provide the following information to the TD:

   a) TD IP address

   b) TD network mask

c) DNS server IP address(es)

d) If available, the remote configuration server IP address

e) Default gateway IP address

The DNG must pass the DHCP OFFER message to the TD transparently.

There are three possibilities at this point reflected in the content of the DHCP OFFER message:

i) If the DHCP server is provisioned with the remote configuration server IP address, then it must include it in the siaddr field of the OFFER message. This is shown as step 3-a in the figure above.

ii) If the DHCP server is provisioned with the remote configuration server domain name but not its IP address, then it must set siaddr = 0.0.0.0 and provide the remote configuration server domain name to the TD. The TD must interact with the DNS to resolve the remote configuration server IP address. This is shown as step 3-b in the figure above.

iii) If the DHCP server is not provisioned with the remote configuration server addressing information (IP address or domain name) and therefore does not provide the remote configuration server IP address or its domain name, then there must be a mechanism in place to allow the end user to manually configure the TD or the TD device may obtain that information from its Service Provider. This is shown as step 3-c in the figure above.

4) The DHCP protocol sequence completes with the standard DHCP REQUEST and DHCP ACK messages.

After acquiring the IP address of the remote configuration server, the TD interacts with the remote configuration server to acquire needed configuration parameters.

I.1.1.2.2 PPPOE

The Terminal device can use DHCP protocol to get it's address. In the case, the DNG should have a dhcp server. When DNG get the network parameters through PPPOE, then TD can acquires the IP address and some network parameters form DNG through DHCP options. If the TD behind the NAT of DNG, TD sends it's IP and ports request to DNG.

Figure I-8 below shows the sequence of events that take place when the DNG and TD is powered up or initialized.

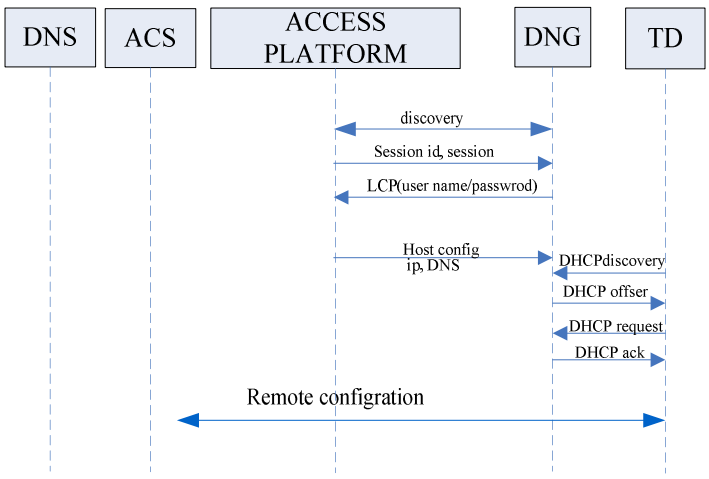


Figure I-8: TD Network Attachment based on PPPOE

I.1.2 Service Provider Discovery

When the ITF attaches to the network, it has to know from where to get the description of the IPTV Service Providers available to it. This is what is called an entry point.

An IPTV Service Provider Description entry point can be a multicast or a unicast address.

There are different ways for the ITF to get IPTV Service Provider Description entry points:

– A well known multicast address registered with IANA,

– Starting with an entry point address provisioned in the Terminal Device Configuration Data

– Starting with a domain name in the Terminal Device Configuration Data and using DNS to acquire entry point addresses

– At network connection, with DHCP, the Terminal Device might be provided with domain names to be used to acquire entry point addresses via DNS.

In ETSI TS 102034: Digital Video Broadcasting (DVB); Transport of MPEG-2 Based DVB Services over IP Based Networks, several ways to discover entry point addresses for non-IMS Terminal Device are described.

Appendix II

Example of Multicast VPN

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

II.1 Requirement on Multicast VPN in IPTV Network Control Aspect

The IPTV multicast VPN operates with the security, management and Quality of Service (QoS) policies of a private network. Figure 1 depicts an example of basic IPTV multicast VPN services. In Figure B.1, the main office offers diverse IPTV application services which are sent from IPTV contents server, to home office, remote office and business partner with IPTV connected on VPN.

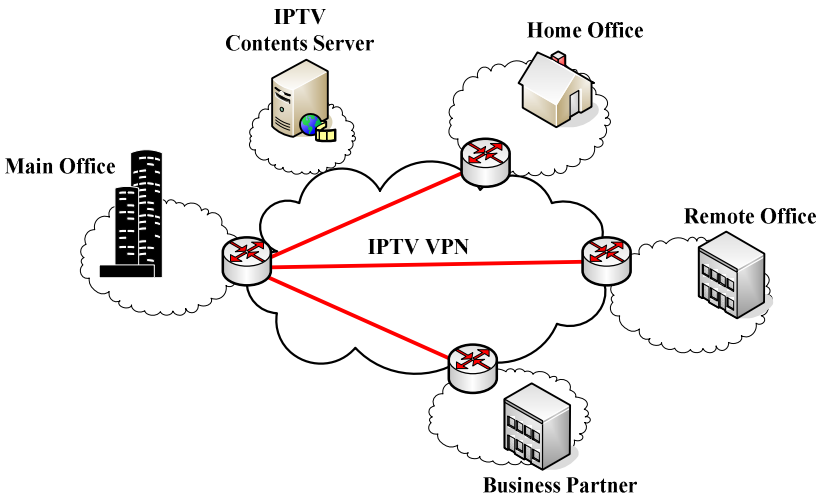


Figure II-1: Example of Basic Configuration in IPTV Multicast VPN

In order to provide IPTV multicast VPN, The IPTV access node will provide secured and encrypted multiple connections between main office and remote office. So, the IPTV multicast VPN will have multiple benefits as follows:

– Extend geographic connectivity

– Improve security

– Reduce operational costs

– Reduce transit time and transportation costs for remote users

II.2 IPTV Multicast VPN Group Management

The IPTV multicast VPN group management is to achieve privacy and integrity in IPTV network. According to features of IPTV service, geographical position of IPTV users or both, IPTV multicast VPN groups can be formed diversely into same IPTV VPN or different IPTV VPN sites. Each IPTV multicast VPN group is assigned according to different security grade and QoS.

In order to support additionally secure group management, IPTV multicast VPN group will be applied to provide the following:

– Limiting of IPTV Multicast VPN Group Member:

  The member limitation of IPTV multicast VPN group needs to optimize the resource usage of IPTV network.

– User Privacy:

  The identity of the IPTV multicast VPN group members is kept secret from other IPTV VPN group. If needed, it is kept secret from other members of the same IPTV group.

– Data integrity:

  The data received by the IPTV multicast VPN group members is coming from an authorized sender and has not been modified during transit.

Appendix III

Mapping between IPTV Overlay Network Capability and IPTV functional architecture

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

The function of IPTV overlay networking is performed under the control of Content Delivery Control Function of IPTV functional reference architecture, and service control function for IPTV overlay networking initiate and manage IPTV overlay sessions to configure service capability of IPTV overlay networking. The control of Content Delivery Control Function is performed with associated operation among overlay nodes, and the service control function for IPTV overlay networking is performed with Session Manager.

IPTV Functional Architecture indicates the additional functional entities for IPTV overlay network in Functional Reference Architecture.

• Session Manager in IPTV overlay networking is mapped to IPTV Service Control Function, and provides the functions to request service requirements/release to RACF for IPTV overlay networking.

- Association among overlay nodes in IPTV overlay networking provides Content Delivery Control Function to control the location of requested contents, and to distribute control functions to the contents servers. Thus, the overlay nodes can be mapped with Content Delivery Control Functions, Location Control Function and Distribution Control Function, functionally.

  – Overlay nodes will perform the function to search the location of IPTV contents sources with dynamic communication capability in overlay networking. Thus, Location Control Function for overlay networking is performed by the search function among multiple overlay nodes in IPTV Overlay Networking.

  – Overlay nodes will perform the function to exchange control information among the IPTV contents servers. Thus, the association of overlay nodes in IPTV Overlay Networking will provide the function of Distribution Control Function.

The procedural functions and interfaces for IPTV Overlay Networking are shown in Figure III-1, which provides the functional model to perform overlay networking capability on IPTV Functional Architecture.

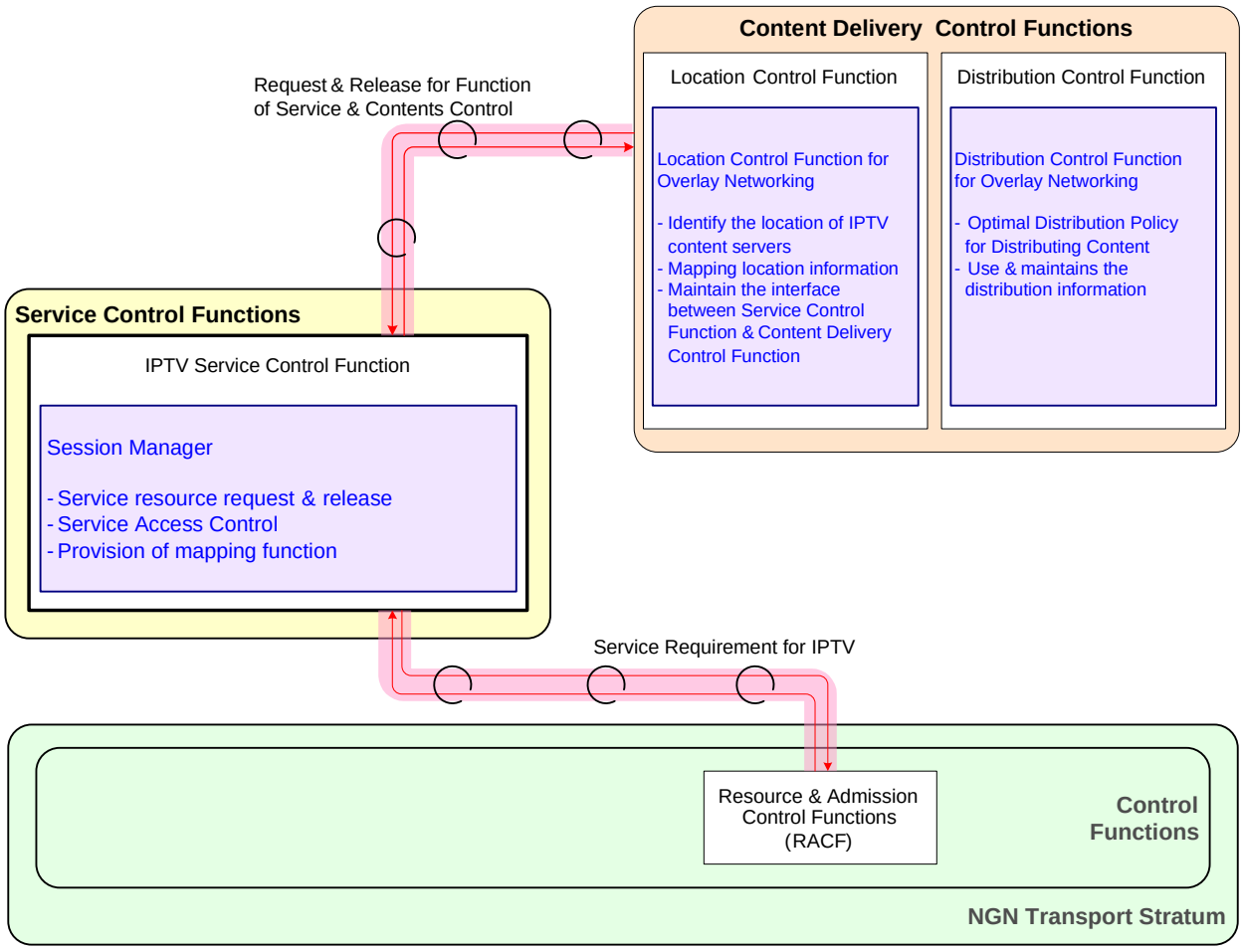


Figure III-1: Overlay Mapping for IPTV Functions

As shown in Figure III-1, Session Manager, Location Control Function and Distribution Control Function for IPTV overlay networking perform the functions for IPTV services features and contents control. And the interface function between SCF and RACF will be request and release for resource reservation and release in accordance with IPTV service requirements. The RACF sends confirmation of resource reservation to Session Manager when the resource has been reserved. Thus, Session Manager performs following functions to function of IPTV Service Control Function.

- Service Resource Request & Release to create and release overlay session according to IPTV service requirements. In order to provide this function, Session Manager configures and manages overlay sessions topology for IPTV service requirements, and requests its resource reservation to RACF.

- Service Access Control to allow service to authenticate IPTV users according to their access rights (e.g. subscriber information, PPV, age limit). And Service Access Control manages the session associated with the content.

- Provision of mapping function between virtual address of overlay node and physical address of transport network to control service features on session topology.

Location Control Function for IPTV services will be provided through association among overlay nodes to provide the following functions in Content Delivery Control Function.

- Identify the location of IPTV content servers for user request with cooperated operation among IPTV overlay nodes (e.g., by DHT: Distributed Hashing Table, content topology table may be created per IPTV channel basis).

- Mapping location Information, e.g., mapping between logical and physical address, for IPTV contents locations Also, Location Control Function translates a logical content reference into a reference to the physical server.

- Maintain the interface between Service Control Function and Content Delivery Control Function to exchange contents control information.

Distribution Control Function for IPTV service will be performed with exchanges the distribution control information among IPTV overlay nodes.

- Establish optimal distribution policy for distribution content for IPTV overlay networking service features. When overlay node receives response message which other overlay nodes have the requested channel, it let Session Manager know about destination information after applying policy of each contents.

- Use & maintains the distribution information about how the contents is distributed among Content Delivery & Storage Functions. It may be obtained through the request and response among IPTV overlay nodes for distribution control function.

Appendix IV

ISP-manageable P2P Network Structure

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

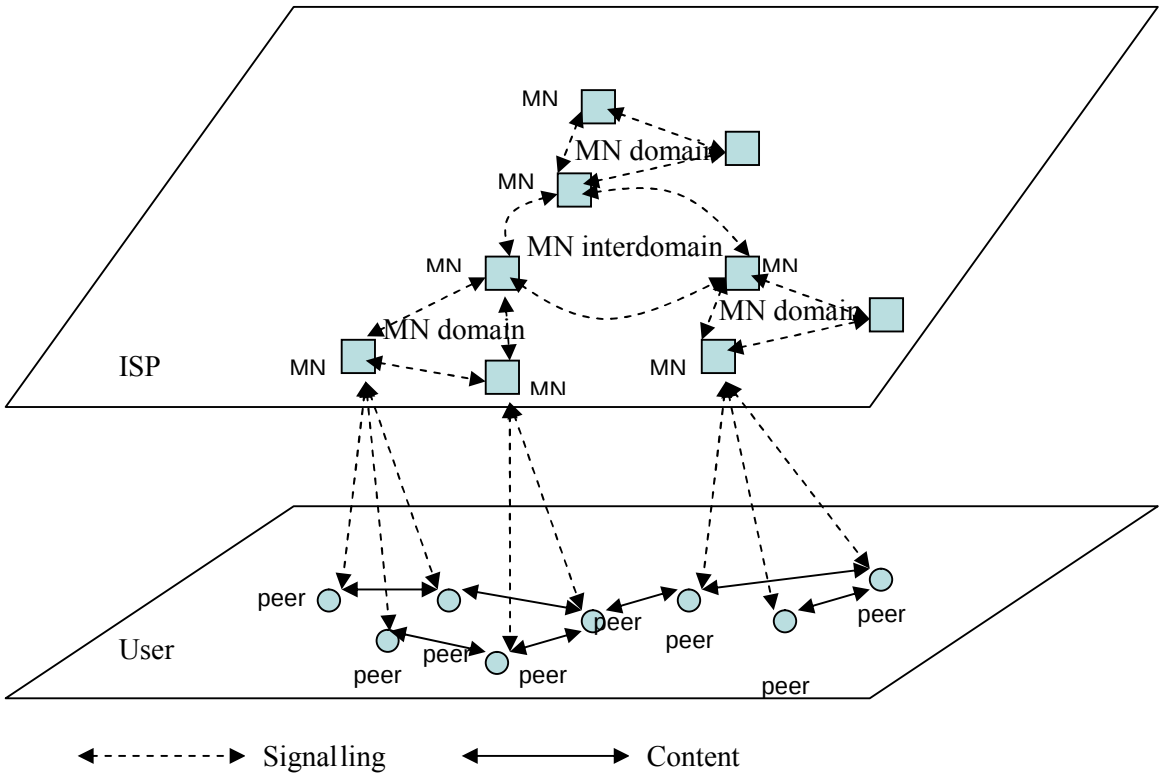


Figure IV-1: ISP-manageable P2P Network Structure

As shown in Figure IV-1, peers are classified into several groups with each group having a management node (MN) deployed by ISP. Peer classification can be done based on either content sharing criterion or physical location criterion. In content sharing criterion, peers with common interest on certain kind of content (e.g. movie, file) are classified into one group. In physical location criterion, peers with short distance (e.g. network distance, geography distant) are classified into one group.

MN performs peer management functions in each group, such as peer registration, maintenance, AAA, etc., as well as P2P signalling proxy including content publish, search, etc. MN may also perform media signalling proxy for peers when media is transferred among peers.

Several MNs are organized in MN domain where MNs share content information using P2P signalling such as content put, get, update, etc. Several MN domains can be further organized in MN interdomain to share the content information among MN domains. Content exchange always happens between peers such that the size of peers will not be bounded.

Management Functions of MN

In peer group, MN implements peers management functions including:

- Peer registration. Peer register with MN about its capabilities, e.g. CPU, storage, bandwidth, etc.
- Peer maintenance. MN periodically collects status, e.g. link, capabilities, etc. from peers.
- Peer AAA. MN can authenticate and authorize peer when it joins the group, and account for peer during service provisioning.

Media Signalling Proxy Function of MN

In order to get media status in peer group, media signalling proxy may be performed by MN. MN implements media signalling proxy function by transferring media connection signalling between peers and obtaining media session status of peers.

P2P Functions of MN

In peer group, MN performs P2P proxy for peers including:

- Peer content publication

As shown in Figure IV-2, peer A publishes its content ID to MN1, together with its contact address. As the P2P proxy of peer A, MN1 publishes the content ID and peer A address to responsible MN (MN3 in Figure 2) in the MN domain which is responsible for the content ID, according to some P2P content publish mechanism such as Chord, Pastry, etc.

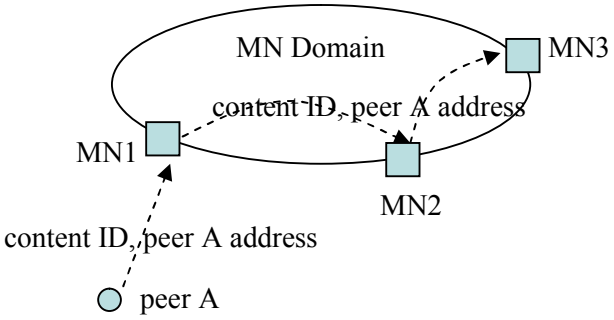


Figure IV-2: Peer content publish

- Peer content search in MN domain

As shown in Figure IV-3, peer B sends content request (e.g. content ID) to MN4. As the P2P proxy of peer B, MN4 finds the responsible MN (MN3 in Figure 3) in the MN domain which stores the content ID, according to some P2P content search mechanism such as Chord, Pastry, etc. MN3 then returns the corresponding peer A address to peer B.

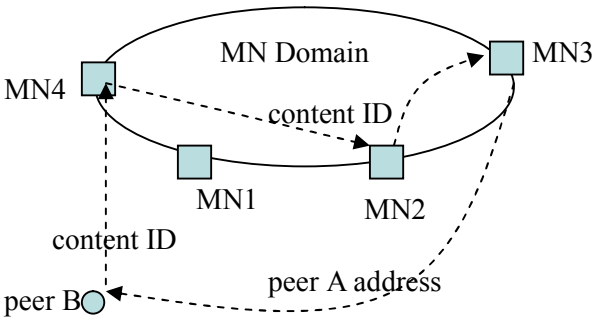


Figure IV-3: Peer content search

- Peer content search in MN interdomain

If the requested content ID can not be found in MN domain, MN could launch a search procedure in MN interdomain. As shown in Figure IV-4, when MN3 does not contain the requested content ID, it could forward the content request to MN5 in another MN domain through the MN interdomain. MN5 then finds the responsible MN (MN6 in Figure 4) in its MN domain which stores the content ID, according to some P2P content search mechanism such as Chord, Pastry, etc. MN6 finally returns the corresponding peer C address to peer B.

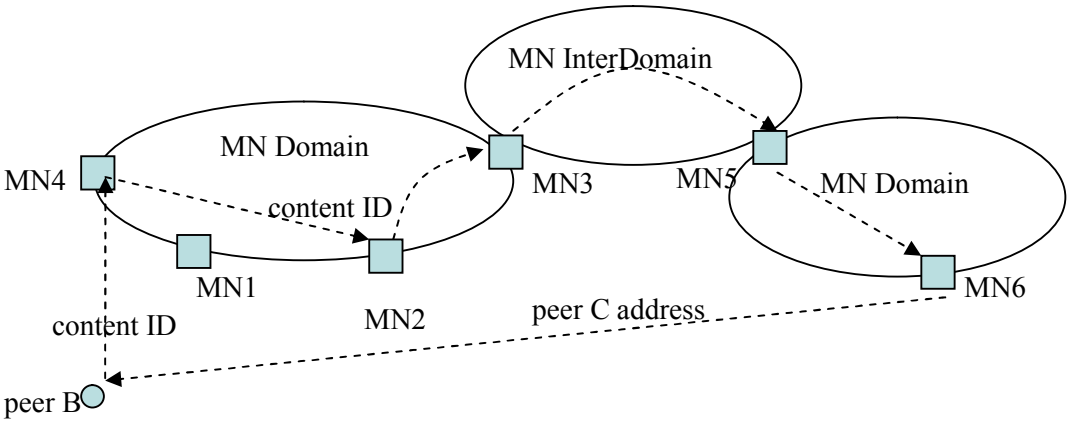


Figure IV-4: Peer content search across MN domain

II.4.2 IPTV multicast frameworks

Summary

This document on IPTV multicast frameworks describes functional requirements and frameworks for supporting multicast capabilities in terms of IPTV network control.

Keywords

IPTV, multicast, unicast

Current status

After carefully reviewing and extensive editing works, this document contains consensus of information from all the contributions addressed to the working group.

This document describes functional requirements and frameworks for supporting multicast capabilities in terms of IPTV network control.

This document mainly focuses on the following multicast aspects.

- IPTV multicast functional requirements
- IPTV multicast architecture
- IPTV multicast scenarios
- Design considerations for IPTV multicast network
- Overlay multicast networking

Dependency on or relationship to other FG IPTV documents:

- IPTV services requirements
- IPTV architecture
- IPTV network control aspects

CONTENTS

		Page
1	Scope	399
2	References	399
3	Definitions	399
3.1	Terms defined elsewhere	399
3.2	Terms defined in this document	400
4	Abbreviations and acronyms	401
5	Conventions	401
6	IPTV multicast requirements	402
6.1	IPTV multicast transport requirement	402
6.2	QoS requirements of IPTV multicast	403
6.3	Security requirements of IPTV multicast	405
6.4	Interoperability requirement of IPTV multicast	406
6.5	Service management requirements of IPTV multicast	406
7	IPTV Multicast Architecture	407
7.1	Description of entities for Non-NGN IPTV functional architecture	407
7.2	Description of reference points for Non-NGN IPTV functional architecture	409
8	IPTV Multicast scenarios	410
8.1	Native IP multicast scenario	410
8.2	Alternative multicast scenarios	412
9	Design considerations for IPTV multicast network	418
9.1	IPTV multicast transport	418
9.2	IPTV multicast QoS	422
9.2.1	Types of IPTV multicast QoS	422
9.3	IPTV multicast interoperability among service providers	424
9.4	IPTV multicast management	426
10	Overlay multicast networking	431
10.1	Control framework for IPTV overlay multicast	431
10.2	Functional framework for IPTV overlay multicast	433
10.3	QoS control in IPTV overlay multicast network	434

IPTV multicast frameworks

1 Scope

This document on IPTV multicast frameworks describes functional requirements and frameworks of supporting multicast capabilities in terms of IPTV network control.

This document considers multicast frameworks for non-NGN environment.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[FG IPTV-DOC-0147] ITU-T FG IPTV document *IPTV services requirements*

[FG IPTV-DOC-0181] ITU-T FG IPTV document *IPTV architecture*

[FG IPTV-DOC-0190] ITU-T FG IPTV document *IPTV multicast frameworks*

[IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*

[IETF RFC 2710] IETF RFC 2710 (1999), *Multicast Listener Discovery (MLD) for IPv6*

[IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3*

[IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for Ipv6*

[IETF RFC 4541] IETF RFC 4541 (2006), *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping switches*

[IETF RFC 4601] IETF RFC 4601 (2006), *Protocol Independent Multicast – Sparse Mode (PIM-SM)*

[IETF RFC 4604] IETF RFC 4604 (2006), *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

[IETF RFC 4605] IETF RFC 4605 (2006), *Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Broadcast [ITU-T M.60]: One-way transmission from one point to two or more other points.

3.1.2 Delivery network gateway (DNG) [ATIS-0800002]: A device implementing the DNGF.

NOTE – DNG also is commonly referred to as the Residential Gateway (RG).

3.1.3 End-user [ITU-T J.112]: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

3.1.4 Network provider [ITU-T Q.1290]: The organization that maintains and operates the network components required for IPTV functionality. A network provider can optionally also act as service provider.

3.1.5 Service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider can optionally or can optionally not be a customer of another service provider.

3.1.6 Subscriber [ITU-T Q.3050.1]: The subscriber is responsible for concluding contracts for the services subscribed to and for paying for these services.

3.1.7 Subscription [ITU-T Q.1741.3]: A subscription describes the commercial relationship between the subscriber and the service provider.

3.2 Terms defined in this document

This document defines the following terms:

3.2.1 Multicast domain management: A multicast domain is a set of multicast routing and forwarding instances than can send multicast traffic to each other. These multicast routing and forwarding instances are referred to as IPTV multicast domain. Thus, multicast domains map all of a customer's multicast groups that exist in particular IPTV service members to a single unique global multicast group. This is achieved by existing or specific group routing and forwarding capability in the network.

3.2.2 Multicast access control functions: Multicast Access Control Functions is that control a multicast user access to IPTV multicast tree. The IPTV user can join a multicast service using these control functions with proper authentication and authorization of the user.

3.2.3 Multicast delivery control functions: Multicast Delivery Control Functions is that can control IPTV multicast delivery among transport functions.

3.2.4 Overlay network: A virtual network of nodes and logical links that is built on top of the underlying network infrastructure with the purpose of implement a network service that is not available in the underlying network infrastructure.

3.2.5 Overlay multicast network: One type of overlay network that provides multicast services to end users on top of the general network infrastructure.

3.2.6 IPTV multicast interoperability: IPTV multicast interoperability is the exchange of IPTV service information amongst multicast based IPTV service providers. And to make the optimal contract and to provide the stable IPTV services amongst multicast based IPTV service providers.

3.2.7 IPTV service exchange point: IPTV SEP (service exchange point) is identified as a reference point for handling the service brokering function between IPTV SPs enabling the optimal contract between IPTV SPs and providing the stable IPTV services amongst IPTV service providers. IPTV SEP can be located in any peering point.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

CAC Connection Admission Control

CCTV Closed-Circuit TV

cIMA child IMA

CP Content Provider

DoS Denial of Service

DRM Digital Rights Management

NOTE – In this document, the term Service and Content Protection is used instead of Digital Rights Management.

ECMP Equal Cost Multiple Path

IGMP Internet Group Management Protocol

IMA IPTV Multicast Agent

IP Internet Protocol

ISP Internet Service Provider

MLD Multicast Listener Discovery

QoE Quality of Experience

QoS Quality of Service

pIMA parent IMA

RP Rendezvous Point

SEP Service Exchange Point

SP Service Provider

5 Conventions

In this document:

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

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document 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/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

NOTE – The terminology and the architecture assumed in this document needs to be checked for alignment with IPTV architecture document.

6 IPTV multicast requirements

6.1 IPTV multicast transport requirement

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

- The IPTV architecture is required to support the addressability of particular device such as ITFs within the end-user network [ATIS-0800002].
- The IPTV architecture is required to allow for the utilization of Internet protocols and standards related with multicast transmission [ATIS-0800002].
- The IPTV architecture is recommended to allow the delivery of IPTV services over different access networks (e.g. cable, optical, xDSL, wireless).
- The IPTV architecture is recommended to adapt dynamically to change in wireless networks characteristics when the service is delivered over a mobile network (e.g. bandwidth, packet loss rate, etc.
- The IPTV architecture can optionally support a replacement algorithm for content caching and distribution.
- The IPTV architecture is required to support a mechanism for NAT traversal [ATIS-0800002].
- The IPTV architecture is recommended to support the ability of both multicasting and unicasting transmission schemes.
- The IPTV architecture is required to support the management and enforcement of the service providers' transport policies by the network provider [ATIS-0800002].
- The IPTV architecture is required to support access networks in case of NGN-based IPTV as defined in NGN architecture.
- The IPTV architecture is required to support multicast means of communication to all end-users [ATIS-0800002].
- The IPTV architecture is required to allow the service provider to utilize the network providers' multicast delivery capabilities [ATIS-0800002].
- The IPTV architecture is recommended to support mechanisms that allow IPTV services to be distributed to specific group of end-users.
- The IPTV architecture is recommended to support mechanisms for transmitting identification information related to end-users who want to receive or are selected to receive IPTV services.
- The IPTV architecture is required to support IP filtering functions in the DNGF in order to prevent selected local multicast traffic on the HNS from appearing on the DN [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to implement standard IP routing functions, per established IETF specifications [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to support routing functions per IPv4 specifications [ATIS-0800002].
- The IPTV architecture is recommended to support both IPv6 and IPv4 [ATIS-0800002].

- The IPTV architecture is recommended to support static and dynamic address allocation schemes for both IPv4 and IPv6 [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to support the routing of IP packets between all interfaces toward the access/core network (WAN side of the HN), and toward the ITF (LAN side of the HN). Specifically, this means [ATIS-0800002]:
  - Routing is recommended to be supported from DN to HNS (downstream flow).
  - Routing is recommended to be supported from HNS to DN (upstream flow).
  - Routing is recommended to be supported from any HNS to any other HNS (bidirectional flows).
- The IPTV architecture is recommended to support the ability for the DNGF to support multiple logical IP interfaces (multiple attachment points at the IP layer) on any particular physical DN interface [ATIS-0800002].
- The IPTV architecture is recommended to support the ability for the DNGF to assign IP addresses to devices in the Home Network [ATIS-0800002].
- The IPTV architecture is recommended to support automated configuration capabilities for the IPTV devices [ATIS-0800002].
- The DNGF is recommended to support NAT/NAPT capability mapping IP address and port numbers between the public WAN and the LAN(s) [ATIS-0800002].

The following are multicast transport functional requirements in addition to the above service requirements.

- The IPTV multicast network is recommended to provide identification of multicast group to the ITF.
- The IPTV multicast network is recommended to maintain multicast session information for each multicast group, and can optionally announce them to the ITFs.
- The IPTV multicast network is recommended to authenticate and authorize an IPTV multicast source.
- The IPTV multicast network is recommended to optionally manage the identification of IPTV multicast tree.
- The IPTV multicast network is required to provide the stable multicast tree management when the IPTV end-users join and leave.

6.2 QoS requirements of IPTV multicast

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

- The IPTV architecture is required to support a framework that identifies the key components and measurement points for Quality of Service Measurement (QoSM) [ATIS-0800002].
- The IPTV terminal device is recommended to be able to declare Media-providing entities their usage environments description – e.g. Type of service, Type of Terminal, Type of transmission medium, User Preferences, Available QoS Level [ATIS-0800002].
- The IPTV architecture, if re-transmission broadcast service is supported, is recommended to provide comparable Quality of Experience to the end-user as the direct reception.

- The IPTV architecture is required to support the service provider to be able to get QoS information from the end-user device.
- The IPTV architecture is required to allow the delivery of IPTV services with a defined Quality of Experience (QoE) for the IPTV end-user [ATIS-0800002].
- The IPTV architecture is recommended to support consistent QoS for the duration of the service.
- The IPTV architecture is recommended to support a mechanism by which network operators can integrate IPTV QoS management functions into a common framework with other services and applications [ATIS-0800002].
- The IPTV architecture can optionally support the delivery of multiple services over the common IP transport with a manageable IP Quality of Service (QoS); services can optionally be delivered from multiple service providers or from a single provider [ATIS-0800002].
- The IPTV architecture is required to support mechanisms for supporting appropriate resiliency in the service provider infrastructure to maintain a high QoE [ATIS-0800002].
- The IPTV architecture is recommended to support means to provide channel changing times with sufficient QoE.
- Networks that support IPTV are required to support the IP QoS class and associated performance requirements specified in Y.1541 [ITU-T Y.1541], which recommends the selection of relevant specific QoS classes based on application requirements.
- The IPTV architecture is required to support a mechanism for assigning traffic priorities [ATIS-0800002].
- The IPTV architecture is required to support the relevant mechanisms for IPTV traffic identification, classification and marking, policing and conditioning, scheduling and discarding.
- The IPTV architecture is recommended to support mechanisms for dynamic IPTV traffic load balancing so as to dynamically accommodate with the network load and congestion conditions at any given time, so as to deliver the set of IPTV services to the end-users with the relevant level of quality.
- The IPTV architecture is recommended to offer an admission control solution for admission of IPTV services over the access and core network resources from the home network to the service source.
- The IPTV architecture is required to support the capability for management of capacity on the services and network elements [ATIS-0800002].
- The IPTV architecture can optionally support mechanisms to support QoS/QoE parameter adjustment due to changes of content characteristics on a channel.
- The IPTV architecture is recommended to support an application layer error recovery mechanism to support sufficient QoE/QoS for unicast distribution of any IPTV service.
- Any application layer error recovery mechanism integrated in the IPTV architecture is recommended to be flexible to cover a range of networks conditions and IPTV services.
- The IPTV architecture is required to define mechanism to appropriately distinguish different forms of traffic – e.g. data and voice [ATIS-0800002].
- The IPTV architecture is recommended to support redundancy and failover mechanisms for infrastructure components [ATIS-0800002].
- The IPTV architecture is recommended not to put any constraint on latency sensitive services [ATIS-0800002].

- The IPTV architecture is required to define traffic management mechanisms for the differential treatment of IPTV traffic [ATIS-0800002].
- The IPTV architecture is required to support the ability to configure QoS rules at the DNGF that govern traffic mapping (upstream or downstream) for the different services [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support the ability to perform the bandwidth management of all HNS networks attached to the DNG [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support performing call admission functions to protect the home network from excessive and harmful traffic on any HNS, between two HNSs attached to the DNG, and between any HNS and any DN [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support the ability for the DNGF to perform policing functions on incoming traffic and drop offending traffic to protect the home network [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support routing IP traffic based on provisionable/manageable mechanisms to guarantee QoS for different service classes [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support mapping downstream traffic to corresponding local flows to provide QoS for the different services. This includes L3 to L2 mapping, based on the local HNS [ATIS-0800002].
- The IPTV architecture (including DNGF) is recommended to support mapping upstream traffic generated by the end-devices to corresponding outgoing flows to provide QoS for the different services. This includes L2 to L3 mapping [ATIS-0800002].
- Where the Home Network transports multiple latency sensitive traffic types (e.g., the IPTV services and frequency distribution protocols, or time distribution protocols), these protocols and the Home Network infrastructure is recommended to be configured such that they do not impact the latency requirements of each service [ATIS-0800002].

The following are multicast QoS functional requirements in addition to the above service requirements.

- IPTV service provider is recommended to guarantee the QoS of IPTV multicast traffic.
- IPTV network provider is recommended to provide recovery mechanism for IPTV multicast traffic due to node failure and link failure.
- IPTV network provider can optionally provide priority based transport for IPTV multicast traffic.

6.3 Security requirements of IPTV multicast

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

- The IPTV architecture is required to support the ability for the service provider to prevent the sending of bulk unsolicited contents to the end-users.
- The IPTV architecture is required to support the service provider to be able to authenticate, authorize and charge the subscriber.
- The IPTV architecture is recommended to take into account the influence/impact on performance, quality of service, usability, scalability and cost constraints on deployment of security.
- The IPTV architecture is required to support protection of content that is transferred over multicast and/or over unicast streams.

- The IPTV architecture is required to support the capability of preventing the DoS attack to network.
- The IPTV architecture is required to support the provision of security measures to block illegal or unwanted traffic.
- The IPTV architecture is required to support network operators to prevent that the network topology and its resources are visible to unauthorized entities.
- The IPTV architecture is required to be hardened against attacks on multicast capabilities.
- The multicast architecture is required to support the capability of multicast protocol adjacency authentication in order to establish a reliable peer.
- The following are multicast security functional requirements in addition to the above service requirements.
- The IPTV multicast network is recommended to support the capability of multicast protocol adjacency authentication in order to establish a reliable peer.
- The IPTV multicast network is recommended to provide the capability of authenticating a multicast source such that it prevents an unauthorized source from becoming the multicast source.
- The IPTV multicast network is recommended to support authentication and authorization for both multicast user as source and multicast user as receiver.

6.4 Interoperability requirement of IPTV multicast

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

- The IPTV architecture is recommended to support a functional component that presents an open interface for the 3rd party applications to use the capabilities and resources of the IPTV network.
- The IPTV architecture is required to support a mechanism that allows for service-based transport QoS to be managed across multiple network domains [ATIS-0800002].
- The IPTV architecture is recommended to support capabilities for exchange of IPTV services information between different IPTV services providers. For instance, the service information can optionally include the source information, channel information, service start/end time, and QoS information.

6.5 Service management requirements of IPTV multicast

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

- The IPTV architecture is required to support the ability to trace the source of incoming content (e.g. messages that have been a cause for complaint by an end-user).
- The IPTV architecture is required to support mechanisms for the IPTV services Provider to Operate, Administer, Maintain, and Provision (OAMP) IPTV equipments [ATIS-0800002].
- The IPTV architecture is required to support the capability of monitoring the network elements (e.g. routers) and service elements (e.g. ITF) that report alarms in the event of faults.

- The IPTV architecture is required to support the service provider be able to upgrade the end-user device remotely.
- The IPTV architecture is recommended to support the service provider to be able to update the end-user device remotely, e.g. update software, firmware and virus list.

The following are multicast service management functional requirements in addition to the above service requirements.

- IPTV network is recommended to support mean(s) for multicast traffic monitoring (including performance monitoring) and for analysis for each service group.

7 IPTV Multicast Architecture

7.1 Description of entities for Non-NGN IPTV functional architecture

The functional architecture for IPTV multicast shows the principal functional groups in non-NGN environment. These functional groups provide a more detailed breakdown of the IPTV multicast functionality.

NOTE – Multicast architecture descriptions are based on IPTV architecture output document [FG IPTV-DOC-0181].

7.1.1 End-user Functions for IPTV multicast

The multicast end-user functions include those functions normally provided by the IPTV Terminal and the end-user Network. The multicast end-user functions are responsible for collecting control commands from the user, and interacting with the multicast application functions to join and leave from IPTV multicast groups. Multicast end-user can request the multicast service information. After receiving this information, they can join the multicast group with some QoS requirements. Then, it receives multicast data through multicast network transport functions.

7.1.1.1 IPTV Terminal Functions for IPTV multicast

The IPTV Terminal Functions for IPTV multicast includes "Application Clients block", "DRM Client block", "Media Client block" and "Control client functional block".

1) Linear TV Application client function: It interacts with Linear TV Application to perform session management, service authorization, presentation of the content metadata, and execution of the service logic of the Linear TV service.

2) DRM Client block: This block for IPTV multicast is for further study.

3) Media Client block: This block for IPTV multicast is for further study.

4) Control Client functional block: It provides the functions required to communicate with the IPTV Service Control Function to identify and prepare for the connection to the content delivery function.

7.1.1.2 Home Network Functions for IPTV multicast

The Home Network Functions for IPTV multicast include "Delivery Network Gateway Function block".

1) Delivery Network Gateway Function block: This block for IPTV multicast is for further study.

7.1.2 Application Functions for IPTV multicast

The multicast application functions interact with end-user functions to join and leave of IPTV multicast services; and this functions support basic multicast control functionality such as IPTV multicast channel change, pause, resume, etc. Application Functions for IPTV multicast include "IPTV application block", "DRM Rights & Key management block", "Application Profile Functions block", and "Content Preparation block".

1) IPTV Application block: This block supports Linear TV application functions to perform session management, service authorization, presentation of the content metadata, and execution of the service logic of the Linear TV service.

2) DRM Rights & Key Management (multicast Key management) block: This block controls the protection of the content and is responsible for the management of the content rights and the keys used to encrypt and decrypt contents. It acquires the content rights (or content licence, originated from Content Provider) from the Content Preparation function, generates and distributes this security information (rights object or keys) to DRM Client, it may also provide the keys to Content Encryption.

3) Application Profile Functions block: This block stores the profiles for the IPTV Applications. Application Profile may be located either within Service User Profile Functions, or within IPTV applications depending on implementation.

4) Content Preparation block: This block is used to aggregate Content, to manage contents, to process metadata and to encrypt contents. It may be used to convert the content, which is delivered by the content owner, into required delivery format.

7.1.3 Service Control Functions for IPTV multicast

The Multicast Service Control Functions for IPTV multicast provides the functions of requesting and releasing the network and service resources required to support the IPTV multicast services; it include "IPTV service control functional block" and "service user profile function block".

1) IPTV service control functional block: It provides functions of handling service initiation and/or termination requests, performing service access control, establishing and maintaining the network and system resources required to support the required IPTV Terminal functionality. For example, it can request the Content Delivery Functions to allocate multicast media server capacity and to request the Network Transport Functions to reserve Network bandwidth for the multicast media Stream.

2) Service user profile function block: It can be used for storing user profiles, subscriber-related location data, and presence status data in the Service stratum. The service user profile functional block performs basic data management and maintenance functions. The service user profile functional block has responsibility of responses to queries for user profiles.

7.1.4 Content Delivery Functions for IPTV multicast

Multicast content delivery functions provide the distributed content servers for the IPTV multicast services. Multicast contents, which are prepared in the application functions, are delivered to the End-Users via the Network Transport Functions through the Content Delivery Functions.

During multicast service, Application Functions send contents to Content Delivery Functions. In order to support the efficient multicast services, contents may be stored/cached in the Content Delivery Functions; which includes "Content Distribution & Location Functions block" and "Content Delivery & Storage Functions block".

1) Content Distribution & Location Functions block: It controls the Delivery & Storage Functions to optimize content distribution, selection and deliver content to the end user.

2) Content Delivery & Storage Functions block: It distributes, caches, stores and delivers the content to the end user. They handle the media control messages; Pause and Fast Forwards.

7.1.5 Network Transport Functions for IPTV multicast

The "Network Transport Functions" provides multicast connectivity with transport functions for all multicast users. The multicast transport functions can support multicast tree construction, multicast traffic replication and multicast member identification functionalities. Then, multicast traffic is forwarded along multicast delivery path.

The Network Transport Functions include "Authentication and IP allocation functional block", "Resource control functional block", "Multicast Control Point Functions block", "Multicast Replication Functions block" and "Access Network Functions block".

1) Authentication and IP allocation functional block: It provides the capability of authenticating the Delivery Network Gate Functions, connecting the Network Transport and Control Functions and allocating IP address to the terminal device.

2) Resource control functional block: It provides the capability of controlling network resources in the Access and Transport networks to allow appropriate resources to be provided to the Content Streams.

3) Multicast Control Point Functions block: It provides the capability of selecting individual Multicast stream that is to be delivered, over the access network, to the IPTV Devices. The request for a Multicast Stream may need to be authorized before it is accepted. This is one of the Transport Network functions.

4) Multicast Replication Functions block: The functions replicate multicast stream to all the Multicast Control Points that need to receive it.

5) Access Network Functions block: This block for IPTV multicast is for further study.

7.1.6 Management Functions for IPTV multicast

These functions for IPTV multicast are for further study.

7.1.7 Content Provider Functions for IPTV multicast

Content can come from a number of different sources; the physical interfaces and signals formats may all be different from each of the sources. E.g. IP networks satellite decoders. It may include functions such as content ratifying, which means it needs to ratify content licence, content access prioritization and parental control level; it can provide distributed storage servers (e.g. CDN) for large volumes of video and audio contents.

These functions for IPTV multicast are for further study.

7.2 Description of reference points for Non-NGN IPTV functional architecture

The following references points, defined in IPTV architecture document [FG IPTV-DOC-0181], are the interfaces among functional blocks which are focused only in the aspect of IPTV multicast.

Reference point E1, E2-Cm, E3, H1, H2, A1, A2, A3, A4, C1, C2, D1, S1, S2, S3, S4, S5, T1, R1, Md, Mc are identified to be related to IPTV multicast architecture and need further study.

8 IPTV Multicast scenarios

8.1 Native IP multicast scenario

8.1.1 Native IP multicast-based IPTV service delivery solution

Figure 8-1 shows the concept of native IP multicast based IPTV service delivery solution.

In this scheme, each member registers IP multicast group by exchanging IGMPv.x messages with its access routers; and then each IP multicast router constructs IP multicast tree by exchanging multicast routing protocol messages; finally data from source flows according to the multicast tree from source to each receivers.

In this scenario, the network provider can fully manage the multicast based IPTV service delivery.

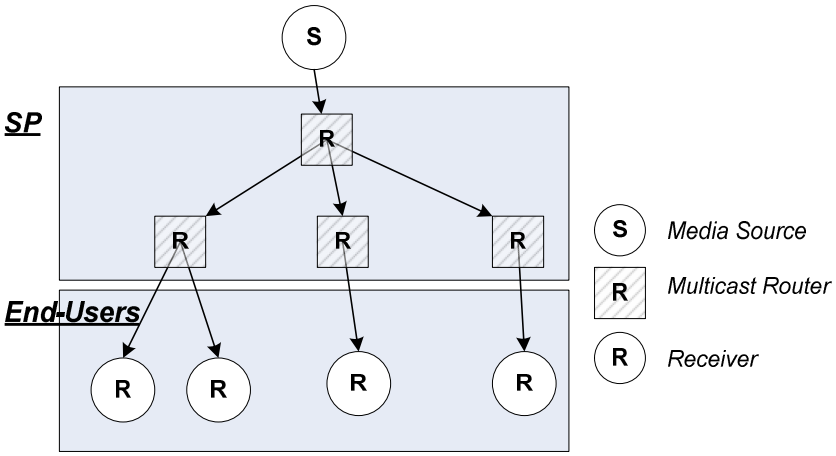


Figure 8-1: Data distribution scheme with native IP multicast

To provide IPTV service based on native IP multicast, it is required for Network Provider (NP) to install multicast-capable routers; and the service solution fully depends on IP multicast network.

The native IP multicast-based IPTV service solution has characteristics of tightly related performance to the condition of NP's network; therefore this service solution has the merit of having full-network-speed because multicast forwarding capability is provided by each network element (i.e., multicast routers).

On the contrary, native IP multicast-based IPTV service solution can support only bounded number IPTV service channels. Because each network element must handle each state per flow, the NP's network may suffer from unbounded number of IPTV service channels.

Therefore, native IP multicast-based IPTV service solution is appropriate for HDTV-quality IPTV service with bounded number of IPTV service channels.

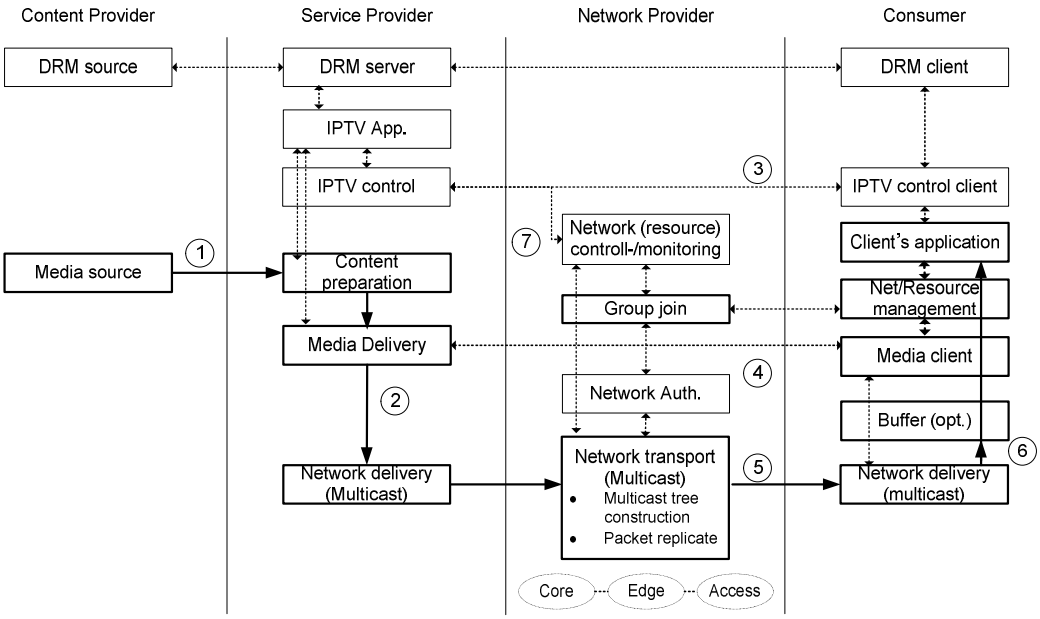


Figure 8-2: High-level information flow for the case of IP multicast-based IPTV service

Figure 8-2 shows scenario when native IP multicast mechanism is applied to IPTV service. To provide IPTV service, not only data delivery mechanism but such as IPTV service control, DRM management are very crucial, but this scenario will only focus on the multicast data delivery capabilities, the left are considered out of scope.

In the native IP multicast-based IPTV service, Content Provider (CP) asks Service Provider (SP) to multicast content media (1), and then SP prepares the content media for multicasting to the announce group (2); but the way of announcing group is also considered as out of scope.

Consumer (IPTV client) exchanges signalling with SP's IPTV control function for initiating IPTV service (3).

In native multicast based IPTV service, NP is in charge of replicating and delivering content media to each receiver; the purpose of network transport function of NP is to configure optimized multicast tree and then forwards replicated data along the configured multicast tree. The network provided by NP consists of access, edge, and core network.

To have multicast delivery service, it is required for IPTV client to subscribe a specific multicast group. IPTV client uses network/resource management function to subscribe the multicast group (4); IPTV client can join a specific multicast group by using IGMP. IPTV client's subscribing a group will be accomplished after following successful NP's network authentication; then the IPTV client can be attached to the specific multicast tree. In case of NP, most optimized multicast tree from SP to consumers is configured by exchanging appropriate routing protocol.

After the successful multicast tree is configured, the content media from SP can be delivered to IPTV client with help of multicast forwarding capabilities provided by NP (5). The content media, finally reached at IPTV client's network transport function, will be delivered to IPTV client application. To improve video quality suffered by jitter or delay, IPTV client may put appropriate size of buffer between network transport and client's application (6).

In case when QoS monitoring is necessary, SP may gather information by asking end IPTV client of experienced QoS report or by asking NP of network statistics (7); but the details are considered as out of scope.

8.2 Alternative multicast scenarios

8.2.1 Server-based IPTV service delivery scenario

Figure 8-3 shows the concept of replicated unicast based IPTV service delivery solution.

In this scheme, service provider (SP) provides a media server or server pool; each member connects media server or server pool; then the media server sends data to every receiver respectively.

Service provider can fully manage the server-based IPTV service delivery, but because media server cannot support infinite number of receivers, the size of the group is tightly bounded by the performance of media server or server pool as well as server-side network bandwidth.

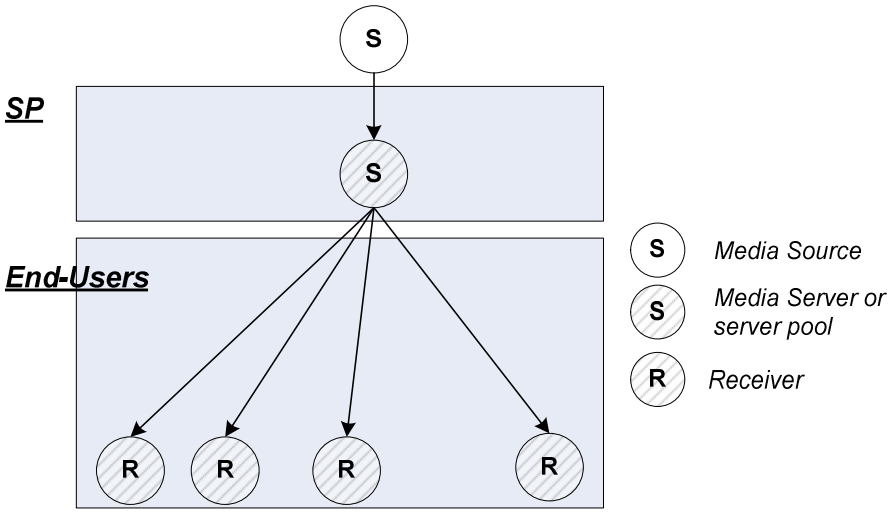


Figure 8-3: Data distribution scheme with replicated unicast

8.2.2 CDN-based IPTV service delivery scenario

Figure 8-4 shows the concept of CDN-based IPTV service delivery solution.

In this scheme, service provider pre-installs CDN servers in an appropriate place; each receiver finds and then connects the nearest CDN server. Then multimedia streams from source are distributed to each receiver along the data delivery path of CDN servers.

Service provider can fully manage the CDN-based IPTV service delivery; but because service provider cannot install CDN servers infinitely, the number of installed CDN servers bounds the size of the group tightly.

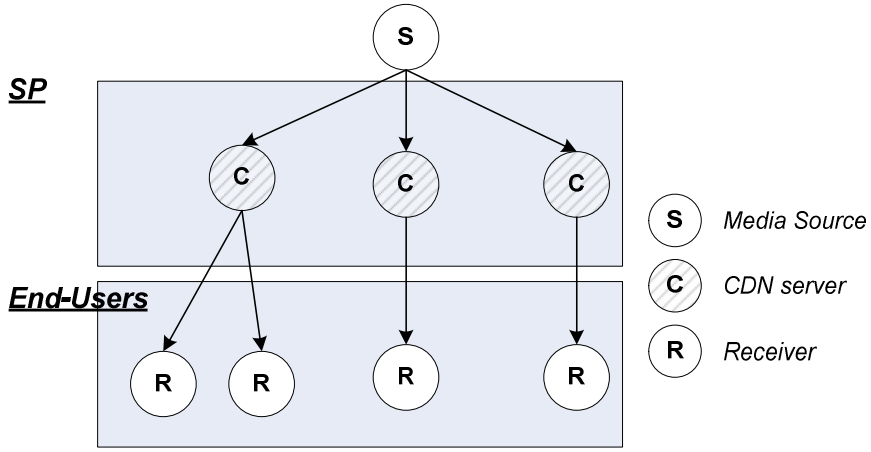


Figure 8-4: Data distribution scheme with CDN

To provide CDN-based IPTV service, it is required SP to position CDN server or server pool. CDN-based IPTV service can be easily deployed; because CDN-based IPTV service can be implemented over current unicast-based network; so, it is not required to install multicast-enabled network.

The CDN-based IPTV service solution has characteristics of tightly related performance to the power of CDN server and the number of CDN servers; because CDN server sends content media to each client repetitiously according to the each IPTV client's connection to CDN server. The number of IPTV clients can be served at a same time totally depends on the power of CDN servers and the number of CDN servers.

However, because each client directly connects to CDN server SP can easily manage each client at any purpose; for example, SP can monitor each IPTV client's presence for billing in real time.

Therefore, CDN-based IPTV service solution is most suitable for IPTV service provider who does not own a network but wants to provide payable IPTV service to the bounded number of IPTV clients.

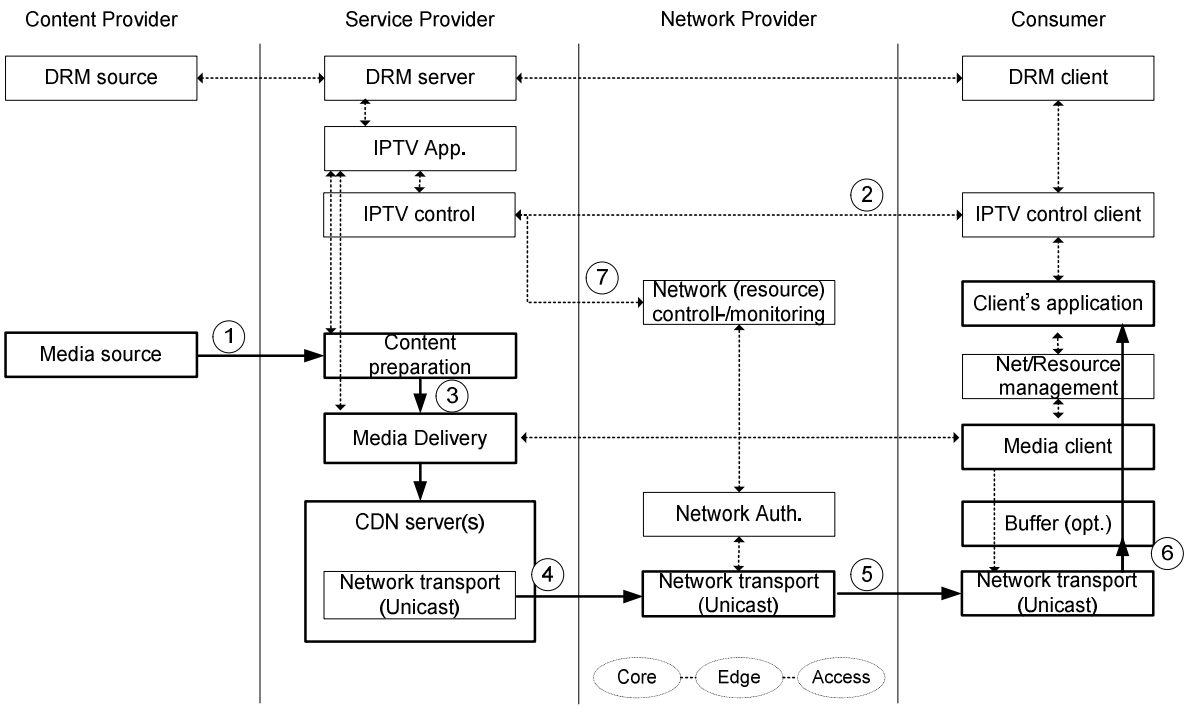


Figure 8-5: High-level information flow for the case of CDN-based IPTV service

Figure 8-5 shows the scenario when CDN mechanism is applied to IPTV service. Because this scenario only focuses on the multicast data delivery capabilities, the left are considered out of scope.

To begin with CDN-based IPTV service, CP asks SP to deliver content media; then SP convert the requested content media into suitable format for IPTV service delivery (1).

To receive IPTV service, IPTV client asks SP for specific IPTV service; and then SP gives available information about CDN servers to connect (2). IPTV client then tries to connect CDN server by using the given information from SP (3). Because unicast mechanism is applied to deliver content media to IPTV clients in CDN-based IPTV service solution (4), NP does not care about multicast delivery; NP is just for unicast data delivery capabilities (5).

The content media, finally reached at IPTV client's network transport function, will be delivered to IPTV client application. To improve video quality suffered by jitter or delay, IPTV client may put appropriate size of buffer between network transport and client's application (6).

In case when QoS monitoring is necessary, SP may gather information by asking end IPTV client of experienced QoS report or by asking NP of network statistics (7); but the details are considered as out of scope.

8.2.3 P2P-based IPTV service delivery scenario

Figure 8-6 shows the concept of P2P-based IPTV service delivery solution.

In this scheme, each end-node can be both a media producer as well as a media consumer. The way of communications is as follows; each node discovers its peers and then connects them; each node can exchange media between themselves.

Because P2P model does not want to have SP's censorship, this model usually does not involve node of SP's. Although the size of group is not logically bounded, it may not be adequate to distribute contemporary media. To improve data receiving, each node tries to finds more peers as possible.

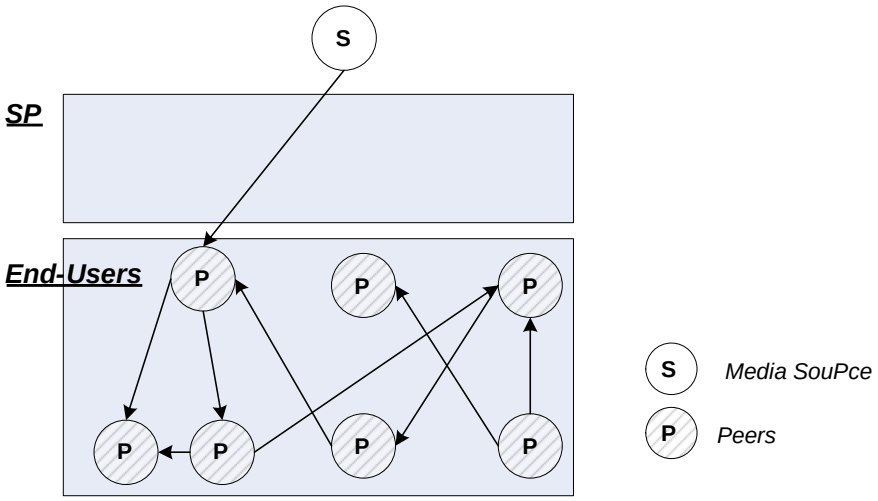


Figure 8-6: Data distribution scheme with P2P

8.2.4 Overlay multicast-based IPTV service delivery scenario

Figure 8-7 and Figure 8-8 shows a brief concept of overlay multicast-based IPTV service delivery solution. In overlay multicast mechanism, special overlay nodes emulate the functions of IP multicast router's; such as multicast data tree configuration, multicast data forwarding, etc.

In this scheme, each overlay node constructs multicast data delivery path from sender to group dynamically as naïve IP multicast router does. Along the constructed path, each overlay node forwards data, which comes from its upstream node, to its downstream nodes. The size of group is not logically bounded, and it is adequate to distribute contemporary media.

The overlay node which substitutes IP multicast router may form a hardware box, a server, or an end-system; the formation is a deployment or implementation issue. Figure 8-7 shows an overlay multicast scheme without SP's participation.

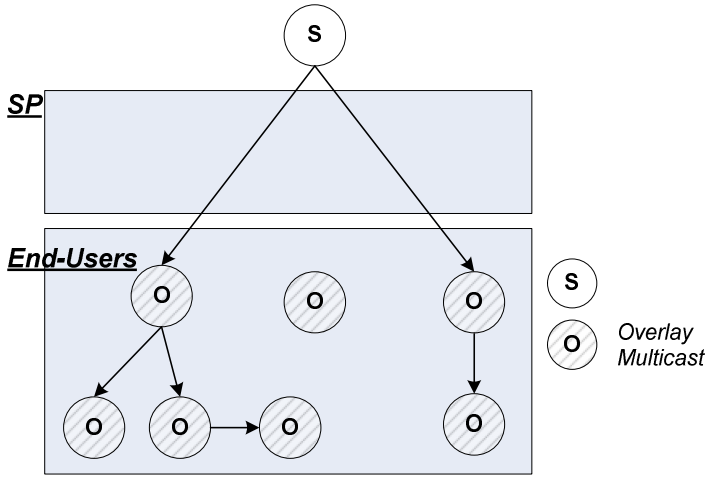


Figure 8-7: Data distribution scheme with overlay multicast without SP

Figure 8-8 shows an overlay multicast scheme with SP's participation.

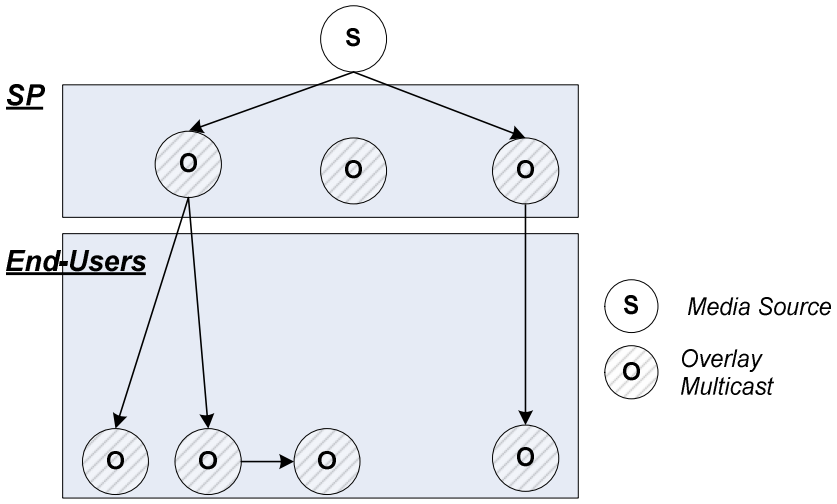


Figure 8-8: Data distribution scheme with overlay multicast with SP

To provide overlay multicast-based IPTV service, it is required for IPTV client's network delivery function to construct overlay multicast tree and to replicate and forward content media.

Overlay multicast-based IPTV service can be easily deployed. Because overlay multicast-based IPTV service can be implemented over current unicast-based network; there is no need to change current network environment.

The noticeable feature of overlay multicast mechanism is that each client can relay received content media; i.e., each client can act like content producer as well as content consumer. Therefore the QoS of overlay multicast-based IPTV service is highly affected by the power of each IPTV client.

However, in overlay multicast-based IPTV service solution, only the participated IPTV clients to a specific IPTV channel share the burden of content media delivery; so it is not required to have centralized server nor specific network element. Therefore, overly multicast-based IPTV service does not have any limitation on the number of IPTV service channel.

On the contrary, it is difficult to manage each IPTV clients for billing and presence, because each contents media delivery elements in overlay multicast-based IPTV service are distributed.

Therefore, overlay multicast-based IPTV service solution is suitable for IPTV service of low-video-quality (low bit rate) and free IPTV service with no limitation on the number of service channel. Especially this service solution can be applied for the cyber community purpose, for personal broadcasting purpose, and for the CCTV broadcasting purpose.

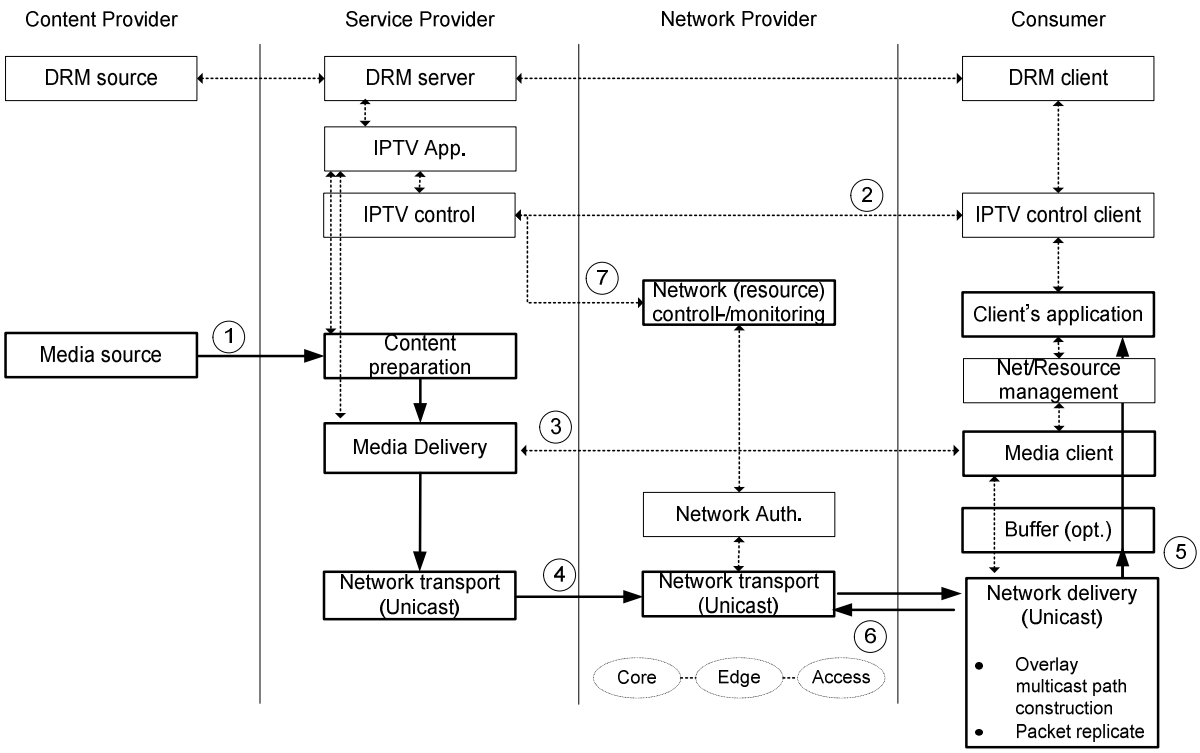


Figure 8-9: High-level information flow for overlay multicast-based IPTV service

Figure 8-9 shows the scenario when overlay multicast mechanism is applied to IPTV service. Because this scenario only focuses on the multicast data delivery capabilities, the left are considered out of scope.

To begin with overlay multicast-based IPTV service, CP asks SP to delivery content media and then SP convert the requested content media into suitable format for IPTV service(1). IPTV client asks SP to provide IPTV service to receive IPTV service (2).

In overlay multicast environment, each IPTV client constructs overlay multicast tree. Along the overlay multicast tree, each IPTV client can receive content media from its parent client and can also relay the received content media to its children clients; therefore it is required for each client to know the location information of other clients participated in same IPTV channel.

To acquire information about other participated IPTV clients, IPTV client exchange signalling with SP (3). In overlay multicast-based IPTV service, unicast mechanism is applied to deliver content media; NP only needs to support unicast data delivery capabilities (4).

The content media, finally reached at IPTV client's network transport function, will be delivered to IPTV client application. To improve video quality suffered by jitter or delay, IPTV client may put appropriate size of buffer between network transport and client's application (5). Then IPTV client forwards the received content media to network to support its children clients (6).

In case when QoS monitoring is necessary, SP may gather information by asking end IPTV client of experienced QoS report or by asking NP of network statistics (7); but the details are considered as out of scope.

9 Design considerations for IPTV multicast network

9.1 IPTV multicast transport

The physical implementation of IPTV multicast transport can be done by the network elements with multipoint configurations.

9.1.1 Any Source Multicast and Source Specific Multicast

Two different service models for IP-Multicast are currently supported: Any Source Multicast (ASM) and Source Specific Multicast (SSM). Within an IPTV Multicast Framework both service models can be used and also deployed in parallel because ASM and SSM are running in different address spaces.

ASM generally deploys IGMPv2 or IGMPv3 (MLDv1/MLDv2) *without* source information and PIM-Sparse Mode in combination with the Multicast Source Discovery Protocol (MSDP), whereas SSM deploys IGMPv3/MLDv2 *with* source information and PIM-Source Specific Multicast as a routing protocol.

The following section describes Any Source Multicast, Source Specific Multicast, related protocols and general mechanisms to be deployed within an IP-Multicast enabled IPTV network.

9.1.1.1 Any Source Multicast

Any Source Multicast (ASM) is the classical variant and uses a model where all decisions are made based on the multicast group address (G) only. Devices are able to join and leave multicast groups in order to receive IPTV streams. The receivers do not have knowledge about the Multicast senders within the network. When two IP Multicast senders are sending to the same IP Multicast group address (G) and a client joins (G), the client receives traffic from both IP Multicast senders.

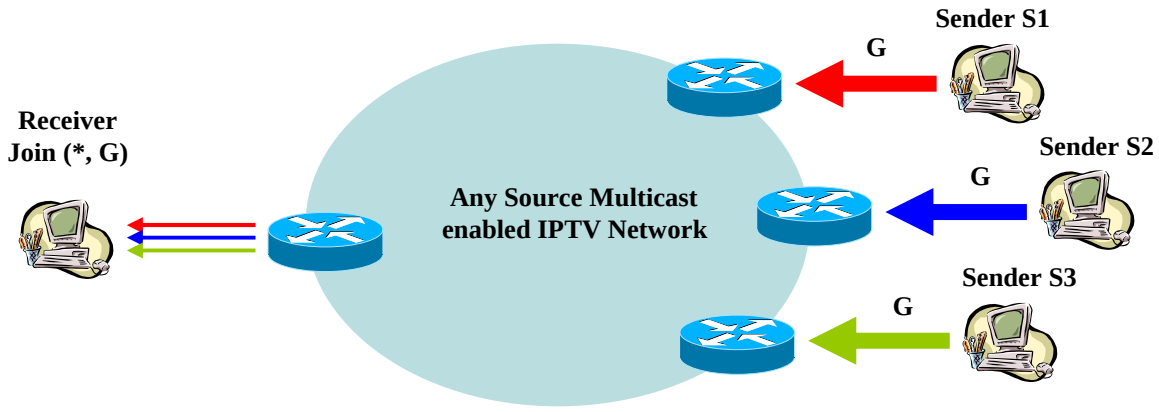


Figure 9-1: Any Source Multicast

This model has some significant drawbacks for IPTV deployment:

1. **Addressing**: Due to the fact that only the IP Multicast address is used it is not possible to distinguish different senders on the network level. Therefore it is necessary to implement an entity which manages the use of IP Multicast addresses. This slows the deployment down because to setup new IPTV channels or change existing IPTV channels it is necessary to obtain a free (unused) IP Multicast address.

2. **Security**: In a group-based model it is easy to disturb existing IPTV channels by simply sending traffic to the same group address. To avoid those attacks complex filter mechanisms are needed at the ingress and/or egress points of the network (and potentially at customer's premises to avoid unwanted and disturbing IP Multicast traffic).

3. **Redundancy**: On the network level Any Source Multicast usually deploys PIM-SM (Protocol Independent Multicast – Sparse Mode) a central Rendezvous Point (RP) which represents a single point of failure. To overcome this problem redundant RPs and additional protocols are necessary.

4. **Complexity**: Taking 1-3 into account (as well as some other drawbacks) the use of Any Source Multicast adds complexity. To reduce the complexity and to overcome the problems with ASM a new model "Source Specific Multicast" was developed.

9.1.1.2 Source Specific Multicast

Source Specific was developed to overcome the problems encountered by Any Source Multicast. The main difference between the two models is the use of the source address of the multicast sender. In contrast to ASM with SSM it is possible to distinguish between a sender (S1) and a sender (S2) sending to the same IP Multicast address (G). Receivers not only specify the group address G but also the address of the sender (S), resulting in an IP Multicast *channel* (S,G). Because the Unicast address within a network uniquely identifies an end system, the combination of (S,G) is unique as well. A receiver joining (S1, G) does not receive the traffic from another system sending to the same IP Multicast address.

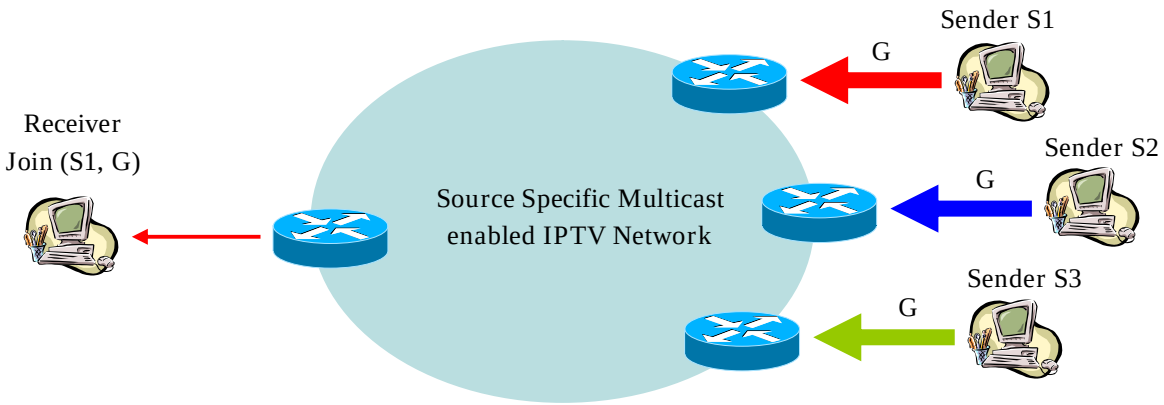


Figure 9-2: Source Specific Multicast

Source Specific Multicast solves the following problems:

- **Addressing**: It is no longer necessary to centrally coordinate the use of IP Multicast addresses. Any sender can send to any existing IP Multicast group. The network and the receivers are able to specify a particular sender using an IP Multicast group. IP Multicast channels (S,G) are handled and routed individually by the network and the clients as well.

- **Security**: Denial of Service (DoS) attacks by simply sending to a Multicast group which is already in use, are no longer possible, because individual senders can be distinguished.
- **Complexity**: Source Specific Multicast reduces the overall complexity within IPTV. It solves several issues related to security and addressing and also removes the need for centralized Rendezvous Points.

SSM is also optimized for One-to-Many deployment scenarios which are typically used within IPTV. In addition ASM and SSM can be used in parallel (deploying different address ranges) if necessary. The use of SSM eases the deployment of IPTV and reduces the complexity, allowing more flexible IPTV services. The IETF has assigned the default address space 232/8 for the use with Source Specific Multicast.

9.1.2 Multicast group management in access node

Internet Group Management Protocol

IGMP is used between an IP-Multicast capable end system (e.g. IPTV Terminal Device) and a IP-Multicast capable router. IGMP is available in different versions: IGMPv1, IGMPv2 and IGMPv3. IGMP is used by end systems to join and leave IP-Multicast groups or channels (depending on the IGMP version).

- IGMPv1 (RFC1112): IGMPv1 is the oldest version of IGMPv1. Due to the fact that IGMPv1 does not support a "Leave Message", IGMPv1 in not widely implemented and was replaced by IGMPv2/IGMPv3. IGMPv1 supports only the ASM model.
- IGMPv2 (RFC2236)/MLDv1 (RFC2710): IGMPv2 added the capability of end system to leave a Multicast group by sending a "Leave Messages" to the next node. IGMPv2/MLDv1 supports only the ASM model; both protocols are widely deployed today.
- IGMPv3 (RFC3376)/MLDv2 (RFC3810): The main difference is the support of filter mechanisms (exclude/include filter) to support Source Specific Multicast. IGMPv3/MLDv2 supports the ASM and the SSM service model.

IGMP transparent snooping

IGMP snooping optimizes the distribution of multicast within an IEEE 802.1 bridging domain so multicast traffic is only sent on bridge ports where there are known to be active receivers and/or multicast routers. IGMP snooping functionality resides on IEEE bridging devices that connect IGMP hosts to IGMP routers and consists of two main components. The first function is the IGMP snooping control section which:

1) Monitors IGMP messages (and optionally other multicast router messages, such as PIM or DVMRP hello packets), to determine the port location of the multicast routers and active receivers within an IEEE bridged domain.
2) Builds per port, per VLAN multicast forwarding tables
3) Maintains basic IGMP membership state on non-router ports to determine when a forwarding entry should be removed.

The second function is the data forwarding section which:

1) Forwards packets in the 224.0.0.0/24 range which are not IGMP messages on all ports.
2) Forwards multicast packets with a destination IP address outside 224.0.0.0/24, which are not IGMP according to per VLAN, per port multicast forwarding tables.

This basic mode of operation is often referred to as "transparent IGMP snooping" and does not absorb, nor alter, nor generate IGMP messages when performing the above functions.

IGMP proxy

IGMP proxy is a function to reduce the number of IGMP/MLD messages in a network and to enable a device to communicate with a Multicast enabled router without using a IP-Multicast routing protocol.

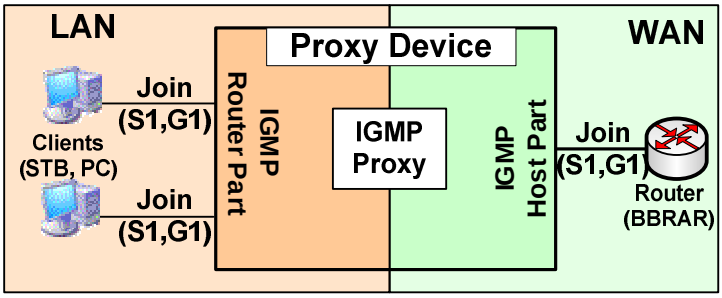


Figure 9-3: IGMP proxy functional description

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 should be possible to select the proxy interface by static configuration or a dynamic mechanism like 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 must 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 9-4).

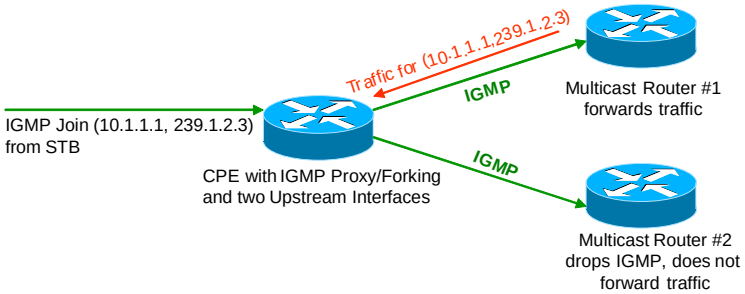


Figure 9-4: IGMP Proxy in Forking Mode

Fast Leave / Immediate Leave

A function associated with IGMP snooping or IGMP routing whereby the switch or router stops sending immediately the multicast stream when receiving an IGMP leave for the last member on this requesting interface, i.e. without sending one or more group specific queries and waiting for its timeout.

9.2 IPTV multicast QoS

9.2.1 Types of IPTV multicast QoS

There are two types of QoS for IPTV multicast.

As the first type of QoS for IPTV multicast, the following should be considered.

- IPTV network is recommended to support of handling multicast traffic differently according to the requested QoS treatment.

- For differentiated handling of multicast traffic, congestion avoidance and congestion management mechanism are required because network congestion may cause quality degradation of IPTV service.

  – IPTV network is recommended to support congestion avoidance mechanism to prevent multicast traffic from being dropped over other lower classes of traffic.

  – IPTV network is recommended to support congestion management mechanism to prioritize multicast traffic over other classes of traffic.

  IPTV network is recommended to provide a certain level of QoS when delivering IPTV service traffic to IPTV end-users. Resource reservation is necessary to guarantee the QoS of IPTV multicast and congestion control is necessary to maintain the QoS of IPTV multicast. IPTV network can guarantee QoS by using of resource pre-reservation mechanism. Pre-reserving mechanism is more efficient than dynamic resource reservation mechanism in that dynamic reservation mechanism needs to manage dynamic membership with many receivers. Moreover, pre-reserving mechanism is simple to control and maintain multicast resources.

As the second type of QoS for IPTV multicast, IPTV multicast network is recommended to provide capabilities to ensure sufficient availability for IPTV services.

- IPTV multicast network is recommended to be restored without service intervention in the event of multicast mechanism abnormalities.

- IPTV multicast network is recommended Multicast distribution trees shall be dynamically restored in the event of multicast mechanism failures.

- IPTV multicast network is recommended to be fully redundant for avoiding a single point of failure affects the whole IPTV service.

- IPTV multicast network is recommended to be distributed in a load balanced manner in order to utilize multicast links efficiently.

9.2.2 QoS aware topology for IPTV multicast service

9.2.2.1 Optimal RP (Rendezvous Point) positioning and RP redundancy

Location of RP affects not only multicast service delay, but also multicast network stability. Rendezvous point is recommended to support optimal RP positioning; optimal RP positioning depends upon Service Providers' network topology and their multicast traffic path which taken consideration of followings:

- Loop free, delay/jitter independent, stability guarantee topology
- Optimal position to exchange source active information amongst multicast service provider

One of main reasons to apply multicast is to reduce backbone traffic produced by redundant customers' request, so it is advantageous to locate RP near the source compare to locate it somewhere in middle of backbone.

Rendez-vous point is recommended to support RP redundancy mechanism; IPTV network should be guaranteed optimized RP redundancy to improve IPTV service stability in case of RP failure. IPTV network should be designed their RP mechanism not only to maximize service stability, but also to minimize service recovery time during RP failure.

Once multicast based IPTV Service Providers decide optimal RP position in their multicast network, they need to consider how to configure RP to maximize service efficiency. There are basically two ways of selecting RP, one is dynamic RP selection, and the other is static RP selection. It is often difficult to define one way is superior to the other such that multicast based IPTV Service Providers should decide which way is the best practice for their own multicast network. When multicast based IPTV Service Providers design their RP, they should consider the followings.

- Service recovery time in RP failure. When there happened RP failure, it should minimize their service recovery time. Normally static RP recovers compare to dynamic RP.
- Operation issues: Configuration & Troubleshooting. RP should be designed in a way that it should not bring too much operational overhead and should be advantageous to troubleshooting. In case of static RP, all routers running multicast routing protocol, such as PIM-SM, must include adequate configuration to designate their RP. However, dynamic RP does not require duplicate of configuration for all routers. For troubleshooting, dynamic RP normally require much more complicated steps to track the problem whereas static RP is relative much simpler to troubleshoot.
- Feasibility issues: Vendor status. When selecting RP with a dynamic way, one thing to keep in mind is, it should always select an identical RP for the groups in a network. RP for a group "A" should be RP "A", it cannot be any other RP for that group. When selecting RP with a dynamic way, router vendors use some algorithm to select a primary RP among their RP candidates, but it could be compatibility issues among vendors. So it is essential to check if they all work with an expected manner.

Anycast RP has been widely adopted in existing IPTV multicast solutions to get service robustness and scalability, as well as load-balancing. The best working examples of anycast RP in IPTV is Anycast RP redundancy and anycast source. The Anycast RP mechanism is intended to address the need for better fail-over (convergence time) and load sharing of source register messages among RPs in a domain.

9.2.2.2 Load balancing of IPTV multicast

When multicast routers receive a join message, multicast routing protocol normally send its join message to one of the multicast interfaces. If some groups have the same source, among multiple multicast interfaces, only one of them is selected and sends the join. In an Equal Cost Multiple Path (ECMP) environment, all multicast interfaces cannot be used to distribute multicast traffic; instead only single interface is used. To load share the traffic, multicast source should be distributed for different groups, and IPTV service provider should be considered for this load sharing requirements.

- IPTV multicast source is recommended to be distributed to different groups to support load balancing.

9.2.2.3 Multiple multicast trees of IPTV multicast

Multiple multicast trees include many multicast trees with each tree being constructed from the multicast source to the receivers and multicast data being delivered among all the multicast trees.

- In multiple multicast trees, every host is recommended to be assigned with equal or similar level of load to handle equal or similar number of input / output data flows.
- In multiple multicast trees, each host is recommended to be assigned to have minimum number of children nodes to avoid a single point failure.
- In multiple multicast trees, node positions are recommended to consider the corresponding hosts capabilities and behaviours. The hosts with higher capabilities for multicast and stable behaviours are more likely to occupy important positions on the multicast trees.

9.3 IPTV multicast interoperability among service providers

In IPTV markets, there will be various types of service providers; like IPTV transport provider, content provider, and contents aggregator. Each service provider need service combination of different type of service providers or need the clear contract with other service provider to get the quick service spreading. With such a clear internetworking contract amongst IPTV service providers, user can get any sources from content providers through the IPTV transport provider, and we can make IPTV service popular.

IPTV service provider should provide capabilities for exchanging IPTV service information between different IPTV service providers for the interoperability. Especially, for IPTV multicast interoperability, the fundamental IPTV service information for each IPTV service provider should be announced to each SP. The purpose of IPTV service information exchange is to share the IPTV source information received from all IPTV service providers in multicast based IPTV service environment.

NOTE – For further study, we need the definition of the IPTV service information for IPTV multicast interoperability.

The IPTV service information for IPTV multicast interoperability can include ID of content aggregator or content provider, source IP address block, multicast group information, service start and end time, QoS/QoE information, traffic rate, video encoding rate.

The following can be considered as the functional requirements to handle multicast address interoperability.

- The assignment of multicast address for each IPTV service channel is recommended to be agreed between different IPTV networks for interoperability; for instance, the multicast address for each IPTV service channel could be unique between different IPTV networks, or optionally changeable when entering other IPTV network.

- IPv4 multicast addresses of [IETF RFC 3180] range (GLOP addressing in 233/8) are recommended to use to support interoperable multicast channels.
- IPv4 multicast addresses of [IETF RFC 3138] range (Extended Assignments in 233/8) or [IETF RFC 2365] range (Administratively scoped block) can be used if there is an agreement between peering IPTV SPs.
- IP multicast address ranges of [IETF RFC 4607]: Source-Specific Multicast for IP] is recommended to be supported to use Source Specific Multicast.

Each IPTV Service Provider may have its own multicast address policy and the policy of IPTV SP's internal multicast address may not match the inter-Service Provider address policy. Therefore, the following is recommended to be supported;

- IPTV Service Provider is recommended to support translating multicast addresses from other IPTV Service Provider to its internal multicast address; the multicast address translation policy is up to IPTV Service Provider.
- IPv6 multicast addresses of [IETF RFC 3307] range (Allocation Guidelines for IPv6 Multicast Addresses) are recommended to support interoperable multicast channels.

The following can be considered for multicast routing interoperability.

- Multicast BGP between different IPTV service providers is recommended to advertise multicast source routes. Multicast border gateway protocol (MBGP) is used to advertise multicast source routes for RPF check. Followings should be considered as the peering policy that MBGP is using for multicast routing protocol between IPTV service providers.
  - Advertising summarized prefixes if possible.
  - Recommended route filtering policy like default routing information, private addresses defined by [IETF RFC 1918], all Multicast groups(224/4), ISP's unicast prefix range from peer ISP.
  - AS Path filtering.
  - Maximum prefix limit.
  - Md5 authentication between MBGP peers.
- Source active filtering of Multicast Source Discovery protocol (MSDP) is recommended to use to prevent bogus (S, G) from sending when MSDP is applied. When the MSDP is used between IPTV Service Providers for their multicast service, MSDP source active filter is necessary to prevent bogus (S, G) from sending. Followings should be taken care as the MSDP filtering policy that MBGP is used for multicast routing protocol between IPTV SPs.
  - Domain-local multicast applications.
  - Auto-RP groups.
  - Administratively scoped groups(239/8).
  - Default SSM range(232/8).
  - Loopback addresses(127/8).
  - Private addresses(RFC1918 range).

- IPTV service provider is recommended to protect its own IPTV network and IPTV source against the malicious traffic injection from peering service providers (SPs). IPTV service providers should protect their own IPTV network and IPTV source against the malicious traffic injection from peering SPs. This function should be implemented in IPTV multicast interoperability peering point. Followings should be considered as the security policy for IPTV multicast interoperability.

  – uRPF (unicast Reverse Path Forwarding) in peering interface.

  – Filtering about non-approved group range, source Block and non approved application port numbers.

  – PIM (Protocol Independent Multicast) neighbour authentication.

  – TCP/ICMP message filtering for 224/4.

  – Protection against multicast source spoofing.

  – BSR (Bootstrap router) message filtering.

  – Capability to limit the maximum number of multicast routing information.

In IPTV multicast interoperability environment, IPTV service providers should provide the QoS monitoring function to handle the IPTV service quality measurement, and also IPTV service providers should provide the QoS management function to keep IPTV service in high quality.

- IPTV service provider is recommended to provide IPTV Service quality measurement and management function for interoperability.

9.4 IPTV multicast management

9.4.1 IPTV multicast user management

As the current multicast protocol (i.e. IGMP) does not consider Multicast user authentication and authorization, it is requested a further development of those functions to support IPTV services efficiently.

Multicast user authentication function controls the authority for users to receive multicast flows. And through authenticating multicast users, the network can distinguish legal multicast users from the illegal ones and then can distribute the multicast traffic to the reasonable receivers. Following procedures should be considered.

- When a user initiates a multicast "join" request to join a certain multicast group with an account, the duplication point should not accept the request and make him join the group at once, it should be sent the request to the authentication point.

- The authentication point inquires the account information database and returns the result to multicast duplication point. The value of the user's multicast property in the account should be set by the service layer system.

- According to the authentication result returned from the authentication point, the Multicast duplication Point should decide whether it allow the user to join the group or not. If allow the user to join the group, the duplication will add it to distribution table. Whereas it will refuse the user to join the group.

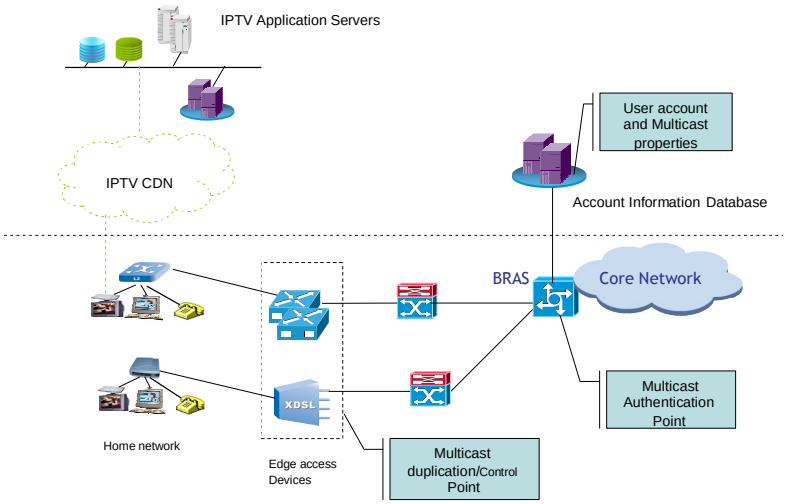


Figure 9-5: Functional components for Multicast user management

9.4.2 IPTV multicast address management

According to IANA rule, several hundred millions of IPv4 and IPv6 multicast addresses can be used in the internet. As one of important resources, these multicast addresses, should be managed effectively.

9.4.2.1 IP multicast address transition

When deploying IPTV broadcasting services, carriers often use one multicast group address representing an IPTV channel. Unlike the unicast addresses, multicast addresses are not distributed depending on different countries, areas and carries all over the world. Therefore, during the operating of IPTV broadcasting service, the corresponding relationship between IPTV channel and multicast address can be overlapping or conflicting among different carriers or different service areas of one carrier. As Figure 9-6 shows, carrier A and carrier B want to interconnect their IPTV direct broadcasting services; or Carrier B created local IPTV broadcasting service platform in service areas C and D , where the local carriers should interconnect some broadcasting service sources. With regard to these IPTV service traffic which cross multiple multicast bearer domains, IPTV MST (multicast service stream transition) needs to be deployed at the edge of each bearer network domain to check the multicast service traffic from other domains.

- Multicast address is recommended to be changed before entering local domain when there is a multicast address conflicting.

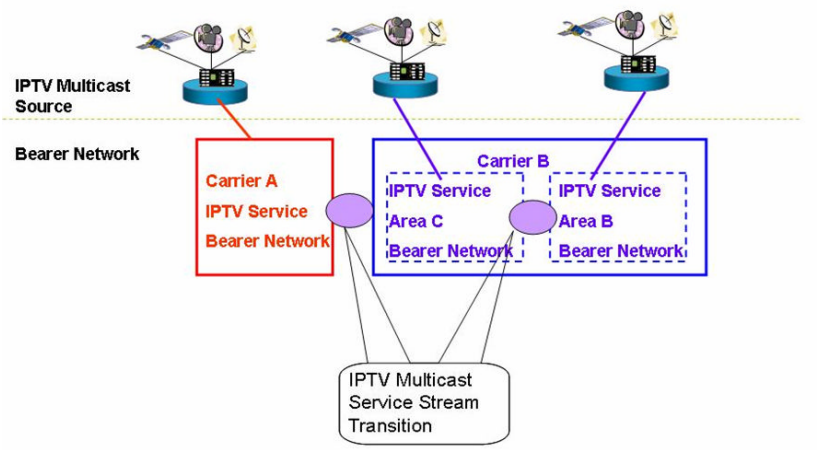


Figure 9-6: IPTV multicast address transition

- IP multicast address mapping function is recommended to support end-user's personal broadcasting service.
- The use of Source Specific Multicast solves the problem with overlapping Multicast addresses. In case of SSM a combination of a Multicast Group address and the Source Address of the Multicast sender is used (this combination is unique and allows several senders to use the same IP Multicast address). It is recommended to deploy Source Specific Multicast.

9.4.2.2 The control of users' multicast address

In order to control the development of multicast services on carrier's network and avoid impact on carriers' IPTV broadcasting services, carriers can deploy multicast service controller to manage the distribution of multicast address uniformly. However, as for the multicast application without registration, carriers will restrict the usage of these multicast addresses at the access point of IPTV network. The procedures of applying for multicast service and multicast address are as follows and shown as Figure 9-7.

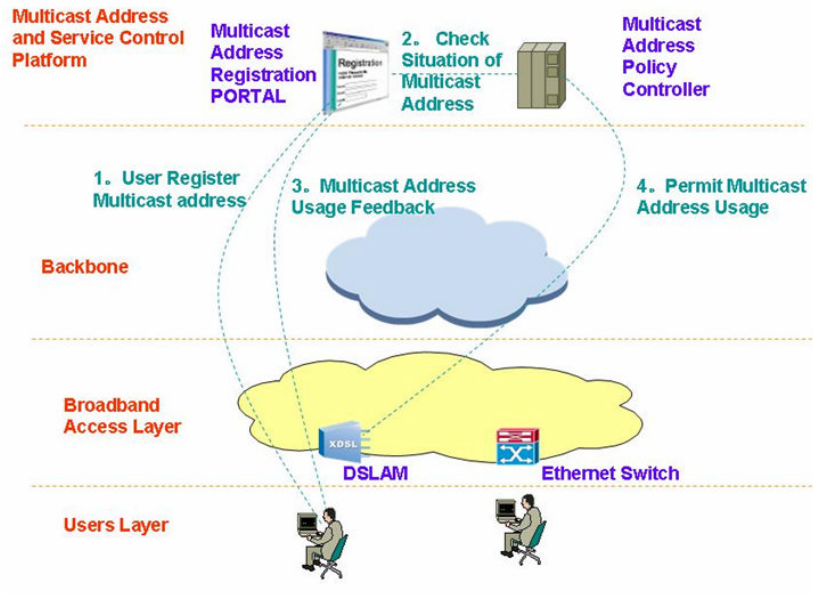


Figure 9-7: Control procedure of multicast address

1) In order to carry out services based upon multicast address users should arrange the inquiry and registration on the PORTAL of carrier-provided Multicast Address and Service Control Platform.

2) The self-service system check the situation of this multicast address from multicast address policy controller

3) If this multicast address is available, users will be told that they are allowed to use it.

4) At the same time, multicast address policy controller sends policies to the access point to allow the multicast services get access.

9.4.2.3 IPTV Multicast Address / Domain Name Management

The function of IPTV Multicast Address / Domain Name Management is an optional one for network operators, to make their management of multicast address resources more efficiently and easily. With this function, network operators do not allocate multicast IP addresses to multicast channels of IPTV service providers directly, but register domain names of these channels, and bind multicast addresses with their domain names dynamically.

- Multicast IP addresses are managed by network operators.
- Network operators can do domain name registration / deregistration on DNS servers.
- IPTV service providers negotiate domain names of their IPTV channels with network operators.
- Network operators register domain names of IPTV channels with multicast addresses dynamically assigned to these channels.
- Network operators inform IPTV service providers about the domain names registered for their IPTV channels.
- When network operators need to do multicast address management work, they just modify domain name registration on DNS servers.
  - Allocate a multicast address to an IPTV channel: register a domain name with a multicast address for the IPTV channel.
  - Revoke a multicast address from an IPTV channel: deregister the domain name of the IPTV channel.
  - Rearrange multicast addresses: modify domain name registration of IPTV channels.
- IPTV service providers get multicast address information of their IPTV channels by DNS query, and send IPTV contents to those multicast addresses.
- End users access these IPTV channels by their domain names.
- Network operators can make use of domain name information of IPTV channels to do IPTV service access control on both multicast sources (IPTV service providers) and multicast group members (end users).

9.4.2.4 IPTV channel domain name management function for IPTV service providers

The function of IPTV channel domain name management is an optional one for IPTV service providers, to represent their multicast IPTV channels with constant identifier – domain names, rather than multicast IP addresses. With this function, IPTV service providers register domain names of their multicast channels with the help of DNS service providers, and bind multicast IP addresses with these domain names dynamically.

- Multicast resources (multicast IP addresses) for IPTV services are managed by network operators.
- Network operators allocate multicast IP addresses to IPTV service providers, with which IPTV service providers can carry their multicast channels into service.

- There are DNS service providers, who maintain DNS servers, and provide DNS services (domain name registration, domain name query) to public.
- With the domain name registration service provided by DNS service providers, IPTV service providers manage domain names of their multicast channels.
  - Channel Registration: Register the domain name of an IPTV channel with a multicast IP address got from network operators.
  - Channel Deregistration: Deregister the domain name of an IPTV channel, and withdraw the multicast IP address assigned to this channel.
  - Channel Rearrangement: Modify domain name registration of IPTV channels.
- IPTV service providers represent their multicast channels with domain names when they release URI information of these channels (such as in EPG).
- Multicast IPTV channel servers get address information of the channel by DNS query, before broadcasting IPTV contents to the multicast address.
- End users access the multicast IPTV channels by their domain names.

Besides the obvious advantages of representing multicast IPTV channels with domain names, this solution benefits IPTV service providers in 2 more aspects.

- The solution makes it possible for IPTV service providers to represent multicast IPTV channels with domain names even network operators do not deploy IPTV multicast address / domain name management function.
- The solution provides an efficient way to IPTV service providers to manage their multicast resources (multicast IP addresses) got from network operators dynamically. Rearranging multicast addresses among their multicast IPTV channels has little impact on other aspects.

9.4.3 IPTV multicast service management

The packet transmission of IPTV Multicast service is usually provided based on UDP, so it can be less-reliable than TCP based delivery. Because of that reason, we absolutely need to provide the service management features including service monitoring one to guarantee the service reliability.

9.4.3.1 Definition of IPTV multicast service management

- IPTV multicast service is recommended to provide service monitoring features for the service status management.
- IPTV multicast service is recommended to provide the statistics as the service reporting feature.
- IPTV multicast service is recommended to manage each service STBs, stream servers, management servers.
- IPTV multicast service is recommended to be capable of recovering or handling for the specific host to get the poor service quality.

9.4.3.2 Necessary information for IPTV multicast service management

- Multicast Group information
  - The multicast groups IP, port information are delivered from streaming server to clients in the live broadcasting connection time. That information is used for checking whether multicast group information is correct or not.

- Client information
  - If the clients start to receive the live broadcasting data, IPTV service management server can get the information of the each client's IP, MAC addresses. That information is used for checking the client's status.
- Video type information
  - When receiving live broadcasting, the clients get the video information like video size and codec type which is received from the streaming server. That information is used for video quality measurement data.
- Video Frame information
  - With checking the timestamp and sequence number of the media data header, we can get the exact time information about frame reception and remaking.
  - The Sequence number is consecutive one, so the unusual increase can be regarded as the case of IPTV service frame loss, so it can be used for service quality measurement factor.
  - From the decoding procedure of media data, we can get the I, P, B frame information which can be used as service quality measurement information.
- Bitrate information
  - The Bitrate information can be also used for IPTV service quality measurement factor
    - √ Bitrate (bit/sec) = data size / time

9.4.3.3 IPTV multicast service monitoring features

- For providing IPTV multicast service monitoring, IPTV multicast service is recommended to provide the performance monitoring feature.
- And, IPTV multicast service is recommended to get the QoS performance data by manipulating of above IPTV service management information.
- And QoS performance data is recommended to include the measurement values such as fps, throughput, loss rate, delay, jitter.
- And, for the service monitoring, IPTV multicast service is also recommended to provide the measurement value of the IPTV multicast service quality, in each period such as daily, weekly, monthly basis.

10 Overlay multicast networking

This section describes the overlay multicast networking. It is recognized that the usage of the overlay multicast networking described in this section for IPTV services requires further study.

10.1 Control framework for IPTV overlay multicast

IPTV overlay multicast networking consists of virtual network topologies on top of the physical network, and it constructs and manages logical multicast path over the unicast/multicast physical transport network.

In order to provide IPTV multicast function in overlay networks, it is necessary to perform multicast session control and management for IPTV overlay multicast networking. The IPTV overlay multicast can use diverse mechanisms for constructing different multicast trees depending on IPTV applications or other requirements. The overlay IPTV multicast supports efficient routing and resource usage by overlay multicast control.

In overlay IPTV multicast framework, a logical multicast control path will be created along the logical delivery path, a multicast data delivery path is constructed over physical transport network, and a logical multicast, the control path will be created along the logical delivery path for reliable data transport. IPTV overlay multicast function is performed with cooperation among upstream and downstream IPTV Multicast Agents (IMAs) at service level. IPTV multicast session management (ISM) function at will be provided for multicast session configuration and maintenance at service level. IPTV logical delivery path is established via ISM and IMA at service level, and IPTV applications can work as if they were in a native IPTV multicast network.

Detailed description of control framework for IPTV overlay multicast are described in Appendix III.

10.1.1 IPTV Session Manager (ISM)

ISM is involved in session configuration and maintenance for IPTV service flows. A single ISM can handle one or multiple sessions simultaneously, and it can provide the following functionalities:

- Session initialization: ISM allocates ISID (IPTV Session ID) for new session
- Session release: Session can be released as needed
- Session membership management
- Session status monitoring: this function enables reporting of the status of data channel, monitoring of data throughput, gathering multicast protocol topology information

10.1.2 IPTV Multicast Agent (IMA)

IMA constructs overlay multicast delivery path over physical transport path, and forwards data along the constructed physical transport path. An IMA consists of two functional modules, multicast control module and multicast session control module. The main function of former is to establish multicast delivery path and that of latter to setup multicast session along the paths constructed by multicast session control module. IMA performs the control functions to exchange control messages with other entities. Its major functions are as follows.

- Session join: each IMA contacts with Session Manager
- Session leave: when an IMA wants leave the session, it gives notice to pIMAs and cIMAs
- Session maintenance: relay request and its response will be exchanged between the two IMAs periodically
- Loop detection & avoidance
- Partitioning detection & recovering
- Parent switching
- IPTV Session status reporting

In order to perform service level multicast of IPTV streaming applications, the functional blocks for IPTV service control are shown as Figure 10-1.

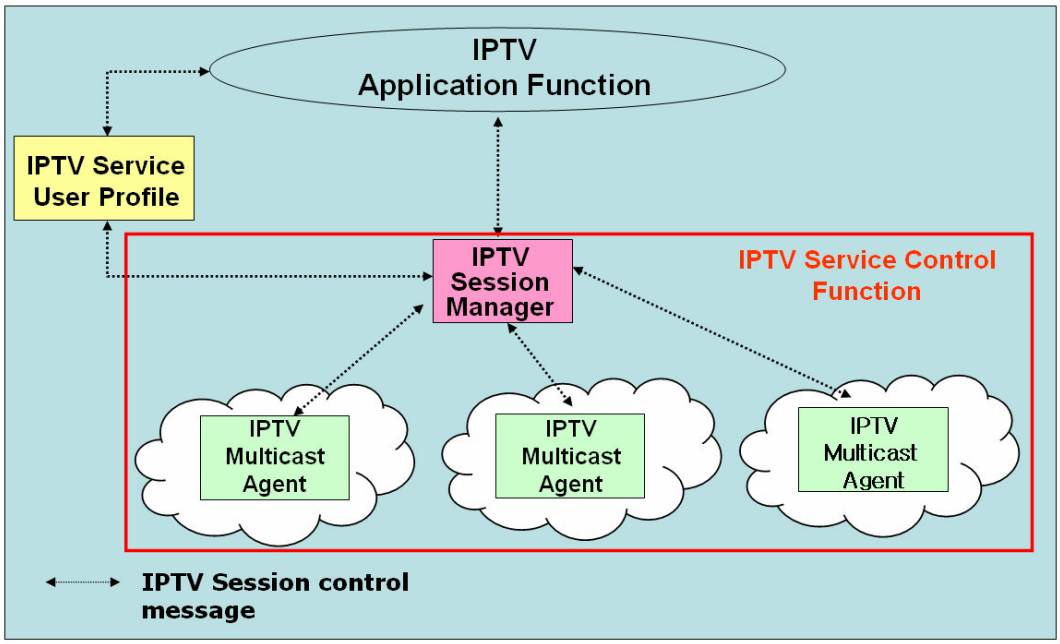


Figure 10-1: Functional blocks of IPTV session control for IPTV application services

10.1.3 IMA Backup

Because data stream will break if IMA goes out of work, it is important to deploy backup function for IMA to guarantee service quality. The following IMA backup selection functions are required:

- IMAs broadcast their load status to other IMAs of multicast overlay.
- IMAs responsible for backup selection select backup IMAs based on the received load status.

10.1.4 Media Signalling Proxy

Media signalling proxy is a function to get media status in overlay multicast network by transfer media connection signalling between end hosts and obtain media session status of end hosts. In order to get media status of overlay multicast network, media signalling proxy is may be supported by IPTV overlay multicast system.

10.2 Functional framework for IPTV overlay multicast

10.2.1 Group membership management

The group membership for IPTV overlay multicast considers group size, number of group member and rate of group membership change. Group membership management function provides the function to create or maintain the multicast groups. If a multicast group in the physical transport network is experiencing serious traffic explosion temporarily, the control function of IPTV overlay multicast will be able to make a global group into multiple sub-groups to avoid the problems.

10.2.2 Admission control for QoS in IPTV overlay multicast network

In order to support QoS for IPTV services in overlay multicast network, resource control function for IPTV overlay network will perform resource management and admission control function in IPTV overlay multicast network.

10.2.3 Security for IPTV overlay multicast

IPTV overlay multicast uses shared network resource and multiple distributed overlay resources to transport data. When a user requests IPTV service, security process needs for IPTV overlay multicast function.

Overlay multicast confronts with various vulnerabilities and risks that impede from being widely deployed in mission critical business systems and applications. There are three important security challenges for the overlay network service model: Confidentiality and Integrity, Authenticity, and Availability. These three important security challenges can be classified with some properties for architectures and algorithms for building secure and scaleable information dissemination services on IPTV overlay networks.

10.2.4 Node functions for IPTV overlay routing

An overlay multicast node function will be designated to perform overlay routing, contents location control and distribution control function for IPTV services. The designated node has full knowledge of other multicast node in the session, information on contents server and distribution control information. In order to keep the updated information on multicast nodes, state updates occur periodically via broadcasting among all multicast nodes.

10.3 QoS control in IPTV overlay multicast network

Resource control function for IPTV overlay multicast provides interface function for IPTV overlay multicast QoS control between physical transport and IPTV overlay network. The function performs collection and management of transport network resource (e.g., DiffServ) via specified interface (e.g. SNMP).

QoS control function in IPTV overlay multicast network will also provide the measurement function of overlay multicast performance to ensure high end-to-end IPTV service quality over IPTV overlay sessions on selected appropriate overlay path. Network measurement includes receiving, measurement and forwarding functions.

- Receiving function receives measurement requests and forwards them to measurement function.
- Measurement function measures network performance between network node and aggregation node or different aggregation nodes based on measurement requests and forwards results to forwarding function which feeds back results to overlay.

Detailed description of QoS control and resource control functions for IPTV overlay multicast are described in Appendix II.

Appendix I

IPTV multicast delivery solutions

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

I.1 Hybrid P2P IPTV service multicast delivery solution

Figure I.1 shows the concept of the Hybrid P2P IPTV service multicast delivery solution.

In this scheme, the receivers join in a multicast group as usual. Then they need to form a P2P group too. When a receiver finds out that he has lost some IP packets, he can send a broadcast message to his peers to request the lost packets. Then the fast response peer can send the lost packets to it. This mechanism needs the receiver to cache some packets in case it needs to retransfer the packets to the peer.

In this model, multicast routers are controlled by SP, so SP can tightly manage the communication. P2P groups do not involve the node of SP, but it is necessary to limit the members in a group because too many peers will aggravate the receivers' burden.

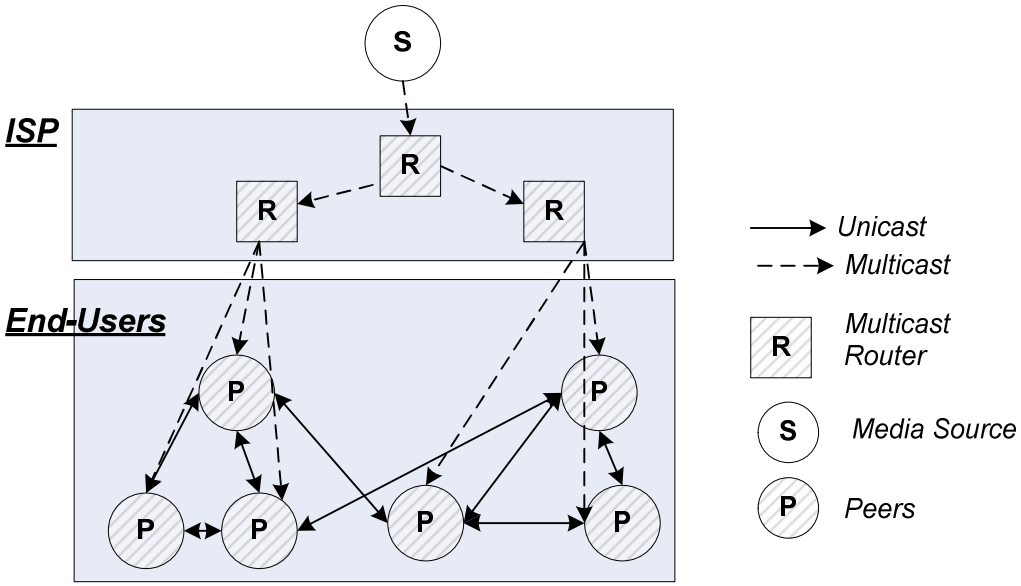


Figure I.1: Hybrid P2P IPTV service multicast delivery

I.2 P2P CDN-based IPTV service multicast delivery solution

Figure I.2 shows a generalized distribution scheme with CDN that have the ability of P2P distribution.

The main problem in this architecture is how to organize CDN servers in SP . In the traditional CDN, it is based on Client/Server technology. Upstream node (i.e. Servers) can forward data to its downstream nodes (i.e. Clients) which is not reversible. Even nodes in the same layer can not exchange data. Nowadays, for the need to improve its high reliability to serve in network, CDN servers can exchange data from each other which even have P2P abilities according to the distribution policy of CDN.

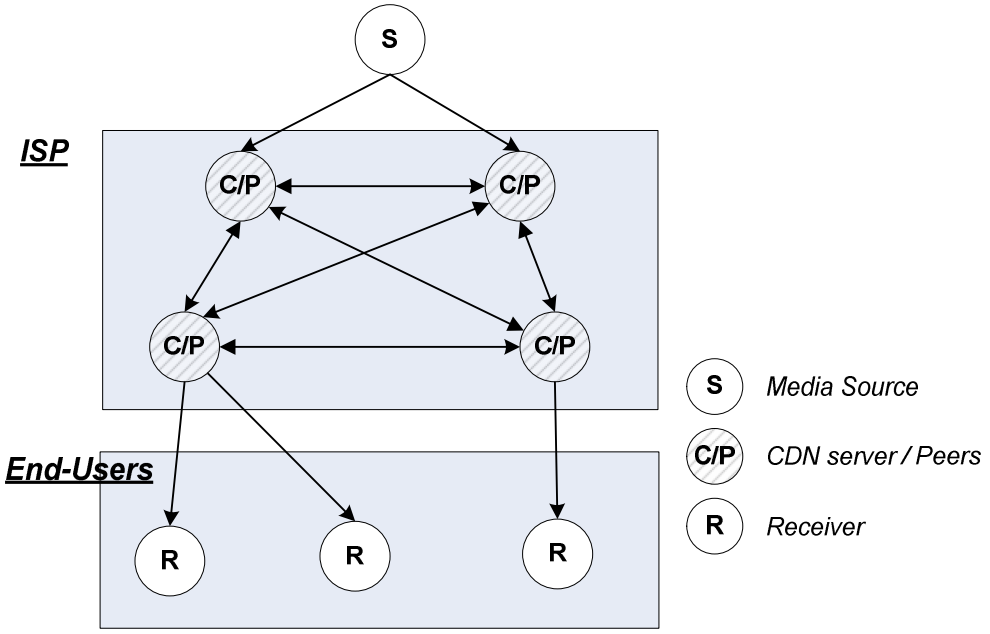


Figure I.2: Data distribution scheme with P2P CDN

Appendix II

QoS and Resource Control Functions for IPTV Overlay Multicast

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

II.1 Resource control function

If the information on IPTV transport networks is directly collected and managed by IPTV overlay nodes to establish overlay transport route and configuration session topology, it will be serious burden to handle overheads in IPTV overlay networks. It is assumed that resource control functions for IPTV overlay network is located between IPTV overlay network and physical transport network, and it performs collection of information about network resource and provides QoS control to transport network.

As shown in Figure II-1 it is necessary that resource control function is introduced to provide interface function for IPTV overlay multicast QoS control between physical transport and IPTV overlay network. This function performs collection and management of transport network resource (e.g., DiffServ) via specified interface (e.g. SNMP). And overlay network nodes create tree topology and optimized route to support QoS requirements of IPTV users through information collected by Resource Control function. And RCF can have the interfaces such as COPS, Diameter and H.248 to install/uninstall the policy decision for transport network. The interface between overlay network and RCF will be further study, and its interface may be proprietary of IPTV service providers.

The requirements for resource control are as follows:

- The Resource Control Function will collect information for resource control from transport network with periodic or a periodic. According to initiation of overlay network nodes, Resource Control function collects data for resource and QoS control.

- Resource control should be able to communicate with Resource Control Function in heterogeneous or other network.
- The following information collected is transferred to overlay network, and then overlay network creates route and optimized tree to support QoS for IPTV overlay network.
  - Link State Information: it includes available bandwidth information, delay, packet loss and jitter of link.
  - Routing Information: it includes routing algorithm that is used to transport network equipments and routing information of them (e.g. neighbour routing information, routing table, etc.).
  - Multicast Traffic Information: it includes multicast traffic parameters (e.g. channel information, type of service, user profile, source content information) per channel or session of IPTV multicast.

II.2 Resource control function for IPTV overlay multicast QoS in wired/wireless/mobile networks.

The Session Manager configures routes among IPTV overlay network nodes and optimizes tree topology for multicast sessions according to information of Resource Control Function. RCF has resource information from transport network such as link state information, routing information, multicast traffic information and so on. Session manager requests the resource information in transport network to RCF. RCF verifies the resource status based on gathered information, and makes the policy decision for the request. Session manager confirms the received message from RCF, and compares with service information. Then session manager sends the policy installing request message to RCF. After receiving the policy request message, RCF sends the policy installing request message to transport network through the configured path for overlay network. Figure II-1 shows the application of Resource Control Function in wired/wireless/mobile networks for IPTV overlay multicast QoS control.

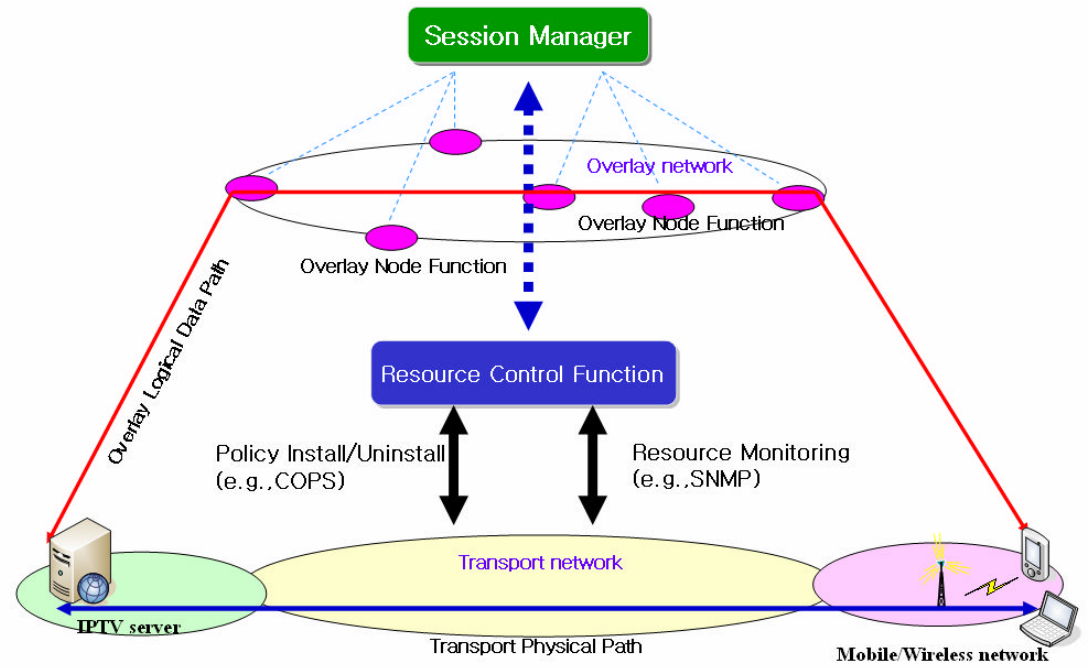


Figure II-1: Application of resource control function in wired/wireless/mobile networks for IPTV overlay multicast QoS control

II.3 Procedure to provide QoS and resource control functions for IPTV overlay multicast

When Session Manger requests information on overlay networking paths to Resource Control Function, and Resource Control Function collects the transport network information using SNMP. Resource Control provides the QoS and resource information of transport networks to Session Manager. In order to compromise the requested requirements on QoS and resource availability of IPTV overlay multicast paths, Session Manager may re-negotiate with Resource Control Function. If the provisioning of Resource Control Function is not satisfied by Session Manager, it is ignored and discarded. Figure II.12 shows procedure to create IPTV overlay multicast service to be with QoS requirements of IPTV overlay multicast paths in IPTV overlay network.

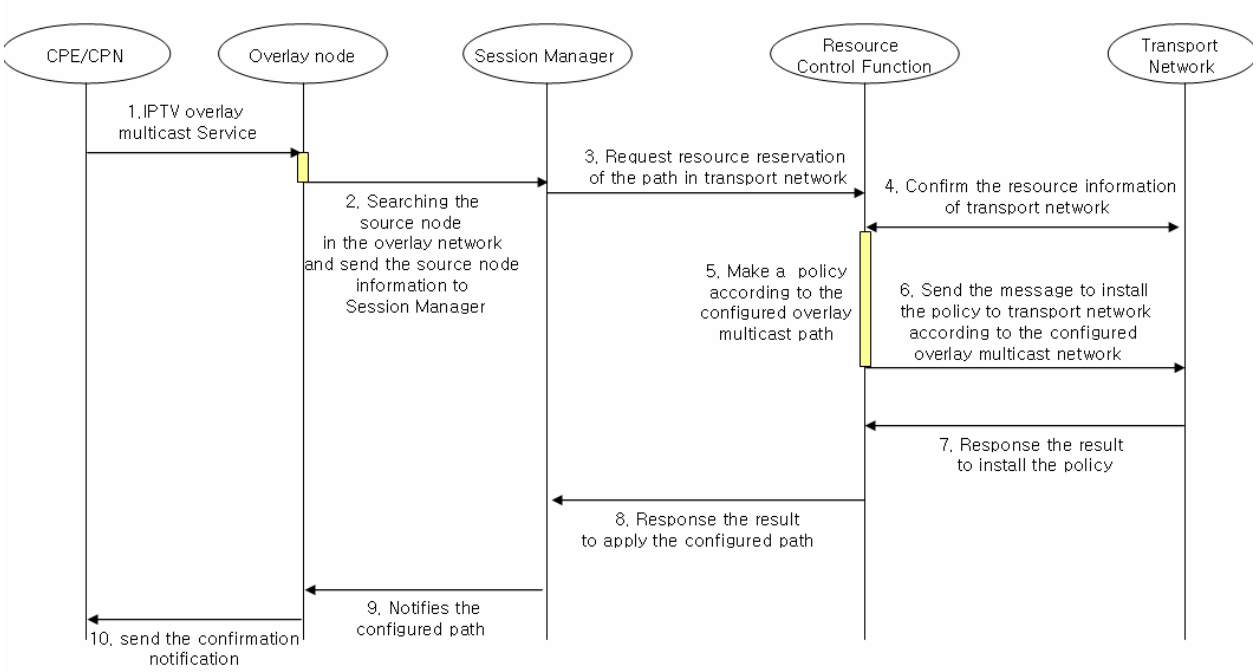


Figure II.2: Procedure to create overlay multicast paths with Resource Reservation and Control in IPTV Overlay Network

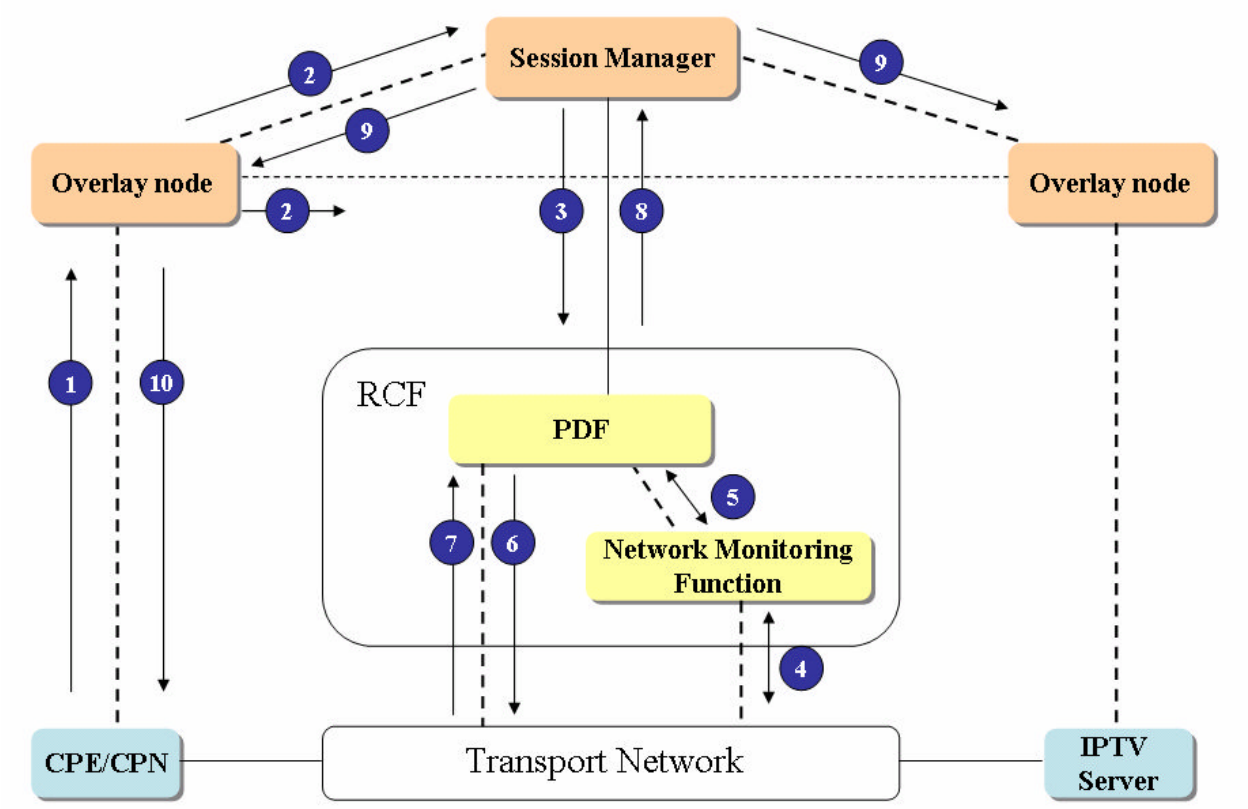


Figure II.3: Procedure to exchange control information for provision of QoS and resource management in IPTV Overlay Network

Figure II.3 shows an example of procedure to exchange control information for provision of QoS and resource management in IPTV Overlay Network (the same procedure of Figure II.2 is likely to Figure II.2). The RCF in IPTV Overlay Network will have similar function with Policy Decision Function. PDF performs control function based on the policies from network provider, service provider or service control function to provide QoS and resource control function to IPTV information delivery path.

The request for resource reservation and QoS control function on physical transport paths, which are mapped with logical paths in IPTV overlay network, is initiated by Session Manager, and delivered to PDF in RCF. PDF installs the policies on physical transport network, and it performs resource control function on the physical paths. The procedures in Figure II.1 and Figure II.2 are as follow.

– When IPTV overlay multicast is requested from CPE/CPN, overlay node search the originating node of contents, and forwards the information of the originating node to Session Manager. (①~②)

– Session Manager requests the Resource Control Function for the paths in accordance with IPTV session and service requirements. (③)

– If the requested requirements are met with the physical transport network, Resource Control Function confirms the resource reservation of the transport network, and applies a policy in accordance with the requests of Session Manager. (④~⑤)

– Resource Control Function sends the message to install the policy to transport network according to configured overlay multicast paths. (⑥~⑦)

– Session Manager notifies the configured path to overlay node and confirmation notification will be sent to the CPE/CPN. (⑨~⑩)

II.4 Network measurement function

In IPTV overlay multicast, the multicast path is constructed between overlay nodes in the application layer to perform media deliver functions. In order to ensure high end-to-end service quality of the IPTV services, overlay multicast measurement system needs to be deployed to measure the IP network performance, e.g. bandwidth, packet loss between overlay nodes such that the appropriate overlay path is selected.

As shown in Figure II-4, as part of resource control, network measurement functions include receiving function, measurement function and forwarding function:

• Receiving function receives measurement requests from session manager and forwards them to measurement function.

• Measurement function measures the network performance between network node and aggregation node or a different aggregation node based on the above measurement requests and forwards the results to forwarding function.

• Forwarding function sends the results to overlay network or other network measurement to share information.

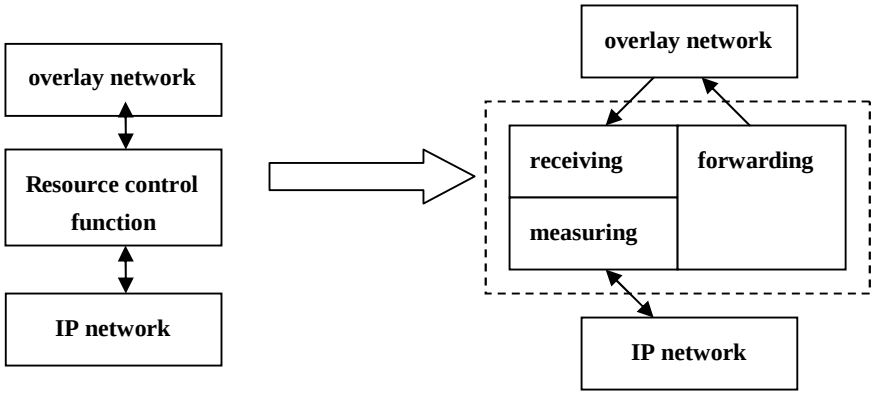


Figure II-4: Network Measurement Functions

Appendix III

Control Framework for IPTV Overlay Multicast

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

III.1 IMA backup

In IPTV overlay multicast, IMA is deployed to control the construction of multicast session and deliver data among the overlay. Data stream will break if IMA goes out of work. So it is important to deploy backup function for IMA to guarantee service quality.

As shown in Figure III-1, nodes of overlay multicast will report its status to others. The report path could be different according to different IMA selection mechanism. For a node (IMA or terminal), report will be transferred to the siblings if backup IMA is selected among siblings or transferred only to PIMA if backup IMA is selected by PIMA. In other scenario, reports will be transferred only to IMA if IMA selects its backup itself or IMAs may even exchange data packets among their siblings to backup each other.

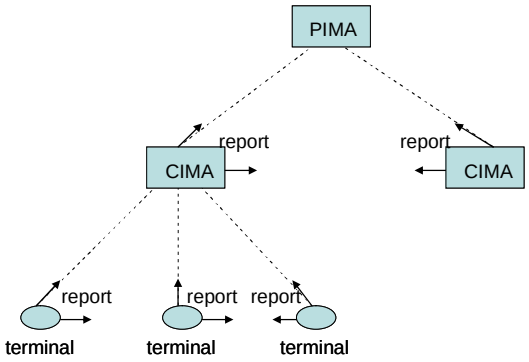


Figure III-1: IMA backup function

Whatever the backup selection mechanism is, following IMA backup selection functions are required:

- IMAs broadcast their load status to other IMAs of multicast overlay.
- IMAs responsible for backup selection select backup IMAs based on the received load status.

III.2 Media signalling proxy

In IPTV overlay multicast, media is connected between end users. If media signalling is directly transferred between end users, IPTV system could not get the exact media connection status to perform related functions such as accounting for each user. It is proposed that media signalling proxy for overlay multicast is located between each two end users to perform media protocol proxy for each two users, hence could report media connection status.

Media signalling proxy is a function to get media status in overlay multicast network by transfer media connection signalling between end hosts and obtain media session status of end hosts.

In order to get media status of overlay multicast network, media signalling proxy is recommended to be supported by IPTV overlay multicast system. Figure III-2 shows how media signalling proxy operates.

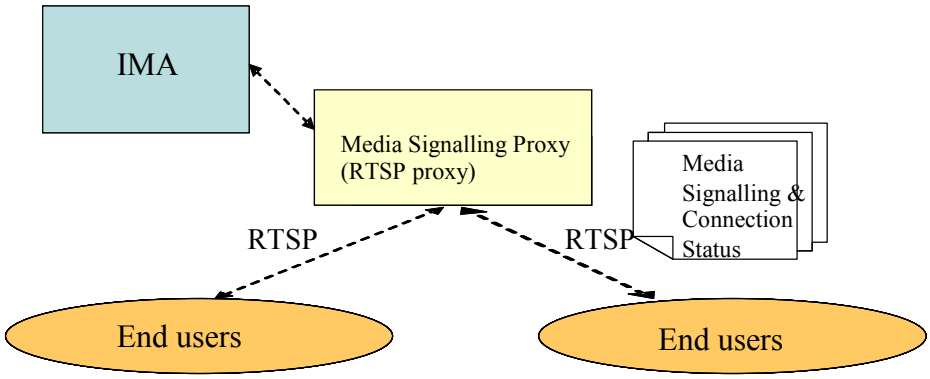


Figure III-2: Media signalling proxy

Appendix IV

A Scenario for Service Control Function of Session Manager in IPTV Overlay Multicast Network

The service control function for IPTV in overlay multicast networking is to provide resource Request/ Release function for IPTV services to Resource Control Function, IPTV service access control function to Resource Control Function, and to request content delivery control function to Content Delivery Control Function of IPTV architecture. In order to provide IPTV service control function, Session Manager in IPTV overlay network performs the following functions:

– Service Resource Request/Release: Session Manger requests resource reservation/release of transport network to create/terminate IPTV overlay session according to IPTV service requirements.

– Service Access Control: Session Manager allows IPTV service access to authenticated IPTV users according to their access rights, subscriber profiles and network policy, etc.

– Request Content Delivery Control Function: Session Manager requests the location of appropriate IPTV content server which can deliver IPTV overlay multicast service to IPTV user.

Session Manager is cooperated with Content Delivery Control Functions and Resource Control Function as shown in Figure IV.1. Content Delivery Control Functions is used to identify appropriate IPTV content server to deliver IPTV overlay multicast service to the IPTV user. Resource Control Function provides resource reservation/release between the IPTV server and IPTV user when Session Manager requests a message to configure and optimize IPTV overlay multicast network. Each functional entity as shown in Figure IV.1 is corresponded with functions of IPTV architecture.

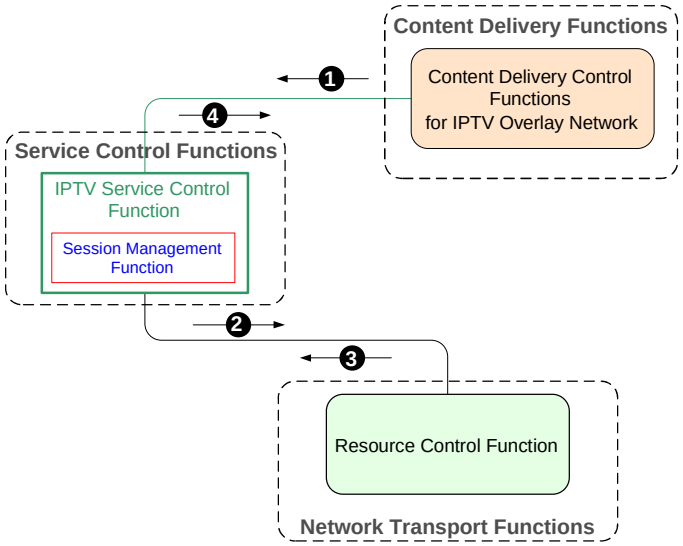


Figure IV-1: Functional entity for IPTV overlay multicast networking

Figure IV.2 shows procedure to perform service control function for IPTV in overlay multicast networking.

– When IPTV overlay multicast service is requested from IPTV user, Content Delivery Control Functions will search appropriate IPTV content server. It forwards IPTV user's request which is contained the location of the IPTV content server and IPTV service requirements to Session Manager. (①)

– Session Manager in IPTV overlay multicast networking derives the IPTV service parameter from the IPTV user's request and it performs authentication between end IPTV user and the IPTV overlay multicast service. Session Manager requests resource reservation of path between the IPTV server and IPTV user to Resource Control Function. (②)

– Resource Control Function reserves optimal delivery path according to IPTV service requirements and network policy after it observes the resource information of transport network. And it sends result of reserved path to Session Manager. (③)

– Session Manager creates/updates the IPTV overlay session according to reserved delivery path by Resource Control Function. It notifies the configured path to Content Delivery Control Functions. Content Delivery Control Functions will update managing IPTV service information according to the result of IPTV overlay session configuration. (④)

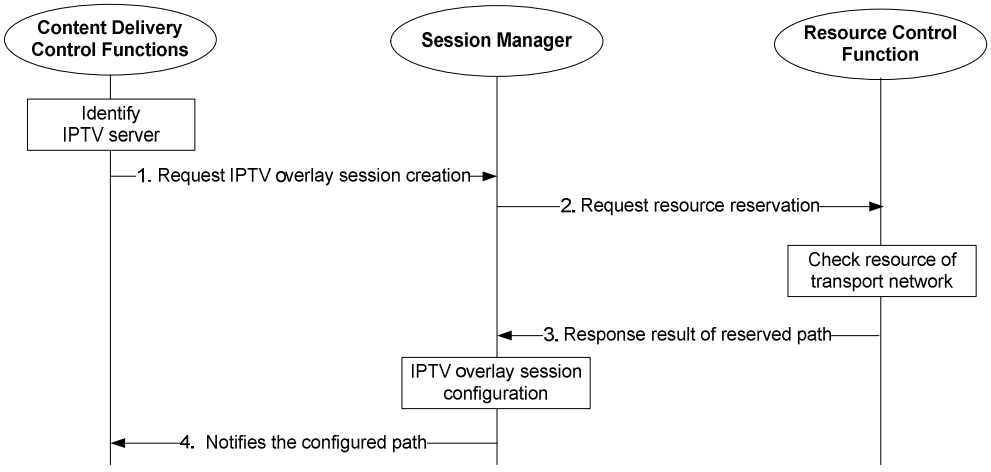


Figure IV-2: Example scenario of service control in IPTV overlay multicast networking

II.4.3 IPTV related protocols

Summary

This document identifies protocols relevant to IPTV services and categorizes these protocols relative to their specific functions in relation to IPTV services.

Keywords

IPTV, Protocol

Current status

This document contains a list of the IPTV related protocols based on inputs from various working groups in the FG. The protocols are categorized according to their specific functions in IPTV services.

Dependency on or relationship to other FG IPTV documents:

- IPTV services requirements
- Quality of experience requirements for IPTV
- Traffic management mechanism for the support of IPTV services
- Application layer reliability error recovery mechanisms for IPTV
- IPTV network control aspects
- IPTV architecture
- IPTV multicast frameworks
- Aspects of IPTV end system – terminal device
- Aspects of home network supporting IPTV services
- IPTV Middleware, Applications, and Content Platforms

CONTENTS

Page

1 Scope 447

2 References 447

3 Abbreviations and acronyms 449

4 Protocols 450

Bibliography 453

IPTV related protocols

1 Scope

This document identifies protocols relevant to IPTV services and categorizes these protocols relative to their specific functions in relation to IPTV services. This document intends to identify and categorize all protocols including end-to-end and access protocols.

NOTE – The list of protocols in this document may not be comprehensive at this stage.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol (UDP)*

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*

[IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol (ICMP)*

[IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol (TCP)*

[IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)*

[IETF RFC 1034] IETF RFC 1034 (1987), *Domain names – concepts and facilities (DNS)*

[IETF RFC 1035] IETF RFC 1035 (1987), *Domain names – implementation and specification*

[IETF RFC 1323] IETF RFC 1323 (1992), *TCP Extensions for High Performance*

[IETF RFC 2018] IETF RFC 2018 (1996), *TCP Selective Acknowledgement Options*

[IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*

[IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*

[IETF RFC 2250] IETF RFC 2250 (1998), *RTP Payload Format for MPEG1/MPEG2 Video*

[IETF RFC 2326] IETF RFC 2326 (1998), *Real Time Streaming Protocol (RTSP)*

[IETF RFC 2373] IETF RFC 2373 (1998), *IP Version 6 Addressing Architecture*

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*

[IETF RFC 2461] IETF RFC 2461 (1998), *Neighbor Discovery for IP Version 6 (IPv6)*

[IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*

[IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*

[IETF RFC 3228] IETF RFC 3228 (2002), *IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)*

[IETF RFC 3265] IETFRFC 3265 (2002), *Session Initiation Protocol (SIP)-Specific Event Notification*

[IETF RFC 3315] IETF RFC 3315 (2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

[IETF RFC 3446] IETF RFC 3446 (2003), *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

[IETF RFC 3513] IETF RFC 3513 (2003), *Internet Protocol Version 6 (IPv6) Addressing Architecture*

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport protocol for Real-Time Applications*

[IETF RFC 3569] IETF RFC 3569 (2003), *An Overview of Source-Specific Multicast (SSM)*

[IETF RFC 3596] IETF RFC 3596 (2003), *DNS Extensions to Support IP Version 6*

[IETF RFC 3611] IETF RFC3611 (2003), *Real Time Protocol Control Protocol Extended Reports (RTCP XR)*

[IETF RFC 3618] IETF RFC 3618 (2003), *Multicast Source Discovery Protocol (MSDP)*

[IETF RFC 3633] IETF RFC 3633 (2003), *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

[IETF RFC 3646] IETF RFC 3646 (2003), *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

[IETF RFC 3736] IETF RFC 3736 (2003), *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*

[IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

[IETF RFC 3913] IETF RFC 3913 (2004), *Border Gateway Multicast Protocol (BGMP): Protocol Specification*

[IETF RFC 4039] IETF RFC 4039 (2005), *Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)*

[IETF RFC 4585] IETF RFC4585 (2004), *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

[IETF RFC 4588] IETF RFC4588 (2005), *RTP Retransmission Payload Format*

[IETF RFC 4602] IETF RFC 4602 (2006), *Protocol Independent Multicast - Sparse Mode (PIM-SM) IETF Proposed Standard Requirements Analysis*

[IETF RFC 4607] IETF RFC 4607 (2006), *Source-Specific Multicast for IP*

[IETF RFC 4608] IETF RFC 4608 (2006), *Source-Specific Protocol Independent Multicast in 232/8*

[IETF RFC 4609] IETF RFC 4609 (2006), *Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements*

[IETF RFC 4610] IETF RFC 4610 (2006), *Anycast-RP Using Protocol Independent Multicast (PIM)*

[IETF RFC 4611] IETF RFC 4611 (2006), *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*

[IETF RFC 4861] IETF RFC 4861 (2007), *Neighbor Discovery for IP version 6 (IPv6)*

[IETF RFC 4862] IETF RFC 4862 (2007), *IPv6 Stateless Address Autoconfiguration*

[IETF RFC 5053] IETF RFC5053 (2007), *Raptor Forward Error Correction Scheme for Object Delivery*

[ETSI TS 102 034] ETSI TS 102 034v1.3.1 (2007), *Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

[ETSI TS 102 471] ETSI TS 102 471 V1.2.1 (2006), *Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Electronic Service Guide (ESG)*

[ETSI TS 102 472] ETSI TS 102 472 (2006), *Digital Video Broadcasting (DVB): IP Datacast over DVB-H: Content Delivery Protocols*

[ETSI TS 102 539] ETSI TS 102 539 V1.1.1 (2006), *Digital Video Broadcasting: Carriage of Broadband Content Guide (BCG) information over Internet Protocol*

[ETSI TS 102 822-3-2] ETSI TS 102 822-3-2 V1.3.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 2: System aspects in a uni-directional environment*

[ETSI TS 102 822-6-1] ETSI TS 102 822-6-1 V1.3.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network; Sub-part 1: Service and transport*

[ETSI TS 102 822-8] ETSI TS 102 822-8 V1.1.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 8: Phase 2 – Interchange Data Format*

[ETSI TS 126 346] ETSI TS 126 346v6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs (3GPP TS 26.346 version 6.2.0 Release 6)*

[OASIS WSBN] OASIS (2006), *Web Services Base Notification 1.3 (WS-Base Notification)*

3 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

AVP Audio-Visual Profile

BCG Broadband Content Guide

BGMP Border Gateway Multicast Protocol

CDP Content Delivery Protocols

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DVB Digital Video Broadcasting

DVB-H Digital Video Broadcasting - Handheld

ESG Electronic Service Guide

ETSI European Telecommunications Sdandards Institute

FEC Forward Error Correction

FLUTE File Delivery over Unidirectional Transport

FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol

ICMP Internet Control Message Protocol

IETF Internet Engineering Task Force

IGMP Internet Group Management Protocol

IP Interent Protocol

IPDC IP Data Cast

IPTV Internet Protocol TeleVision

LC Layered Coding

LCT Layered Coding Transport

MBMS Multimedia Broadcast/Multicast Service

MLD Multicast Listener Discovery
MPEG Moving Picture Experts Group
MSDP Multicast Source Discovery Protocol
OASIS Organization for the Advancement of Structured Information Standards
PIM Protocol Independent Multicast
RFC Request for Comments
RP Rendevous Point
RTCP Real-Time Control Protocol
RTP Real Time Protocol
RTSP Real Time Streaming Protocol
SIP Session Initiation Protocol
SNTP Simple Network Time Protocol
SM Sparse Mode
SSM Source-Specific Multicast
TCP Transmission Control Protocol
TLS Transport Layer Security
TS Transport Stream
UDP User Datagram Protocol
UMTS Universal Mobile Telecommunications System
WSBN Web Services Base Notification

4 Protocols

In support of an IPTV service offering, the following protocols may need to be utilized and supported by different aspects and functions of the IPTV system. Specific protocol support is implementation specific, and the following list is meant to provide a quick reference to protocols that may need to be supported for an IPTV service offering.

Table 4-1: Standards documents which may be used for application layer protocols

Protocol	Document	Document title
DHCP	[IETF RFC 2131]	Dynamic Host Configuration Protocol (DHCPv4)
	[IETF RFC 3315]	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
	[IETF RFC 3633]	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
	[IETF RFC 3736]	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
	[IETF RFC 4039]	Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)
DNS	[IETF RFC 1034]	Domain names – concepts and facilities (DNS)
	[IETF RFC 1035]	Domain names – implementation and specification
	[IETF RFC 3596]	DNS Extensions to Support IP Version 6
	[IETF RFC 3646]	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

Table 4-1 (*end*)

Protocol	Document	Document title
DVB-IPTV	[ETSI TS 102 034]	Transport of MPEG 2 Transport Stream (TS) Based DVB Services over IP Based Networks
FEC	[b_IETF RFC 5052]	Forward Error Correction Building Block
	[IETF RFC 5053]	Raptor Forward Error Correction Scheme for Object Delivery
FLUTE	[b_IETF RFC 3926]	FLUTE – File Delivery over Unidirectional Transport
FTP	[IETF RFC 959]	File Transfer Protocol
http	[IETF RFC 2616]	Hypertext Transfer Protocol – HTTP/1.1
	[IETF RFC 2617]	HTTP Authentication: Basic and Digest Access Authentication
IPDC CDP	[ETSI TS 102 472]	Digital Video Broadcasting: IP Datacast over DVB-H: Content Delivery Protocols
LC	[b_IETF RFC 3450]	Asynchronous Layered Coding Protocol Instantiation
	[b_IETF RFC 3451]	Layered Coding Transport (LCT) Building Block
MBMS	[ETSI TS 126 346]	Universal Mobile Telecommunications System (UMTS); Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs
Metadata	[ETSI TS 102 471]	Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Electronic Service Guide (ESG)
	[ETSI TS 102 539]	Digital Video Broadcasting: Carriage of Broadband Content Guide (BCG) information over Internet Protocol
	[ETSI TS 102 822-3-2]	Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 2: System aspects in a uni-directional environment
	[ETSI TS 102 822-6-1]	Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network; Sub-part 1: Service and transport
	[ETSI TS 102 822-8]	Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 8: Phase 2 – Interchange Data Format
	[OASIS WSBN]	Web Services Base Notification 1.3 (WS-BaseNotification)
RTP	[IETF RFC 2250]	RTP Payload Format for MPEG1/MPEG2 Video
	[IETF RFC 3550]	RTP: A Transport protocol for Real-Time Applications
	[IETF RFC 3611]	Real Time Protocol Control Protocol Extended Reports (RTCP XR)
	[IETF RFC 4585]	Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)
	[IETF RFC 4588]	RTP Retransmission Payload Format
RTSP	[IETF RFC 2326]	Real Time Streaming Protocol (RTSP)
SIP	[IETF RFC 3265]	Session Initiation Protocol (SIP)-Specific Event Notification
SNTP	[b_IETF RFC 2030]	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
TSL	[IETF RFC 2246]	The TLS Protocol Version 1.0

Table 4-2: Standards documents which may be used for transport layer protocols

Protocol	Document	Document title
TCP	[IETF RFC 793]	Transmission Control Protocol (TCP)
	[IETF RFC 1323]	TCP Extensions for High Performance
	[IETF RFC 2018]	TCP Selective Acknowledgement Options
UDP	[IETF RFC 768]	User Datagram Protocol (UDP)

Table 4-3: Standards documents which may be used for network layer protocols

Protocol	Document	Document title
BGMP	[IETF RFC 3913]	Border Gateway Multicast Protocol (BGMP): Protocol Specification
ICMP	[IETF RFC 792]	Internet Control Message Protocol (ICMP)
	[IETF RFC 4862]	IPv6 Stateless Address Autoconfiguration
IGMP	[IETF RFC 2236]	Internet Group Management Protocol, Version 2
	[IETF RFC 3228]	IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)
IP	[IETF RFC 791]	Internet Protocol
	[IETF RFC 2373]	IP Version 6 Addressing Architecture
	[IETF RFC 2460]	Internet Protocol, Version 6 (IPv6) Specification
	[IETF RFC 2461]	Neighbor Discovery for IP Version 6 (IPv6)
	[IETF RFC 3513]	Internet Protocol Version 6 (IPv6) Addressing Architecture
	[IETF RFC 4861]	Neighbor Discovery for IP version 6 (IPv6)
MLD	[IETF RFC 3810]	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
MSDP	[IETF RFC 3618]	Multicast Source Discovery Protocol (MSDP)
	[IETF RFC 4611]	Multicast Source Discovery Protocol (MSDP) Deployment Scenarios
PIM-SM	[IETF RFC 4602]	Protocol Independent Multicast – Sparse Mode (PIM-SM) IETF Proposed Standard Requirements Analysis
	[IETF RFC 4609]	Protocol Independent Multicast – Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements
Anycast-RP	[IETF RFC 3446]	Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
	[IETF RFC 4610]	Anycast-RP Using Protocol Independent Multicast (PIM)
SSM	[IETF RFC 3569]	An Overview of Source-Specific Multicast (SSM)
	[IETF RFC 4607]	Source-Specific Multicast for IP
	[IETF RFC 4608]	Source-Specific Protocol Independent Multicast in 232/8

Bibliography

[b_IETF RFC 2030] IETF RFC 2030 (1997), *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.*

[b_IETF RFC 3450] IETF RFC 3450 (2002), *Asynchronous Layered Coding Protocol Instantiation*.

[b_IETF RFC 3451] IETF RFC 3451 (2002), *Layered Coding Transport (LCT) Building Block.*

[b_IETF RFC 3962] IETF RFC 3962 (2004), *FLUTE – File Delivery over Unidirectional Transport.*

[b_IETF RFC 5052] IETF RFC 5052 (2007), *Forward Error Correction (FEC) Building Block*.

II.5 END SYSTEMS AND INTEROPERABILITY ASPECTS

II.5.1 Aspects of IPTV end system – terminal device

Summary

This terminal device (TD) document outlines functional requirements of the terminal device, capabilities expected to be supported by the terminal device, and the terminal device architecture.

Keywords

IPTV, TD, Terminal Device, STB, ITV, CPE, Set-top box

Current status

All clauses of the document are complete.

Dependency on or relationship to other FG IPTV documents

- IPTV service requirements
- IPTV security aspects
- IPTV architecture
- IPTV middleware, applications, and content platforms
- Service scenarios for IPTV
- Application layer error recovery mechanisms for IPTV
- Toolbox for content coding
- IPTV middleware
- IPTV related protocols
- IPTV network control aspects

CONTENTS

Page

1. Scope 458
2. Reference 458
3. Definitions 461
   - 3.1 Terms defined elsewhere 461
   - 3.2 Terms defined within this document 461
4. Abbreviations and acronyms 462
5. Conventions 464
6. Services supported by the IPTV Terminal Device 465
   - 6.1 Broadcast Services 465
   - 6.2 Electronic Program Guide (EPG) 465
   - 6.3 On-Demand Services 465
   - 6.4 Personal Video Recorder (PVR) Services 466
     - 6.4.1 Client PVR (cPVR) 466
     - 6.4.2 Network PVR (nPVR) 466
     - 6.4.3 Distributed PVR (dPVR) 467
   - 6.5 Advertising Services 467
   - 6.6 Audience Rating Information 468
   - 6.7 Interactive Services 468
     - 6.7.1 Network-based Interactive Services 469
   - 6.8 Public Interest Services 469
     - 6.8.1 Consideration for Accessibility of IPTV Terminal Device 469
   - 6.9 Linear TV with Trick Mode 470
   - 6.10 Personal IPTV Broadcast 470
7. IPTV Terminal Device Functionality and Architecture 471
   - 7.1 Functional Requirements 471
     - 7.1.1 Service Navigation 471
     - 7.1.2 Provisioning and Management 471
     - 7.1.3 IP-based Command and Control Signalling 472
     - 7.1.4 Security 473
     - 7.1.5 Privacy 473
     - 7.1.6 Parental Control 473
     - 7.1.7 Mobility 473
     - 7.1.8 Video 474
     - 7.1.9 Audio 475
     - 7.1.10 Diagnostics 476

Page

7.2 Functional Architecture 476
7.2.1 General functional architecture block diagram 476
7.2.2 IPTV Terminal Device Interfaces 480
7.3 Software Architecture 482
7.3.1 OS/Driver Layer 485
7.3.2 Resource Abstraction Layer (RAL) 483
7.3.3 Middleware and Applications Layer 483
7.4 Protocols 483
7.5 Terminal Device Attachment and Initialization 483
7.5.1 Service Provider Description Entry Points 483
7.5.2 Service Provider Discovery and Service Attachment 484
7.6 Quality Monitoring 484
7.6.1 No-reference methods [ITU-T J.mm-noref] 484
7.6.2 Reduced-reference methods [ITU-T J.mm-redref] 485
7.6.3 Quality monitoring using transmission error information at the head-end [ITU-T J.242] 486
7.6.4 Hybrid perceptual/bit-stream models [ITU-T J.bitvqm] 487

Appendix I – Service Information (SI) 491

Appendix II – Removable Security TD-SM Interface 491

Bibliography 492

Aspects of IPTV end system – terminal device

1 Scope

This document identifies functions needed for the IPTV terminal device (IPTV TD) to support IPTV services. It further provides procedures and sets criteria to verify compliance of IPTV terminal devices to the identified rules and requirements.

2 Reference

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this document 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 document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.790] ITU-T Recommendation F.790 (2007), *Telecommunications accessibility guidelines for older persons and persons with disabilities*

[ITU-T F.902] ITU-T Recommendation F.902 (1995), *Interactive services design guidelines*

[ITU-T G.9951] ITU-T Recommendation G.9951 (2001), *Phoneline networking transceivers – Foundation*

[ITU-T G.9952] ITU-T Recommendation G.9952 (2001), *Phoneline networking transceivers – Payload format and link layer requirements*

[ITU-T G.9953] ITU-T Recommendation G.9953 (2003), *Phoneline networking transceivers – Isolation function*

[ITU-T G.9954] ITU-T Recommendation G.9954 (2007), *Home networking transceivers – Enhanced physical, media access, and link layer specifications*

[ITU-T H.262] ITU-T Recommendation H.262 (2000), *Information technology – Generic coding of moving pictures and associated audio information: Video*

[ITU-T H.264] ITU-T Recommendation H.264 (2005), *Advanced video coding for generic audiovisual services*

[ITU-T J.181] ITU-T Recommendation J.181 (2004), *Digital program insertion cueing message for cable television systems*

[ITU-T J.242] ITU-T Draft new ITU-T Recommendation J.242 (2006), *A method to reconstruct the received video sequence seen at the receiver using transmission error information to monitor the perceptual video quality at the receiver in digital cable television and video telephony*

[ITU-T J.280] ITU-T Recommendation F.280 (2005), *Digital Program Insertion: Splicing application program interface*

[ITU-T J.bitvqm] ITU-T Draft New Recommendation J.bitvqm, *Hybrid perceptual/bit-stream models for objective video quality measurements*

[ITU-T J.mm-noref] ITU-T Draft New Recommendation J.mm-noref, *Perceptual audiovisual quality measurement techniques for multimedia services over digital cable television networks in the absence of a reference*

[ITU-T J.mm-redref] ITU-T Draft New Recommendation J.mm-redref, *Perceptual audiovisual quality measurement techniques for multimedia services over digital cable television networks in the presence of a reduced bandwidth reference*

[ITU-T M.3000] ITU-T Recommendation M.3000 (2000), *Overview of TMN Recommendations*

[ITU-R BT.1361] Recommendation ITU-R BT.1361 (1998), *Worldwide unified colorimetry and related characteristics of future television and imaging systems*

[ITU-R BT.1700] Recommendation ITU-R BT.1700 (2005), *Characteristics of composite video signals for conventional analogue television systems*

[ITU-R BT.2052] Report ITU-R BT.2052 (2006), *Protection of end-users' privacy in interactive broadcasting systems*

[FG IPTV-DOC-0147] FG IPTV-DOC-0147, *IPTV services requirements*

[FG IPTV-DOC-0181] FG IPTV-DOC-0181, *IPTV Architecture*

[FG IPTV-DOC-0182] FG IPTV-DOC-0182, *Service Scenarios for IPTV*

[FG IPTV-DOC-0186] FG IPTV-DOC-0186, *Application layer error recovery mechanisms for IPTV*

[FG IPTV-DOC-0188] FG IPTV-DOC-0188, *IPTV Security Aspects*

[FG IPTV-DOC-0189] FG IPTV-DOC-0189, *IPTV network control aspects*

[FG IPTV-DOC-0191] FG IPTV-DOC-0191, *IPTV Related Protocols*

[FG IPTV-DOC-0194] FG IPTV-DOC-0194, *IPTV Middleware, Applications, and Content Platforms*

[FG IPTV-DOC-0195] FG IPTV-DOC-0195, *Toolbox for Content Coding*

[FG IPTV-DOC-0196] FG IPTV-DOC-0196, *IPTV Middleware*

[FG IPTV-DOC-0197] FG IPTV-DOC-0197, *Service Navigation System*

[ANSI/SCTE-20] ANSI/SCTE 20 (2004), *Method for Carriage of Closed Captions and Non-Real Time Sampled Video*

[ANSI/SCTE-21] ANSI/SCTE 21 (2006), *Standard for Carriage of NTSC VBI data in cable Digital transport streams*

[ANSI/SCTE-127] ANSI/SCTE 127 (2007), *Carriage of Vertical Blanking Interval (VBI) Data in North American Digital Television Bitstreams*

[CEA-608-D] CEA-608-D (2005), *Line 21 Data Services*

[CEA-708-C] CEA-708-C (2006), *Digital Television (DTV) Closed Captioning*

[DSLF TR069] DSL Forum TR069 (2004), *CPE WAN Management Protocol*

[ETSI EN 300 743] ETSI EN 300 743 V1.3.1 (2006), *Digital Video Broadcasting (DVB); Subtitling systems*

[ETSI EN 301 775] ETSI EN 301 775 V1.2.1 (2003), *Digital Video Broadcasting (DVB); Specification for the carriage of Vertical Blanking Information (VBI) data in DVB bitstreams*

[ETSI TS 102 034] ETSI TS 102 034 v1.3.1 (2007) – *Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

[GB/T 20090.2] GB/T 20090.2 (2006), *Information technology – Advanced coding of audio and video – Part 2: Video*

[IEC 60958] IEC 60958 (2006), *Digital audio interface*

[IEC 62360] IEC 62360 (2004-03), *Baseline specifications of satellite and terrestrial receivers for ISDB (Integrated Service for Digital Broadcast)*

[IEEE 1394] IEEE 1394 (1995), *IEEE Standard for a High Performance Serial Bus – Firewire*

[IEEE 802.3] IEEE 802.3 (2002), *Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

[IEEE 802.11] IEEE 802.11 (1997), *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*

[IEEE 802.15.1] IEEE 802.15.1 (2005), *Part 15.1: Wireless MAC and PHY Specifications for Wireless Personal Area Networks (WPANs)*

[IEEE 802.16] IEEE 802.16 (2004), *Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*

[IETF RFC1350] IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2)*

[IETF RFC2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*

[IETF RFC2132] IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*

[IETF RFC2578] IETF RFC 3418 (2002), *Structure of Management Information Version 2 (SMIv2)*

[IETF RFC3411] IETF RFC 3418 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

[IETF RFC3412] IETF RFC 3418 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

[IETF RFC3413] IETF RFC 3418 (2002), *Simple Network Management Protocol (SNMP) Applications*

[IETF RFC3414] IETF RFC 3418 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

[IETF RFC3415] IETF RFC 3418 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

[IETF RFC3416] IETF RFC 3418 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

[IETF RFC3417] IETF RFC 3418 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*

[IETF RFC3418] IETF RFC 3418 (2002), *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

[ISO/IEC DIS 29341] ISO/IEC DIS 29341, *Information technology – UPnP Device Architecture 1.0*

[SMPTE 421M] SMPTE 421M (2006), *VC-1 Compressed Video Bitstream Format and Decoding Process*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Content Tracing [FG IPTV-DOC-0147]: A process to enable the identification of the (arbitrary) origin of content, and/or the responsible party (e.g. the end-user), to facilitate subsequent investigation in the event of unauthorized content copying or distribution.

3.1.2 Home Network (HN) [FG IPTV-DOC-0147]: A communication system designed for the residential environment, in which two or more devices exchange information.

3.1.3 Hybrid terminal device [FG IPTV-DOC-0147]: An IPTV terminal device that can also receive content from different types of transmission systems (e.g. satellite, cable).

3.1.4 IPTV TD [FG IPTV-DOC-0147]: A terminal device which has ITF functionality, e.g. a STB.

3.1.5 IPTV terminal function (ITF) [FG IPTV-DOC-0147]: The functionality that is responsible for processing the content conveyed by the IP transport.

3.1.6 Network personal video recorder (nPVR) [FG IPTV-DOC-0147]: Same as PVR except that the recording device is located at the service provider premises.

3.1.7 Personal video recorder (PVR) [FG IPTV-DOC-0147]: An end-user controlled device that records, stores and plays back multimedia content. PVR is also known as personal digital recorder (PDR).

3.1.8 Terminal device (TD) [FG IPTV-DOC-0147]: A device which typically presents and/or processes the content, such as a personal computer, a computer peripheral, a network appliance, a mobile device, a TV set, a monitor, a VoIP Terminal or an audio-visual media player.

3.2 Terms defined within this document

This document defines the following terms:

3.2.1 Client PVR (cPVR): An instance of PVR, where the end-user terminal device contains the recording capability that can be solicited and operated by end-users to record and store video, audio, and other associated data locally for subsequent playback.

3.2.2 Distributed PVR (dPVR): Multiple instances of PVR, where a combination of cPVRs and nPVRs can be used to record and store video, audio, and other associated data for subsequent playback. For example, this usually occurs within a Home Network containing multiple cPVRs in order to distribute storage of video, audio, and other data.

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

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

3.2.5 IPTV End System (IES): A single or set of consumer devices that support IPTV Services (i.e. everything from Gateway to Display).

3.2.6 **IPTV Network:** An entity encompassing the full group of IPTV Architecture functions expected to be within the Network Provider and Service Provider functional domains.

3.2.7 **Residential Gateway (RG):** A logical element that acts as a bridge between the access network and the home network, providing in premise and aggregated security management, provisioning and addressing services for logical elements within a compliant IPTV Network.

3.2.8 **Watermark:** Machine readable data in the form of a signal embedded in a digital media stream so as to be imperceptible to the consumer, but persistent through faithful transformations of the content. Note that this definition pertains to watermarks in the context of IPTV service and is not a universal definition of a watermark. In the IPTV context, watermarks are used to facilitate Rights Management and media piracy investigation.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

API	Application Program Interface
BC	Broadcasting
BML	Better Markup Language
CAS	Conditional Access System
cPVR	client Personal Video Recorder
DB	Database
DCAS	Downloadable Conditional Access System
DD	Display Device
Demux	Demultiplex
DHCP	Dynamic Host Configuration Protocol
DNG	Delivery Network Gateway
DNS	Domain Name System
dPVR	distributed Personal Video Recorder
DRM	Digital Rights Management
DVD	Digital Video Disc
DVD-R	Digital Video Disc – Recordable
DVI	Digital Video Interface
EAS	Emergency Alert System
ECG	Electronic Contents Guide
EPG	Electronic Program Guide
FEC	Forward Error Correction
GUI	Graphical User Interface
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface

HN	Home Network
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IANA	Internet Assigned Numbers Authority
ID	Identification
IES	IPTV End System
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPG	Interactive Program Guide
IR	Infrared
ITF	IPTV Terminal Function
MIB	Management Information Base
MoCA	Multimedia over Coaxial Alliance
MPEG	Moving Picture Experts Group
Mux	Multiplex
NGN	Next-Generation Network
NTSC	National Television System Committee
NW	Network
nPVR	network Personal Video Recorder
OFDM	Orthogonal frequency-division multiplexing
OS	Operating System
OSD	On-Screen Display
PAL	Phase Alternating Line
PC	Personal Computer
PD	Peripheral Device
PID	Personal Identifier
PIN	Personal Identification Number
PLC	Power-line Communication
POD	Point-of-Deployment
PPV	Pay-Per-View
PVR	Personal Video Recorder
QAM	Quadrature Amplitude Modulation
QoE	Quality of Experience
QoS	Quality of Service
RAL	Resource Abstraction Layer
RAM	Random Access Memory

RCA	Radio Corporation of America
RF	Radio Frequency
RG	Residential Gateway
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
SCP	Service and Content Protection
SECAM	Sequential Colour with Memory
SI	Service Information
SIM	Subscriber Identity Module
SM	Security Module
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
S/PDIF	Sony/Philips Digital Interconnect Format
SSL	Secure Socket Layer
SSM	Source Specific Multicast
STB	Set-Top Box
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TD	Terminal Device
TFTP	Trivial File Transfer Protocol
ToD	Time of Day
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VBI	Vertical Blanking Interval
VCR	Video Cassette Recorder
VoD	Video on Demand
VoIP	Voice over IP
WPAN	Wireless Personal Area Network
WSDL	Web Service Definition Language
XML	Extensible Markup Language

5 Conventions

None.

6 Services supported by the IPTV Terminal Device

The IPTV terminal device (IPTV TD) may support the following services. Furthermore, the IPTV services described in the "Service Scenarios for IPTV" document [FG IPTV-DOC-0182] may also be supported.

6.1 Broadcast Services

The IPTV TD should be capable of decoding and processing digital video streams from the network. Examples of digital video include MPEG-2 [ITU-T H.262], MPEG-4 AVC [ITU-T H.264], AVS [GB/T 20090.2], and VC-1 [SMPTE 421M] based encoding formats. Digital video may include associated digital audio services. Stand-alone audio services may also be offered.

Content may be service-provider or subscriber generated (see sub-clause 6.10 on Personal IPTV Broadcast).

6.2 Electronic Program Guide (EPG)

The IPTV TD should support an electronic program guide (EPG) application selected by the network and/or service operator. The EPG supports all available video and audio services including broadcast, on-demand, time shifted multimedia services (i.e., PVR), and provides utilities that include but are not limited to:

- Available subscriber and service provider content lists
- Search and navigation tools of available content
- Channel and content selection including last channel recall and favourite channel lists
- PVR client recording control including reminders
- Parental control including block by time, channel, ratings, title, and content type
- Services control including enabling and disabling access to pay per view (PPV) content
- Refer to the "IPTV Middleware, Application and Content Platforms" document [FG IPTV-DOC-0194] for Implementation Guidelines of EPG.

6.3 On-Demand Services

The IPTV TD should be able to provide functionality to support on-demand services (as described in the "Service Scenarios for IPTV" document [FG IPTV-DOC-0182]) and should interoperate with the network and service providers' on-demand infrastructure. On-demand enables television viewers to select from an extensive library of content stored on a video server, and have it delivered via the IPTV network. Most on-demand services should allow the viewer to pause, fast forward, and rewind programming, similar to a video cassette recorder (VCR) or digital video disc (DVD). Audio-only on-demand programming and games on-demand should also be supported.

On-demand services available using multiple authorization modes that should be supported include services detailed in the "Service Scenarios for IPTV" document [FG IPTV-DOC-0182].

From the standpoint of the end-user's experience, authorization modes can operate differently depending on the subscriber relationship with the network and service providers. Each offers play, pause, stop, fast-forward and rewind capabilities. Authorization flexibility allows multiple viewing conditions which include the ability to watch any movie, as often as the customer wishes, for a service provider-defined period of time.

6.4 Personal Video Recorder (PVR) Services

It is recommended that the IPTV terminal device be capable of supporting PVR services. The IPTV terminal device should be capable of supporting three envisioned PVR services:

1. Client PVR (cPVR)
2. Network PVR (nPVR)
3. Distributed PVR (dPVR)

While each of the envisioned PVR technologies may be unique, the service that is required to be supported by the IPTV terminal device remains constant to the end-user. In all cases, the end-user can interact with a GUI (such as the EPG or PVR OSD) in order to schedule, modify, playback, erase, etc., recordings.

It is recommended that the PVR service support the ability to:

- Schedule recordings (end-user specified times, channels, etc. or through the use of an EPG)
- Schedule repeating recordings (end-user specified times, channels, etc. or through the use of an EPG – e.g. Record the whole season of a program)
- Display a list of pre-recorded programs/content and a list of upcoming recordings
- Modify pre-existing recordings
- Rank recordings according to priority (higher priority recordings take precedence when recording, over lower priority recordings)
- Play-back pre-recorded programs/content
- Erase pre-recorded programs/content (whether viewed or not)
- Copy pre-recorded programs/content to removable or external local storage devices. Such services are required to ensure that copyright enforcement mechanisms are preserved and that content tracing information is embedded in the copy insofar as required by the content provider.

6.4.1 Client PVR (cPVR)

In the case of Client PVR, the IPTV terminal device contains (or is directly connected to) some sort of storage buffer or memory, such as a hard disk drive (HDD), removable media (e.g. DVD-R), or solid state memory (e.g. Flash RAM). The end-user can interact with the GUI (such as the EPG or PVR OSD) in order to schedule, modify, playback, erase, etc., local recordings.

In the case of Client PVR, all storage is done locally, within the IPTV terminal device or by means of an external storage device connected directly (not through the Home Network) to the terminal device by means of the TD-PD interface described in clause 7.2.2.4.

6.4.2 Network PVR (nPVR)

In the case of Network PVR, the IPTV terminal device does not necessarily contain some sort of storage buffer or memory. Instead, the IPTV terminal device interacts with a network element containing a partitioned storage device (a separate storage allocation for each end-user). The end-user can interact with a GUI (such as an EPG or PVR OSD) in order to schedule, modify, playback, erase, etc., network recordings. All storage is done somewhere within the IPTV Network, with interaction being done by means of a consistent GUI.

The end-user should not be able to recognize the difference between using cPVR or nPVR. The PVR service should function identically, with the only difference being the location of the storage device.

An nPVR implementation would function in much the same way as a VoD implementation, with the primary difference being that each end-user has their own storage allocation within the network element containing the partitioned storage device and that personally recorded content is not available to all end-users.

6.4.3 Distributed PVR (dPVR)

The end-user can interact with a GUI (such as an EPG or PVR OSD) in order to schedule, modify, playback, erase, etc., recordings. All storage is done within the home network on multiple cPVRs or with a combination of multiple nPVRs and cPVRs, with interaction being done by means of a consistent GUI.

As with Network PVR, the end-user should not be able to recognize the difference between using cPVR, nPVR, or dPVR. The PVR service should function identically, with the only difference being the location or distribution of the storage device(s).

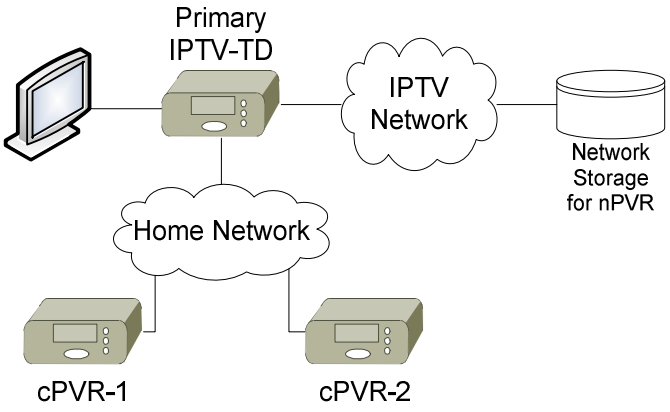


Figure 6-1: Distributed PVR

In Figure 6-1, the "Primary IPTV-TD" implements the PVR service by means of a PVR OSD. The storage may be physically done by the Primary IPTV-TD in combination with one or more cPVRs (connected to the Home Network) or nPVRs (Network Storage in the IPTV Network), or may be done by one or more cPVRs or nPVRs alone, without storage taking place in the Primary IPTV-TD.

6.5 Advertising Services

The IPTV terminal device should be capable of supporting the following advertising services. The "Service Scenarios for IPTV" document [FG IPTV-DOC-0182] details advertising services, and should be consulted for further details on specific service offerings. The following description is meant to call out the specific capabilities that the IPTV TD should contain in order to support the described services.

The IPTV TD should support the functionality to provide the following content insertion services per [ITU-T J.280] and [ITU-T J.181]:

- Digital into Digital advertising includes the capabilities to insert, or splice, one digital program (the ad) into a second digital program (the content being viewed). Insertion should include both video and audio content. The insertion may occur in the headend, the hub, the IPTV TD, or a combination of any to deliver a particular ad to the viewer. Advertising content can be streamed in real time as part of the transport multiplex for a video service, stored in a on-demand ad insertion system, or available in the hard drive of a PVR capable IPTV TD and streamed to the IPTV TD across the home network. The IPTV TD should support seamless splicing of ads in all supported formats from any supported source into a video stream as it is being displayed.

- Targeted (geographic grouping) and addressable (demographic grouping) advertising delivers a particular ad to a more targeted audience of viewers. This is normally accomplished by putting multiple ads into the same digital stream multiplex and the IPTV TD selects which ad to present to the viewer based on tagging data on the ads and information present in the IPTV TD.
- Interactive advertising provides the ability for the subscriber to interact with the advertisement using the remote control to, for example, request a coupon or additional information.
- In an SCP protected video stream, splicing of content may not be appropriate. Advertisement insertion can be accomplished via alternative methods, for example, overlay.

6.6 Audience Rating Information

Audience rating information is the channel transition information indicating when a client watches a TV program. Ideally, this information consists of channel number before and after channel change, time of change, and user information (e.g. a Unique Identifier). With audience/user permission, information can be collected at several points, such as terminal device (STB, PC, TV, etc.), home gateway and network component. As the IPTV Network is used for TV service in IPTV, the home gateway and/or network component may also detect channel transition information by monitoring IP packets between terminals and network.

The IPTV Network is used to upload the collected information to the content distribution side at predetermined timing intervals. Figure 6-2 shows the outline of audience rating system on IPTV.

Refer to clause 7.1.5 and [ITU-R BT.2052] for issues relating to privacy of audience rating information.

In typical use cases, audience rating information is applied to a multicast or broadcast service.

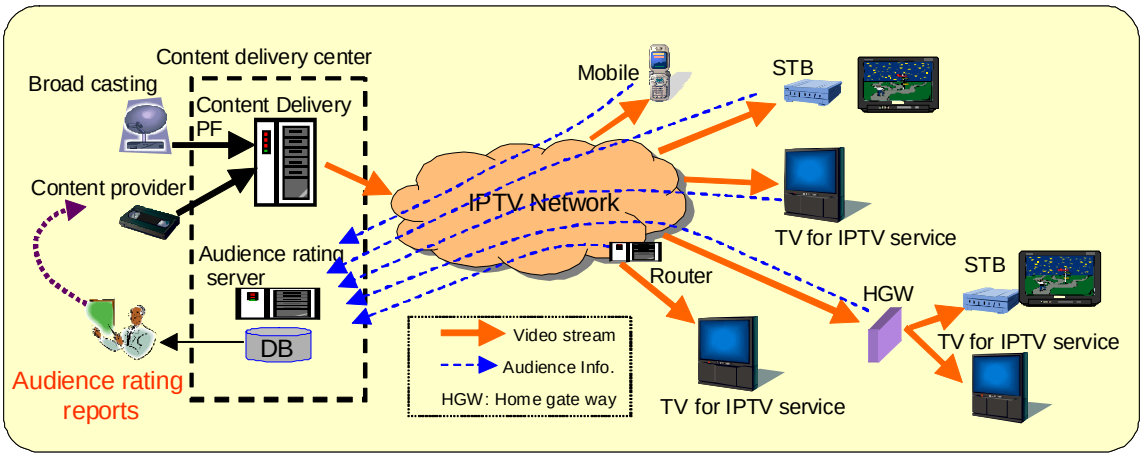


Figure 6-2: System architecture of audience rating system

6.7 Interactive Services

The IPTV TD should support network-based and client-based interactive services/applications, as described in the "Service Scenarios for IPTV" document [FG IPTV-DOC-0182]. These services are supported by the IPTV TD at the application layer. The IPTV TD should provide resource capacity, including processing and memory, to provide an interactive user experience.

6.7.1 Network-based Interactive Services

Access to Web Browsing Services is a recommended feature of any IPTV terminal device. Giving the end-user the ability to interact with the World Wide Web through the IPTV terminal device will enable to end-user to customize their experience and will provide him/her with a fully interactive experience. The IPTV TD should have the ability to communicate with the remote interactive content server via channels that are analogous to HTTP or HTTPS protocols. A web browser (presentation engine) included at the application layer would allow the presentation of interactive content using standard languages such as HTML and BML.

It may also be possible to present the end-user with applications such as an EPG, VoD OSD, or PVR OSD through a web browser interface, with the interface (EPG, OSD, etc.) being hosted by a remote location on the Internet.

Access to Web Services by interactive TV applications is expected to be an important service offering by an IPTV terminal device. Examples might include display of information tickers, such as weather and stock quotes, content ratings or descriptions, and maps.

For the purposes of the IPTV functional model, a web service is a data source accessible over the Internet though a well known interface. Several technologies exit for exposing a web service interface, an example being the use of a protocol such as Simple Object Access Protocol (SOAP).

TV application access to web services may utilize internet connection capabilities, such as TCP/IP and sockets. Higher level protocol support, such as SOAP, may be provided as an option. It is for further study as to what higher level protocols may be used on specific interfaces for web service support within the IPTV functional model, but a few potential supporting protocols include HTTP, XML, SOAP, and WSDL.

6.8 Public Interest Services

The IPTV TD should support needed community and accessibility services required by the local customer-base or regulations, for example:

- Emergency alert system (EAS)
- Closed caption, subtitles, audio description and sign language interpretation
- Real-time text communication between users of the system, if applicable

For further information, refer to the Telecommunications Accessibility Guidelines [ITU-T F.790]. Further references dealing with accessibility can be found in the bibliography, which includes pointers to the Telecommunications Accessibility Checklist.

6.8.1 Consideration for Accessibility of IPTV Terminal Device

To facilitate the concerns of people with needs outside the majority population, the following functionalities are recommended:

- The ability to transmit the captions through an external interface on the terminal.
- The ability to select and receive two (related) video sources (e.g. one with sign language translation).
- The methods for activating and deactivating captioning, extra video source and extra audio source should be easy to use and should not incur an excessive delay.

- Result of the use of the controls is recommended to be available in the form of voice output.

- Any on-screen display (OSD) facilities for control of the terminal and the programs are recommended to be easy to read and not difficult to understand.

- Any on-screen display (OSD) facilities are recommended to also be available via external interfaces and also be able to control the capability to transmit captions and information provided by on-screen display facilities to conform to the assigned content protection. For further information, refer to the Telecommunications Accessibility Guidelines [ITU-T F.790]. Further references dealing with accessibility can be found in the bibliography, which includes pointers to the Telecommunications Accessibility Checklist.

6.9 Linear TV with Trick Mode

In order to support a linear TV with trick mode service, as described in the "Service Scenarios for IPTV" document [FG IPTV-DOC-0182], the IPTV TD should have the following capabilities:

- provide the interface for user to access the contents without time limitation, including pause, rewind, fast forward, and etc.;

- provide the interface for user to enable or disable the service of TV with trick mode;

- provide the interface to set the expiration time.

Functional support for linear TV with trick mode is detailed in the "IP-based Command and Control" sub-clause 7.1.3, below.

6.10 Personal IPTV Broadcast

The personal IPTV broadcast service is described in the "Service Scenarios for IPTV" document [FG IPTV-DOC-0182]. For a personal IPTV broadcast scenario, the terminal device can play a role as content source or head-end. Some portion of both capabilities is needed within the IPTV TD in order to support the scenario.

- IPTV terminal device can optionally support A/V capturing capability

    - The end-user can generate a content source with their IPTV terminal device. The IPTV TD can be a mobile device with embedded camera, a PC with capability of capturing A/V being locally played out, or any other devices that support A/V input interfaces

- IPTV terminal device can optionally support A/V encoding capabilities

    - For an IPTV terminal device with low processing power, at least low-bandwidth encoding profile (e.g., MPEG2 simple profile, H.264 AVC Baseline profile) is required. For higher processing power IPTV terminal devices, a better-quality encoding profile may be applied.

- IPTV terminal devices can optionally have streaming protocols for real-time transmission of content (e.g., RTP/RTCP)

- There are security aspects associated with broadcasting of customer-generated content.

7 IPTV Terminal Device Functionality and Architecture

7.1 Functional Requirements

7.1.1 Service Navigation

The IPTV TD should support service navigation functionality. Service navigation can be through the use of, for example, HTML data, XML data or Service Information (SI), detailed in Appendix I. The "Service Navigation System" document [FG IPTV-DOC-0197] should be consulted for more details. The IPTV TD should provide appropriate functionality and mechanisms to utilize Service Navigation as described in the "Service Navigation System" document [FG IPTV-DOC-0197], one such mechanism is described as an EPG in clause 6.2 above.

7.1.2 Provisioning and Management

Provisioning and Management support is recommended to include:

- Dynamic and static provisioning of the IPTV TD (STB, Media Adaptor, etc.).
- Common provisioning changes should not require reboot of the IPTV TD.
- Remote operation of the IPTV TD.
- Dynamic assignment and management of IP addresses for subscriber devices.
- Ensuring that real-time provisioning and configuration of software does not adversely affect subscriber service.
- Defining additional MIB modules for managing customer IPTV TD using the IETF network management framework or ITU-T related methods.

The IPTV TD is recommended to support mechanisms for provisioning and management, such as:

- ITU-T M.3000 series for telecommunications management network [ITU-T M.3000]
- DHCP [IETF RFC2131], [IETF RFC2132]
- TFTP [IETF RFC1350]
- Time of Day (ToD)
- UPnP [ISO/IEC DIS 29341]
- DSLF TR069 [DSLF TR069]
- SNMPv2/v3 [IETF RFC2578 / IETF RFC3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418]

The IPTV TD is recommended to use well established industry standard protocols for provisioning and management.

7.1.2.1 Device Configuration and Control

The IPTV TD should support configuration and control messages transmitted by the head-end controller to the IPTV TD for the purpose of setting the network address, assigning streams to specific packet identifier (PID) processors, activating/deactivating certain features of the interactive user guide and/or console interface, setting time zone information, clearing a customer personal identification number (PIN), or resetting the IPTV TD.

7.1.2.2 Code Download

The IPTV TD should support code download and upgrade capability via the remote download interface using multicast or unicast.

The code downloaded to the IPTV TD may be classified into three types: firmware, middleware, and conditional access code.

7.1.2.3 Polling and Report-back

The IPTV TD should support Polling and Report-back messages from the head-end controller to poll the IPTV TD for purchase information as well as diagnostic and configuration information. Purchases may be retrieved by the controller and passed on to the billing system. The process of collecting IPTV TD report-backs is initiated and managed by the head-end controller or may be initiated by the IPTV TD in the form of an "unsolicited report-back"

7.1.3 IP-based Command and Control Signalling

Signalling and Control includes:

- A preferred signalling architecture for establishing new sessions, modifying existing sessions, and tearing down sessions.
- Feature capabilities of the selected signalling protocol(s), including channel change and trick-mode (VCR) operation including pause, rewind, fast forward, resume, and stop.

The following are standard mechanisms for IP-based Command and Control of video services:

- RTSP for Unicast content

  The IPTV TD is required to support RTSP for the delivery of unicast on-demand content or for the support of linear TV with trick mode (described in clause 6.9), and the remote control of a streaming media server. A session ID is used to keep track of sessions, this way no permanent TCP connection is required. RTSP messages such as "describe", "setup", "play", "pause", "record", and "teardown" are sent from the IPTV TD to the streaming media server for controlling the delivery of the selected media stream.

  Assuming that the IPTV TD supports AL-FEC [ETSI TS 102 034], Annex E as described in clause 7.2.1.13 and the "Application layer error recovery mechanisms for IPTV" document [FG IPTV-DOC-0186], is used, additional options within the transport header are defined for Application Layer FEC in [ETSI TS 102 034] clause 6.3.2.2, to specify the addresses, ports, and parameters of the FEC layers.

- IGMP for Multicast content

  Assuming that the IPTV TD supports IGMPv3 and that SI info supports IP transmission as described in clause 7.1.1, the IPTV TD uses multicast destination address and/or the Source IP address (if using Source Specific Multicast – SSM) in SI to join (using) the appropriate multicast flow transporting the content requested from the end-user.

  Assuming that the IPTV TD supports AL-FEC [ETSI TS 102 034], Annex E as described in clause 7.2.1.13 and the "Application layer error recovery mechanisms for IPTV" document [FG IPTV-DOC-0186], the IPTV TD uses the multicast destination address and/or the source IP address (if using Source Specific Multicast – SSM) in SI to join the appropriate multicast flow transporting the FEC layer(s) requested from the end user.

In order to support the linear TV with trick mode service (described in clause 6.9) using local buffer/storage, the IPTV TD should have a buffer capability for caching content for subsequent end-user control of playback.

7.1.4 Security

There are many security concerns and requirements that are addressed to and should be supported by the IPTV TD. The "IPTV Service Requirements" document [FG IPTV-DOC-0147] should be consulted for a detailed list of security requirements placed on the IPTV TD. Furthermore, the "IPTV Security Aspects" document [FG IPTV-DOC-0188] should be consulted for detailed security related issues directly affecting an IPTV system.

The IPTV TD should support SCP functionality, possibly consisting of renewable security means, detailed below in clause 7.2.1.3 and 7.2.1.14, respectively.

In all cases, the IPTV TD is required to securely make known to the content source, its SCP capabilities, and ensure that SCP means required by the content provider are present and operable, prior to descrambling a content item.

7.1.5 Privacy

There are many privacy concerns and requirements that are addressed to and should be supported by the IPTV TD. The "IPTV Service Requirements" document [FG IPTV-DOC-0147] should be consulted for a detailed list of privacy requirements placed on the IPTV TD. Furthermore, the "IPTV Security Aspects" document [FG IPTV-DOC-0188] should be consulted for detailed privacy related issues directly affecting an IPTV system.

An IPTV terminal device can be a major source of private information. The following are examples of items that should be kept private within the IPTV TD:

- Viewing history
- Return/interaction channel usage and Audience Rating Information
- History of interactive operation
- Personal profiles and preferences
- ID number

In some interactive broadcast systems, the ID number is used for the purpose of content copy control even in free-to-air services. [ITU-R BT.2052].

Audience Rating Information requires privacy aspects to protect the user/audience identity, such as by encrypting the user's unique identifier (e.g. MAC or IP Address).

NOTE – The "IPTV Security Aspects" document [FG IPTV-DOC-0188] details security and privacy related concerns that may affect an audience rating information service, and should be consulted for more details.

7.1.6 Parental Control

Parental locks are applied by an application to prevent access to content unless authorized.

7.1.7 Mobility

In case an IPTV TD is mobile, it is recommended to support mobility functionalities for service continuity when in motion.

An optional signalling architecture for exchanging wireless network characteristics between an IPTV TD (mobile device) and DNG (or Service Provider Server). It allows DNG (or Service Provider Server) to adjust their sending rate for ongoing video service according to the received information (e.g., bandwidth, packet loss, etc.) from the IPTV TD. Piggybacking the information on the existing IP based Protocol is available.

7.1.8 Video

7.1.8.1 Video Formats

The IPTV TD is expected to support commonly used video formats, an exemplary list of which can be found in the "Toolbox for Content Coding" document [FG IPTV-DOC-0195], which should be consulted for specific video format support. The IPTV TD should enable the reception and display of the video formats required by the "Toolbox for Content Coding" document [FG IPTV-DOC-0195].

Colorimetry of video signals is required to be in compliance with [ITU-R BT.1361] in all video formats.

The document titled "Toolbox for Content Coding" [FG IPTV-DOC-0195] defines codecs to be used in video processing.

The IPTV TD should be capable of displaying video and graphics output at the standard NTSC, PAL, and SECAM video resolutions interlaced on the Composite and S-Video outputs.

IPTV TDs that support high definition outputs should be capable of displaying video and graphics output on Component and HDMI outputs. The IPTV TD should be capable of converting a chosen specified input decoded picture source format/resolution to a chosen output format/resolution through a combination of video scaling and de-interlacing. IPTV TDs that support high definition outputs should provide native mode video output support so that it automatically changes output resolution formats to match the broadcast format.

7.1.8.2 Video Codecs

The IPTV terminal device is required to handle (decode/encode) the digital transport streams recommended or required in accordance with the "Toolbox for Content Coding" document [FG IPTV-DOC-0195]. The "Toolbox for Content Coding" document [FG IPTV-DOC-0195] should be consulted for specific video codec support. The IPTV terminal device should enable the reception and display of the video using the codecs required by the "Toolbox for Content Coding" document [FG IPTV-DOC-0195].

7.1.8.2 Video Processing

The IPTV TD should support the following video processing features:

- Independent horizontal and vertical scaling ranging from 1/32 (downscaling) to 32 (upscaling)
- De-interlacing
  - 3:2 pull-down cadence detection
  - Reverse 3:2 pull-down detection and filtering
- Digital noise filtering
- Edge enhancements

Video outputs (RF and baseband) should conform to accepted international standards.

The IPTV TD should support the scaling of a video source for display. In particular, the IPTV TD is recommended to support this functionality due to potential restricted capabilities.

7.1.8.3 VBI Data Processing

The IPTV TD should be capable of passing through, extracting, decoding and rendering vertical blanking interval (VBI) lines carried in an encoded content stream and should make the VBI data available to the operating system and applications for processing.

The IPTV TD may support the following closed captioning standards and VBI capabilities such as: [ANSI/SCTE-20], [ANSI/SCTE-21] and [ETSI EN 301 775] (modified by [ANSI/SCTE-127]), [CEA-608-D], and [CEA-708-C].

In the event both [ANSI/SCTE-20] and [ANSI/SCTE-21] closed captions are present simultaneously, the preference is to select [ANSI/SCTE-21] closed captioning data.

In support of legacy standards, an IPTV terminal device should be capable of decoding closed caption, teletext, or subtitles traditionally present in VBI Data, which are instead carried in the IP multimedia stream and re-creating as VBI signals. Correct timing and formatting of such information should be maintained.

NOTE – This is one possible means of delivering closed captions to the IPTV terminal device, although other methods are available (e.g. [ETSI EN 300 743]).

7.1.9 Audio

7.1.9.1 Audio Formats

The IPTV TD is expected to support commonly used audio formats, an exemplary list of which can be found in the "Toolbox for Content Coding" document [FG IPTV-DOC-0195], which should be consulted for specific audio format support. The IPTV TD should enable the reception of the audio formats required by the "Toolbox for content coding" document.

Some exemplary audio formats that the IPTV TD may support include:

- 5.1 channel audio
- 2 channel audio

The IPTV terminal device may be capable of performing audio transcoding on output audio signals. The process of transcoding implies the implementation of the respective decoder (if a single codec is used) or decoders (if two codecs are requested) in the IPTV terminal device. This gives IPTV operators the possibility to avoid simulcasting stereo and multi-channel streams. With the decoder in place, the IPTV terminal device may feature a downmix from multi-channel to stereo for either all devices or at least those which are not offering the transcoding feature, respectively S/PDIF interface.

The IPTV TD should be capable of responding to user preference for adjusting Dolby digital audio dynamic range compression. The IPTV TD should be capable of supporting user or network selection among a minimum of three levels of audio dynamic range compressions: uncompressed, intermediate and heavy

For specific interface requirements, see the "TD-OD and TD-PD" clause 7.2.2.4.

7.1.9.2 Audio Codecs

The IPTV TD is required to handle (decode/encode) the digital transport streams recommended or required in accordance with the "Toolbox for Content Coding" document [FG IPTV-DOC-0195]. The "Toolbox for Content Coding" document should be consulted for specific audio codec support. The IPTV terminal device should enable the reception of audio using the codecs required by the "Toolbox for Content Coding" document.

7.1.10 Diagnostics

The IPTV TD should provide diagnostic information about its configuration and operation both locally using on-screen display (OSD) graphics and over the network. The intent of the IPTV TD related diagnostics is to provide a mechanism for identifying the IPTV TD's operational state such that any IPTV TD or network issue can be quickly understood and resolved, preferably remotely.

The IPTV TD diagnostics are split between an IPTV diagnostic application and an IPTV TD client software diagnostic component. The IPTV diagnostic application should implement the diagnostic screens. On-screen display (OSD) for diagnostics should be available regardless of the state of the network or any application.

Support for the following requirements should be provided by the diagnostics:

1. The IPTV TD should support the following fault management requirements:
   - Fault management requirements specified by the network and service providers
   - Event notifications
2. The IPTV TD should support remote diagnostics as specified by the network and service providers.

7.2 Functional Architecture

7.2.1 General functional architecture block diagram

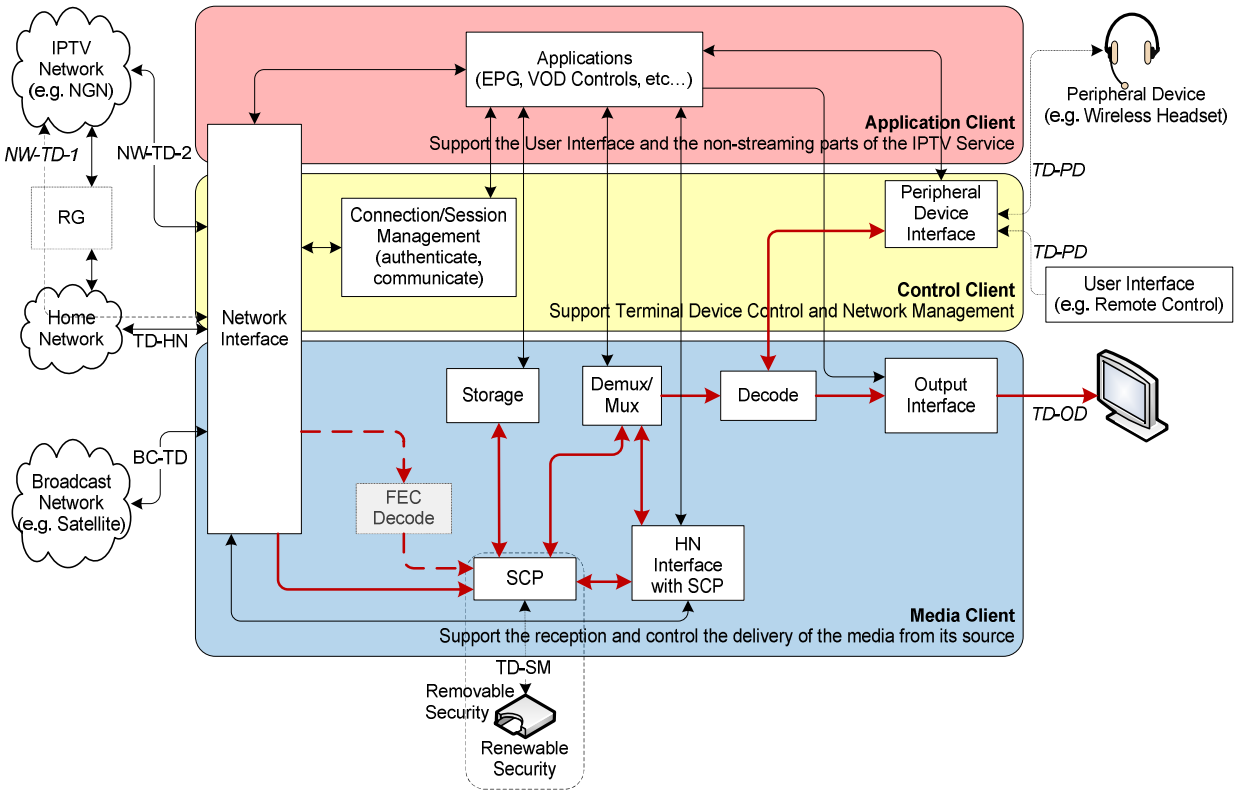


Figure 7-1: Functional Architecture Block diagram of IPTV terminal device

A brief explanation of each component/functional entity in Figure 7-1 is presented below:

7.2.1.1 RG (Residential Gateway):

1) A logical element that acts as a bridge between the access network (within the IPTV Network) and the home network.
2) Provides in-premise and aggregated security management.
3) Provides provisioning and addressing services for logical elements within a compliant IPTV Network.

7.2.1.2 Network Interface:

The Network Interface functional entity includes the following functions:

1) Send and receive signals.
2) Processing of layer 2 functions.
3) Processing of IP packets.
4) Processing of TCP/UDP packets.
5) Handling of the control flows.
6) IPTV terminal device attachment and initialization process.
7) Management and reception of content over the BC-TD interface described in clause 7.2.2.1, "BC-TD", for the connection to a broadcast network (e.g. Satellite, Terrestrial, Cable).
8) Management and reception of content over the NW-TD interface described in clause 7.2.2.2, "NW-TD", for the connection to the IPTV Network (e.g. NGN).

7.2.1.3 SCP:

The SCP functional entity includes the following functions:

1) Handling of authentication mechanisms including key exchange and processing.
2) Creation of content tracing information to be bound to the content, if required by the content provider.
3) Embedding of content tracing information, or enforcing subsequent embedding of content tracing information, if required by the content provider.
4) Processing of SCP entitlement issues.
5) Descrambling of input stream.
6) SCP can optionally be a software implementation (e.g. Downloadable).
7) See the Renewable Security clause 7.2.1.14.

7.2.1.4 Demux/Mux:

The Demux/Mux functional entity is responsible for the following functions:

1) De-multiplexing of video, audio, and data streams.
2) May include Re-multiplexing functionality to combine video, audio, and/or data streams, for potential distribution over the Home Network.
3) Embedding of content tracing information if required by the content provider and not done previously (see 7.2.1.3).

7.2.1.5 Decode:

The Decode functional entity is responsible for:

1) Decoding the compressed video and audio streams.

2) Decoding textual data i.e. closed caption.

3) Embedding of content tracing information if required by the content provider and not done previously (see 7.2.1.3, 7.2.1.4).

7.2.1.6 Output Interface:

1) The Output Interface functional entity is responsible for the TD-OD interface which is described in Clause 7.2.2.4, "TD-OD and TD-PD".

2) The Output Interface is responsible for handling graphics overlay and OSD for applications.

3) If the IPTV TD includes display functionality, the interface for an external display device is optional.

7.2.1.7 HN Interface with SCP:

1) The HN Interface entity is responsible for managing the TD-HN interface described in Clause 7.2.2.3, "TD-HN".

2) Encryption and decryption of content streams for storage, display, and propagation to home network.

3) Transferring applicable SCP rights/privileges throughout the home network.

4) The HN Interface is optional.

7.2.1.8 Storage:

1) The Storage entity is responsible for the caching/storage of content and other application data.

2) The Storage entity may be implemented internally or externally (i.e. by means of the TD-PD interface).

3) The Storage entity is optional.

7.2.1.9 Applications:

1) Applications include the software components capable of enabling functional and observable behaviour, such as the GUI, EPG, VoD Controls, and other service related applications.

2) Some applications are responsible for basic management of the IPTV TD, such as power management and event management.

3) Some applications are responsible for supporting services, including but not limited to SCP applications, plug-in applications, browser applications, media player applications, and graphical user interface (GUI) applications.

7.2.1.10 Peripheral Device Interface:

1) The Peripheral Device Interface is responsible for interaction between the user devices and the appropriate applications.

2) The Peripheral Device Interface receives input from any number of desired peripheral devices (e.g. Remote Control, Wireless Headset) in order to provide bi-directional interaction between the end-user and the IPTV TD.

3) The Peripheral Device Interface functional entity is responsible for the TD-PD interface which is described in Clause 7.2.2.4, "TD-OD and TD-PD".

7.2.1.11 User Interface:

1) A user interface is a combination of software and hardware components through which a user can interact with the user input functional entity [ITU-T F.902]. It can manifest itself in such forms as:
   - A remote control
   - A keyboard

2) The user interface is recommended to support a minimum set of input events, as described in the "IPTV Middleware" document [FG IPTV-DOC-0196].

7.2.1.12 Connection/Session Management:

1) The Connection/Session Management functional entity is responsible for authentication, communication, and management of the connection to the IPTV server through the IPTV Network (i.e. NGN).

2) The Connection/Session Management functional entity is also responsible for managing the protocols necessary to stream and control the flow of media and other contents arriving at the IPTV terminal device, using protocols such as IGMP and RTSP.

3) Aid the Network Interface functional entity in the IPTV TD attachment and initialization process.

7.2.1.13 FEC Decode:

1) The Forward Error Correction Decode functional entity is responsible for decoding a received signal using the redundant data sent by the sender, without the need for the IPTV TD to request more information from the sender, in order to aid in ensuring QoS.

2) FEC functionality is recommended to support the functionality described by the "Application layer error recovery mechanisms for IPTV" document [FG IPTV-DOC-0186].

3) The FEC Decode functional entity is an optional entity.

7.2.1.14 Renewable Security:

1) The Renewable Security functionality may be used in a system where renewable security is required or desired.

2) Renewable security encompasses removable (e.g. Smart Card, Cable Card) and/or downloadable (e.g. DCAS) security.

3) Removable security is an optional component.

4) The Removable Security functionality is described in more detail in clause 7.2.2.5, "TD-SM".

7.2.1.15 Peripheral Device:

1) A peripheral device, such as a video camera, wireless headset, Bluetooth USB Adapter, or other component may be used by the end-user to interact with applications.

2) The peripheral device is an optional component.

3) The peripheral device interface is described in more detail in clause 7.2.2.4, "TD-OD and TD-PD".

7.2.2 IPTV Terminal Device Interfaces

Figure 7-1 identifies possible IPTV terminal device interfaces. These interfaces, physical or logical, may not all be present simultaneously and their existence depends on the configuration and the use of IPTV terminal device. The following sub-clauses provide descriptions of these interfaces.

7.2.2.1 BC-TD interface

This interface is between non-IPTV broadcasting network such as satellite, terrestrial and cable network and the IPTV terminal device. This interface facilitates transfer of content and related information by way of radio signals, such as QAM or OFDM.

7.2.2.2 NW-TD interface

7.2.2.2.1 NW-TD-1

NW-TD-1 represents a logical connection by which the IPTV terminal device connects to the IPTV Network via the RG using physical connection between the IPTV Network and the RG and the TD-HN connection. The IPTV Network should maintain two logical connections, one for IPTV and another for other services. At the end system side, the IPTV connection is maintained by IPTV terminal device, and the other connection is maintained by other device, such as RG itself.

In other configurations, the RG has only one connection to the IPTV Network, and the IPTV terminal device shares the connection with other HN devices. The connection between the IPTV Network and the RG is maintained by RG.

7.2.2.2.2 NW-TD-2

NW-TD-2 represents a direct physical connection between the IPTV Network and the IPTV terminal device.

This interface is between an IPTV terminal device or RG and the IPTV Network. The interface facilitates content and metadata transfer by multicast or unicast operation.

If a direct connection (NW-TD-2) between the IPTV Network and the IPTV terminal device is present, the IPTV terminal device is required to support at least one of the following:

– 10/100BASE-TX (as defined in [IEEE 802.3])

– 1000BASE-T (as defined in [IEEE 802.3])

– IEEE 802.16*x* (WiMAX, Mobile WiMAX, *x*: a and e) (as defined in [IEEE 802.16])

– IEEE802.11*x* (*x*: a, b, g and n) (as defined in [IEEE 802.11])

– 3G Wireless Internet as defined by 3GPP and 3GPP2

If a direct connection (NW-TD-2) between the IPTV Network and the IPTV terminal device is not present, the RG is required to support at least one of the above-mentioned connection methods and the IPTV terminal device is required to be connected to the RG by the TD-HN interface.

7.2.2.3 TD-HN interface

The followings are the specification for TD-HN.

- An interface that provides a connection to the home network. TD-HN is used for the connection between the IPTV terminal device and other in-home devices such as video recorders.
- TD-HN is an optional interface if a direct connection (NW-TD-2) between the IPTV Network and the IPTV TD is present.
- An IPTV TD should be equipped with one of the interfaces listed below for TD-HN.
  - Non-IP interface
  - IP interface
- If a non-IP interface is used for TD-HN, the IPTV TD can optionally be equipped with one of the interfaces listed below:
  - IEEE 1394 [IEEE 1394]
  - USB
  - Wireless Personal Area Network (WPAN) [IEEE 802.15.1]

If an IP interface is used for TD-HN, the IPTV TD should be equipped with at least one of the interfaces listed below:

- 10/100BASE-TX
- 1000BASE-T
- IEEE802.11a/b/g/n
- MoCA (Multimedia Over Coaxial Alliance)
- HomePNA [ITU-T G.9951, G.9952, G.9953, G.9954]
- PLC (Power-line Communication)

NOTE – Any device that operates on the TD-PD or the TD-OD interface could instead operate on the TD-HN interface; however, even though the device may technically be a "Peripheral Device" or "Output Device", since it is not a dedicated paired device with the IPTV TD (it could operate with multiple IPTV TDs within the home network), it cannot be classified under the TD-PD or TD-OD interfaces.

7.2.2.4 TD-OD and TD-PD

7.2.2.4.1 Physical Interface

An IPTV TD is required to support at least one of the following:

- support of analogue video signal output interface:
  - D connector as per [IEC 62360] or a combination of three RCA pins
    - For 1080p/1080i/720p/480p/480i component output
  - RCA pins
    - For NTSC/PAL/SECAM composite output (as defined in [ITU-R BT.1700])
  - S or S2 Connector
    - For NTSC/PAL/SECAM Y/C output

- support of digital video signal output interface:
  - DVI (Digital Video Interface)
  - HDMI (High-Definition Multimedia Interface)
- support of analogue and digital audio signals:
  - Analogue
  - S/PDIF as per [IEC 60958]
  - HDMI (High-Definition Multimedia Interface)
- USB
- [IEEE 1394]
- Bluetooth [IEEE 802.15.1]
- IR

If copy protection is required, the interface is required to be equipped with an appropriate copy guard management system and should, for example, support the following:

- All analogue outputs may be enabled or disabled based on service provider configuration.
- HDCP copy protection on the HDMI digital video output.

7.2.2.4.2 TD-PD Logical Interface

This interface is between a peripheral device and the IPTV terminal device. It allows transfer of information, such as Bluetooth protocol or those dealing with infrared to facilitate communication between the IPTV terminal device and, for example, a Bluetooth universal serial bus (USB) adaptor or mobile phone headset.

The devices operating on the TD-PD interface are connected either through a dedicated interface (e.g. USB) or through TD-HN interface.

7.2.2.4.3 TD-OD Logical Interface

This interface is between an Output Device (e.g. Display, Home Theatre System, External PVR, etc.) and IPTV terminal device and facilitates transfer of audio and video signals from IPTV terminal device to the Output Device.

7.2.2.5 TD-SM interface

TD-SM is the interface between the IPTV TD and an optional removable security function, such as an IC card. The followings are the specification for TD-SM interface.

If removable security is to be implemented, the IPTV TD is required to be equipped with at least one interface for TD-SM. The possible interfaces for TD-SM are included in Appendix II, the interfaces to support TD-SM are not limited to those described in Appendix II, but are meant as exemplary interfaces to be used by the IPTV TD for security-related issues.

The "IPTV Security Aspects" document [FG IPTV-DOC-0188] should be consulted for details relating to the security issues of the IPTV system.

7.3 Software Architecture

The document titled "IPTV Middleware" [FG IPTV-DOC-0196] was used as a basis for this information. Please refer to the "IPTV Middleware" document for more specific and detailed information related to the IPTV terminal software architecture.

A multi-level approach to software architecture was adopted and recommended in the "IPTV Middleware" document [FG IPTV-DOC-0196]. Some of the software levels are briefly described in this clause. The IPTV TD is recommended to support software architecture as described in the "IPTV Middleware" document.

7.3.1 OS/Driver Layer

The OS/Driver Layer provides components such as kernel modules and user-mode modules which provide access to and control of the IPTV TD hardware and devices.

7.3.2 Resource Abstraction Layer (RAL)

The Resource Abstraction Layer is an interface layer between resource and middleware service which encapsulates OS operations and resources layer and provide abstract view for resource layer.

The RAL provides the necessary interfaces to the lower layers of hardware (RAM, network access, hard drive, USB-port, etc.).

7.3.3 Middleware and Applications Layer

Middleware is defined as the layer of software between applications and resources, which consists of a set of service enablers that allow multiple functionalities running on one or more devices in an IPTV system to interact across a network. The "IPTV Middleware" document [FG IPTV-DOC-0196] should be consulted for any details regarding the middleware and application layers and their interactions with each other and lower layers (such as RAL or OS/Driver Layer).

7.4 Protocols

The IPTV TD is expected to support relevant protocols to operate within an IPTV System. The "IPTV Related Protocols" document [FG IPTV-DOC-0191] should be consulted for an in-depth list of protocols for consideration and support.

7.5 Terminal Device Attachment and Initialization

The IPTV TD attachment and initialization process is the process by which the IPTV TD is configured to attach to the network to discover the service provider and services offered in an IPTV system. The "IPTV Network Control Aspects" document [FG IPTV-DOC-0189] should be consulted for details regarding the process of terminal device attachment and initialization.

7.5.1 Service Provider Description Entry Points

When the IPTV TD attaches to the network, it has to know where to get the description of the IPTV service providers available to it. An IPTV TD is recommended to be provisioned with an IPTV service provider description entry point, which can be a multicast or unicast address.

The IPTV terminal device may receive its IPTV service provider description entry points by means of:

- A well known multicast address registered with IANA,
- An entry point address embedded in the IPTV terminal device configuration data,
- A domain name embedded in the IPTV terminal device configuration data, using DNS to acquire entry point addresses,
- At network connection, with DHCP, the IPTV terminal device might be provided with domain names to be used to acquire entry point addresses via DNS.

7.5.2 Service Provider Discovery and Service Attachment

Service provider discovery is the process by which an IPTV TD becomes aware of the available IPTV service providers, learns the location of their service discovery (SD) servers and the means for attaching to each SD server. As a result, by contacting the discovered SD server(s), an IPTV TD can perform the subsequent services discovery and service attachment procedures.

Service provider discovery procedures are described in detail in the "IPTV network control aspects" document [FG IPTV-DOC-0189] and service attachment procedures (service provider service discovery) are detailed in the "IPTV Middleware" document [FG IPTV-DOC-0196].

The service provider discovery process is defined as a set of alternative procedures/cases defined in the "IPTV network control aspects" document [FG IPTV-DOC-0189], which can be extended further.

7.6 Quality Monitoring

The following methods can be used, if video quality monitoring is required.

- no reference methods [ITU-T J.mm-noref] (clause 7.6.1)
- reduced reference methods [ITU-T J.mm-redref] (clause 7.6.2)
- quality monitoring using transmission errors [ITU-T J.242] (clause 7.6.3)
- Hybrid perceptual/bit-stream models [ITU-T J.bitvqm] (clause 7.6.4)

As an optional functionality, the IPTV terminal device may have quality monitoring capability. IPTV services are different from traditional TV services such as satellite TV or cable TV. If satellite or cable TVs are properly installed, video quality will be consistently good. This is not true for IPTV. If demands exceed the bandwidth or there are transmission errors, video quality will deteriorate. For this reason, quality monitoring is more important in IPTV, particularly for some applications such as PPV or VoD.

For video quality monitoring in IPTV applications, there are three possibilities: reduced-reference (RR) models, no-reference (NR) models and the quality monitoring method using transmission errors [ITU-T J.242].

7.6.1 No-reference methods [ITU-T J.mm-noref]

In the no-reference method (Figure 7-2), perceptual video quality evaluation is made based solely on the processed video sequence (PVS) without using the source video sequence (SRC). Although the performance of no-reference methods is inferior to that of full-reference and reduced-reference methods, it is expected that upcoming bit-stream NR methods will provide improved performance [ITU-T J.bitvqm].

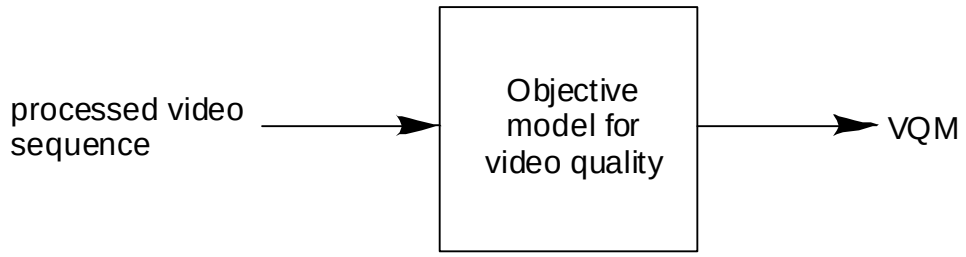


Figure 7-2: A no-reference model

7.6.2 Reduced-reference methods [ITU-T J.mm-redref]

In the reduced-reference method, features are extracted from the source video sequence and the processed video sequence (Figure 7-3). From these features, perceptual objective measurements of video quality are computed. If a reduced-reference method is used at the terminal, the head-end needs to transmit feature data for video quality measurement in addition to video data (Figure 7-4). It is desirable that the feature data should be available at the terminal in a timely manner. It is preferred that the feature data is sent with a time advance and the terminal stores the feature data in a local storage. Thus, the terminal should have adequate computing power and storage. It is also expected that upcoming bit-stream RR methods will provide improved performance [ITU-T J.bitvqm].

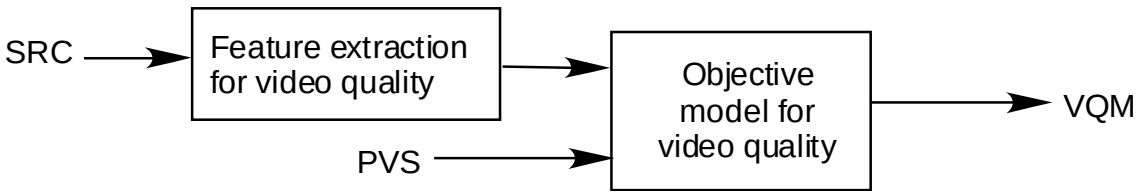


Figure 7-3: A reduced-reference model
(SRC: source video sequence, PVS: processed video sequence)

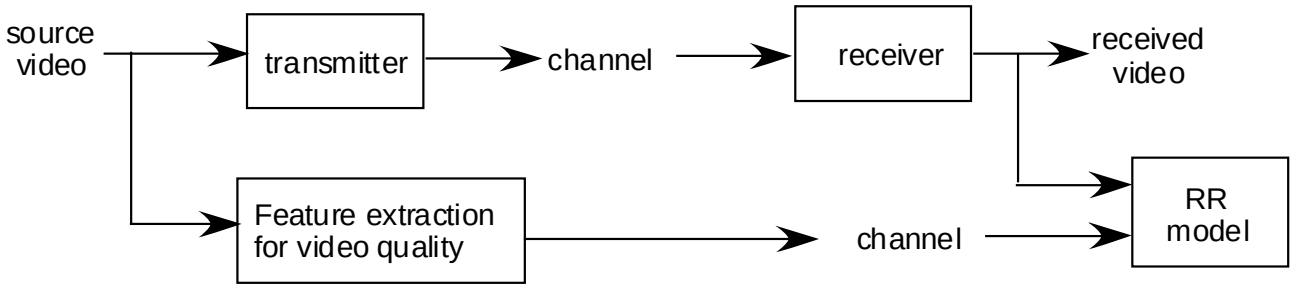


Figure 7-4: A block diagram of video quality monitoring using an RR model

7.6.3 Quality monitoring using transmission error information at the head-end [ITU-T J.242]

In digital communications, transmission errors include packet loss and packet delay and their effects can be exactly identified when video data is transmitted using packets. Furthermore, if there is no transmission error, the video quality at the receiver will be identical to the video quality of the video sent by the transmitter. Therefore, if the receiver sends transmission error information which includes information on packet loss and delay in packetized video transmission, the head-end (service provider) can exactly reconstruct the received video seen at the receiver (Figure 7-5). Finally, the head-end may use a FR or RR method to evaluate the video quality of the received video seen at the receiver. Table 7-1 describes messages for sending transmission error information to the service provider.

Table 7-2 shows an example of error message format capable to send information on transmission errors. Thus, the terminal (e.g., set top box, or mobile terminals) is designed to send transmission error information (e.g., Table 7-2), quality monitoring can be efficiently done at the head-end using the transmission error information.

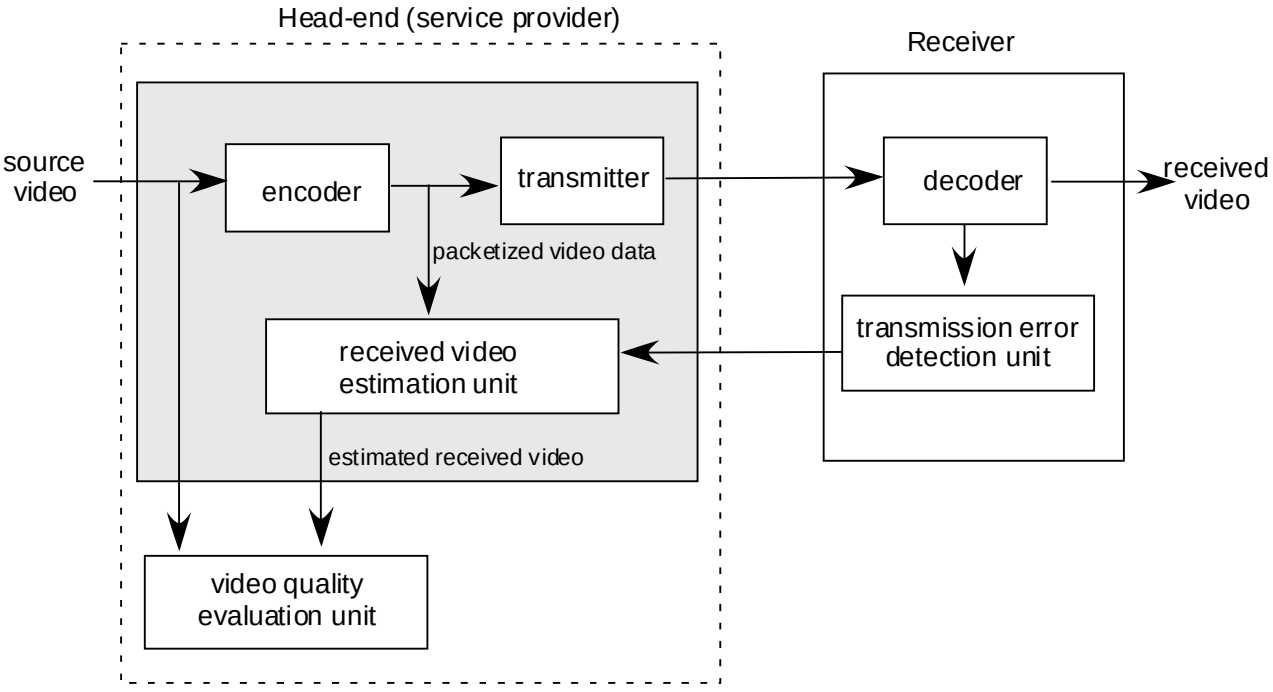


Figure 7-5: A method for a head-end to monitor video quality at the terminal using transmission error information

Table 7-1: Message description

Type of transmission errors	Message descriptions
Information on the terminal	A model identification message
Source Identifier	A source identification message
Information on a lost packet	A lost packet index
Information on lost packets	A starting packet index and an ending packet index of the lost packets
Information on a delayed frame	A delayed frame index and the amount of delayed time
Information on a skipped frame	A skipped frame index
Information on skipped frames	A starting frame index and an ending frame index of the skipped frames

Table 7-2: Error Message Formats [ITU-T J.242]

Type of transmission errors	Transmission error messages in hexadecimal	Descriptions
Information on a lost packet (5 bytes)	6C XX XX XX XX	"l" + packet index in long integer
Information on lost packets (9 bytes)	4C XX XX XX XX XX XX XX XX	"L" + starting packet index in long integer + ending packet index in long integer
Information of a delayed frame (7 bytes)	64 XX XX XX XX XX XX	"d" + frame index in long integer + delay time in short integer
Information on a skipped frame (5 bytes)	73 XX XX XX XX	"s" + frame index in long integer
Information of skipped frames (9 bytes)	53 XX XX XX XX XX XX XX XX	"S" + starting frame index in long integer + ending frame index in long integer
Information of the receiver (32 bytes)	6D + 31-byte string	"m"+31 byte string
Source Identifier (5 bytes)	69 XX XX XX XX	"I" + 4 bytes (32 bits)

7.6.4 Hybrid perceptual/bit-stream models [ITU-T J.bitvqm]

It is possible that an objective model may have access to bit stream data from which the model can obtain additional information on transmission errors (e.g., delay, packet loss), codec parameters (e.g., type, bit-rates, frame rates, codec parameters), etc. This kind of information is easily available from bit-stream data at the receiver. It is expected that such models may provide improved performance in terms of accuracy and speed compared to objective video quality models which use only processed video sequences.

If an IPTV terminal device is to use such a hybrid perceptual/bit-stream model for quality monitoring, it should provide bit-stream data to the model [ITU-T J.bitvqm]. The input requirements for hybrid perceptual/bit-stream models are shown in Figures 7-6 ~ 7-8. For quality monitoring in the IPTV TD, RR or NR methods can be used.

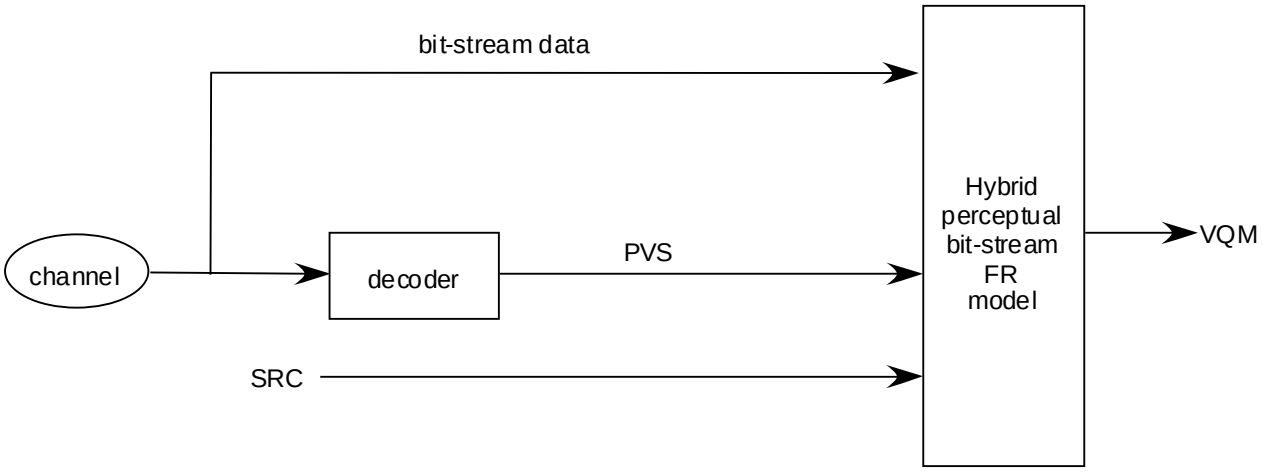


Figure 7-6: Input requirements for FR hybrid perceptual/bit-stream models

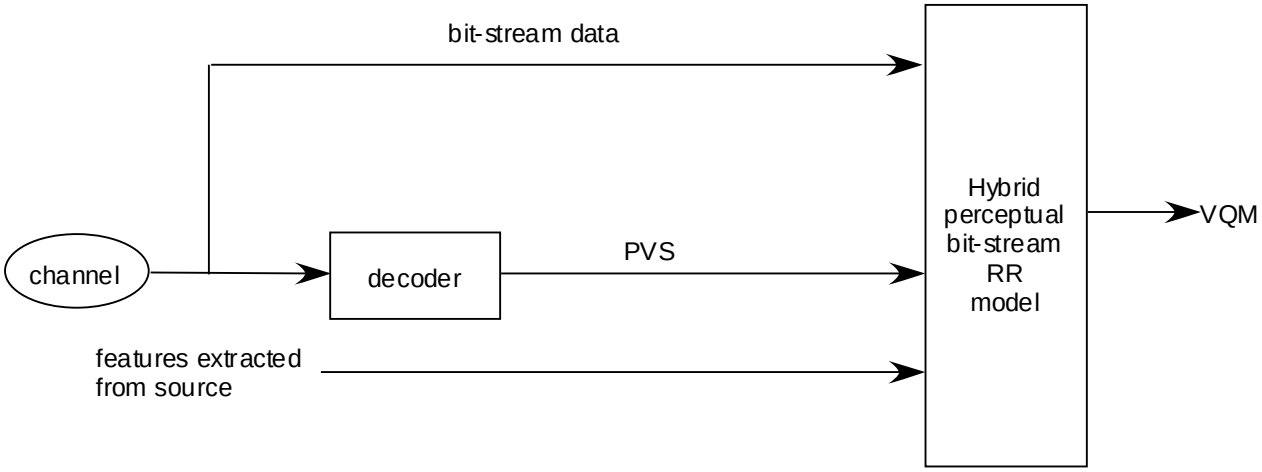


Figure 7-7: Input requirements for RR hybrid perceptual/bit-stream models

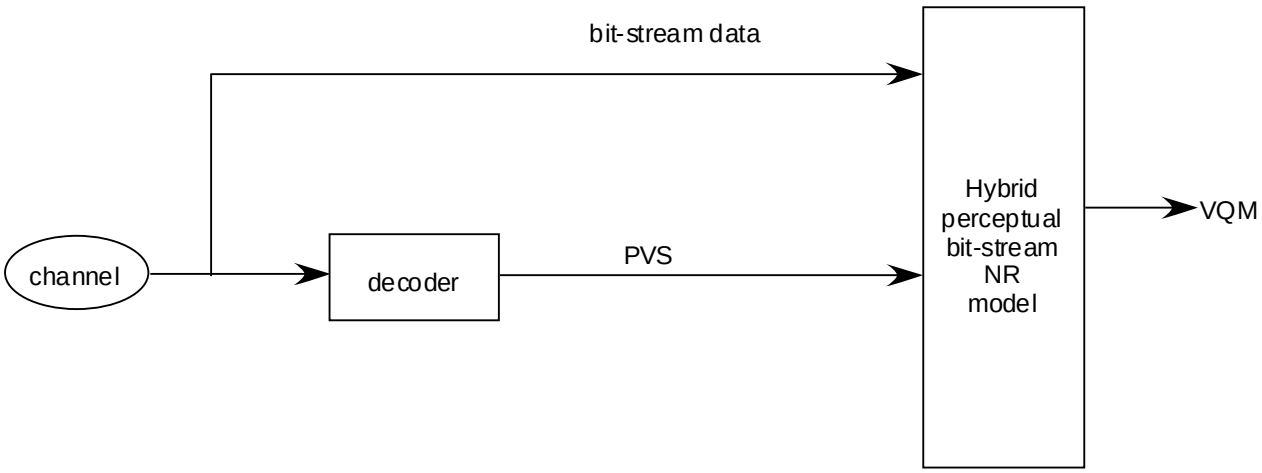


Figure 7-8: Input requirements for NR hybrid perceptual/bit-stream models

In order to improve the accuracy of objective models, it is also possible to transmit video quality scores of the compressed video data which are transmitted (Figure 7-9). It has been known that if video quality measurements are made every half second, they will provide sufficient information on the video quality of the processed video sequence. If there are no transmission errors, the video quality at the receiver would be the same as that of the transmitted video sequence. If transmission errors occur, the received video sequence suffers from both compression impairments and transmission error impairments. With video quality scores available, an objective model which measures the video quality of the received video sequence may be improved, particularly for NR models. The video quality scores can be transmitted as meta-data. Alternatively, they can be transmitted using watermark techniques.

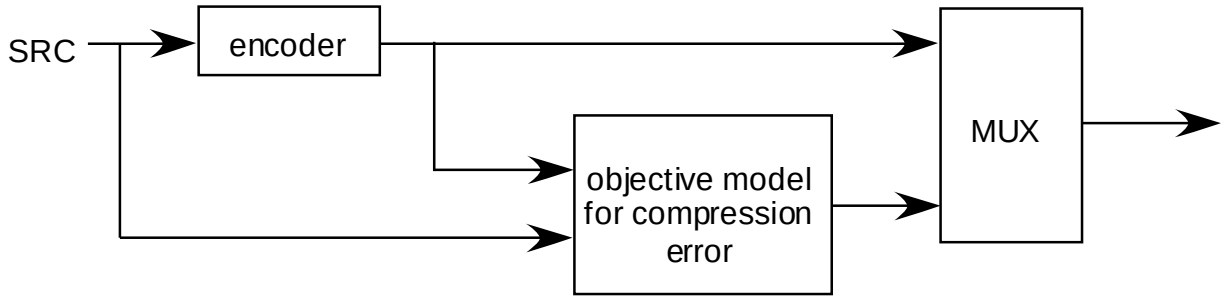


Figure 7-9: Generating and transmitting video quality scores of compressed data [Figure A4/J.bitvqm]

If an IPTV terminal device is to use these objective models for quality monitoring, the input requirements are shown in Figures 7-10 ~ 7-12.

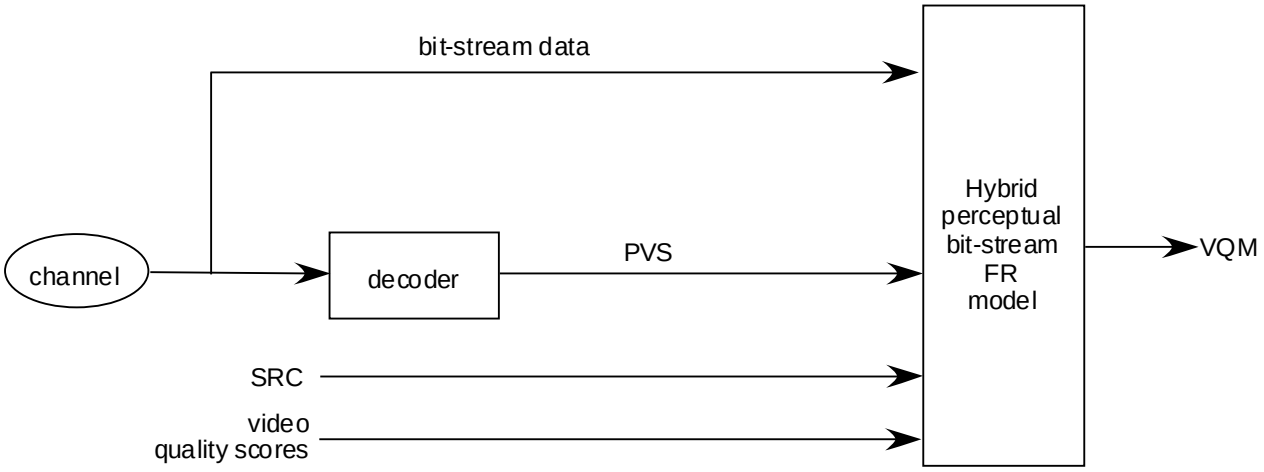


Figure 7-10: Input requirements for a FR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data

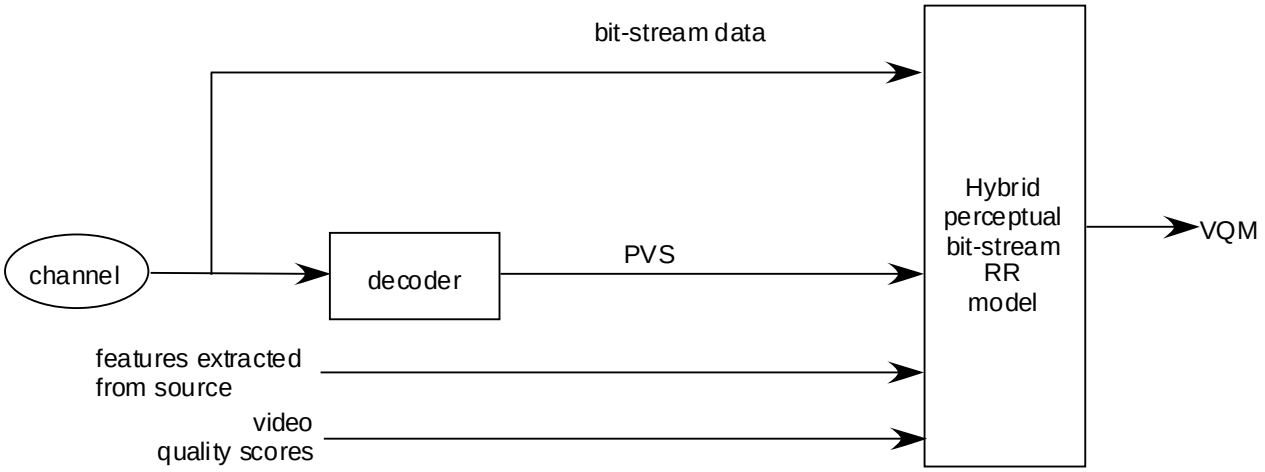


Figure 7-11: Input requirements for a RR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data

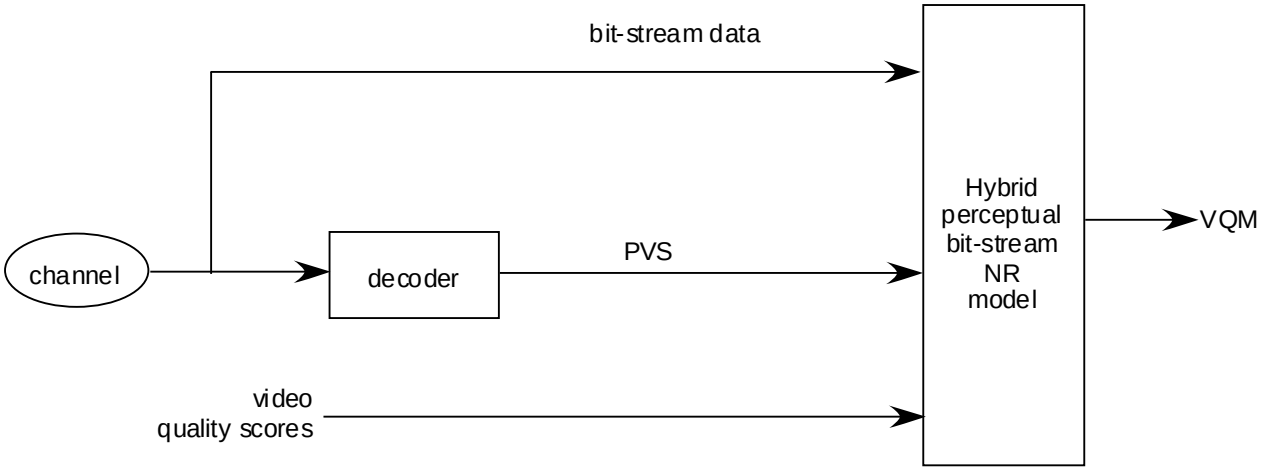


Figure 7-12: Input requirements for a NR hybrid perceptual/bit-stream model which uses the video quality scores of transmitted compressed video data

Appendix I

Service Information (SI)

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

The IPTV TD can use the Service/System Information in order to find out where on the network to access any content that the user selects. In order to support an IPTV TD, existing Service/System Information data need to be updated and modified to provide the data necessary for an IPTV TD to discover and access digital/analogue services offered available on the network. In addition to the existing RF/frequency-related information, the updated SI data must support at least the following (this is not an exhaustive list) in order to allow for IP transmission: Source IP address (to allow for SSM), Multicast Destination IP address and UDP Port, different IP encapsulation methods (e.g. UDP/RTP/MPEG2-TS), stream bandwidth information, etc.

The IPTV TD software should accept the Program Specific Information and Service Information (PSI/SI) including program association table (PAT), program map table (PMT), network information table (NIT), virtual channel table (VCT), event information table (EIT), and system time table (STT).

The IPTV TD should use the system time message to synchronize its local clock and should provide a clock signal to the middleware and applications. The IPTV TD should be capable of maintaining a channel map and make it available to middleware and applications.

SI standards are region-specific, and the following are some of the regional standards that apply:

- In North America: [ANSI/SCTE-65]
- In Europe: [ETSI EN 300 468]
- In Japan: [ARIB STD-B10]

Appendix II

Removable Security TD-SM Interface

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

If optional removable security is to be implemented, the IPTV terminal device is required to be equipped with at least one interface for TD-SM.

- The interface for TD-SM may optionally support ISO Smart Card specifications defined in:
  - [ISO/IEC 7816-1]
  - [ISO/IEC 7816-2]
  - [ISO/IEC 7816-3]
- The interface for TD-SM may optionally support SCTE Cable Card (POD Module) specifications:
  - [ANSI/SCTE-28]
  - [ANSI/SCTE-41]
  - [ANSI/SCTE 51-1], [ANSI/SCTE-51-2], and/or [SCTE-106] (for bi-directional communication)
- The interface for TD-SM may optionally support ETSI Smart Card specifications:
  - [ETSI TS 102 225]
  - [ETSI TS 102 226]

  - [ETSI TS 102 569]
- The IPTV smart card is recommended to follow a common uniform format similar to SIM.
- The IPTV smart card is recommended to have the ability to support prepay and post-pay mode.
- The IPTV smart card is recommended to support [ITU-T E.118], [ITU-T E.164], and [ITU-T T.50], according to charging and numbering needs.

Bibliography

[b_ITU-T E.118] ITU-T Recommendation E.118 (2006), *The international telecommunication charge card*

[b_ITU-T E.164] ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan*

[b_ITU-T FSTP-TACL] Telecommunications Accessibility Checklist (2006), http://www.itu.int/publ/T-TUT-FSTP-2006-TACL/en

[b_ITU-T T.50] ITU-T Recommendation T.50 (1992), *International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) – Information technology – 7-bit coded character set for information interchange*

[b_ARIB STD-B10] ARIB STD-B10 Ver.4.4 (2007), *Service Information for Digital Broadcasting System*

[b_ANSI/SCTE-28] ANSI/SCTE 28 (2007), *Host-POD Interface Standard*

[b_ANSI/SCTE-41] ANSI/SCTE 41 (2004), *POD Copy Protection System*

[b_ANSI/SCTE-51-1] ANSI/SCTE 51-1 (2002), *Digital Broadband Delivery System: Out Of Band Transport Part 1: Mode A*

[b_ANSI/SCTE-51-2] ANSI/SCTE 51-2 (2002), *Digital Broadband Delivery System: Out Of Band Transport Part 1: Mode B*

[b_ANSI/SCTE-65] ANSI/SCTE 65 (2002), *Service Information Delivered Out-of-Band for Digital Cable Television*

[b_ETSI EN 300 468] ETSI EN 300 468 v1.8.1 (2007), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*

[b_ETSI TS 102 225] ETSI (2006), *Secured packet structure for UICC based applications*

[b_ETSI TS 102 226] ETSI (2007), *Remote APDU structure for UICC based applications*

[b_ETSI TS 102 569] ETSI (2007), *UICC Security Service Module (USSM)*

[b_ISO/IEC 7816-1] ISO/IEC 7816-1 (1998), *Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics*

[b_ISO/IEC 7816-2] ISO/IEC 7816-2 (1999), *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts*

[b_ISO/IEC 7816-3] ISO/IEC 7816-3 (1997), *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Cards with contacts – Electrical interface and transmission protocols.*

[b_SCTE-106] SCTE 106 (2007), *DOCSIS® Set-Top Gateway (DSG) Specification*

II.5.2 Aspects of home network supporting IPTV services

Summary

The document addresses the home network architecture aspects in the context of IPTV.

Keywords

Home network, delivery network gateway, residential gateway, IPTV services

Current status

The major parts of the document are complete or near completion. Remaining issues are mostly editorial and minor issues.

Dependency on or relationship to other FG IPTV documents

- IPTV Services Requirements
- IPTV Architecture
- Traffic Management Mechanisms for the Support of IPTV Services
- IPTV Security Aspects
- IPTV related protocols
- IPTV network control aspects

CONTENTS

		Page
1	Scope	496
2	References	496
3	Definitions	499
	3.1 Terms defined elsewhere	499
	3.2 Terms defined here	499
4	Abbreviations and acronyms	499
5	Conventions	501
6	Home Network	502
	6.1 Home Network Architecture	502
	6.2 QoS	503
	6.2.1 Home Network QoS architecture	504
	6.2.2 Quality of Service requirements	509
	6.3 Security	515
	6.3.1 Home Network Security Threats	515
	6.3.2 Home Network Security Requirements	516
	6.4 Interoperability between IPTV core/access network and home network	516
	6.4.1 Protocols	516
	6.4.2 Interface	516
	6.5 Interoperability among home network devices	516
	6.5.1 IEC62481 (DLNA) based	516
	6.5.2 ISO/IEC 29341 (UPnP) based	517
	6.6 The DNG	517
	6.6.1 DNG Functional Overview	517
	6.6.2 IPI-4 Interfaces	519
	6.6.3 IPI-3 Side Interfaces	522
	6.6.4 Packet processing	522
	6.6.5 Service Support	524
	6.6.6 IGMP Functionality	525
7	Remote management	526
	7.1 Management Architecture	527
	7.1.1 Device Management	530
	7.1.2 QoS Management	534
	7.1.3 Security Management	534
	7.1.4 Performance Monitoring and Diagnostics & Troubleshooting	534
	7.1.5 Local Management Application	535

Page

7.2 Management requirement 536
7.2.1 Northbound Interfaces 536
7.2.2 RMS requirements 536
7.2.3 General DNG configuration and management 536
7.2.4 End-device management 537
7.2.5 Security management 538
7.2.6 End-device recommendations 538
7.3 IPTV service information report 539
7.4 Remote management protocol 539
7.4.1 SNMPv2/v3 539
7.4.2 DSL Forum TR069 539
Annex A – Considerations on ISO/IEC15045-1 for IPTV services 540
A.1 Introduction 540
A.2 Comparison of terminology 540
A.3 Packet processing and interfaces of the DNG 541
A.4 Security consideration 541
Appendix I – An explanation of the layered models for IPTV Home Network 542
Appendix II – Home network (HN) use case scenarios 543
II.1. HN IPTV TD acting as an HN server 543
II.2 HN IPTV TD acting as an HN client 544
Appendix III – UPnP based Home Network 544
Appendix IV – Consideration of re-transmission of Free-to-Air broadcasting 546
IV.1 Middleware aspect 546
IV.2 Content protection issue 546
IV.3 Privacy protection issue 546
IV.4 Delivery control of retransmission 546
IV.5 Provision of Emergency broadcast 546
Appendix V – Example configurations for an IP-based home network 547
Bibliography 548

Aspects of home network supporting IPTV services

1 Scope

This document describes relationship between the home network (HN) and IPTV related entities. It also identifies functions needed for the home network to support IPTV services. It further provides procedures and sets criteria to verify compliance of IPTV terminal devices to the identified rules and requirements.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.983] ITU-T Recommendation G.983.1 (1998), *Digital transmission systems – Digital sections and digital line system – Optical line systems for local and access networks*

[ITU-T G.984] ITU-T Recommendation G.984.1 (2003), *Gigabit-capable Passive Optical Networks (GPON): General characteristics*

[ITU-T G.992.1] ITU-T Recommendation G.992.1 (1999), *Asymmetric digital subscriber line (ADSL)*

[ITU-T G.992.3] ITU-T Recommendation G.992.3 (2005), *Asymmetric digital subscriber line transceivers 2 (ADSL2)*

[ITU-T G.992.5] ITU-T Recommendation G.992.5 (2005), *Asymmetric Digital Subscriber Line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2plus)*

[ITU-T G.993.2] ITU-T Recommendation G.993.2 (2006), *Very high speed digital subscriber line transceivers 2 (VDSL2)*

[ITU-T G 994.1] ITU-T Recommendation G.994.1 (2007), *Handshake procedures for digital subscriber line (DSL) transceivers*

[ITU-T I.361] ITU-T Recommendation I.361 (1999), *B-ISDN ATM layer specification*

[ITU-T I.365] ITU-T Recommendation I.365 (1993), *Frame relaying service specific convergence sublayer (FR-SSCS)*

[ITU-T J.190] ITU-T Recommendation J.190 (2007), *Architecture of MediaHomeNet*

[ITU-T I.610] ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*

[ITU-T X.1111] ITU-T Recommendation X.1111 (2007), *Framework of security technologies for home network*

[ITU-T Y.1541] ITU-T Recommendation Y.1541 (2006), *Network performance objectives for IP-based services*

[FG IPTV-DOC-0147] FG IPTV-DOC-0147, *IPTV Services Requirements*

[FG IPTV-DOC-0188] FG IPTV-DOC-0188, *IPTV Security Aspects*

[FG IPTV-DOC-0191] FG IPTV-DOC-0191, *IPTV Related Protocols*

[ATIS-0800002] ATIS IPTV Interoperability Forum (IIF) Standards (2006), *IPTV Architecture Requirements*

[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*

[IETF RFC 1305] RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*

[IETF RFC 1918] RFC 1928 (1996), *Address Allocation for Private Internets*

[IETF RFC 2236] RFC 2236 (1997), *Internet Group Management Protocol, Version 2*

[IETF RFC2684] RFC2684 (1999), *Multiprotocol Encapsulation over ATM Adaptation Layer* 5

[IETF RFC3376] RFC3376 (2002), *Internet Group Management Protocol, Version 3*

[IETF RFC 3489] RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*

[IETF RFC 4122] RFC 4122 (2005), *A Universally Unique IDentifier (UUID) URN Namespace*

[IEEE 802.1D] IEEE Std. 802.1D (2004), *IEEE standard for local and metropolitan area networks – Media access control (MAC) Bridges (Incorporates IEEE 802.1t-2001 and IEEE 802.1w)*

[IEEE 802.1Q] IEEE Std. 802.1Q (2005), *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks – Revision*

[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.*

[IEEE 802.3ah] IEEE Std. 802.3ah (2004), *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

[IEEE 802.11a] IEEE802.11a (1998), *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 – Amendment 1: High-speed Physical Layer in the 5 GHz band*

[IEEE 802.11b] IEEE802.11b (1999), *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: Higher-Speed Physical Layer in the 2.4 GHZ Band-Supplement to IEEE Std 802.11-1999; IEEE Computer Society Document; Amendment 802.11D – 06/14/2001; Corrigendum 1 – 10/2001*

[IEEE 802.11g] IEEE.802.11g (2003), *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 – Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band*

[IEEE1394] IEEE Std. 1394 (1995) *IEEE Standard for a High Performance Serial Bus*

[DSLF TR-062] DSL Forum TR-062 (2003), *Auto-Config for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM*

[DSLF TR-068] DSL Forum TR-068 (2005), *Base Requirements for an ADSL Modem with Routing*

[DSL-F TR069] DSL Forum TR-069 (2004), *CPE WAN Management Protocol*

[DSLF TR-098] DSL Forum TR-098 (2005), *DSLHome™ Gateway Device Version 1.1 Data Model for TR-069*

[DSLF TR-104] DSL Forum TR-104 (2005), *DSLHome™ Provisioning Parameters for VoIP CPE*

[DSLF TR-106] DSL Forum TR-106 (2005), *DSLHome™ Data Model Template for TR-069 Enabled Devices*

[DSLF TR-111] DSL Forum TR-111 (2005), *DSLHome™Applying TR-069 to Remote Management of Home Networking Devices*

[ISO/IEC15045-1] ISO/IEC15045-1 (2004), *Information technology – Home electronic system (HES) gateway – Part 1:A residential gateway model for HES*

[IEC62481-1] IEC62481-1 Ed.1: *DLNA Home networked device interoperability guideline – Part 1: Architecture and Protocols*

[IEC62481-2] IEC62481-2 Ed.1: *DLNA Home networked device interoperability guideline – Part 2: Media Formats*

[HGI] Home Gateway Initiative, *Home Gateway Technical Requirements: Release 1.0 (1 July 2006)*.

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

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

NOTE – There are some terms such as HA (Home Access) [ITU-T J.190], Home Gateway, Residential Gateway, Delivery Network Gateway and so on used for the same device. Relevant terms will be defined.

3.1.2 Home network (HN) [FG IPTV-DOC-0147]**:** A communication system designed for the residential environment, in which two or more devices exchange information.

3.1.3 Hybrid terminal device [FG IPTV-DOC-0147]**:** An IPTV terminal device that can also receive content from different types of transmission systems (e.g. satellite, cable).

3.1.4 IPTV End System (IES) [FG IPTV-DOC-0147]**:** A single or set of consumer devices that support IPTV Services (i.e. everything from Gateway to Display).

3.1.5 IPTV TD [FG IPTV-DOC-0147]**:** A terminal device which has ITF functionality, e.g. a STB.

3.1.6 IPTV terminal function (ITF) [FG IPTV-DOC-0147]**:** The functionality that is responsible for processing the content conveyed by the IP transport.

3.1.7 Terminal Device (TD) [FG IPTV-DOC-0147]**:** A device which typically presents and/or processes the content, such as a personal computer, a computer peripheral, a network appliance, a mobile device, a TV set, a monitor, a VoIP Terminal or an audio-visual media player.

3.2 Terms defined here

This document 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 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.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

AAL5 ATM Adaptation Layer 5

ACL Access Control List

ACS Auto Configuration Server

ADSL Asymmetric Digital Subscriber Line

ALL Application Layer Logic

ALG Application Layer Gateway

AN	Access Network
ATM	Asynchronous Transfer Mode
BC-NW	Broadcast Network
CBR	Constant Bit Rate
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
DS	Downstream
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
ECG	Electronic Contents Guide
EPG	Electronic Program Guide
GUI	Graphical User Interface
HA	Home Access
HN	Home Network
IES	IPTV End System
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPI	Internet Protocol Infrastructure
IPTV-NW	IPTV Network
L2	Layer 2
MAC	Media Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface Crossover
MPEG	Moving Picture Experts Group
NAT	Network Address Translation
NAPT	Network Address Port Translation
NT	Network Terminal
NW	Network
OAM	Operation, Administration & Maintenance
PLT	Power Line Transmission
PPP	Point-to-Point Protocol

PPPoE	PPP over Ethernet
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
PVR	Personal Vide Recorder
QoE	Quality of Experience
QoS	Quality of Service
RG	Residential Gateway
RMS	Remote Management System
RTSP	Real Time Streaming Protocol
SA	Source Address
SIP	Session Initiation Protocol
SNTP	Simple Network Time Protocol
SP	Service Provider
SSID	Service Set Identifier
STB	Set-Top Box
TCP	Transmission Control Protocol
TD	Terminal Device
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
USB	Universal Serial Bus
VBR	Variable Bit Rate
VC	Virtual Channel
VCI	Virtual Channel Identifier
VDSL	Very high bitrate Digital Subscriber Line
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VoD	Video on Demand
VoIP	Voice over IP
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

5 Conventions

In this document:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document 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/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

[HGI_Rn] means the nth requirement as identified in [HGI]. For example [HGI_R100] means R100 requirement identified in "Home Gateway Technical Requirements: Release 1.0 (1 July 2006)" [HGI].

6 Home Network

6.1 Home Network Architecture

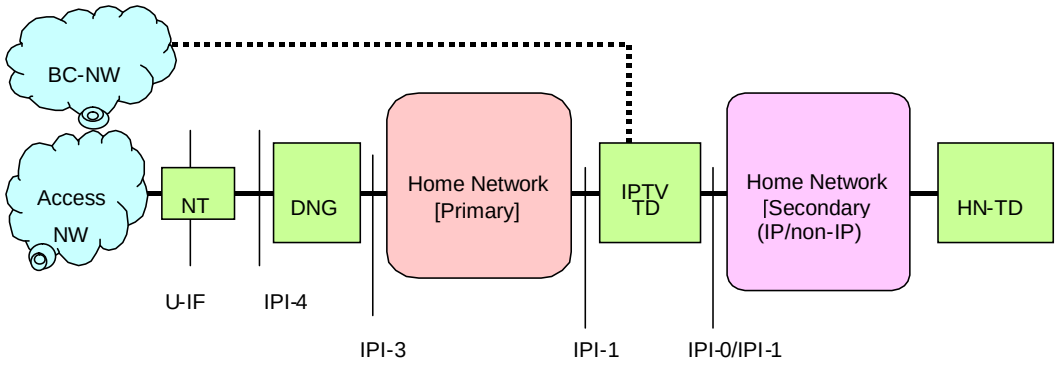


Figure 6-1: Home Network architecture

The following provides description of home network architecture components.

Primary Domain (IP-HN-P)

The primary domain deals with IPTV related IP traffic between the access network and IPTV terminal device (IPTV TD) including audio and/or video streams. Traffic in the primary domain is associated with traffic to/from the access network. The devices and traffic related to the primary domain are required to be configured to be reachable to and/or 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 needed.

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/or from the access network. For example, there may be a case where locally assigned IP addresses are enough for this domain. The secondary domain can be divided into 2 parts, IP and non-IP, depending on the network layer protocol.

IP Secondary Domain (IP-HN-S)

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

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 IEEE 1394.

The above architecture contains some interfaces indicating boundaries between devices and domain. These interfaces are summarised in the table 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
	IPI-3b	IPI-3 interface used for Ethernet (10/100/1000 BASE-T)
	IPI-3c	IPI-3 interface used for Home PNA
	IPI-3d	IPI-3 interface used for coaxial
	IPI-3e	IPI-3 interface used for wireless
IPI-4		Upstream side interface of DNG (See clause 6.6.2)
	IPI-4a	IPI-4 interface used for connection with copper access network (See clause 6.6.2.1 and 6.6.2.2)
	IPI-4b	IPI-4 interface used for connection with optical access network through Ethernet interface (See 6.6.2.3)
	IPI-4c	IPI-4 interface used for connection with optical access network through coaxial interface (See clause 6.6.2.5)
	IPI-4d	IPI-4 interface used for connection with wireless access network (See clause 6.6.2.6)
	IPI-4e	IPI-4 interface used for connection with optical access network (See clause 6.6.2.7)
U interface		Interface between Access NW and Home Network The U interface and the NT are outside of the Home Network

6.2 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 service.

There are mainly two QoS techniques that are being used in an IP network: priority (or class-based) QoS and parameterized QoS. With the priority-based 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 (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 get better QoS than others that have 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 setup 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 quality of service 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 clause 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.

6.2.1 Home Network QoS architecture

NOTE – QoS mechanisms are also described in the HGI document [HGI] in the context of bi-directional services like VoIP. Refer to [HGI] for more details.

6.2.1.1 Potential Congestion Points

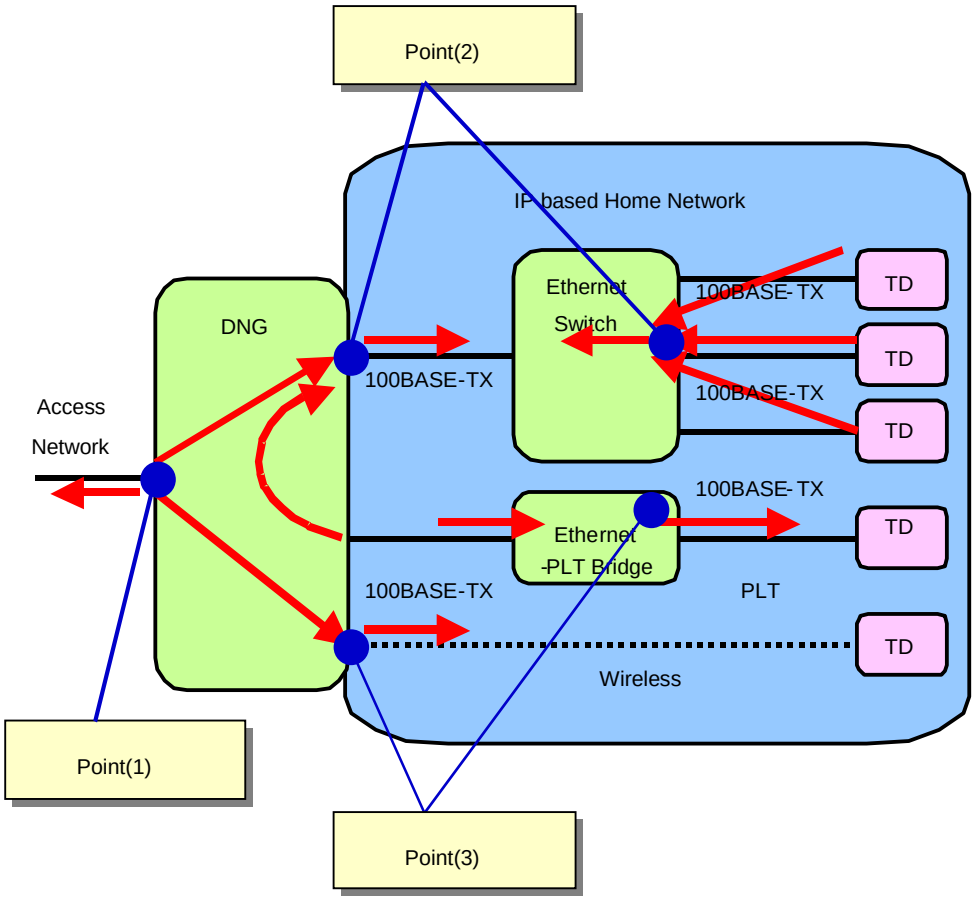


Figure 6-2: Potential congestion point in a typical home network

Home Network QoS needs to accommodate a variety of both Access and Home Network technologies. There are a number of potential congestion points as shown in Figure 6-2. Note that the degree to which these are actual congestion points will depend on the technologies used.

Three potential congestion points are identified in the IP-based Home Network.

- Congestion Point (1)

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

- Congestion Point (2)

Congestion Point (2) is at the egress port of the device in which traffic from two or more network link is collected. Typical example is Ethernet switch. If combined traffic from several ports/links exceeds a certain amount, the congestion at the egress port will happen. Congestion Point (2) is also possible at the DNG, if it contains switching capability for home network side traffic.

- Congestion Point (3)

Congestion Point (3) is where the transmission capacity changes. The bridge device interconnecting between different network segments with different capacity, for example between Ethernet and PLC, is a typical example. Congestion Point (3) is possible at the DNG because of the difference of transmission capability between Access Network and Home Network.

6.2.1.2 Basic principle of operation

QoS approach is mainly concerned with managing QoS through DNG itself. It works on the basis of a packet by packet, service classification. The service classifiers are combinations of the ingress packet header fields. QoS markings of incoming packets from HN side are generally untrusted, but can be used if trust is established by some other means, and/or in combination with other service classifiers.

The service classification is used to assign the packet to the appropriate queue, and may be used to set the L2 markings for a particular HN technology. It is also possible to drop packets on the basis of classification. Management function can optionally provide service classifiers 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 DNG itself. There is no session awareness, except for that associated with this overload control mechanism. Class-based queuing is used. DSCP markings of incoming packet at IPI-3 interface can be overwritten to zero or a per service configurable value. There is a QoS mapping table for L2 parameters for transit traffic at DNG. 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].

6.2.1.3 DSCP and VLAN Usage

Some current L3 QoS schemes are based on DSCP markings, with VLANs and Ethernet priority markings being used in L2 schemes. Although all of these features to some degree in the scheme for IPTV, they are not the main mechanisms. The reasons for this are as follows. There are two problems with relying upon DSCP. Firstly, all traffic of the same type would have the same marking but what is required is the ability to differentiate on a service basis. Secondly, the DSCP markings need to be trusted, but since they, particularly in case of upstream and transit, can be set by an end-user application they can be easily spoofed, unless there is a mechanism to establish trust with end devices.

In principle VLAN IDs and/or priority tags could be used as a QoS classifier within the Home Network, however this approach is not a preferred solution for IPTV. Adding a VLAN header or priority tags increases the Ethernet frame size; some small, unmanaged Ethernet switches simply drop such frames. Since there are at least some infrastructure devices which will drop tagged frames, DNG does not add VLAN headers to any frames. However certain DLNA devices may send tagged frames. DNG needs to be able to receive such frames and in the case of bridged traffic, will forward them transparently.

NOTE – See clause 5.5.5 of [HGI].

6.2.1.4 Traffic Classification

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

There are in fact rather different requirements for the classification of the three basic directions of traffic flow through the Gateway i.e. upstream, downstream and transit. Different from the bidirectional service like VoIP, QoS consideration of downstream traffic is more important than upstream. Thus, this document specifically describes downstream traffic. Other types of traffic are also mentioned, but discussed in this context. (Note 2) In the downstream direction, the main aim is to maintain QoS characteristic of incoming traffic, and ensure that it is not compromised by transit traffic. The classifiers are briefly described below with a brief rationale as to when and how they might be used.

NOTE 1 – See clause 5.5.6 of [HGI].

NOTE 2 – In case of bidirectional applications like VoIP, QoS treatment on the upstream traffic merits special considerations, particularly in case of using Access Network technologies with asymmetrical bandwidth like DSL, in which relatively limited transmission capability is provided for upstream. For such case, upstream traffic could experience the most significant congestion at the DNG. Please refer to other documents such as [HGI] for details of this topic.

NOTE 3 – In interactive applications such as gaming, QoS treatment for upstream traffic is also important. Refer to "IPTV service requirements" for details.

6.2.1.5 Downstream Classifiers

The main requirement in the downstream direction is to be able to distinguish between managed and unmanaged services. Classifiers such as IP DA/SA, physical port, packet length, MAC SA/DA, TCP/UDP port number, and protocol type fields, which are identified as upstream classifiers (see [HGI]), are also included in the downstream (DS) scheme, as they may be required on occasion.

6.2.1.6 Transit Classification

The SP is not directly involved with the transit traffic; his main concern is to prevent it adversely impacting his managed service traffic. This could be done by always separating out DS and transit traffic, and simply giving absolute priority to the DS traffic. However there may be an opportunity to distinguish between (transit) streaming and data traffic on the HN, and prioritize the former. The problem is that if this traffic is simply bridged, then it may not be seen by what is essentially a L3 classification engine, and indeed if all such traffic was forced via the full classifier, this would require it to be able to operate at a line rate. Further, the SP has no awareness of these transit flows as services which makes a service-based classifier hard to configure. Therefore there is 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. Separation between DS and transit traffic is still maintained.

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

6.2.1.7 Classifier used in the Home Network

6.2.1.7.1 IP Destination Address (IP DA)

This is a particularly useful service 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 unicast address since the use of multicast is likely in the IPTV service. The traffic classification based on both of 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.
- 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 above text is imported from clause 5.5.7.1 of [HGI] with modifications.

6.2.1.7.2 IP Source Address (IP SA)

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

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

6.2.1.7.3 MAC Source Address (SA) and Destination Address (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].

6.2.1.7.4 TCP/UDP Port number

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

6.2.1.7.5 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]. Refer to the document "IPTV related protocols" [FG IPTV-DOC-0191]**.**

6.2.1.7.6 QoS Mapping between different HN technologies

In the case of bridging the HN with the network function, the DNG bridging between different HN technologies needs considerations in order to provide well-harmonized QoS within Home Network. Consideration includes mapping between L2 and L3 marker/classifier and use of marking in the different HN segments.

NOTE – The details of QoS mapping require further study.

6.2.1.8 Downstream and Transit Queue Structure

The main functionality required is to avoid excessive delay and jitter as well as packet loss for multimedia services like IPTV, to provide sufficient bandwidth for them, and to prevent best-efforts traffic being completely starved by higher priority queues.

In the downstream direction there are two concerns, ensuring that traffic from AN is not blocked by transit traffic, and if there is downstream congestion due to a rate mismatch caused by a slow HN technology (Congestion Point (3)), that the value added traffic gets priority. There may be two different types of transit traffic, simple data, and streaming e.g. from a media player. The downstream needs a somewhat simpler queue structure, with four queues (Managed Services from AN, Best Effort from AN, Managed Services within IP-HN-S/P, Best Effort within IP-HN-P/S) per IPI-3 interface.

NOTE – There are three fundamentally different types of traffic with regard to QoS, voice, video and data. Each of these traffic may require its own queues. Also there may be a need to further distinguish between two different types of data (e.g. for higher priority control data or to support a premium data service). Further, the overload protection mechanism requires an additional queue. Counting all of these traffic types with different requirement QoS treatment, five queues as a minimum number may be needed as a result. However, there is a technical possibility to have a smaller number of queues by merging some of these queues. Also, it should be noted that the larger number of queues may increase the implementation difficulty of HN device like DNG. Further study is needed.

NOTE – The above text is imported from clause 5.5.11.1 of [HGI] with modifications.

6.2.1.9 Class Based QoS, Sessions and Policy

QoS approach is essentially traffic class-based, i.e. the QoS treatment is the same for all flows belonging to the same class. This is for reasons of simplicity and scalability. However there is some limited flow awareness to support an overload protection mechanism. Flows are closely related to sessions, which have two possible uses in a QoS scheme – allowing a different per session QoS policy to be applied, and preventing new sessions if they would adversely impact existing ones. 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 below). Therefore a static policy approach has been adopted. The potential downside of this is that there is no mechanism to prevent a new session overloading the class so that the entire class suffers.

NOTE – It is possible for different kinds of IPTV services to be given different QoS treatment. For example, the required QoS treatment for VoD service would be different from 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.

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. DNG is not involved in signalling (except where the service terminates in 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.

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 recognised and an unrecognised 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 IPTV TD. Any packet with the known service class, but unknown instance would be put into a different queue to recognised instances. Each classification rule has an optional pointer to an Application Layer Logic (ALL). For overload protection, the ALG 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 are given along with the requirements in clause 6.4.

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

6.2.2 Quality of Service requirements

This clause specifies the QoS datapath functions which must 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 6-3 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. This diagram is not meant to determine the implementation structure of the QoS functions nor those of the related datapath functions.

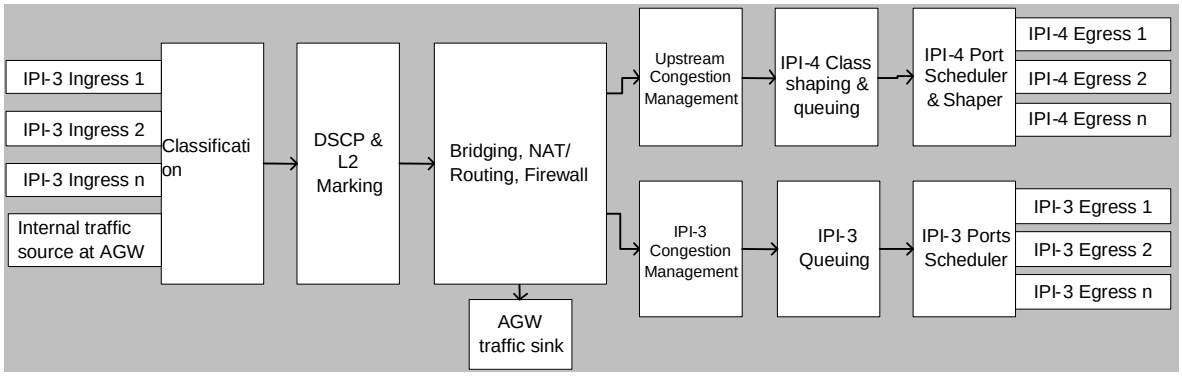


Figure 6-3: QoS Functions from IPI-3 interfaces

Figure 6-4 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.

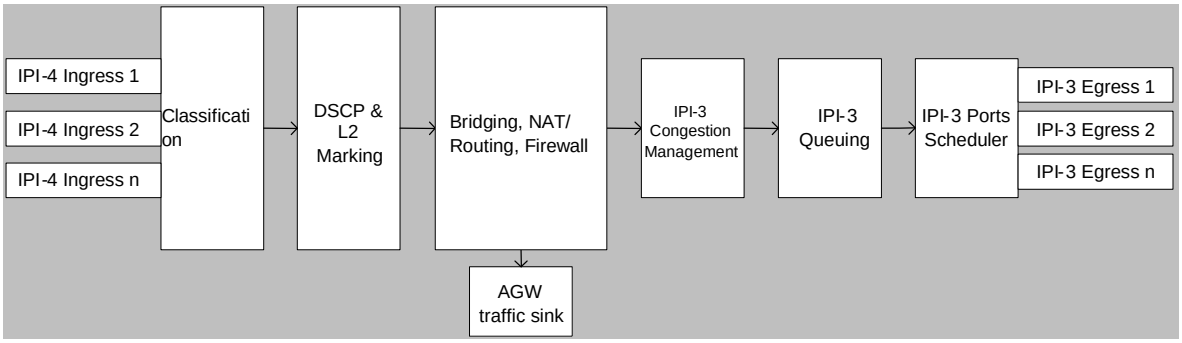


Figure 6-4: QoS Functions from IPI-4 interface

These functions are described in turn below.

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

6.2.2.1 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 above text is imported from clause 6.4.1 of [HGI].

6.2.2.1.1 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 – the packet drop in this context refers to an ingress security 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 required to be able to classify packets based upon any combination of up to 5 of the IPI-4 ingress classification parameters. [HGI_R112]

NOTE – Further study is needed on the number of classification parameters.

- The DNG is recommended to be able to classify packets on any combination of the IPI-4 interface classification parameters. [HGI_R113]

For ATM based access systems, the following requirements also apply

- The DNG is required to be able to classify packets based upon ATM VPI/VCI. [HGI_R114]

Where Ethernet is present on the access link, 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 – The above text is imported from clause 6.4.1.1 of [HGI].

6.2.2.1.2 Requirements for Classification of transit traffic

Normally, traffic which enters the gateway on an Ethernet port and leaves from another Ethernet port is subject to the simple classification described in clause 6.2.2.1.4. In some cases such traffic may require deeper classification. For example, traffic destined to a particular Ethernet port may require deeper classification. The following requirements pertain to the handling of traffic received on the Ethernet ports at IPI-3 interface.

- The DNG is required to support the simple classification of bridged packets as described in clause 6.2.2.1.4. [HGI_R122]
- The DNG is recommended to be able to classify packets received on IPI-3 interfaces and destined to designated IPI-3 Ethernet egress ports according to the multi-field classification described in clause 6.2.2.1.3. These designated IPI-3 Ethernet egress ports is required to be configurable from the management function. Note that multi-field classification of transit traffic may have performance implications. [HGI_R123]

NOTE – The above text is imported from clause 6.4.1.2 of [HGI].

6.2.2.1.3 Requirements for Multi-field Classification 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]

NOTE – At the classification stage, the means of determining whether the packet will be bridged to the LAN is beyond the scope of this specification.

- 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]

NOTE – At the classification stage, the means of determining whether the packet will be sent to the WAN is beyond the scope of this specification.

- 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 required to be able to classify packets received at the IPI-3 interface based upon any combination of up to 5 of the classification parameters. [HGI_R144]
- The DNG is recommended to be able to classify packets received at the IPI-3 interface on any combination of the classification parameters. [HGI_R145]

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

6.2.2.1.4 Requirements for Classification of bridged 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 HN, i.e. simply bridged in DNG.

- The DNG is required to classify all packets received on the IPI-3 interfaces. [HGI_R152]
- The DNG is required to assign each packet to the appropriate egress queues on the basis of the classification result combined with the forwarding decision. [HGI_R153]
- The DNG is recommended to be able to classify packets based upon MAC source or destination address. [HGI_R154r1]
- The DNG is required to be able to classify packets based upon a combination of the classification parameters described in this clause. [HGI_R156]

NOTE – The above text is imported from clause 6.4.1.4 of [HGI].

6.2.2.2 VLAN support at IPI-3 interfaces

- 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 configurable from the remote management server. [HGI_R159]

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

6.2.2.3 Classification Rule Sets

6.2.2.3.1 Overview

This clause describes requirements in the DNG for classification rule sets, which are sets of individual classification rules. This clause also describes requirements for sequencing among the classification rule sets.

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

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

There are distinct classification rule sets which are present in the DNG. They are:

- IPI-4_Rule_Set, which embodies the classification rules for packets arriving on the IPI-4 interface.
- IPI-3_Rule_Set, which embodies the classification rules for transit traffic which is bridged through DNG with no multifield classification.

NOTE – The above text is imported from clause 6.4.3.1 of [HGI].

6.2.2.3.2 Requirements for Classification Rule Sets

- The DNG is required to support a classification rule set for IPI-4 interface (IPI-4_Rule_Set). [HGI_R160]
- The classification rules associated with IPI-4_Rule_Set is recommended to be able to be configured by remote download from the management function. [HGI_R161]

- The DNG is required to support at least one classification rule set for IPI-3 interface: IPI-3_Rule_Set. [HGI_R162]
- IPI-3_Rule_Set contains additional rules for bridged, transit traffic. Individual rules associated with IPI-3_Rule_Set are formed according to requirements in clause 6.2.2.1.4. These are required to be able to be downloaded from the management function, and are recommended to be able to be entered locally by the user. [HGI_R165]
- For each rule in LAN tables 1 and 2 it is required to be possible to configure a pointer to an additional, per packet operation (e.g., application layer logic). [HGI_R166]

NOTE – The above text is imported from clause 6.4.3.2 of [HGI].

6.2.2.3.3 Requirements for Sequencing among Classification Rule Sets

- The first rule match in any RuleSet is required to terminate the classification process for that packet. Note; that if more than one rule match is possible for a given packet, the terminating match will depend on the order in which the rules are specified. [HGI_R172]
- The gateway is required to process the rules in the sequence in which they are configured. [HGI_R173]
- For downstream traffic, the rules in the IPI-4_Rule_Set is required to be tested. [HGI_R175]
- It is required to be possible to configure a default classification in the event of no rule match. [HGI_R176]

NOTE – Testing means that all the classifiers in a rule are checked for a match with the corresponding field in each packet. A rule-match occurs when all the classifiers match.

NOTE – The above text is imported from clause 6.4.3.3 of [HGI].

6.2.2.4 Overload Protection Mechanism

The following requirements relate to the overload protection mechanism which is described in clause 6.2.1. This description is an example of a protection mechanism; alternative protection mechanisms may be employed.

The 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 vendor-specific.

- The DNG is recommended to support a mechanism (e.g. an ALG) which:
  - I. differentiates instances of a service on the basis of one or more single, configured parameters (e.g. IP SA);
  - II. creates a service instance Table entry, for each newly recognised instance of the specified service, subject to a configurable limit. This allows the maximum number of service instances to be constrained if required. There needs to be a Table for each service for which this technique is used;
  - III. increments a packet count every time a recognised 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, a new classification rule is added to the Rules Table. This rule which is a copy of the non-instance specific rule, with the appropriate instance identifier added, and the queue changed to that appropriate for an established flow;

VII. when the lower limit is not met, the instance specific rule is deleted 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 above text is imported from clause 6.4.4 of [HGI].

6.2.2.5 QoS Mappings

In case of using class based QoS in which marker like DSCP is used for traffic prioritisation, each service requiring better QoS treatment needs to be associated with relevant marking. This requires various considerations including, but not limited to, technical requirement and social importance/recognition. ITU-T Rec. Y.1541 gives a good guidance for this discussion.

Also, the marking scheme needs to be well aligned with other marking scheme, 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 mapping table giving association between different mapping schemes. Several documents, for example clause 6.4.5 of [HGI], provide examples and practices.

Hence, QoS mapping is not described in this document and is for further study.

6.2.2.6 Class Queue structure and Scheduling

6.2.2.6.1 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]
- The DNG is required to support at least two strict priority queues per IPI-3 output interface. [HGI_R202]
- The DNG is required to support at least 2 queues which use Weighted Round Robin scheduling per IPI-3 output interface. [HGI_R203]
- The Round Robin weights is required to be individually configurable. [HGI_R204]
- The first strict priority queue (note 1) is required to be given priority over all other queues i.e. served until exhaustion. [HGI_R205]
- The second strict priority queue (Note 2) is required to be given priority over all other queues except the first strict priority queue, but might not be served to exhaustion. [HGI_R206]
- When all strict priority queues are empty, the WRR queues (Note 3) is required to be serviced according to their weighting priority. [HGI_R207]

NOTE 1 – This queue would typically be used for WAN ingress Managed Services

NOTE 2 – This queue would typically be used for transit streaming (audio/video/voice) traffic.

NOTE 3 – One of the WRR queues would typically be used for WAN ingress best efforts traffic, and the other for transit best efforts traffic.

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

6.2.2.7 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 powerline access devices that are connected via Ethernet.

NOTE – The above text is imported from clause 6.4.9 of [HGI].

- 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 – The above text 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 device within IP-HN-S and IP-HN-P is recommended to determine the QoS treatment accorded to packets by internally translating the received DSCP value to User Priority.

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

6.3 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. virus, on a home network device (e.g. a PC) on the home network may make the device unusable. Attacks on information that are 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" [FG IPTV-DOC-0188] for more details on security issues in home networks.

6.3.1 Home Network Security Threats

Home networks that are used to deliver IPTV services have the same characteristics as defined in ITU-T Recommendation X-1111 [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/Interception attacks.

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

6.3.2 Home Network Security Requirements

The security for Home Network is required to support the following requirements:

- The DNG needs to be authenticated by management system;
- The DNG authentication is required to be service independent;
- Support a specified list of ALGs, and the list can be upgraded;
- Provide a Firewall function which is remotely configurable;
- 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 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].

6.4 Interoperability between IPTV core/access network and home network

6.4.1 Protocols

The DNG is connected to the Access Network and functional entities beyond it by the protocols specified for IPTV service. Refer to the document "IPTV related protocols" [FG IPTV-DOC-0191].

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

6.4.2 Interface

Refer to clause 6.1 for the interface definition.

6.5 Interoperability among home network devices

6.5.1 IEC62481 (DLNAH) based

The IPTV TD should support [IEC62481-1] and [IEC62481-2] for interconnection with HN-TD devices, such as display devices. The Home Network area associated with IEC62481 is IP-HN-S (see Note 2).

In this model, the IPTV TD and HN-TD should work as the DMS and DMP, respectively (see Note 1 below). It is also noted that there might be a possibility for the IPTV TD to act as a DMP, but this is up to the implementation.

NOTE 1 – Some types of HN-TD, such as external PVR may act as a DMS.

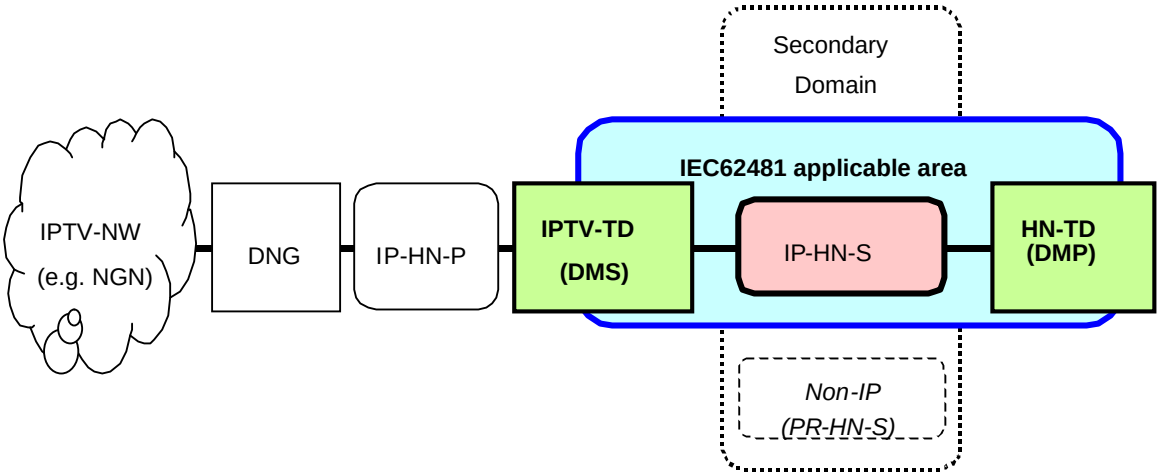


Figure 6-5: Usage of IEC62481 in the IPTV context

The HN-TD connected to IPTV TD should 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 PVR residing in the IPTV TD (Note 3, 4, 5).

NOTE 2 – The applicability of IEC62481 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 3 – There may be other service cases that are enabled by IEC62481 or technologies based on it. Further study is needed.

NOTE 4 – There is a possibility that IEC62481 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 usage cases defined in IEC62481 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.

6.5.2 ISO/IEC 29341 (UPnP) based

NOTE – Refer to Appendix II.

6.6 The DNG

6.6.1 DNG Functional Overview

There are multiple possible implementations of a DNG device. The clauses below are based on the HGI document [HGI] with some modifications that are specific to IPTV.

ISO/IEC15045-1 also provides a generic framework of a DNG device. For details, Annex A describes ISO/IEC15045-1 and necessary considerations for IPTV services.

6.6.1.1 Basic Assumptions

The DNG is an always on, always connected device, which acts as the central point for distributing IPTV contents in the residential environment. It is supposed that there is only one DNG per household which is connected to a single 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 HN, as well as on bi-directional communication flows between the Home Network and the (broadband) Access Network. Given the variety of Access Network technologies, DNG Architecture has to be flexible in terms of providing the support for different IPI-4 interfaces 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 enable important features related to provisioning and OAM, remote management of DNG, 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 processing and software capabilities to deliver the service (i.e. legacy TV display used for an IPTV service).

The gateway 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 – The above text is imported from clause 5.3.1 of [HGI].

6.6.1.2 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 6.6.2, 6.6.3, 6.6.4 and 6.6.5.

The information flows 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 DNG itself. OAM information flows are included here.

The functionality of interfaces and functionalities of a DNG is described as follows:

IPI-4 interface: This block describes 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: This block describes the physical interfaces towards the home network and the related functionalities at layer 1 and 2. A number of different interfaces $I_1 \ldots I_n$, are included. A distinction should be made between the interfaces corresponding to different HN technologies (Ethernet, Wi-Fi, USB, …) 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. Wi-Fi security (WEP/WPA keys and ACL management) is included here.

Packet processing: This block describes the interconnection functions at layer 2 and/or layer 3 for upstream, downstream and transit traffic. This means relaying, forwarding, bridging, and also NA(P)T functions if appropriate. The internal connection functions also include the routing of IP-traffic which is meant for, or coming from, DNG itself (local traffic). The block also includes the classification and queuing functions related to QoS management and the filtering and encryption functions related to security, as well as specific

service-related functions. These tasks are performed only on the basis of information contained on the Ethernet or IP header; this block does not perform any functions involving an analysis of the packet payload.

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

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

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

Management: This block consists of the management communication stacks and the management handling. It contains all the functionality needed to manage 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 DNG.

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

Basic system features: This part contains the powering and the processing performance blocks. These two blocks 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 document.

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

6.6.2 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 statements:

- DNGIPI-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. (Note) [HGI_R2]

NOTE – The relevant IPI-4 interface requirements are provided in clause 6.6.2.1, 6.6.2.2, 6.6.2.3 and 6.6.2.4.

NOTE – The above text is imported from clause 6.1 of [HGI].

6.6.2.1 Type 1: ATM over DSL Interface

- DNG, if NT with ATM over DSL interface is incorporated, is required to support ADSL2+ access network technology as per [ITU-T G.992.5]. [HGI_R5]
- DNG, if NT with ATM over DSL interface is incorporated, is required to support backward compatibility with ADSL [ITU-T G.992.1] and ADSL2 with Annex L [ITU-T G.992.3]. [HGI_R6]

- Upgradeability from ADSL2+ to VDSL2 [ITU-T G.993.2] (profile 8a,b,c,d) is recommended to be provided by DNG. [HGI_R11]
- DNG, if NT with ATM over DSL interface is incorporated, is required to support ATM over ADSL2+, ADSL2 and ADSL [ITU-T I.361/365] and [RFC2684] with PVC management. [HGI_R12]
- DNG, if NT with ATM over DSL interface is incorporated, is required to be preconfigured either with a "search list" of possible VPI/VCI values (at least 0/35, 0/38, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 1/32, /32, 8/48) or DNG is required to be preconfigured with a set of VPI/VCI default values specified by the operator. [HGI_R13]
- DNG, if NT with ATM over DSL interface is incorporated, is recommended to support ILMI (Integrated Local Management Interface protocol) to configure ATM and encapsulation parameters, following the guidelines in DSL Forum [DSLF TR-062] and ILMI ATM Forum 4.0 specification. [HGI_R14]
- If both DNG and the network support ILMI, then ILMI is required to override the ATM and encapsulation parameters. [HGI_R15]
- DNG, if NT with ATM over DSL interface is incorporated, can optionally support auto-discovery of other VPI/VCI sets (NOTE – auto-discovery should only be used when all other ATM mechanisms have failed). [HGI_R16]
- DNG, if NT with ATM over DSL interface is incorporated, is required to be capable of supporting at least 8 PVCs in order to manage multiple service provisioning to LAN attached End Devices. [HGI_R17]
- Dual bearer/Dual Latency (interleaved and fast channels) is recommended to be supported. [HGI_R18]
- If Dual Bearer/Dual latency is supported, the related parameters such as min rate, max rate and bandwidth ratio between interleaved and fast is required to be configurable per PVC. [HGI_R19]
- The following ATM traffic classes are required to be supported: CBR, VBR-rt, VBR-nrt, and UBR. [HGI_R20]
- DNG, if NT with ATM over DSL interface is incorporated, is required to be able to reply to OAM F5 cells conforming to ITU-T I.610. [HGI_R21]
- DNG, if NT with ATM over DSL interface is incorporated, is required to reply to F5 VC-AIS cells with VC-RDI. [HGI_R22]

NOTE – The above text is imported from clause 6.1.1 of [HGI].

6.6.2.2 Type 2: Ethernet over DSL Interface

- DNG, if NT with Ethernet over DSL interface is incorporated, is required to support VDSL2 ITU-T G.993.2 (profile 8a, 8b, 8c and 8d) access technology for Central Office deployments with co-existence with ADSL2+. [HGI_R23]
- DNG, if NT with Ethernet over DSL interface is incorporated, is required to support VDSL2 ITU-T G.993.2 (profile 12a, 12b, 17a and 30a) access technology for MDU deployments with short loop lengths and no co-existence with ADSL2+. [HGI_R24]
- DNG, if NT with Ethernet over DSL interface is incorporated, is required to support backward compatibility with ADSL, ADSL2 and ADSL2+. [HGI_R25]
- DNG, if NT with Ethernet over DSL interface is incorporated, is required to support PTM-TC (Packet Transfer Mode – Transmission Convergence) for Ethernet packets [IEEE EFM 802.3ah standard]. [HGI_R27]
- DNG, if NT with Ethernet over DSL interface is incorporated, is recommended to support Dual Bearer for PTM-TC. [HGI_R28]

- DNG, if NT with Ethernet over DSL interface is incorporated, is recommended to support Dual Latency for PTM-TC. [HGI_R29]
- DNG, if NT with Ethernet over DSL interface is incorporated, is required to support Pre-emption for PTM-TC. [HGI_R30]
- DNG, if NT with Ethernet over DSL interface is incorporated, is required to support the related Ethernet protocols at layer 2, with VLAN management (support for untagged frames and 802.1Q tagged frames containing priority-tagged information (IEEE 802.1p and VLAN-ID information) on the WAN side. [HGI_R31]

NOTE – The above text is imported from clause 6.1.2 of [HGI].

6.6.2.3 Type 3: IPI-4b Interface

- DNG, if IPI-4b interface equipped, is required to support Ethernet 100Base-TX technology for twisted pair (Cat-5 or Cat-6). [HGI_R32]
- 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 802.1Q tagged frames containing priority-tagged information [IEEE 802.1p] and VLAN-ID information) on the IPI-4 interface. [HGI_R33]

NOTE – The above text is imported from clause 6.1.3 of [HGI].

6.6.2.4 Combination of IPI-4a and IPI-4b

- DNG can optionally be equipped with a combination of Type 1 & Type 3 or Type 2 & Type 3 interfaces. [HGI_R34]
- In the above case the Type 3 interface is required to be separate from the Type 1 or Type 2 interface and presented on a dedicated physical connector. [HGI_R35]
- Only one of these interfaces is required to be active at any time. [HGI_R36]

NOTE – The above text is imported from clause 6.1.4 of [HGI].

6.6.2.5 IPI-4c for coaxial interface

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

6.6.2.6 IPI-4d for wireless interface

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

6.6.2.7 IPI-4e for optical access network

- DNG, if contains NT function, is required to comply with one of the following access network.
  - ITU-T Rec. G.983.
  - ITU-T Rec. G.984.
  - IEEE Std. 802.3ah.

6.6.3 IPI-3 Side Interfaces

The requirements in this clause are related to the physical interfaces and MAC layers of the Home Network technologies supported in the DNG. These include both wired and wireless standards for device connectivity. Any higher layer protocols are not covered in this clause.

- 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 is required to support auto sense between full or half duplex and auto sense between 10 and 100 Mbps and auto sense between MDI and MDI-X. [HGI_R39]
- DNG is required to support a MAC frame format which complies with [IEEE 802.3] (length/type formats) and [IEEE 802.1q] (VLAN). [HGI_R41]
- If DNG is equipped with Wi-Fi and Bluetooth, then it is required to include a hardware synchronization mechanism, to avoid mutual interference. [HGI_R47]

NOTE – The above text is imported from clause 6.2 of [HGI].

6.6.3.1 IPI-3e Interface requirements

If wireless interface is used for IPI-3, the following requirements are applied.

- DNG is required to include an IEEE 802.11b/g access point. [HGI_R49]
- DNG can optionally include an IEEE 802.11a interface. [HGI_R50]
- DNG is required to comply with the regional/national regulations. [R1]
- DNG is required to be configurable either to broadcast or hide every single SSID it supports. [R58]
- By default, DNG is recommended to hide SSIDs. [HGI_R59]
- DNG is required to implement an automatic radio channel selection mechanism to choose the channel with least interference on power up or following a manual request. [HGI_R60]
- Periodic channel selection can optionally be performed provided that service is not affected. [HGI_R61]
- Automatic radio channel selection is required to be able to be enabled/disabled from the local configuration interface as well as from the management functions. [HGI_62]

NOTE – The above text is imported from clause 6.2.1 of [HGI].

6.6.4 Packet processing

6.6.4.1 Support of routed model and extensions IPI-4 side

- DNG is required to support at least one IPI-4 interface as logical interface. [HGI_R64]
- DNG, if IPv4 is used, is required to acquire from IPI-4 interface using DHCP or PPP IPCP all the information needed to support the routed mode of operation (i.e. DNS primary & secondary address, IP address, subnet mask, gateway address). [HGI_R65]
- DNG is required to support static provisioning of the above information, via local configuration. [HGI_R66]
- DNG is required to support a method to make its IPI-4-side IP address known to the management functions, for remote access and configuration purposes. [HGI_R67]

NOTE – The above text is imported from clause 6.3.1 of [HGI].

6.6.4.2 Support of routed model and extensions IPI-3 side

6.6.4.2.1 NAT

If NAT is supported in the DNG, the following requirements are applied.

- DNG is required to support NAT/NAPT as described in [IETF RFC 2663], IETF RFC 3022], [IETF RFC 3027] and [IETF RFC 3489]. [HGI_R71]
- DNG is required to support either "full cone" or "restricted cone" or "port restricted cone" NAT implementation as described in [IETF RFC 3489]. [HGI_R72]
- DNG is required to support configurable port forwarding for access to devices on the HN. [HGI_R73]
- DNG NAT tables is required to be filled either by the remote management system or by the user. [HGI_R74]
- Rules defined by the Remote Management System are required to have a higher priority than rules defined by the user. [HGI_R75]
- NAT/NAPT capability of DNG is required not to give any negative impact on the traffic associated with IPTV service across the gateway.

NOTE – The above text is imported from clause 6.3.2.1 of [HGI].

6.6.4.2.2 IP Addressing schemes

- DNG is required to support partial L2 bridging for upstream PPPoE traffic recognizing the related broadcast messages and creating appropriate bridging for correct MAC addresses. [HGI_R76]
- DNG is required to allocate a private IP address to its IPI-3 side interface. [HGI_R77]
- DNG IPI-3 side IP address is required to be on the same subnet as the devices on the Home Network. [HGI_R78]
- DNG IPI-3 side IP address is required to be used as the Default Gateway in DHCP replies. [HGI_R79]

NOTE – As all IPI-3 interfaces are bridged, only one IP address is needed, which is used by all interfaces.

- DNG is required to allow LAN bridging between different interfaces, enabling intra-LAN connectivity. [HGI_R80]

NOTE – The above text is imported from clause 6.3.2.2 of [HGI].

6.6.4.2.3 IPI-3-side DHCP requirements

- An IPI-3 side DHCP server, if IPv4 is used in Home Network, is recommended to be available on DNG. [HGI_R81]
- DNG, if IPv4 is used in Home Network, is recommended to support a means to remotely configure its own DHCP server. [HGI_R82]
- The DHCP server is required to support fixed IP address allocation to specific device name or MAC addresses to be used in combination with port forwarding/DMZ host. [HGI_R85]
- The DHCP server can optionally provide the same IP address to each device. [HGI_R86]
- Where the DHCP server assigns private IP addresses to requesting devices on the home network, they are required to be on the same subnet [IETF RFC 1918]. [HGI_R87]
- DNG is required to support use of public IP addresses (that are within the proper subnet mask defined for the IP connection to AN) on the HN and properly route the device traffic. [HGI_R88] (Note)

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

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

6.6.4.3 Support of Hybrid Model and Extensions

- If DNG has an ATM IPI-4 interface, it is required to support [IETF RFC 2684] for multi protocol Ethernet bridged encapsulation over AAL5. [HGI_R89]
- DNG is required to support configuring and enabling multiple instances of bridging between WAN side logical interfaces (PVC, VLAN …) and LAN side physical (Ethernet Port, SSID …) interfaces. [HGI_R90]
- DNG is required to support configuring and enabling one or more IPI-4 logical interfaces and one or more physical IPI-3 interfaces, to be routed (as described in clauses 6.6.4.1 and 6.6.4.2). [HGI_R91]
- DNG is required to run both bridging and routing simultaneously. [HGI_R92]
- DNG is required to be able to forward traffic over the right connection (in the case of multiple PVCs, multiple PPPoE sessions, multiple VLANs, etc.), on the basis of a number of parameters to be used as classifiers, and defined in [DSLF TR-068]. [HGI_R93]

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

6.6.4.4 Session Initiation and Support

- DNG is required to operate an "always on" mode for connections. If DSL access network is used, the DNG is required not to time out DSL sessions (ATM, 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 above text is imported from clause 6.3.4 of [HGI].

6.6.5 Service Support

- A dynamic DNS client is recommended to be provided on 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]
- DNG is required to have a unique hardware ID for authentication and remote management purposes, composed of an organizationally unique identifier (OUI) + serial number. [HGI_R350]
- DNG is required to support a time server client to obtain the time and date.[HGI_R351]
- A NTP [IETF RFC 1305] or SNTP [IETF RFC 2030] client is required to be implemented to allow synchronization with the provider's NTP server. [HGI_R352]
- DNG is required to advertise all the information related to the network NTP or SNTP server towards the home devices. [HGI_R353]
- Information related to the network NTP or SNTP server towards the home devices is required to be retrieved using DHCP option 42 (or 4 in case of SNTP). [HGI_R354]

DNG is required not to implement any explicit function to reset time and date. [HGI_R355]

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

6.6.5.1 ALGs

- DNG is recommended to support an Application Layer Gateway to support the interoperability with NAT mechanisms for the protocols listed in the document "IPTV related Protocols" [FG IPTV-DOC-0191]. [HGI_R356]
- DNG ALGs is required to be able to be switched off in case of conflicts with external devices using STUN for NAT traversal. [HGI_R358]

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

6.6.5.2 Multimedia Services Support

- DNG is required to support IGMP v1/v2 according to [IETF RFC2236]. [HGI_R384]
- DNG is recommended to support v3 Querier function according to [IETF RFC3376]. [HGI_R385]
- If a multicast stream data flow coming from the AN is NOT terminated in DNG, DNG is required to keep a record of which devices are subscribed to which multicast group. This can be done via IGMP snooping or RTSP ALG techniques. [HGI_R386]
- If a multicast stream data flow coming from the AN is NOT terminated in DNG, 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 DNG, 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 this is a multicast stream in the home network, DNG is required to support a capability to perform a link layer multicast to unicast translation. [HGI_R389]

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

6.6.6 IGMP Functionality

6.6.6.1 IGMP Proxy

An IPTV TD should support IGMP proxy for IGMPv2 and IGMPv3. 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 should be possible to select the proxy interface by static configuration or a dynamic mechanism like 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 must 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 6-6).

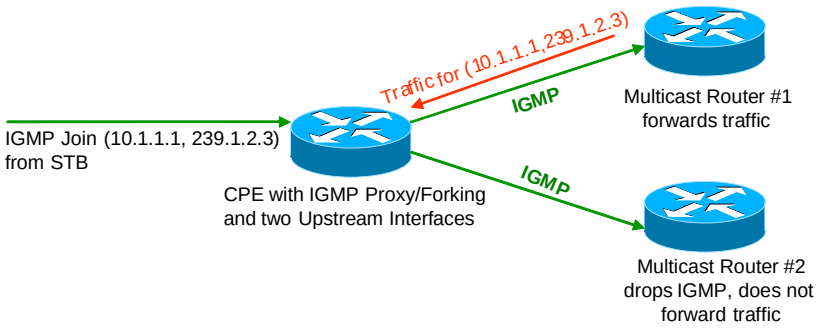


Figure 6-6: IGMP Proxy in Forking Mode

6.6.6.2 Source Specific Multicast

The proxy must support Source Specific Multicast in the standard SSM address range 232/8. SSM should be supported in other address ranges as well. All IGMPv3 filter modes should be supported.

6.6.6.3 Filter

L3 Filters for IGMP should be supported. It should be possible to exclude 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. A mechanism should be provided to configure the filters (e.g. analogue to port forwarding rules or firewall rules).

7 Remote management

When IPTV services are deployed, a large number of IPTV terminal devices must be managed by the service provider, and these devices may need to be managed remotely. Thus it is very important for service providers to have a standardized way to remotely manage numerous terminal devices in an efficient and economical way. This clause discusses the remote management aspect of IPTV services.

NOTE – There are many remote management standards that are being used in the industry. Refer to the "Aspects of IPTV End System – Terminal Device" document [FG IPTV-DOC-0192] for an exemplary list of such standards. For example, the TR-069 based scheme proposed by the DSL Forum and the OMA-DM based scheme that was proposed by the Open Mobile Alliance (OMA) and is being used by the wireless industry. Since the discussion on the remote management aspect of the home network in this document is based on the HGI Release 1 document [HGI] the following clause refers mainly to the techniques described in the TR-069 on which the HGI Release 1 was based. The OMA-DM standards is relatively new and its application to this document will be the subject for further study.

7.1 Management Architecture

Remote management is an aspect of the specification of the DNG. The main remote management functionalities are divided into a list of general management requirements. These requirements helped to determine the best mechanisms to implement them. One solution is using the approach based on the work of DSL Forum remote management procedures that are described in [DSLF TR-069]. Various amendments, additions and the selection of some options from the DSL Forum specification are detailed in this document.

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

The Remote Management System (RMS) or Auto Configuration Server (ACS) has a TR-069 interface and data model to control and configure the DNG and TR-069 enabled devices located in the home network (HN) remotely.

The DSL Forum has defined several device management protocol standards.

- TR-069: defines the CPE Remote Management Protocol (CWMP); also defines v1.0 of the Internet Gateway Device data model but HGI Release 1 specifications [HGI] are based on v1.1 of this data model, which is defined in [DSLF TR-098].

- TR-111 part 1: allows an ACS managing a device to identify the associated HG through which that device is connected.

- TR-111 part 2: allows an ACS to initiate a TR-069 session with an ED that is operating behind a NAT gateway.

The following data model standards are also defined by the DSL Forum:

- TR-106: defines baseline data model requirements for all TR-069 HGs and EDs.

- TR-098: defines v1.1 of the Internet Gateway Device HG data model.

- TR-104: defines v1.0 of the VoIP ED data model.

The DNG is under the control of a single RMS. When an end-device is being managed this is done using the mechanism described in [DSLF TR111] part 2 which means that DNG is transparent to this process.

The high level management architecture and the entities involved are shown in Figure 7-1.

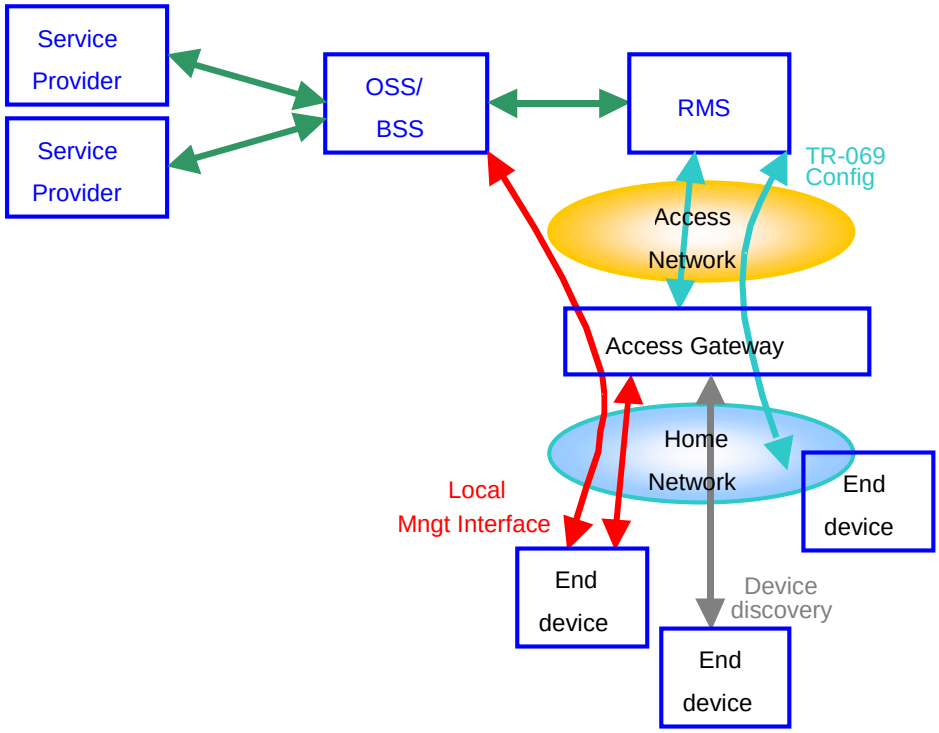


Figure 7-1: Management entities interactions

NOTE – The "Access Gateway" is the figure above is same as the DNG in this document.

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

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

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

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

The management architecture of the DNG is shown in Figure 7-2 from a functional perspective. The main components and external interfaces are illustrated. The figure also includes the Remote Management System (RMS) and the managed and unmanaged end devices (ED) in the home network. This is done as both the ACS (a TR-069 capable RMS) and the EDs are part of the end-to-end management behaviour.

DNG management architecture can be broken down into these main functions:

- Device Management
- QoS Management
- Security Management
- Configuration Management
- Firmware Upgrade Management
- Performance Monitoring
- Diagnostics and Troubleshooting (alarms/notifications and log management)

Two other components are identified:

- CWMP Client
- Local Management Application

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

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

The main DNG management interfaces are:

- $I_{HG\text{-}LM}$ for local management, which is an HTML interface
- $I_{HG\text{-}ACS}$ for remote management, which is a CWMP interface

The ED interfaces are:

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

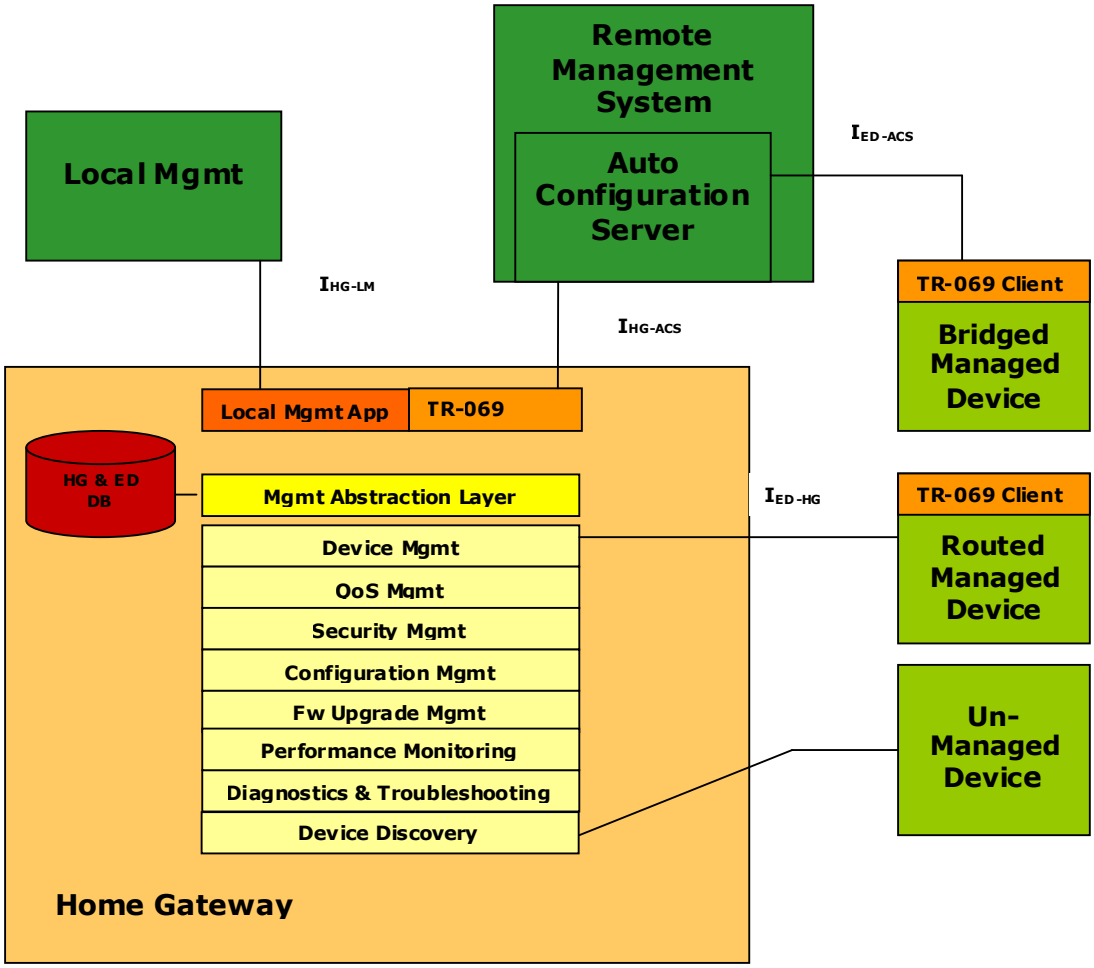


Figure 7-2: Management Architecture

NOTE – The above text is imported from clause 5.4 of [HGI].

7.1.1 Device Management

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

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

The DNG should also enable some remote management of simple end devices that do not support TR-069, but rather UPnP or even only DHCP. Release 1 only deals with the discovery of such non-TR-069 managed devices. The service provider can use this information to optimize the remote management of the (TR-069) managed devices and to optimize customer service. It is assumed that the RMS only communicates with the HN using TR-069, and therefore three remote management models can be distinguished. The models are depicted in Figure 7-3, Figure 7-4 and Figure 7-5. They are:

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

- the remote management model for UPnP- and DHCP-enabled end devices with the DNG operating in proxy (routed) mode.

This document supports all three models.

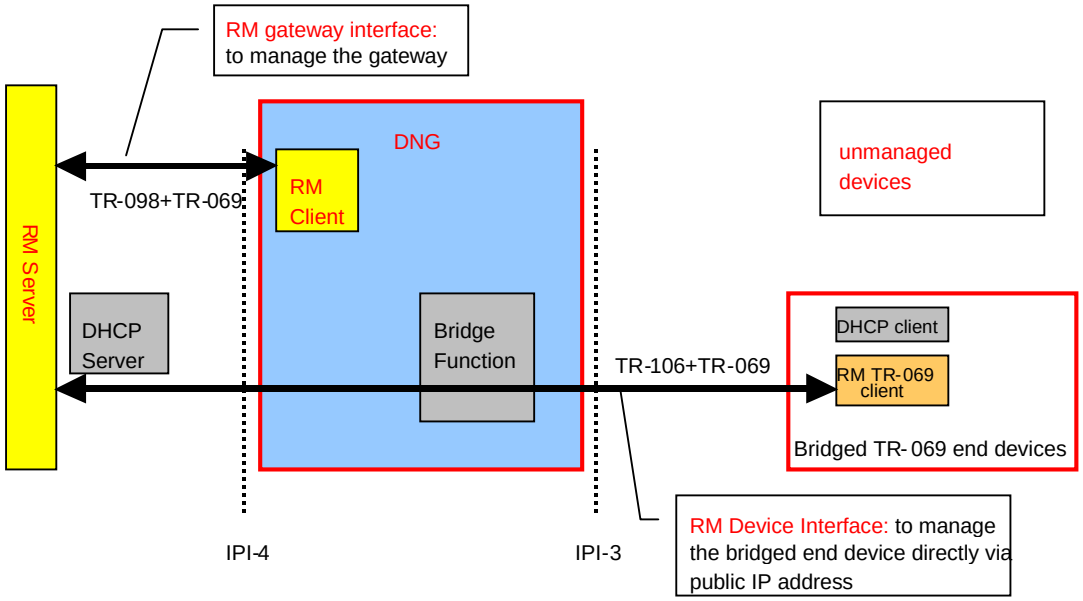


Figure 7-3: Remote management model for TR-069-enabled end devices with the Home Gateway operating in bridged mode

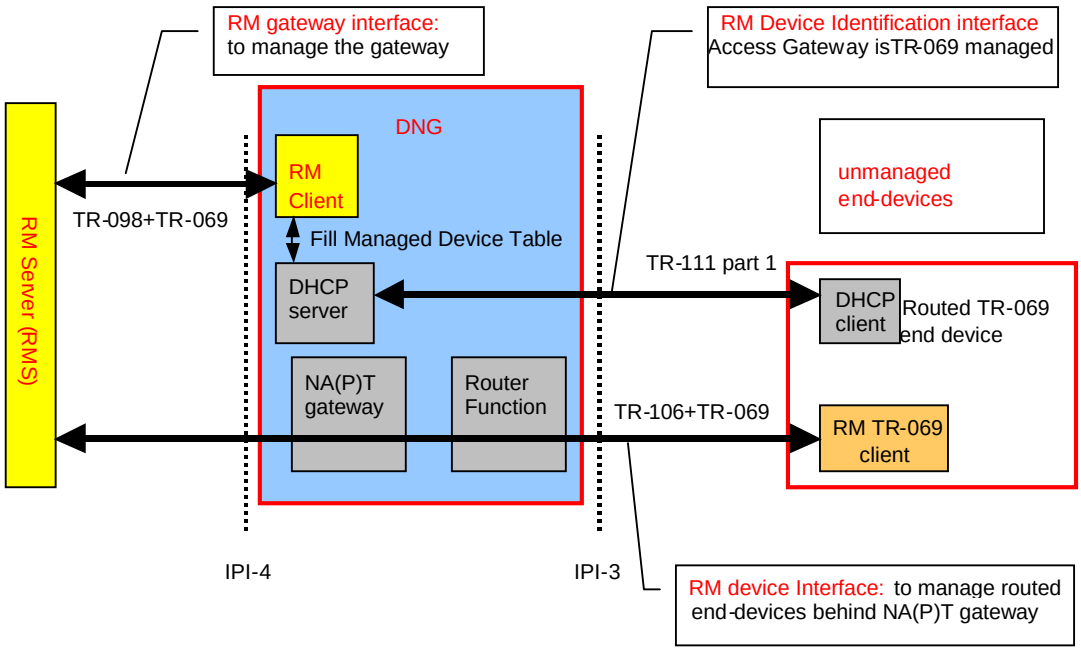


Figure 7-4: Remote management model for TR-069-enabled end devices with the Home Gateway operating in routed mode

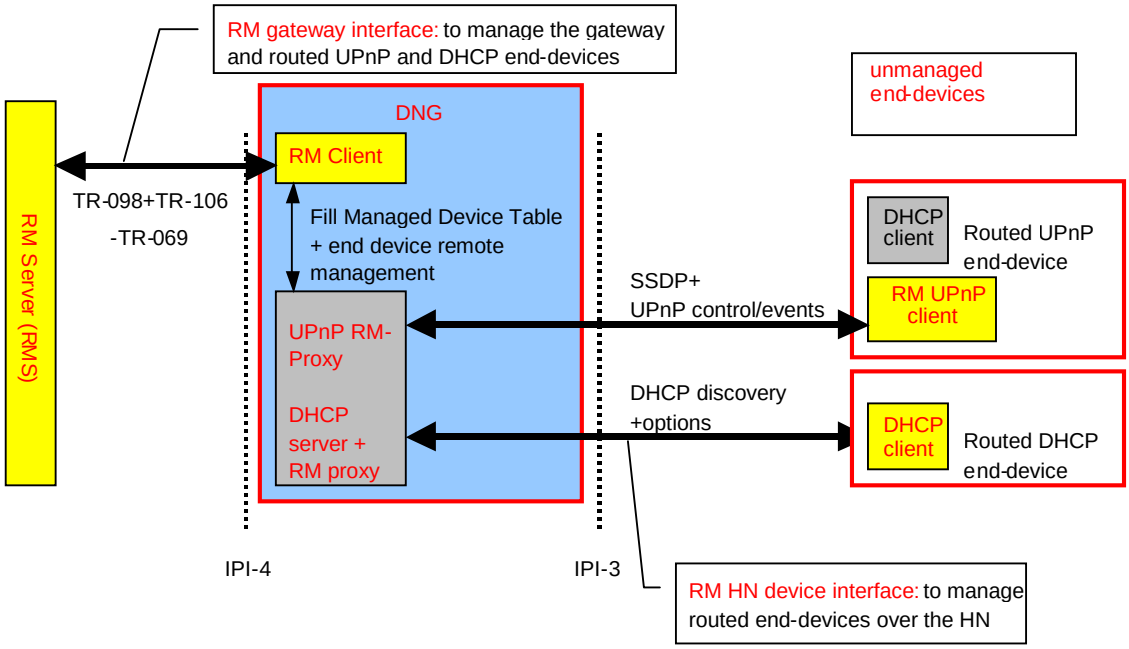


Figure 7-5: Remote management model for UPnP and DHCP-enabled end devices with the Home Gateway operating in proxy mode.

A distinction is made between managed and unmanaged end devices.

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

In the requirements clause the terms "manageable device" and "unmanageable device" are also used. Their definitions are slightly different from the ones above:

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

This is summarized in Table 7-1:

Table 7-1: Schematic representation of the definitions of (un)managed and (un)manageable devices

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

Legend: In the above table "X" means applicable, "-" means not applicable and "?" means may or may not apply.

This document requires the DNG to discover and identify uniquely the managed devices, and it should discover and identify uniquely the manageable but unmanaged devices connected to the home network. From Table 7-1 it follows that all end devices with a remote management client should be discovered (or "must" be in the case where they are managed). It is useful to distinguish these devices by way of the remote management client(s) they support. Six types can then be distinguished. These are given in Table 7-2 and are referred to in the requirements clause. The columns represent the various device types, and the rows show which remote management client stack is supported by the each device types.

Table 7-2: Types of managed and (manageable) unmanaged devices

Client\Type	Z	D	U	CD	CU	C
CWMP				X	X	X
UPnP			X		X	
DHCP		X	X	X	X	

Table 7-2 can be read as follows:

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

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

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

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

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

The discovered ID information is used by DNG to fill a Managed Devices Data Base that can be read by the remote management server. In Figure 7-6 the Managed Devices DB is given as a logically separate unit. However, it should be included in DNG data model as defined by the DSL Forum, in order to be readable by the ACS with CWMP.

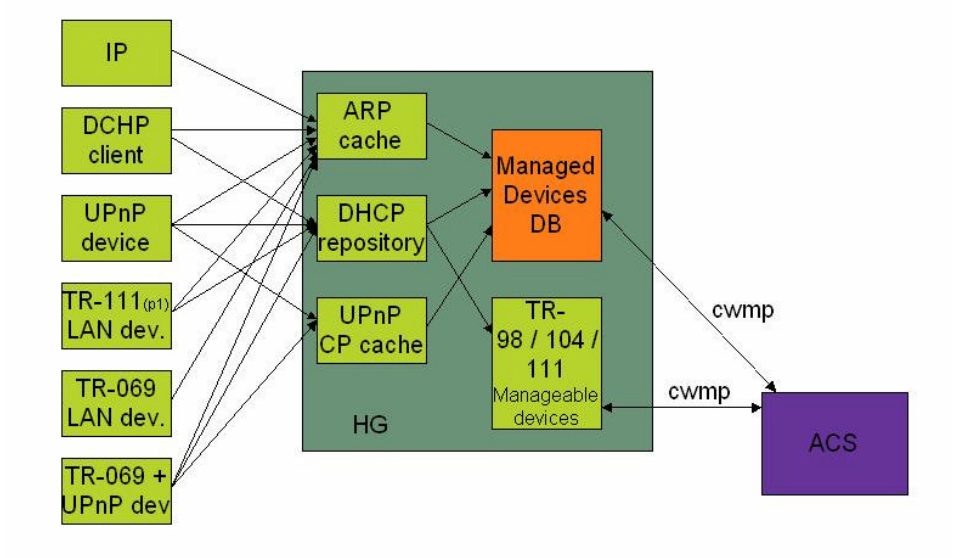


Figure 7-6: Device management and discovery

NOTE – The above text is imported from clause 5.4.1 of [HGI].

7.1.2 QoS Management

QoS Management is a critical aspect of ensuring the correct delivery of the services. However the definition and mechanisms of QoS management are covered in QoS clauses 6.2.1 and 6.2.2.

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

7.1.3 Security Management

Security and privacy are critical issues in the home environment. 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 above text is imported from clause 5.4.3 of [HGI].

7.1.4 Performance Monitoring and Diagnostics & Troubleshooting

Any DNG system level fault (e.g. Hardware, O.S. and SW 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 request.
- Performance monitoring will be also available in order to see statistics (for example at 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 will affect the normal working operation of the DNG).

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

7.1.5 Local Management Application

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

The Local Management interface is the access method the end user will have to view or make changes to DNG configuration, user managed services, user managed end devices and other "safe" settings.

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

- ACS management (super user) can manipulate all managed objects in DNG including lower order user rights
- Administrator management can manipulate objects that do not interfere with ACS or managed service operation. 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 to limit this to a local Administrator. This 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 7-7, an overview of the local management interface is provided. On the access network side, the RMS or ACS will configure parameters of this interface through the CWMP management interface as defined in Figure 7-2.

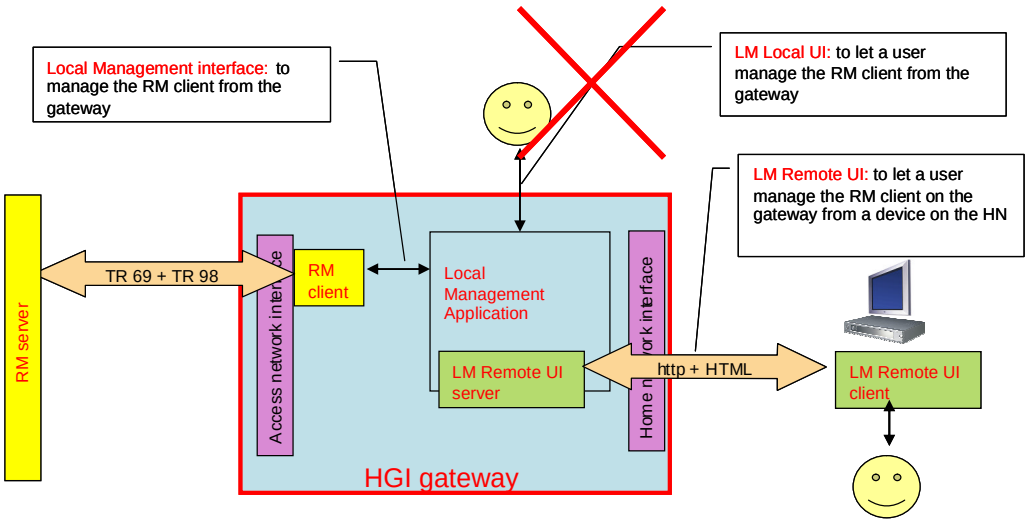


Figure 7-7: Local Management Interface overview

NOTE – The term "HGI gateway" in the figure above is same as DNG in this document.

In 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 DNG and therefore DNG must be able to connect to a display device and some input device (such as IR remote control). This is not supported in Release1.

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

7.2 Management requirement

As one solution this clause is compliant with [DSLF TR-069], [DSLF TR-098], [DSLF TR-104], [DSLF TR-106] and [DSLF TR-111] except where this is explicitly mentioned. If there are still any ambiguities or conflicts in the text, it must be assumed that compliance with the above mentioned TR documents supersedes any other requirements.

NOTE – The above text is imported from clause 6.5 of [HGI].

7.2.1 Northbound Interfaces

- DNG/ACS communication interface is recommended to comply with all the mandatory requirements of the CWMP protocol v1 as defined in [DSLF TR-069]. [HGI_R214]

NOTE – The above text is imported from clause 6.5.1 of [HGI].

7.2.2 RMS requirements

- The RMS is recommended to be able to manage the DNG using the CWMP protocol as described in [DSLF TR-069] (the ACS referenced there is a TR-069 capable RMS in this specification), including device configuration, software updates, and device diagnostics. [HGI_R216]
- The RMS is recommended to be able to support TR-098, TR-104, and TR-106 data models and their extensions as defined by HGI. [HGI_R217]
- The RMS is recommended to support extensibility for vendor-specific data model extensions. [HGI_R218]
- The RMS is recommended to be able to manage end user devices behind the DNG using CWMP. [HGI_R219]

NOTE – The above text is imported from clause 6.5.2 of [HGI].

7.2.3 General DNG configuration and management

- DNG can optionally support and implement a local management graphical user interface. [HGI_R225]

The DNG is recommended to automatically establish a CWMP management session with the ACS in the following cases, as defined in [DSLF TR-069]:

- Each time the IP address of DNG changes.
- On power-up or reset.
- After a time-out following management session period expiration.
- After configuration changes in the DNG and the related notifications are activated and the related Active Notification attributes are set.
- After a connection Request from the RMS (or ACS). [HGI_R226]
- The data exchanged between the DNG and the management functions is recommended to be encrypted, except for the firmware images for in-band management (note). It is recommended to be encrypted for out-of-band management (note). The level of encryption of the exchanged data is the one defined in [DSLF TR-069] (SSL or TLS level). [HGI_R227]

NOTE – In-band management: The management session is established in the same communication channel as the data (same VC, VLAN…)

NOTE – Out-of-band management: The management session is established in a separate communication channel from the rest of data (dedicated VC, VLAN…)

- All authentication and configuration traffic from local clients to the DNG and vice-versa can optionally be encrypted. [HGI_R228]

- The firmware image file recommended to be signed to ensure its correctness and integrity during the transmission. [HGI_R229]
- Service provider or customer specific data, such as password or personal information, is required not to be located in any software file image or software module file image. Therefore software that is transferred between RMS and the DNG can optionally be encrypted. [HGI_R230]
- In order to be able to start communication with the ACS, the DNG is required to be able to discover its address by one of the following mechanisms:
  - The ACS URL is preconfigured
  - The ACS URL is locally inserted in a secure way through the LM Remote UI. [HGI_R231]
- The DNG is required to allow the ACS to modify the ACS URL remotely. [HGI_R232]
- The DNG is required to identify itself to the ACS with its serial number and OUI, as defined in TR-069. If the serial number is not unique across the product line, the product class is also required to be provided. [HGI_R233]
- The DNG is required to support auto-provisioning of basic L2 and L3 connectivity for the management communication channel:
  - When using DHCP, authentication is required to be based on the hardware address of the DNG WAN interface or the line identification.
  - When using PPP, authentication is required to be based on a generic username/password burnt in the firmware of the DNG or provided locally in a secure way.
  - When using ATM networks, the DNG is required to be preconfigured with ATM VC configuration. Nevertheless it is recommended to support ILMI to configure automatically ATM connectivity. HGI_R234]

NOTE – The above text is imported from clause 6.5.3 of [HGI].

7.2.4 End-device management

7.2.4.1 Device Identification

- If IPTV TD is a managed device, the DNG is required to discover and identify uniquely it. [HGI_R254]
- If IPTV TD is an unmanaged device, the DNG is recommended to discover and identify uniquely it. [HGI_R255]
- A database of devices (device repository) can optionally be held in the DNG. This database contains the results of the device discovery and capabilities detection mechanisms. [HGI_R257]
- For every ED (managed and unmanaged), the DNG is recommended to determine the IP address and hardware address from its ARP cache, if not obtained via DHCP. [HGI_R263]
- The discovery mechanism is required to apply to any new managed IPTV TD that is connected to the HN. [HGI_R271]
- The discovery mechanism is required to apply to unmanaged IPTV TD. [HGI_R272]
- DNG is required to discover the managed IPTV TD placed behind an access point or a bridge in the same way as those directly connected to DNG. [HGI_R273]
- DNG is required to determine if the newly discovered IPTV TD supports DHCP, and/or UPnP, and/or CWMP. [HGI_R274]
- IPTV-TD that follow the TR-069 specs can be discovered as such, if they also use TR-111. Therefore, DNG is required to follow the TR-111 specifications. [HGI_R275]
- DNG is required to discover if IPTV TD or HN-TD is still present in the home network or not. [HGI_R276]

NOTE – The above text is imported from clause 6.5.6.1 of [HGI].

7.2.5 Security management

The RMS has to support the remote management of the main security functionalities of DNG: the stateful firewall and the ALG.

NOTE – The above text is imported from clause 6.5.9 of [HGI].

7.2.5.1 Firewall management

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

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

- DNG supports a stateful firewall, which is required to be remotely manageable by the RMS using a firewall rules configuration file. [HGI_R330]
- NAT/PAT mechanisms, like port mapping capability to enable remote access to home based devices or servers (HTTP, FTP, SFTP, SSH, TELNET), is required to be remotely manageable as defined in the WANPPPConnection or WANPPPConnection objects of DSL Forum TR-098 define in the Baseline:1 profile. The RMS via the management abstraction layer has the capability to enable/disable the port mapping of the usual protocols. [HGI_R331]

NOTE – Further study is needed for NAT mechanism.

- The integrated firewall module of DNG is recommended to be manageable and is recommended to support the remote download by RMS request through the download RPC defined in the DSL Forum TR-069. [HGI_R332]
- The version of the firewall is recommended to be also accessible by the RMS to help to determine if an update is necessary. [HGI_R334]

NOTE – The above text is imported from clause 6.5.9.1 of [HGI].

7.2.5.2 Application Layer Gateway Management

- The ALG list (see ALG clause 6.6.5.1) stored in DNG is required to be remotely accessible by the RMS. [HGI_R337]
- DNG is required to allow the RMS to enable or disable the ALG. These changes can be made either by the RMS or by the user through the local management interface (some restrictions may apply to the latter case). [HGI_R338]

NOTE – The above text is imported from clause 6.5.9.2 of [HGI].

7.2.6 End-device recommendations

– IPTV TD, if it operates in IPv4 environment, is recommended to support the use of DHCP to configure IP connectivity during the start-up phase. [HGI_R340]

– Managed IPTV TD is required to provide IP and hardware address information by broadcasting a gratuitous ARP whenever their IP stack is initialized. [HGI_R341]

– Managed IPTV TD of type D is also required to include "DeviceType" in the Encapsulated Vendor-Specific Option-Data fields of DHCP option 125. The contents and format of this value are identical to the device type suffices as defined by the UPnP forum (i.e.: "urn:uuid"). [R344]

– Managed IPTV TD of types U and CU MUST include "UUID" (Universally Unique IDentifier) in the Encapsulated Vendor-Specific Option-Data fields of DHCP option 125. The contents and format of this value are given by [IETF RFC 4122]. [HGI_R345]

– Managed IPTV TD that is directly configurable by the ACS (interface IACS_ED) is required to follow the TR-069 and TR-106 specifications. [HGI_R346]

– Managed IPTV TD directly configurable by the ACS is also recommended to also follow the TR-111 part 1 and part 2 specifications. [HGI_R347]

NOTE – The above text is imported from clause 6.5.10 of [HGI].

7.3 IPTV service information report

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

7.4 Remote management protocol

7.4.1 SNMPv2/v3

SNMP is a network management protocol defined by the IETF and is widely used by the telecommunications industry to manage IP networks. SNMPv2 or SNMPv3 can optionally be used to manage home networks supporting IPTV services.

7.4.2 DSL Forum TR-069

Auto-configuration of the IPTV TD is recommended to be performed using the approach described in TR-069 "CPE WAN Management Protocol".

Figure 7-8 given below is copied from TR-069 document. It represents the position of CWMP in the auto-configuration architecture. Therein, the Managed CPE (LAN Device) is just the position of IPTV TD.

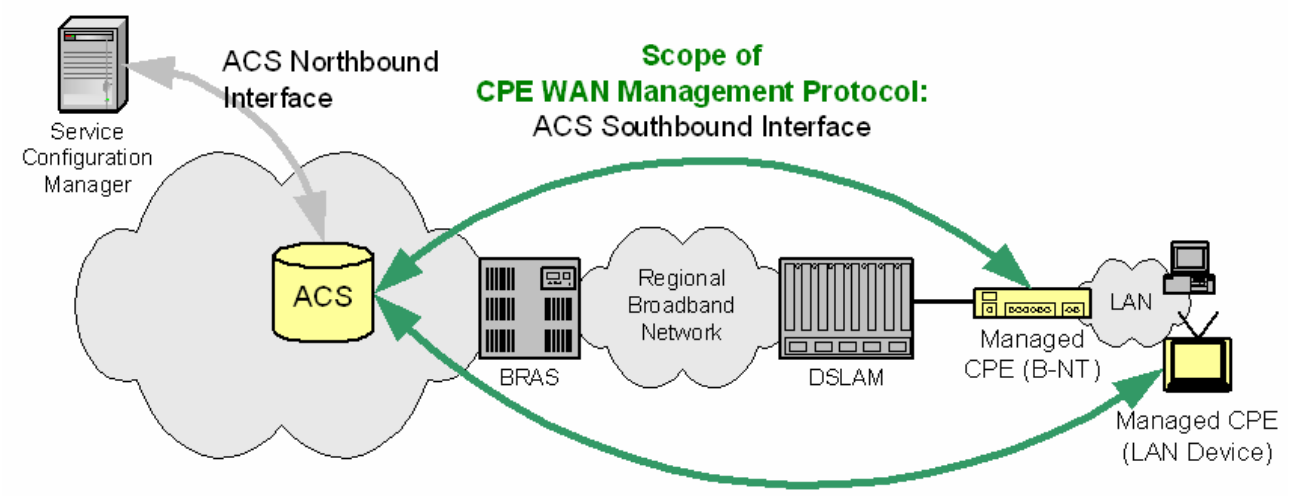


Figure 7-8: Scope of CPE WAN Management Protocol

The flow of auto-configuration provided by CWMP is introduced as follows.

• Step 1, ACS Discovery

The CWMP defines the following mechanisms that may be used by a CPE (e.g. IPTV TD) to discover the address of its associated ACS:

– The CPE may be configured locally with the URL of the ACS.

- The CPE may obtain the URL of the ACS through DHCP protocol from a DHCP server. The CPE put the string "dslforum.org" (all lower case) anywhere in the Vendor Class Identifier (DHCP option 60) and get the values received from the DHCP server in the Vendor Specific Information (DHCP option 43).
- The CPE may have a default ACS URL that it may use if no other URL is provided to it.

• Step 2, Connection Establishment

The CPE may at any time initiate a connection to the ACS. A CPE establish a connection to the ACS by issuing an Inform RPC method which is defined by [DSLF TR069] under the following conditions:

- The first time the CPE establishes a connection to the access network on initial installation.
- On power-up or reset.
- Once every Periodic Inform Interval (for example, every 24-hours).
- When so instructed by the optional ScheduleInform method.
- Whenever the CPE receives a valid Connection Request from an ACS.
- Whenever the URL of the ACS changes.
- Whenever a parameter is modified that is required to initiate an Inform on change.
- Whenever the value of a parameter that the ACS has marked for "active notification" via the SetParameterAttributes method is modified by an external cause (a cause other than the ACS itself).

(See TR-069 document for detail)

• Step 3, Configuration File Transmission

TR-069 defines a number of events which could be included in Inform message. If the ACS received an Inform message including a BOOTSTRAP event, the ACS calls a CPE Download RPC method (sending a Download message to CPE) to tell the CPE the configuration file name and it's location (URL) and some other indications. The CPE can get the configuration file with these arguments.

Annex A

Considerations on ISO/IEC15045-1 for IPTV services

(This annex forms an integral part of this document.)

A.1 Introduction

ISO/IEC15045-1 describes the model and key functions of DNG. Since the key subject of the standard 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 IPTV specific issues.

A.2 Comparison of terminology

Since ISO/IEC15045-1 is developed by the different body, it uses different terminologies from this document. For convenient of the reader, the following table is provided for the comparison of both documents.

Table A-1 Comparison of terminologies with ISO/IEC15045-1

IEC15045	Corresponding term	Note
HAN	Home Network (HN)	If it means all the networks and entities placed beyond DNG.
	IP-HN-P	If it means only the network and entities directly connected with 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 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/IEC15045-1 allows the use of both IP and non-IP at the interface, IPI-4 or IPI-3, of DNG. In case of IPTV, the network transmission technology by the IPTV TD is limited to IP by its definition. Although it is possible to use non-IP protocol, for example IEEE1394, beyond IPTV TD as a part of Secondary Domain as depicted in the architecture, the Access and Home Network around DNG needs to be IP based network except the case where DNG is incorporated in the IPTV TD. The DNG without IPI-3and IPI-4 specified in the Working Document for HN is not relevant for IPTV service.

The interface and traffic across DNG is described in its clause 5. The packet processing in the sense of QoS and multicast at the gateway device, which is important aspects for IPTV, is not mentioned in the standards. The technical information relevant for the Home Network supporting IPTV service is described in the clauses 6.2 and 6.6 of this document. ISO/IEC15045-1 compliant device is also required to meet these requirements.

A.4 Security consideration

In its clause 6 and 7, ISO/IEC15045-1 describes security issues necessary for the DNG. Some consideration is described in the context of remote control of consumer electronics device from outside controller. Different from IPTV TD, some kinds of consumer electronics devices potentially carry the risk caused by physical action that may result in the loss of physical property and, in the worst case, serious damages of human body. While 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 the "IPTV Security Aspects" document.

In addition to the protection of device and information, the designing DNG product requires the operational aspects of IPTV service. 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 mechanism. Designing the filtering mechanism requires detail analysis of IPTV and associated traffic. In this sense, the "IPTV related protocols" [FG IPTV-DOC-0191] document gives a good guidance.

Appendix I

An explanation of the layered models for IPTV Home Network

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

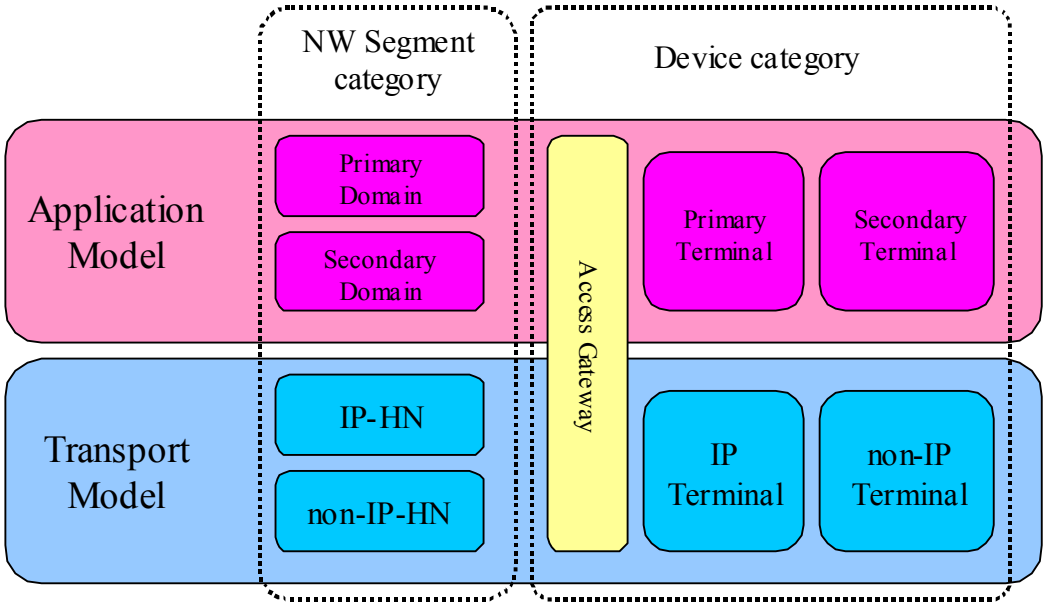


Figure I-1: The conceptual diagram of layered model

The layered function architecture includes two layers. There 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 is corresponding to lower layers basically bottom of three layers. That is to say, the function of physical correction, data link connection and choosing the best router for package are realized in this model. Transport model is the main subject of [draft] Recommendation [G.hnta].

b) The **application model** is responsible for allowing users to interact with the networks, including defining format of data, designing service and designing interface. There are many services at present, such as TV gaming, TV education, linear TV, etc. Providing more IPTV services may help drive user toward widespread use of IPTV, so it is necessary to design more kinds of service. Format of data in different services are various, so designation of data format is an important component of the application function model. Application model is the main subject of [draft] Recommendation [H.ghna].

Functional components are relevantly defined for each model. These components can be associated with the Home Network architecture in this document as table 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, Primary Domain is limited to 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

Home network (HN) use case scenarios

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

II.1. HN IPTV TD acting as an HN server

Case 1: An HN IPTV TD takes content traffic and reprocesses it. An HN IPTV TD receives IPTV content from IPTV network and serves this content to multiple HN TDs.

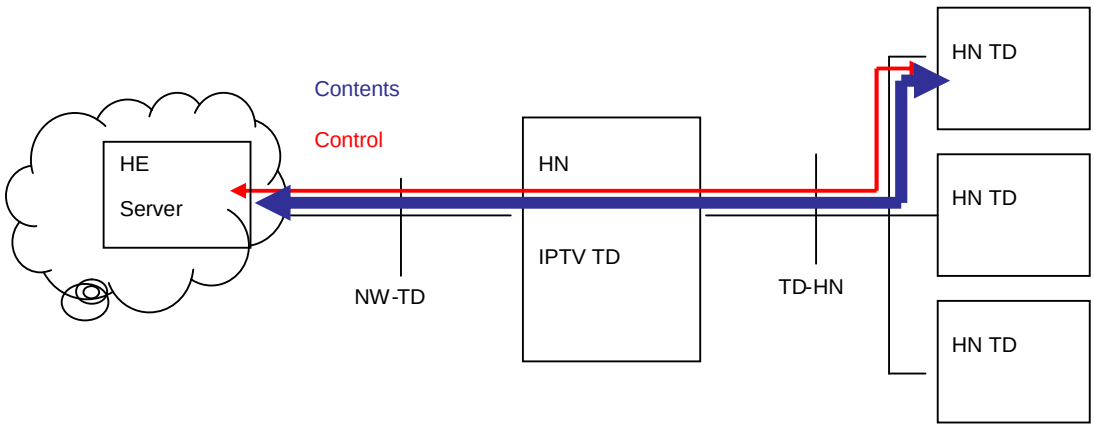


Figure II-1: HN IPTV TD acting as an HN server

Case 2: An HN IPTV TD assists HN TD to connect Headend server directly. An HN IPTV TD authenticates multiple HN TDs and gives required URL to respective HN TD. Each HN TD connects to Headend server with this URL for content streaming/downloading.

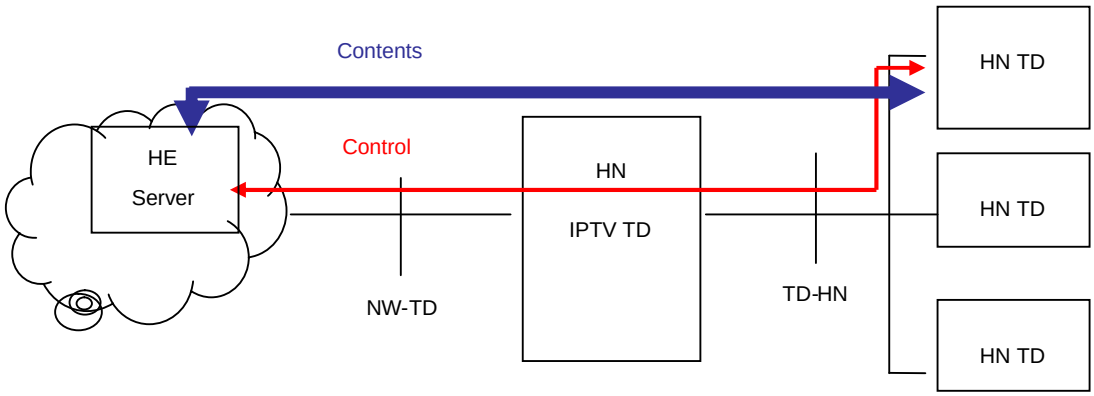


Figure II-2: An HN IPTV TD assists HN TD to connect Headend Server directly

In both cases, required information such as EPG/ECG metadata should be translated to HN-aware format in HN IPTV TD.

Typical examples

If an HN TD is DTV, user can watch IPTV contents with the help of HN IPTV TD.

If an HN TD is PVR, user can save IPTV contents with the help of HN IPTV TD.

II.2 HN IPTV TD acting as an HN client

An HN IPTV TD discovers HN server(s) by HN protocol.

An HN IPTV TD reviews/browses a specific HN server's content information and presents those contents by HN protocol.

Appendix III

UPnP-based Home Network

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

UPnP Audio/Video architecture consists of Media Renderer, Media Server and Control Point (regarding document UPnP A/V architecture).

Media Renderer obtains content from Media Server and renders it (e.g. display, decodes). For example the role of media renderer is playing of TV set, MP3 player, etc.

Media Server is used to make content available in home network and transfer it to the other device. It supports multiple transfer protocol and data format and It has functionality of conversion from one format to another one in the real time.

The main tasks of Control Point are synchronization and management of A/V devices in home network. It allows end user to select, play, pause and stop content from Media Server and display it on Media Renderer.

Control Point is able to control Media Renderer characteristic like: brightness, contrast, volume. An example of control point is TV set with remote control.

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

Additionally IPTV TD should be compatible with UPNP specification for Media Server in order to locate and transmit content for instance to the HN Device and other device in home network. Content could be selected remotely from IPTV NW or locally from hard disc. End user has possibility of recording A/V files with using UPNP scheduled recording functionality. IPTV TD should also work as a Control Point in order to allow end user to select and control content. This scenario is compatible with Figure I-1 in working document when HN IPTV TD acting as an HN server. When HN IPTV TD works as standalone device, It should have also Media Renderer functionality as an option.

HN Device should play role of Media Renderer and Control point. In that case HN Device uses content delivered from Media Server. Connection between IPTV TD and HN Device is established automatically with using UPNP protocols (e.g. SOAP, HTTP) and based on XML discovery mechanism. Control Point functionality allows end user to locate, choose and control content flows from Media server. The transport protocol and data format are chosen automatically depending on fact which of them are supported by Media Renderer. The proposal of IPTV end system architecture which use UPnP is shown below on Figure III-1.

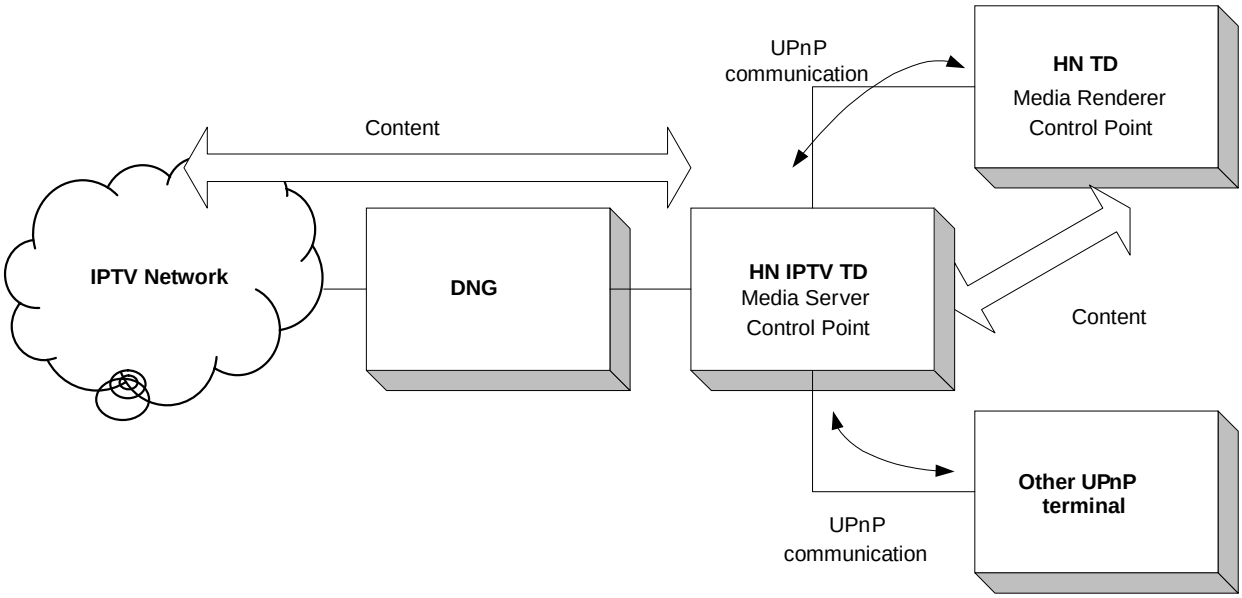


Figure III-1: UPnP Home Network architecture for IPTV end system

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 document when UPnP is approved by other organizations such as ISO/IEC.

Appendix IV

Consideration of re-transmission of Free-to-Air broadcasting

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

IV.1 Middleware aspect

IPTV services can comprise interactive TV applications. Recommendations ITU-R BT.1699 and 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.

IV.2 Content protection issue

Followings are comments on this issue for retransmission of free-to-air broadcast content, from the viewpoint of Recommendation 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.

– In clause 7.6, redistribution control capability for external interfaces to transmit captions and information provided by On Screen Display facilities will be required to conform to the content protection assigned by the content provider.

IV.3 Privacy protection issue

Report ITU-R BT.2052 describes overall analysis of end-user's privacy protection in 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.

IV.4 Delivery control of retransmission

In case that delivery control for retransmission of free-to-air broadcast content is needed, the IPTV system is requested to provide such functionality. ITU-T Recommendation J.281 describes the requirement of similar control.

IV.5 Provision of Emergency broadcast

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

Appendix V

Example configurations for an IP-based home network

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

Figure V-1 shows an example of a physical configuration of IP-based Home Network. Two Home Network areas, IP-HN-P and IP-HN-S, can overlap physically as shown in the lower half of Figure V-1. HN-TD deals with IPTV related traffic only. Devices which do not handle IPTV traffic is required to be connected to IP-HN-S.

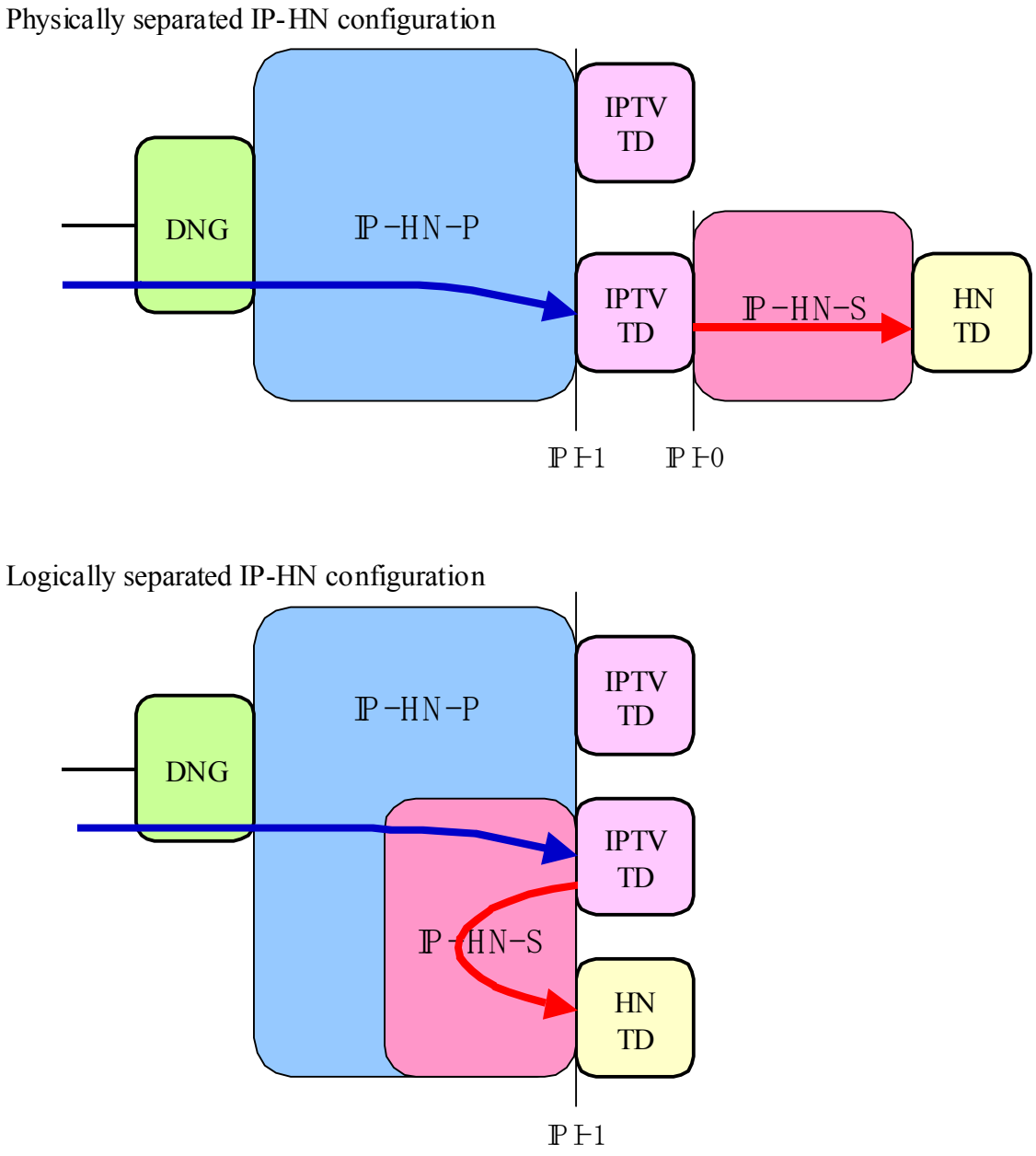


Figure V-1: Example configurations for an IP-based home network

Bibliography

[b_IETF RFC 2030] RFC 2030 (1996), *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*.

[b_IETF RFC 2663] RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations.*

[b_IETF RFC 3022] RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.

[b_IETF RFC 3027] RFC 3027 (2001), *Protocol Complications with the IP Network Address Translator.*

[b_UPnP 1] *UPnP AVTransport:1, AVTransport:1 Service Template Version 1.01*, UPnP Forum, June 25, 2002.

[b_UPnP 2] *UPnP ConnectionManager:1, ConnectionManager:1 Service Template Version 1.01*, UPnP Forum, June 25, 2002.

[b_UPnP 3] *UPnP ContentDirectory:1, ContentDirectory:1 Service Template Version 1.01*, UPnP Forum, June 25, 2002.

[b_UPnP 4] *UPnP Device Architecture Version 1.0, UPnP Device Architecture Version 1.0, UPnP Forum*, June 13, 2000.

[b_UPnP 5] *UPnP MediaRenderer:1, MediaRenderer:1 Device Template Version 1.01*, UPnP Forum, June 25, 2002.

[b_UPnP 6] *UPnP MediaServer:1, MediaServer:1 Device Template Version 1.01,* UPnP Forum, June 25, 2002.

[b_UPnP 7] *UPnP PrintBasic:1, PrintBasic:1 Service Template Version 1.01*, Shivaun Albright, Tom Hastings, Harry Lewis, Paul Moore, Gerrie Shults, Peter Zehler, UPnP Forum, August 8, 2002.

[b_UPnP 8] *UPnP Printer:1, Printer:1 Device Template Version 1.01*, Shivaun Albright, Tom Hastings, Harry Lewis, Peter Zehler, UPnP Forum, August 8, 2002.

[b_UPnP 9] *UPnP Printer:1 Annex A V1.0, Printer:1 Device Template Version 1.01 with Annex A – Optional Service Addition V1.0*, UPnP Forum, May 4, 2005.

[b_UPnP 10] *UPnP PrintEnhanced:1, PrintEnhanced:1 Service Template Version 1.01,* UPnP Forum, May 4, 2005.

[b_UPnP 11] *UPnP RenderingControl:1, RenderingControl:1 Service Template Version 1.01*, UPnP Forum, June 25, 2002.

NOTE – UPnP documents are currently under the approval process at ISO/IEC JTC 1. These documents will be changed to normative reference if successfully approved.

II.6 MIDDLEWARE, APPLICATION AND CONTENT PLATFORMS

II.6.1 IPTV middleware, application and content platforms

Summary

This document identifies and defines middleware platforms, including applications, content formats, and their uses, that facilitate effective and interoperable use of an IPTV system for presenting and interacting with IPTV services. This document is a general document for IPTV middleware, application and content platforms. It describes content provisioning, service discovery, channel and content identification and location resolution, and profiling. This document refers to text on middleware, content coding, metadata, which can be found in other documents.

Keywords

IPTV, middleware, applications

Current status

Since the scope of this document is very broad, there are still some clauses, especially on Profiling, that need more text. This document is currently about 80% complete.

Dependency on or relationship to other FG IPTV documents

- Toolbox for content coding [FG IPTV-DOC-0195]
- IPTV Middleware [FG IPTV-DOC-0196]
- IPTV Metadata [FG IPTV-DOC-0197]
- Standards for IPTV Multimedia Application Platforms [FG IPTV-DOC-0198]

CONTENTS

		Page
1	Scope	551
2	References	551
3	Definitions	552
3.1	This working document uses the following terms defined elsewhere	552
3.2	This working document defines the following terms	554
4	Abbreviations and acronyms	555
5	Content provisioning	557
5.1	Introduction	557
5.2	Interface between content/metadata providers and service providers	557
5.3	Gap analysis for content and metadata provisioning	558
6	Service Discovery	558
7	Channel Identification and location resolution	561
8	Profiling	561
9	Events	562
9.1	Input events	562
9.2	Other events	562
10	Service navigation systems	562
Appendix I – Profiling		564
I	Profiling Process for IPTV Service	562
I.1	Overview	562
I.2	Description of each profile	563
Appendix II – Input events		567
Appendix III – Example of assignement of input events		566
Appendix IV – Service navigation systems		567

IPTV middleware, application and content platforms

1 Scope

This document identifies and defines middleware platforms, including applications, content formats, and their uses, that facilitate effective and interoperable use of an IPTV system for presenting and interacting with IPTV services.

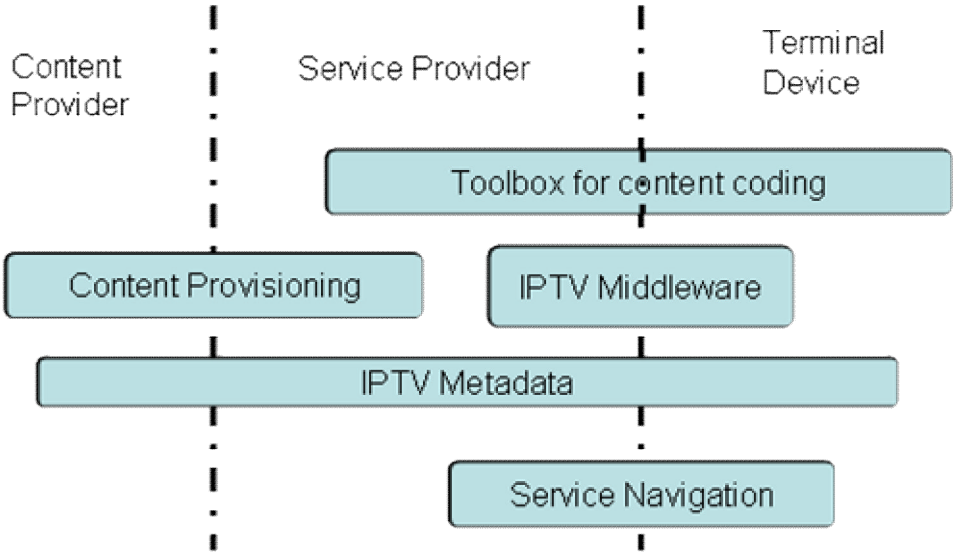


Figure 1-1: Scope of this document

For practical reasons the following topics are included in other documents

- Toolbox for content coding [FG IPTV-DOC-0195]
- IPTV Middleware [FG IPTV-DOC-0196]
- IPTV Metadata [FG IPTV-DOC-0197]
- Standards for IPTV Multimedia Application Platforms [FG IPTV-DOC-0198]

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.700] ITU-T Recommendation T.700 (2000), *Framework Recommendation for multimedia services*

[ITU-T H.222AM1] ITU-T Recommendation H.222.0 Amd 1(2002), *Information technology – Generic coding of moving pictures and associated audio information: Systems Amendment 1: Carriage of metadata over ITU-T Rec. H.222.0 | ISO/IEC 13818-1 streams*

[ITU-T J.90] ITU-T Recommendation J.90 (2000), *Electronic programme guides for delivery by digital cable television and similar methods – Reference operating scenario and requirements*

[ITU-T J.94 AM1] ITU-T Recommendation J.94 Amendment 1 (1998), *Annex B – Service information delivered out of band for digital cable television systems*

[ITU-T J.98] ITU-T Recommendation J.98 (2003), *Metadata requirements for video-on-demand in cable networks*

[ITU-T J.148] ITU-T Recommendation J.148 (2003), *Requirements for an objective perceptual multimedia quality model*

[ITU-T J.190] ITU-T Recommendation J.190 (2002), *Architecture of MediaHomeNet that supports cable-based services*

[ITU-T J.200] ITU-T Recommendation J.200 (2001), *Worldwide common core – Application environment for digital interactive television services*

[ITU-T Q.1702] ITU-T Recommendation Q.1702 (2002), *Long-term vision of network aspects for systems beyond IMT-2000*

[ITU-T T.171] ITU-T Recommendation T.171 (1996), *Protocols for interactive audiovisual services: Coded representation of multimedia and hypermedia objects*

[ITU-T T.174] ITU-T Recommendation T.174 (1996), *Application programming interface (API) for MHEG-1*

[ITU-T Y.101] ITU-T Recommendation Y.101 (2000*), Global Information Infrastructure terminology: Terms and definitions*

[ISO/IEC 13818-2] ISO/IEC 13818-2 (2000), *Information technology – Generic coding of moving pictures and associated audio information: Video*

[ISO/IEC 14496-12] ISO/IEC 14496-12 (2005), *Information technology – Coding of audio-visual objects – – Part 12: ISO base media file format*

[ETSI EN 300 468] ETSI EN 300 468 V1.8.1 (2007), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*

[ETSI TS 102 323] ETSI TS 102 323 V1.2.1 (2005), *Digital Video Broadcasting (DVB); Carriage and signalling of TV-Anytime information in DVB transport streams*

[ATIS-0800002] ATIS standard ATIS-0800002(2006), *IPTV Architecture Requirements*

3 Definitions

3.1 This working document uses the following terms defined elsewhere:

3.1.1 Application [ITU-T Y.101]: A functional implementation realized as software running in one or spread over several interplaying hardware entities.

3.1.2 Application manager [ITU-T J.200]: The entity that is responsible for managing the lifecycle of the applications. It manages applications running in both the Presentation engine and Execution engine if both are present.

3.1.3 Application Programming Interface (API) [ITU-T J.200]: Consists of software libraries that provide uniform access to system services. [ITU-T J.200]

NOTE – In the case of middleware, it is an interface between application layer and middleware service which encapsulates the services offered by the middleware and enable application developer to develop new application.

3.1.4 Character [ITU-T J.200]: A specific "letter" or other identifiable symbol, e.g. "A".

3.1.5 Character encoding [ITU-T J.200]: Mapping between an integer input value, and the textual character that is represented by this mapping, e.g. in ASCII value 65 (decimal) is character "A", or shift-JIS for Japanese characters.

3.1.6 Content [ITU-T T.174]: Encoded generic value, media or non-media data

3.1.7 EPG provider [ITU-T J.90]: The entity that collects, collates and assembles the elements of information that constitute the EPG database.

3.1.8 Execution engine (EE) [ITU-T J.200]: instructions and associated data and media content. An execution engine may be implemented with an operating system, computer language compilers, interpreters, and Application Interfaces (APIs), which a procedural application may use to present audiovisual content, interact with a user, or execute other tasks, which are not evident to the user. A common example of an execution engine is the JavaTV software environment, using the Java programming language and byte code interpreter, JavaTV APIs, and a Java Virtual Machine for program execution.

3.1.9 Home network (HN) [ITU-T J.190]: Short-range communications system designed for the residential environment, in which two or more devices exchange information under some sort of standard control.

3.1.10 Metadata format [ITU-T H.222AMD1]: Identifies the coding format of metadata.

3.1.11 Metadata service [ITU-T H.222AMD1]: Coherent set of metadata of the same format delivered to a receiver for a specific purpose.

3.1.12 Multimedia [ITU-T J.148]: The combination of multiple forms of media such as audio, video, text, graphics, fax, and telephony in the communication of information.

3.1.13 Multimedia application [ITU-T T.174]: An application which involves the presentation of multimedia information to the user.

3.1.14 Multimedia service [ITU-T Q.1702]: A service in which the interchanged information consists of more than one type, such as text, graphics, sound, image and video.

3.1.15 Multimedia representation [ITU-T T.171]: The property of handling several types of representation media.

3.1.16 Presentation [ITU-T T.411]: The operation of rendering the content of a document in a form perceptible to a human being.

3.1.17 Presentation engine [ITU-T J.200]: A subsystem in a receiver that evaluates and presents declarative applications consisting of content, such as audio, video, graphics, and text primarily based on presentation rules defined in the presentation engine. A presentation engine also responds to formatting information, or "mark-up", associated with the content, to user inputs, and to script statements, which control presentation behaviour and initiate other processes in response to user input and other events. A common example of a presentation engine is an HTML browser, capable of displaying text and graphic content formatted in HTML, with interactive behaviour programmed in ECMA script.

3.1.18 Service [ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.19 Stream [ITU-T J.200]: A unidirectional continuous flow of content.

3.1.20 Telecommunication service [ITU-T F.700]: Set of telecommunication capabilities that work in a complementary and cooperative way in order to let users perform applications.

3.1.21 User device [ATIS-0800002]: Also known as Home Network End-Device (HNED), Home Network Device (HND), Consumer Equipment (CE), terminal and physical device. A piece of hardware equipment running its software and attached to a Home Network and being identified by a GUID, e.g. a MAC address. A single device can be used by one or more users.

3.2 This working document defines the following terms:

3.2.1 Application instance: An occurrence of an application

3.2.2 Broadcast TV: One-way transmission of TV signals from one point to two or more other points.

3.2.3 Character set: See character encoding.

3.2.4 Content protection: Act of preventing unauthorized use of any content.

3.2.5 Electronic Content Guide (ECG): A service navigation interface used especially for content streaming and download.

NOTE – It is sometimes used synonymously with EPG.

3.2.6 Electronic Program Guide (EPG): A service navigation interface which is used especially for programs.

NOTE – in some traditional Broadcast Services, EPG is defined as an on-screen guide used to display information on scheduled live broadcast television programs, allowing a viewer to navigate, select, and discover programs by time, title, channel, genre. This traditional definition does not cover "catalogues" for on-demand and download services (sometimes called ECG) and bi-directional interactive service (sometimes called IPG) for end-user interaction with a server or head-end.

Some EPGs utilize web-pages, or teletext to realize this function.

3.2.7 Electronic Service Guide (ESG): A service navigation interface used especially for available services and contents.

3.2.8 Extended channel: Means to organize different operation content together, including live channel, TVOD, information service, EPG and so on. For each extended channel, there is a related channel number. [0062]

3.2.9 Globally Executable MHP (GEM): A terminal specification based on MHP that enables applications to interoperate across OCAP, MHP and other GEM based platforms.

3.2.10 IPTV Terminal Function (ITF)*: The functionality within the home network that is responsible for terminating the IP signal, and converting the content into a renderable [i.e. enabling to be seen and/or heard] format, e.g. an STB.

*: Based on [ATIS-0800002] with modification

3.2.11 Interactive Program Guide (IPG): A service navigation interface used especially for bi-directional interactive service with a server or head-end.

NOTE – It is sometimes used synonymously with EPG.

3.2.12 Interactive Television (iTV): A service in which the user can send requests, within a browser environment, to the service provider in order to obtain additional information. This capability requires channels to have what is known as a "return path".

3.2.13 Lifetime/Lifecycle of an application: Characterizes the time from which the application is loaded to the time the application is destroyed.

3.2.14 Metadata: Structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities.

NOTE – EPG metadata has many applications and may vary in depth from merely identifying the content package title or information to populate an EPG to providing a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold.

3.2.15 Middleware: A layer of software between applications and resources, which consists of a set of service enablers that allow multiple functionalities running on one or more devices in an IPTV system to interact across a network.

3.2.16 Segmentation: Division of content into different parts, e.g. scenes and chapters.

3.2.17 Service Navigation: The presentation of information that allows the end-user to discover, select and consume services.

3.2.18 Service Navigation Interface: A user interface which is intended to provide information on available services, including content that may be accessed by end-users for service navigation.

3.2.19 Set-top box (STB): A device that contains demodulator, de-multiplexer, decoder, other functionalities and interfaces related to signal reception and presentation of the distributed programme at the subscriber's site.

3.2.20 Time shifting: A function which allows playback of content after its initial transmission.

3.2.21 Time-shifted TV: A TV program that has been time shifted.

3.2.22 User Interface (UI): Also known as UI, a user interface is the sensory and behavioural aspects of a program that are presented to a user. The term is generally used to denote the menuing and navigational constructs of a program.

3.2.23 Video-on-Demand (VoD): A service in which the subscriber can view video content whenever desired. The operating assumption is that the content is stored on the provider's VoD server. Subscriber accesses the movie from a library directory which may include search engine that accesses movie description and rating. Subscribers typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time when using this service.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

API	Application Programming Interface
AV	Audio Video
DVB	Digital Video Broadcasting
EPG	Electronic Program Guide
ESG	Electronic Service Guide
ETSI	European Telecommunications Standards Institute
GEM	Globally Executable MHP
GIF	Graphics Interchange Format
GUI	Graphical User Interface
HN	Home Network
HTML	Hyper Text Mark-up Language

HTTP	Hyper Text Transport Protocol
I/O	Input / Output
ID	IDentifier
IETF	Internet Engineering Task Force
IHDN	In Home Digital Network
IP	Internet Protocol
IPR	Intellectual Property Rights
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITV	Interactive Television
JDK	Java Development Kit
JFIF	JPEG File Interchange Format
JPEG	Joint Picture Expert Group
LMDS	Local Multipoint Distribution System
MAC	Media Access Control
MHP	Multimedia Home Platform
MIME	multipurpose internet mail extensions
MMDS	Multipoint Microwave Distribution System
MPEG	Moving Picture Experts Group
NTSC	National Television Systems Committee
NVOD	Near-Video-On-Demand
OCAP	OpenCable Application Platform
OS	Operating System
OSD	On Screen Display
PFR	Portable Font Resource
PNG	Portable Network Graphics
PSI	Program Specific Information
PSIP	Program and System Information Protocol
RAM	Random Access Memory
ROM	Read Only Memory
SI	Service Information
TCP	Transmission Control Protocol
TS	Transport Stream
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
UTF8	Universal Transformation Format 8
VM	Virtual Machine

WAN Wide Area Network

XML eXtensible Markup Language

5 Content provisioning

5.1 Introduction

Content provisioning in IPTV is the activity of providing TV channels, programs, movies, music and other contents between content providers and service providers. Service providers may sign contracts with content and metadata providers, import contents and metadata from content/metadata providers.

To protect content rights, content provider may encrypt the content before delivery to service provider.

In this clause we focus on the interface between content/metadata providers and service providers and not on the content/metadata processes inside the service provider domain.

5.2 Interface between content/metadata providers and service providers

Content providers can provide audiovisual channels, contents and metadata together or separately.

Pure metadata providers also exist.

In the case of broadcast retransmission, broadcast service platforms such as terrestrial, cable, or satellite digital broadcasting can provide audiovisual channels, metadata and contents for interactive services to IPTV Service platforms for retransmission.

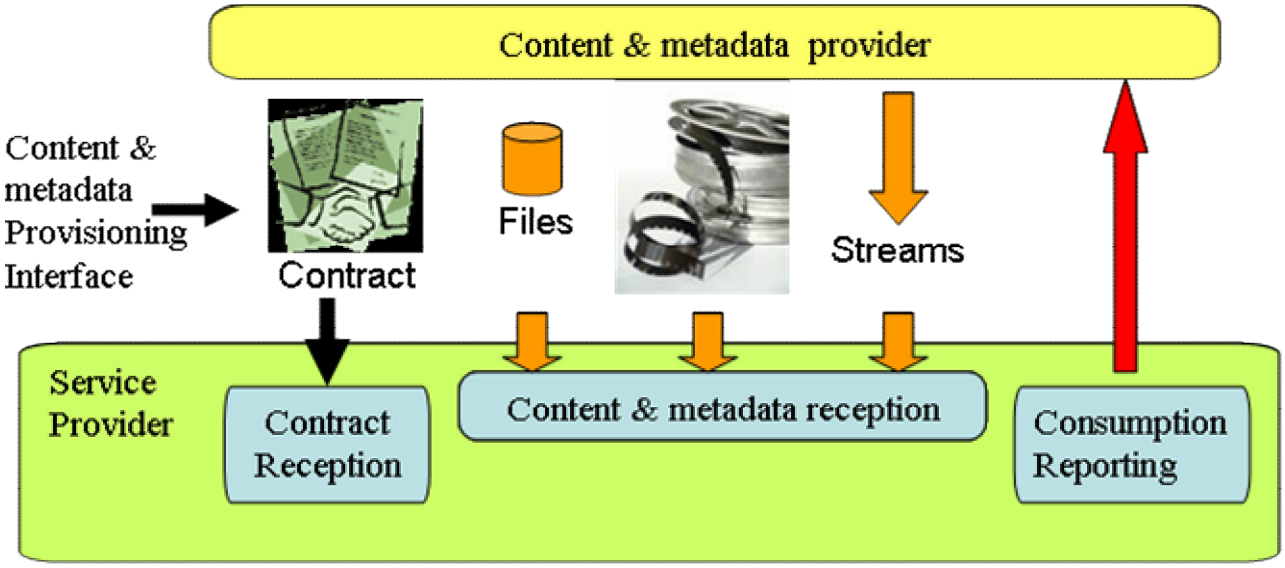


Figure 5-1: Relations between content providers and service providers

"Streams" stands for single programme streams and for multiple programme streams.

For content provisioning, a set of interfaces is needed and identified:

- Contract exchange (not to be standardized)
- Content & metadata provisioning interface
- Consumption reporting

Standards are needed for the content & metadata provisioning interface.

The metadata elements for provisioning are recommended to be as common as possible with the metadata elements made available to the end-user, however with elements specific to the relation between "content provider" and "service provider" (such as distribution conditions).

5.3 Gap analysis for content and metadata provisioning

Table 5-1: Content provisioning standards

Content provisioning method	Identified standards
File format for content provisioning	[ISO/IEC 14496-12]
File format for metadata provisioning	[SMPTE-380M]
File format for combined content & metadata provisioning	[ISO/IEC 14496-12] (need to be extended)
Stream format for channel/content provisioning	[ISO/IEC 13818-2]
Content provisioning transport protocol	[ISO/IEC 13818-2], [IETF RFC3550], [IETF RFC768], etc.
Stream format for combined channel/content & metadata provisioning	[ETSI EN 300 468] & [ETSI TS 102 323]

6 Service Discovery

There are different IPTV configurations to be considered, such as:

- Configuration with only one IPTV service provider on the network
- Configuration with multiple IPTV service providers on the network with preconfigured specific IPTV service provider
- Configuration with multiple IPTV service providers on the network without preconfigured specific IPTV service provider

In the case where there is only one IPTV service provider on the network or when there is a preconfigured service provider, here are the different steps in the service discovery:

- step 1: discovery of IPTV service provider entry point
- step 2: acquisition of the description of the IPTV services offered by the service provider and IPTV Service Selection

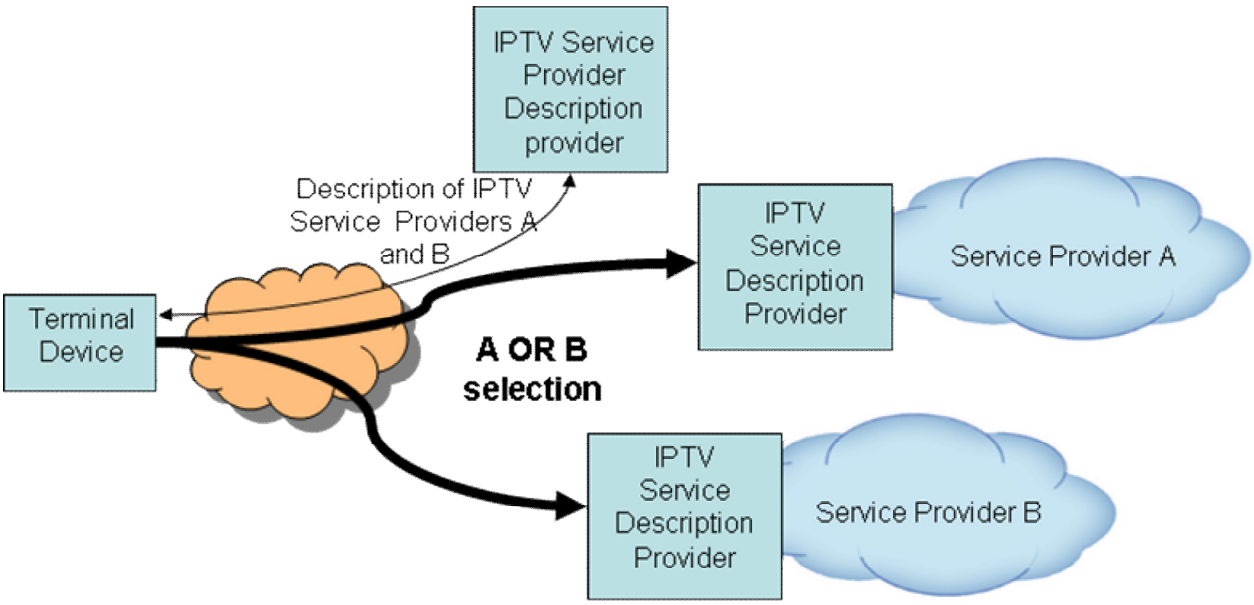


Figure 6-1: Service discovery with configuration of several IPTV service providers on the network

In the case where there are several service providers and there is no preconfigured service provider (see figure above), here are the different steps in the service discovery:

- step 1: discovery of the IPTV service provider description provider entry point
- step 2: acquisition of the description of the IPTV service providers and IPTV service provider selection
- step 3: acquisition of the description of the IPTV services provided by the selected service provider and IPTV service selection

Step 1 is always the discovery of the starting entry point and this is dealt with in the document "IPTV Network Control Aspects". [FG IPTV-DOC-0189]

The starting entry point might be:

- An IPTV service provider description provider entry point (when there are several IPTV service providers on the network and no specific service provider entry point is provided in the terminal device configuration data).
- An IPTV service provider entry point (when there is only one IPTV service provider on the network or when a specific service provider entry point is provided in the terminal device configuration data). The IPTV service provider maybe running a web-based solution, a metadata-based one or a mixture of them.

Here are two examples showing how descriptions of available IPTV service providers can be acquired by terminal devices, when the entry point is an IPTV service provider description provider entry point, the first one making of HTTP or S-HTTP protocols and the second making use of the IGMP protocol.

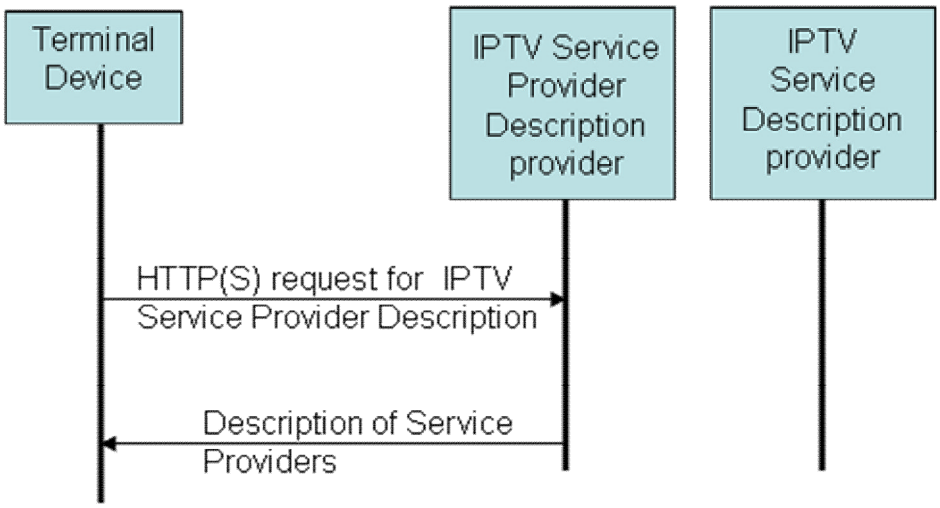


Figure 6-2: HTTP or S-HTTP request to get the description of the available IPTV service providers

In this case the service provider description provider may answer with a set of metadata containing the description of the available service providers.

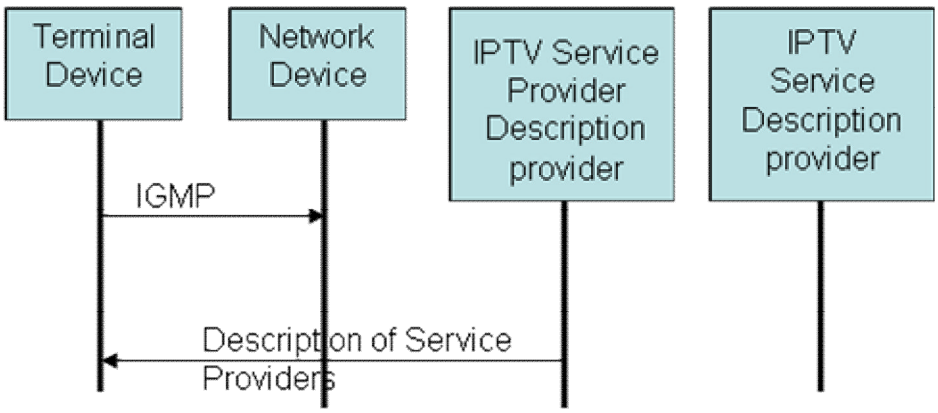


Figure 6-3: IGMP join request to receive the description of the available IPTV service providers

In this case the service provider description provider sends periodically the set of metadata containing the description of the available service providers.

The metadata related to the description of the available IPTV service providers can be found in the IPTV metadata document [FG IPTV-DOC-0198].

Here are two examples showing how descriptions of IPTV services offered by an IPTV service provider can be acquired by IPTV terminal devices, when the entry point is an IPTV service provider entry point, the first one making of HTTP or S-HTTP protocols and the second making use of the IGMP protocol.

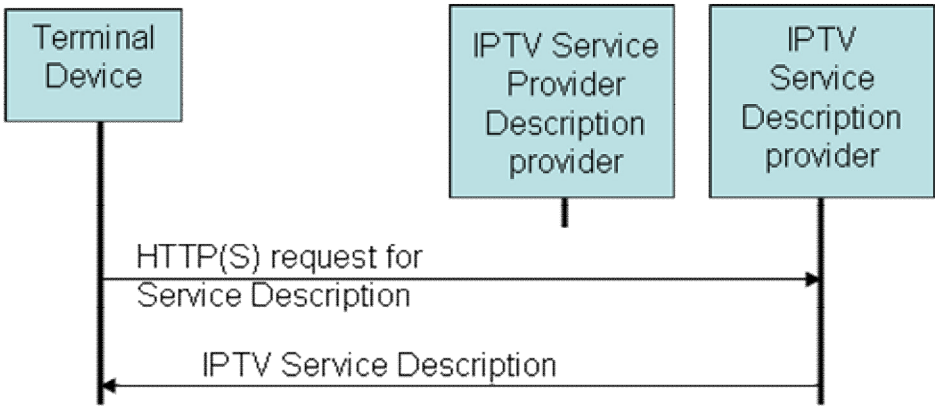


Figure 6-4: HTTP or S-HTTP request for description of the IPTV services offered by a service provider

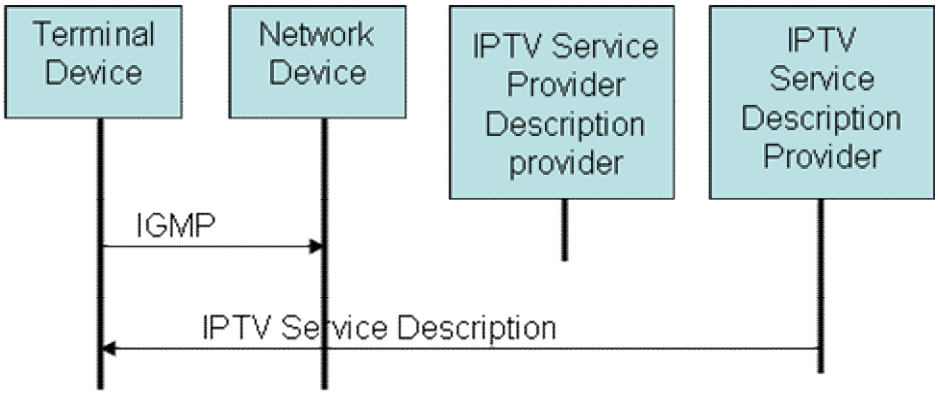


Figure 6-5: IGMP join request to receive the description of the IPTV services offered by a service provider

7 Channel Identification and location resolution

Domain names (DNS) could be used to identify destination multicast addresses of channels in EPG. These domain names would be registered on DNS servers with their corresponding multicast addresses. When end users try to access multicast channels in the EPG, their IPTV terminal devices resolve the domain names with DNS servers. When they get the multicast addresses for the domain names, they issue out group membership reports to join the multicast groups, and receive contents from the multicast channels.

8 Profiling

Appropriate information can be found in Appendix I.

9 Events

9.1 Input events

Appropriate information can be found in Appendix II.

9.2 Other events

For further study.

10 Service navigation systems

Appropriate information can be found in Appendix III.

Appendix I

Profiling

(This Appendix does not form an integral part of this document.)

This appendix includes material for discussion on profiling. Although the IPTV FG did not have time to discuss it, it was felt valuable to keep it to be the basis for further discussion in the IPTV GSI.

I Profiling Process for IPTV Service

I.1 Overview

The "IPTV service scenarios" and "IPTV service requirements" documents define IPTV services and requirements for IPTV network. The IPTV network should satisfy all the requirements identified. But it is difficult to develop the complete IPTV specifications satisfying all the requirements in single step. In this document, the IPTV standardization process is classified into three profiles.

In classifying profiles, the following principles are considered.

- Market urgency – the services that are widely deployed in the market should be standardized with high priority.
- Technical difficulty – the level of standardization effort should be considered.
- Consistency – the results of each profile should be aligned with the results of other profiles.
- Compatibility – as a result of profiling process, there will be end devices and networks having different capability sets. The end device is expected to be used in the network with different capability set. Thus, the capability set of latter profile should include all the capabilities of previous profiles.

I.2 Description of each profile

Table I-1shows the characteristics of each profile on user perspectives. In profile 1, users may recognize the IPTV service as terrestrial/cable/satellite digital TV service providing CoD service. In profile 2, users may recognize the IPTV service as internet service enabled TV. Users access web applications and internet content with IPTV end devices. Complete set of IPTV service that satisfying all the requirements are provided in profile 3.

Table I-1: Profiles on User Perspectives

	Profile 1	**Profile 2**	**Profile 3**
	TV/CoD over IP Network	Internet Service Enabled TV	Complete IPTV on NGN
Service Category	Linear/Broadcast TV Content On Demand	Web Services Interactive Data Services	Telephony Services Converged Service Mobile IPTV Service
Content Diversity	SP Provisioned Content	3rd Party Content Internet Content User Created Content	
Interactivity	Content Selection/View (Play/Pause)	Various Content Manipulation (Search, Save, Copy, Transfer, …) Internet Services	Telephony

End devices are classified into five profiles on their service capability. End devices will be implemented with different profiles. Thus, compatibility between different profiles is required.

Table I-2: End Device Profile

	Profile 1			**Profile 2**	**Profile 3**
	Minimal 1	Minimal 2	Basic	Enhanced	Full
Channel	X		X	X	X
CoD		X	X	X	X
Interactive Data and /or Storage				X	X
Telephony					X

Table I-3 lists the deliverable services for each profile.

Table I-3: Services for each Profile

1st Level	2nd Level	Profile 1	Profile 2	Profile 3
Content	Channel	Linear/Broadcast TV and Audio Broadcast Ad.	Trick Mode PPV NPVR Multi-angle PVR Content Sharing User Created Channel 3rd Party Channel	Mobile IPTV Targeted Ads
	On Demand	Real/Near Content on Demand	Push Content on Demand User Created Content 3rd Party Content	Mobile IPTV
	Content Navigation	EPG Content Advisory	IPG IPTV/Internet Portal	
Interactive Data			Internet Access E-mail Chat Presence Interactive Ad. T-Information (news, weather, transportation, government) T-Entertainment (games) T-Commerce (banking, shopping, ticketing)	Location-based Service
Telephony-based				SMS Caller ID Voice Call/conference Video call/conference Converged Service

Table I-4 summarizes the target environment and required functionalities for each profile.

NOTE – Interfaces and signalling protocols between each domain are not classified here. Priorities and capabilities on interfaces and signalling protocols are needed for describing architectural aspects.

Table I-4: Target Environment and Required Functionalities

	Profile 1	**Profile 2**	**Profile 3**
Target End Device	STB without storage	PC / STB with storage	PC/STB/Mobile device with storage
Target Network Infrastructure	Wired IP network	Wired/wireless IP network	NGN including mobile network
Target Network QoS Model	Best-effort or Diffserv	SLA-based QoS control	NGN QoS control
Security Aspects	Content security(select/view only) Service security	Content security(various manipulations) End device security	Network security
QoS/Performance Aspects	Dedicated/Provisioned QoS	Dynamic QoS	Dynamic QoS on NGN QoE/Performance monitoring
Middleware Aspects	Content metadata	Content delivery/ licensing metadata Content provisioning	User metadata
End System Aspects	A/V format Terminal management	Remote management Home networking	
Network Control Aspects	Identification Stream control Transport packet format	Content distribution Session control	Multicast network control

Appendix II

Input events

(This Appendix does not form an integral part of this document.)

This appendix includes material for further consideration by the IPTV-GSI.

A number of input events have been identified and can be found in some specifications as follows:

In GEM 1.0.2 specification, clause G.5, "Input events", in Annex G specifies that the minimum set of input events which shall be available to the applications if they are interested in receiving them. The defined minimum set of input events by inclusion of the clause G.5 of MHP 1.0.3 specification are as follows:

VK_0 to VK_9

VK_UP

VK_DOWN

VK_LEFT

VK_RIGHT

VK_ENTER

VK_TELETEXT

VK_COLORED_KEY_0

VK_COLORED_KEY_1

VK_COLORED_KEY_2

VK_COLORED_KEY_3

Among these input events, GEM based terminal specifications are allowed to make optional the VK_TELETEXT and VL_COLORED_KEY_3 input events.

This can be found in clause G.5, "Input events", in Annex G of ARIB STD-B23 with following text:

This clause conforms to GEM1.0 "G.5 Inputs events", Note that VK_TEKETEXT shall not be used. Form mapping of actual buttons to remote controller and so on, it shall be specified in operational guideline.

In Addition, similar definition for support of a user input events can be found in clause 5.4.13.4 of ARIB STD-B24, Vol.2 that defines a declarative content format and its middleware.

However no agreement was possible on the proposed minimum set of input events listed in the following table.

Table II-1: Proposed minimum set of input events

Input event
Digit from 0 to 9
Direction of up, down, left and right
Determination of a choice (ENTER)
3 special buttons (Coloured buttons)

Appendix III

Example of assignment of input events

For information, Table III.1 shows relationship between minimum set of input events listed in Table III.1 and middleware for procedural and declarative content format. GEM is chosen for procedural content format case and BML for declarative one as examples.

Table III-1: Example of assignment of input events

Input event	GEM	BML
Digit from 0 to 9	VK_0 to VK_9	"numeric-tuning" keygroup of used-key-list attribute.
Direction of up, down, left and right	VK_UP VK_DOWN VK_LEFT VK_RIGHT	"basic" keygroup of used-key-list attribute.
Determination of a choice (ENTER)	VK_ENTER	"basic" keygroup of used-key-list attribute.
special buttons (Coloured buttons)	VK_COLORED_KEY_0 VK_COLORED_KEY_1 VK_COLORED_KEY_2 VK_COLORED_KEY_3	"data-button" keygroup of used-key-list attribute.

NOTE 1 – GEM-based terminal specifications are allowed to make optional the VK_COLORED_KEY_3 input event.

NOTE 2 – BML defines used-key-list attribute that is a part of CSS properties to request input event available for interactive content.

Appendix IV

Service navigation systems

(This Appendix does not form an integral part of this document.)

This appendix includes material for discussion on service navigation systems. Although the IPTV FG did not have time to reach an agreement, it was felt valuable to keep it to be the basis for further discussion in the IPTV GSI.

The material in this appendix may be a candidate to be incorporated in the main body of this document or be considered to form an independent document after further work.

CONTENTS

		Page
1	Scope	569
2	References	569
3	Definitions	569
4	Abbreviations and acronyms	570
5	Generic Service Navigation System	570
5.1	Introduction	570
5.2	Examples of Service Navigation Model	572
5.3	Service navigation system generic architecture	573
6	Web-based service navigation system	574
6.1	Web-based service navigation system	574
6.2	Web-based service navigation system reference architecture	575
7	Middleware-based service navigation system	576
8	Syndication-based service navigation system	576
8.1	Overview	576
8.2	Operational Modes	577
8.3	Representation formats	577
8.4	Model for enhanced metadata capabilities	577
9	Possible extensions to all types of service navigation systems	578
9.1	Delivery and use of unsolicited metadata	578
Appendix I – Electronic Program Guide (EPG)		581

IPTV Service Navigation System

1 Scope

This document presents a generic service navigation system architecture and its functional entities, and gives a web-based service navigation system model and a syndication-based service navigation system model.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU T.174] ITU-T Recommendation

[ITU Y.2012] ITU-T Recommendation Y.2012

3 Definitions

3.1 This working document uses the following terms defined elsewhere:

3.1.1 Content [ITU T.174]: encoded generic value, media or non-media data.

3.1.2 Functional Entity [ITU Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.3 Metadata: Structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities.

3.1.4 Service: A set of functionalities enabled by a provider for end users; for example, providing IP connectivity with managed quality of service, providing an IPTV Service, providing a content on demand service, etc.

3.2 This working document defines the following terms:

3.2.1 Metadata Syndication: is a subscription based association of multiple metadata sources and terminals for distributing metadata to the terminals.

3.2.2 Lifetime/Lifecycle of an application: Characterizes the time from which the application is loaded to the time the application is destroyed.

3.2.3 Service Navigation: The presentation of information that allows the end-user to discover, select and consume services.

3.2.4 **Service Navigation Interface:** A user interface which is intended to provide information on available services, including content, that may be accessed by end-users for service navigation.

3.2.5 **IPTV Portal:** An entry point to IPTV services, including subscription and purchasing, often by providing service navigation, e.g. EPG, ECG, an IPTV-page, and the "last channel"

3.2.6 **IPTV page:** a single instance of presentation on a display of information to the end-user.

3.2.7 **Presentation:** The operation of rendering content in a form perceptible to a human being.

4 Abbreviations and acronyms

This working document uses the following abbreviations and acronyms:

API Application Programming Interface

BOSS Business and Operational Support System

CP Content Provider

CPE Customer Premises Equipment

DB DataBase

ECG Electronic Content Guide

EPG Electronic Program Guide

ESG Electronic Service Guide

HTML HyperText Markup Language

HTTP HyperText Transfer Protocol

IPG Interactive Program Guide

PVR Personal Video Recorder

RSS Real Simple Syndication

SP Service Provider

STB Set-Top Box

VoD Video on Demand

XML Extensible Markup Language

5 Generic Service Navigation System

5.1 Introduction

Service Navigation is a process of presenting information that allows the end-user to discover, select and consume services.

Service Navigation is an integral part of IPTV because it is expected that there are many services possible on IPTV and without service navigation, it is very difficult, if not impossible, to obtain services. A typical means of service navigation is by way of service navigation interface, a user interface which is intended to provide information on available services, including content, that may be accessed by end-users for service navigation. Examples of Service Navigation Interfaces include EPG, IPG, ECG, and ESG.

Service Navigation comprises nodes, server and client, and three abstract functional entities: metadata, navigation logic, and presentation. Depending on the way these abstract entities are realized, there may be many different systems or models of service navigation. In addition to these, (metadata) transport and interval management are the components to be taken into account.

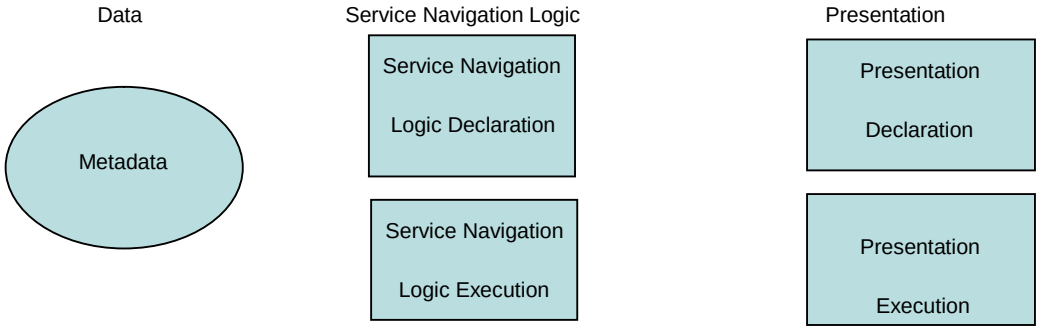


Figure 5-1: Abstract components of Service Navigation

(1) Metadata

Metadata is structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities. Metadata has many applications and may vary in depth from merely identifying the content package title or information to populate an service navigation interface to providing a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold.

(2) Service navigation logic

Navigation logic is a means to characterize the process in which service navigation is conducted through service navigation interface.

(3) Service Navigation Logic Description

Navigation logic description is the description of the navigation logic in a clearly defined language.

(4) Navigation Logic Execution

Navigation logic execution is the execution of the navigation logic described by the navigation logic description.

(5) (Navigation) Presentation

Navigation Presentation is the operation of rendering content in a form perceptible to a human being.

(6) Presentation Description

Presentation description is the description, in a clearly defined language, of how the navigation logic is to be presented and displayed, e.g., layout, design, and style, through service navigation interface.

(7) Presentation Execution

Presentation execution is the actual presentation and displaying of the service navigation logic through the service navigation interface according to the presentation description.

5.2 Examples of Service Navigation Model

Various service navigation models are possible by combining the above functional components in various ways. Figure 5-2 shows one of these, which is often called "web-based" because the service navigation interface is often realized by a "web-browser" application.

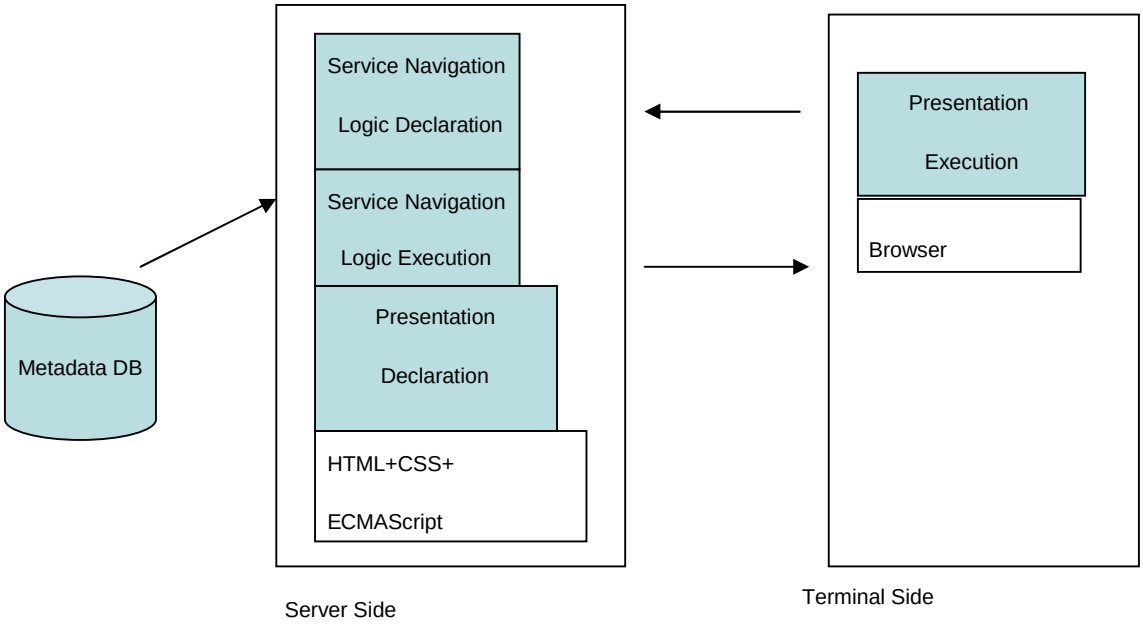


Figure 5-2: An example of a Web-based Service Navigation

In this simple model, navigation logic is executed on the server side, meaning that the application on the client side only displays and does not interact dynamically with the end user.

Another example of service navigation is given in Figure 5-3, in which service navigation logic and presentation are all executed on the client side. The server side only delivers metadata. This is an extreme case of middleware-based service navigation model.

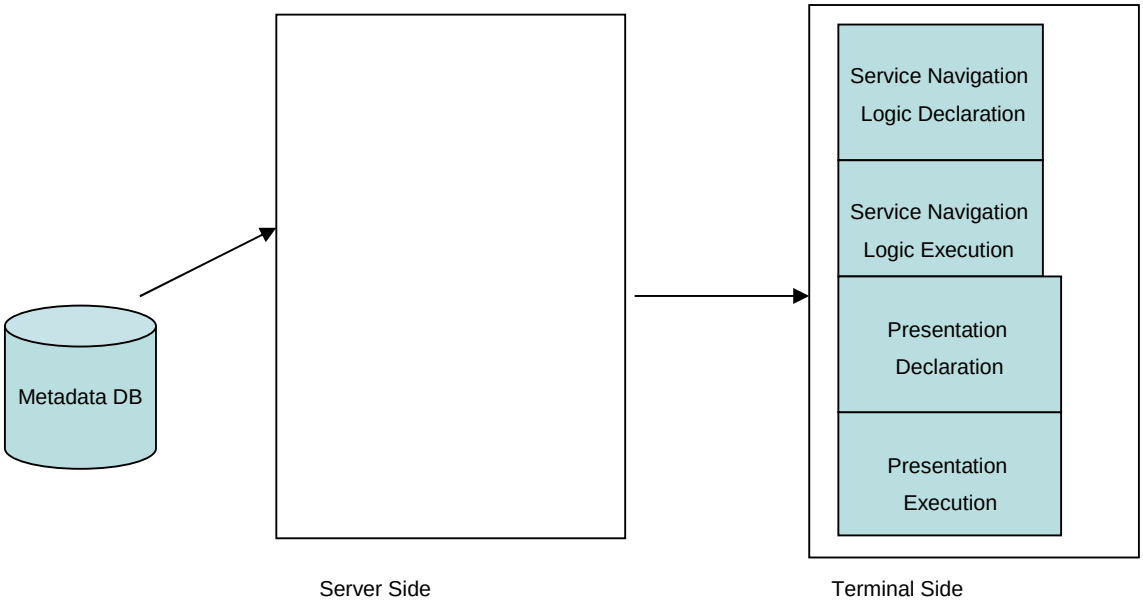


Figure 5-3: Middleware-based Service Navigation Model

As mentioned above, metadata transport and interval management need to be taken into account.

(1) Metadata transport

Metadata over IP is usually transported in either of two ways: Unicast or Multicast.

(2) Interval management

Interval management is a process in which temporal intervals between metadata delivery are managed. For example, interval management involves decisions such as, e.g., how often certain metadata is to be updated within a day.

Depending on the way these abstract entities are realized, there may be many different systems or models of service navigation.

5.3 Service navigation system generic architecture

EDITOR'S NOTE – Contributions needed for a more conceptual model/description.

Figure 5-4 shows generic service navigation system architecture. This architecture can support navigation through the presentation of various kinds of services and contents irrespective of implementation.

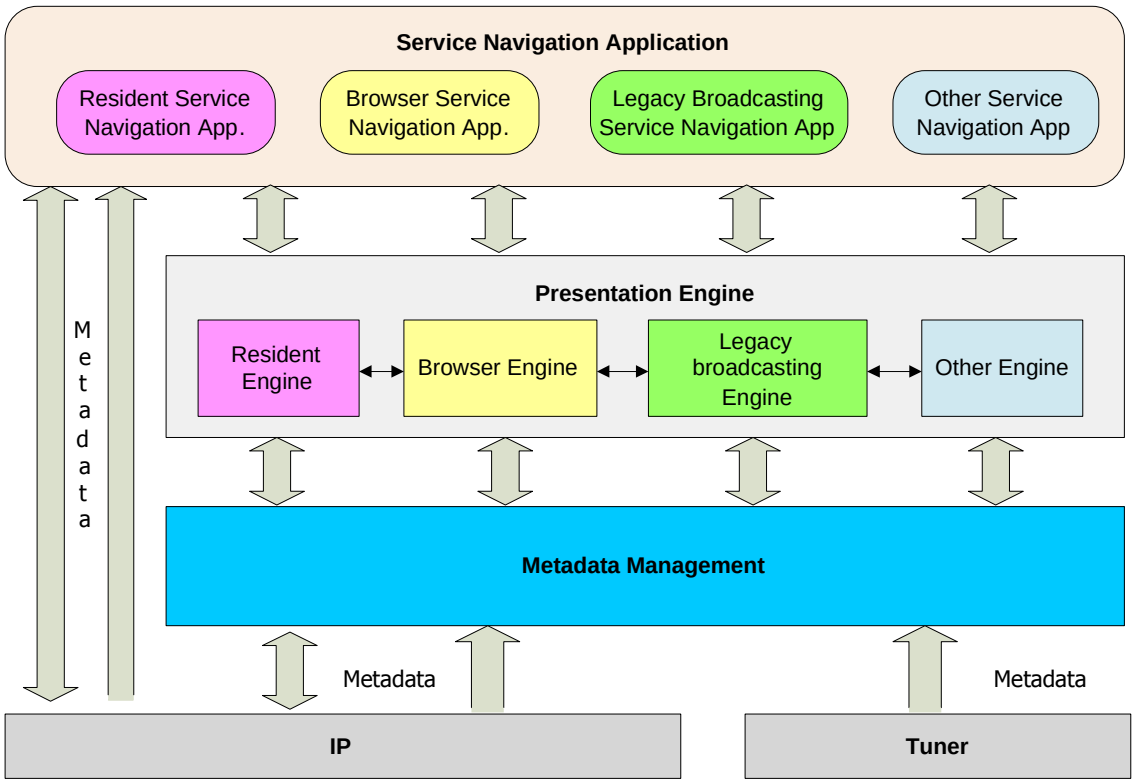


Figure 5-4: Generic Service Navigation System Architecture

The service navigation manager of base middleware receives the metadata based on XML from the IP connection, parses and stores it into the local storage. The metadata can be retrieved through the metadata API by the presentation engine. The IPTV terminal may have tuner to receive broadcasting services (e.g. through the MPEG-2 transport stream) and in that case, the service information can be retrieved through the metadata API by the presentation engine.

Various solutions exist for the presentation engine. The presentation engine displays the metadata according the design template and the navigation.

The service navigation application provides the navigation functionality for the services and the contents.

It could be possible for the application to request metadata directly from the remote server using HyperText Transfer Protocol (HTTP).

6 Web-based service navigation system

EDITOR'S NOTE – Introduction needed.

6.1 Web-based service navigation system

The web-based service navigation system is a service navigation system in which the service navigation application is located in a web-server, and the presentation is based on the presentation engine, e.g. a browser.

The web-based service navigation system consists of three functional entities: service/application management, metadata DB, and page production and presentation (see Figure 6-1).

- The service/application management functional entity obtains users' information from IPTV BOSS (such as user name, password, service-ordered information, price, etc.) and the media location information from CDN and manages them. It responds to the user's request for VoD, linear TV and time-shift TV as well as other services and applications. The service/application management functional entity also fulfils the service/application logical processing of the end-user's requests.
- The metadata database functional entity stores and manages metadata.
- The page production and presentation functional entity provides a service navigation interface or an IPTV portal. It offers an interface for user interaction with the IPTV platform. This functional entity produces IPTV pages based on HTML and/or XML and presents them.

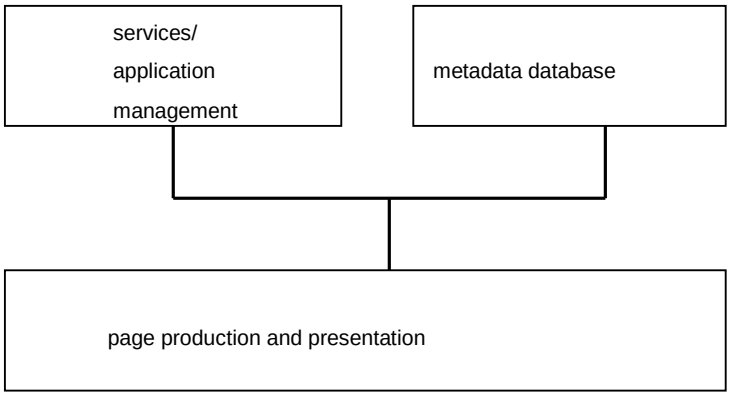


Figure 6-1: Web-based Service Navigation System Architecture

6.2 Web-based service navigation system reference architecture

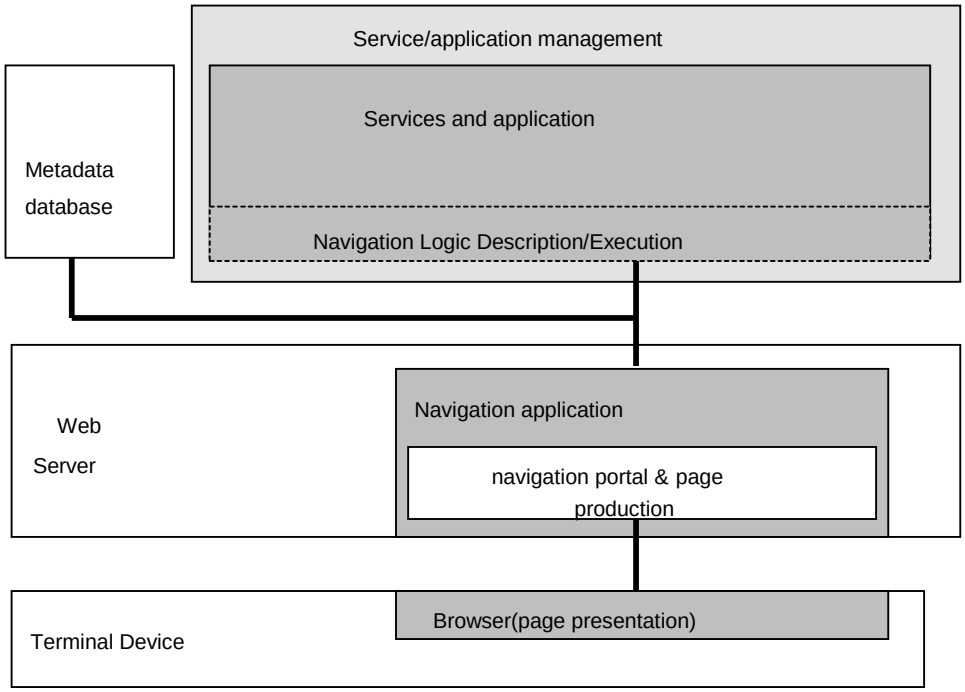


Figure 6-2: Web-based service navigation system reference model architecture

The service provider(s) obtain users' service-ordered information from IPTV BOSS, and send them to the service navigation system. The service-ordered information includes user's information and service information.

Service/application management interacts with BOSS and CDN to get user's information (such as user name, password, service-order information, etc.) and service information (such as price, location of media, etc.), and use these information to provide service/application logical process. For example, Service/application management encapsulates these logic processes as service/application logic APIs, and these APIs are called by navigation application located in Web server.

Navigation application obtains metadata from metadata database and uses the service-ordered information to produce customized pages (based on HTML/XML). Operators often provide many service page templates for users to choose, and these templates correspond to the service-ordered information. The introduction of intermediate layer (Web Server) will improve the capability of service navigation system and accelerate browsing. Through the intermediate layer (Navigation application), the logical process of service/application management are shielded and simultaneously, customized pages could be produced.

The service/application logical process is independent of the set-top box (STB). The navigation application of Web server produces IPTV Portal and pages and delivers them to STB, and the STB presents them to users by browser. The user's requests are sent to navigation application of Web server, and the navigation application invokes the service/application logic (APIs) to respond user's requests or redirect to other application servers.

7 Middleware-based service navigation system

A middleware based service navigation interface (MW-SNI) is a service navigation interface whose design and navigation logic are typically defined by the application on the terminal. Using the metadata which is pre-provided by the content distribution service provider, MW-SNI with the resident function of the terminal device, can provide the end-user with the content retrieval, information presentation, play, a method to purchase the content, and the interactive functions with the portal.

As with other service navigation interface such as EPG and IPG, MW-SNI typically provides the following functions:

– A function to receive all or the designated metadata with the search conditions, by each service provider.

– A function to receive the metadata from many service providers.

– A function to present the listing or the details of the received metadata to the users.

– A function to move from the shown metadata to the purchasing page of the contents and packages.

– A function to indicate the contents and packages purchased by the users.

– A function to play the purchased contents.

MW-SNI receives metadata and temporarily store it as cache. The implementation of the cache depends on the terminal device, but its envisaged storing capacity varies from the minimum value of the searched content displayed on a monitor to the maximum value of all the metadata from all the service providers.

The cache procedure will vary from the RAM which is temporarily stored as a memory media to a method to be stored in the hard disc drive. In order to carry out the function like searching without any stress, the terminal device used for the MW-SNI may use received metadata to construct a certain metadata database and control it. The method to control the metadata in the terminal device depends on the implementation.

For MW-SNI to receive the metadata, the following points are important. It is also important to remember to protect the data by such a way as exceeding the cache capacity of its own when receiving the metadata, because the cache capacity maintained by the NW-SNI varies depending on the terminal device.

The MW-SNI has at least a listing display and a detailed display.

The MW-SNI functions need to interact with the metadata server to provide the end user with the metadata search functions.

Using the MW-SNI functions, the end user may be able to purchase content. The MW-SNI can typically show the available contents and the package and play the selected contents.

MW-SNI can For a VOD, the distribution of the content with the age viewing restrictions is envisaged. For such contents, the parental control is recommended to be considered, not only for the content play, but also for the ECG viewing using the metadata.

8 Syndication-based service navigation system

8.1 Overview

Figure 8-1 shows the service overview for the syndication-based service navigation system, which can be consisted of client-server modules. Service navigation by syndication can give various enhanced service capabilities to end-user, e.g., personalized, customized navigation. To support this syndication-based method, the syndication server needs to have cooperation with metadata server and other kinds of application servers together.

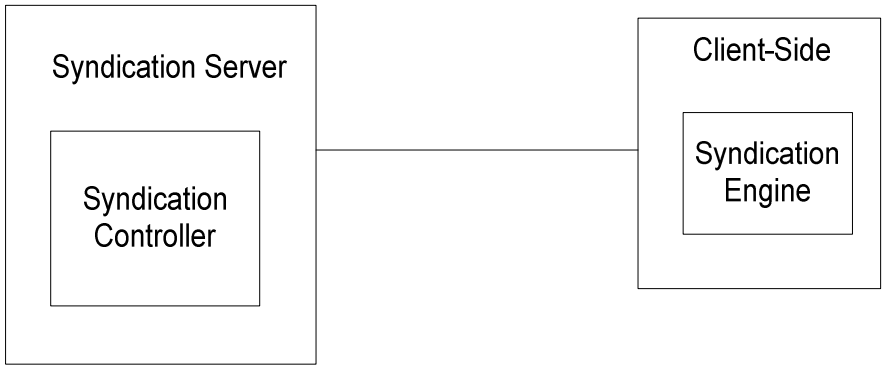


Figure 8-1: Architecture of syndication-based service navigation system

8.2 Operational Modes

Syndication-based method is required to aggregate syndication metadata from local or remote networks. In addition, syndication service needs to consider the optimal metadata file size, network bandwidth and gathering mechanism from different located servers.

From the views of aggregation function and pull mechanism, the operation modes can be categorized into two ways: one is client-based operation and the other is server-based operation.

- Client-based mode: Syndication-based metadata is aggregated by client side engine. This is possible for end-user to support dynamic customized capabilities in client-side.
- Server-based mode: Syndication-based metadata is aggregated by server-side controller. Here, aggregation can be happened between server systems or by agent system for server systems.

8.3 Representation formats

To support syndication capabilities in service navigation service, the formats and metadata elements need to support and expand associate with standard specifications that are already used in the industry. To support interoperability in multi-devices and multi server environments, service navigation system needs to consider common, flexible and extendible formats for syndication.

As well, the formats need to provide metadata considering such as enhanced, interactive and internet service environments. For example, it will include seamless rendering interface in diverse terminals, scalable processing for partial metadata. Also, IP protocol's bidirectional features is necessary metadata for bidirectional processing.

8.4 Model for enhanced metadata capabilities

Figure 8-2 shows implementation model to support the enhanced metadata capabilities of EPG. It contains the necessary modules for customization and for multiple terminals environment. The enhanced metadata server consists of three modules, i.e., syndication controller module, metadata adaptation module and device management module. And, this server is also interoperable with metadata and navigation system.

In enhanced metadata server, syndication controller and syndication engine have capabilities to provide customized IPTV service. It can be implemented by RSS based syndication mechanism. This module provides client to reconstruct channel/program information easily and supports consistent service UI (User Interface) under the case of different types of devices. Syndication controller has several functionalities. For example, it receives the channel's RSS feed information through metadata adaptation module from metadata. Then it supports RSS information management and search capabilities.

Metadata adaptation module is for metadata transformation from other metadata to standardized syndication format such as RSS format. And it also can get metadata from external system and then provide to syndication format to syndication controller.

Device management module is for the processing of multiple types of devices in client. Customer can have different types of devices. Once customer is set up of his/her own personalized EPG, the EPG needs to support UI consistency through different devices. For this operation, device management module can support the device's profile information between syndication controller and client.

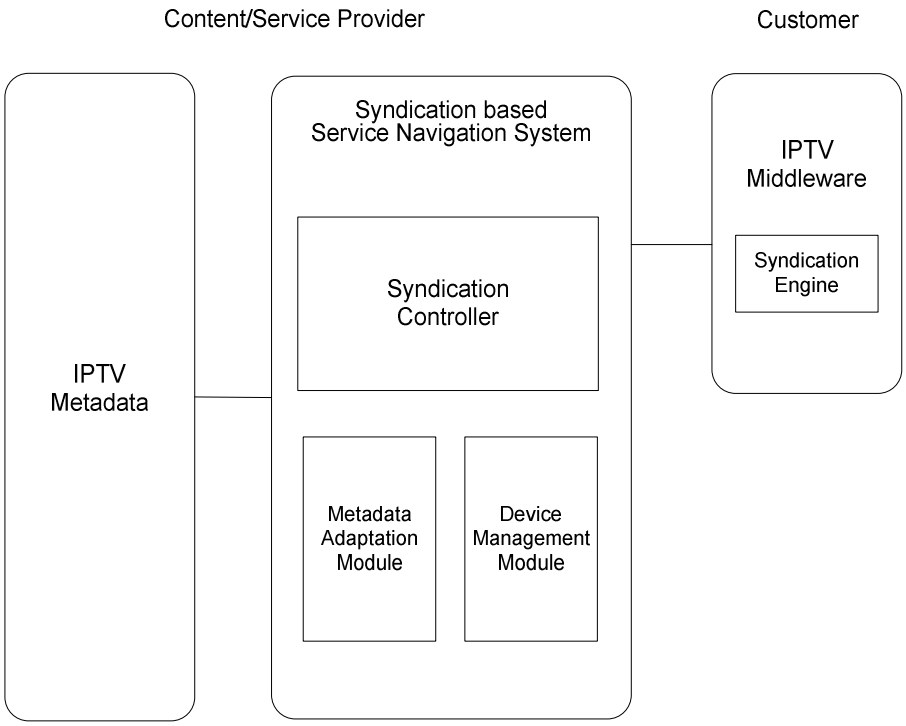


Figure 8-2: Enhanced Metadata Server Model

9 Possible extensions to all types of service navigation systems

9.1 Delivery and use of unsolicited metadata

In line with the generic service navigation system Architecture, metadata may arrive in the terminal device either as a response to a specific retrieval request or as data received over a channel after a listening request.

Below is an illustration of the reception of unsolicited metadata with AV streams from head-ends.

Although this metadata is unsolicited, it might be of interest for the application to access it; this is why a metadata component and metadata extractor are introduced in the diagram.

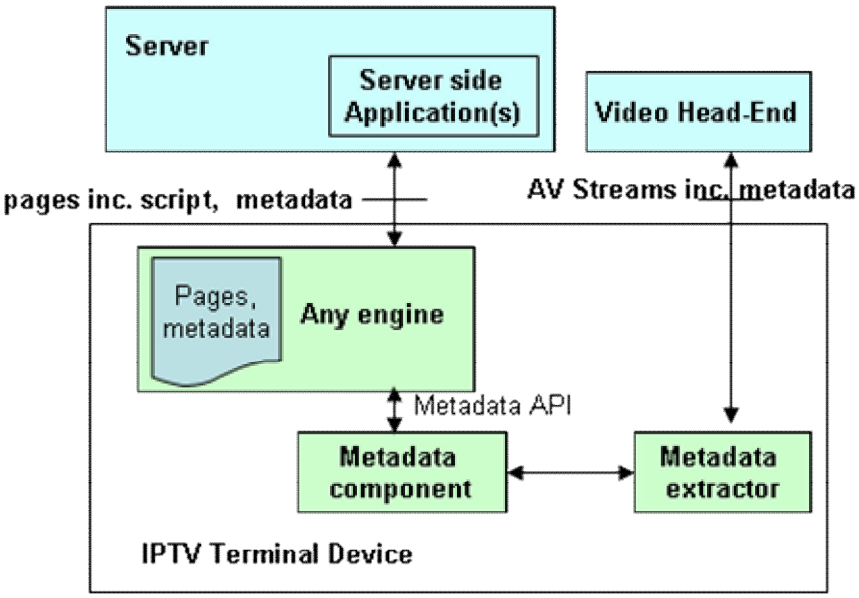


Figure 9-1: Delivery and use of unsolicited metadata

Appendix I
(to Appendix IV)

Electronic Program Guide (EPG)

(This Appendix does not form an integral part of this document.)

EDITOR'S NOTE – More contributions are expected on this appendix.

CONTRIBUTOR'S NOTE – Text is needed to explain what the purpose of this appendix is.

Electronic Programme Guide (EPG)

- EPG supports retrieval capabilities including fast search, semantic search and quick selection.
  - EPG information should be selectable by various methods. This can be implemented by keyword-based search and/or menu-driven selection for program. In order to provide the intelligent EPG search function, semantic mechanism such as ontology-based program search or semantic tagging could be used.
- EPG can have customized capabilities including on-demand feeding, transforming, filtering, and gathering function.
  - It allows customer to retrieve the EPG information as required at anytime. This can be implemented by using of syndication technique such as RSS based information feeding.
  - Using this kind of customized capability, it can implement distributed IPTV service for service provider which can support different content providers over the network. It can also provide personalized EPG service for end-users and flexible EPG service for various terminals. For example, EPG information might be converted to lightweight format to support the mobile terminal.

- EPG can have layout flexibility on various devices

  – EPG information allows client to present various layouts as client's environment. It also allows EPG server to convert or to transform the EPG information for different client environments (e.g., Mobile client).

  – This can be implemented using web-based techniques such as XML-based EPG as a data format and CSS as layout form.

- An EPG application can support PVR applications (recording, storing).

  – Using EPG information, EPG application should support a recording operation for selected program at client side as reservation-basis and/or time-shift basis. It can also support multiple-recording operation which enables to record the multiple programs which are selected by user simultaneously unlikely with traditional PVR operation.

II.6.2 Toolbox for content coding

Summary

This document addresses the use of video and audio coding in services delivered over Internet Protocols (IP). It describes the use of H.264/AVC video, VC 1 video, AVS video, HE AAC v2 audio, HE AAC v2 audio, Extended AMR WB (AMR WB+) audio, and AC-3 and Enhanced AC-3 audio. In addition, this document describes the use of speech codecs within an IPTV environment and the specified codecs for this use. This document adopts a "toolbox" approach for the general case of IPTV applications delivered directly over IP and MPEG-2 TS. This document is not a specification for the use of Audio and Video Codec's for use in IPTV Services.

Keywords

IPTV, coding, codec, AVS, AAC

Current status

This document is complete.

Dependency on or relationship to other FG IPTV documents:

- IPTV service requirements document

CONTENTS

		Page
1	Scope	584
2	References	584
3	Definitions	585
	3.1 Terms defined elsewhere	585
	3.2 Terms defined in this document	585
4	Abbreviations and acronyms	585
5	Available Codecs	586
6	Audio Codecs	587
	6.1 AC-3 (Dolby Digital)	587
	6.1.1 Overview of AC-3	587
	6.1.2 Transport of AC-3	589
	6.2 Enhanced AC-3 (Dolby Digital Plus)	589
	6.2.1 Overview of Enhanced AC-3	589
	6.2.2 Transport of Enhanced AC-3	590
	6.2.3 Storage of AC-3 and Enhanced AC-3 Bitstreams	590
	6.2.4 AC-3 and Enhanced AC-3 Track definition	590
	6.2.5 AC-3 and Enhanced AC-3 Sample definition	591
	6.2.6 AC3SpecificBox	591
	6.2.7 EC3SpecificBox	593
	6.3 Extended AMR-WB (AMR-WB+)	594
	6.3.1 Overview of AMR-WB+ codec	594
	6.3.2 Transport and storage of AMR-WB+	596
	6.4 MPEG-4 High Efficiency AAC v2 (HE AAC v2)	596
	6.4.1 Overview of HE AAC v2	596
	6.4.2 Transport and storage of HE AAC v2	599
	6.4.3 HE AAC v2 Levels and Main Parameters for DVB	599
	6.4.4 Methods for signalling of SBR and/or PS	600
	6.5 MPEG-1 Layer 2 Audio	600
	6.6 MPEG-2 AAC	601
	6.6.1 Overview of MPEG-2 AAC	601
	6.6.2 Overview of Encoder	603
	6.6.3 Overview of decoder	604
	6.7 MPEG Surround	605
	6.7.1 Introduction	605
	6.7.2 MPEG Surround features	607
	6.7.3 Introduction to MPEG Surround Baseline profile	607
	6.7.4 Binaural Decoding	607

Page

6.7.5 External stereo mix 607
6.7.6 Enhanced Matrix Mode 608
6.7.7 MPEG Surround for MPEG-1 Layer II – Baseline Profile 609
6.7.8 MPEG Surround for MPEG 4 AAC, HE AAC and HE AAC v2 – Baseline Profile 609
6.8 ITU-T G.722.1 and G.722.1 Annex C 609
6.9 ITU-T G.729.1 – An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729 612
6.9.1 Overview of Encoder 613
6.9.2 Overview of Decoder 614
6.9.3 RTP payload 615
6.10 ITU-T G.722 615
6.10.1 Overview of main functional features 616
6.10.2 Overview of G.722 SB-ADPCM encoder 616
6.10.3 Lower sub-band ADPCM encoder 617
6.10.4 Higher sub-band ADPCM encoder 617
6.10.5 Overview of G.722 SB-ADPCM decoder 617
6.11 ITU-T G.722.2 (3GPP AMR-WB) 619
6.11.1 Overview of AMR-WB codec 619
6.11.2 Transport and storage of AMR-WB 621
7 Video codecs 621
7.1 H.264/AVC Video 621
7.1.1 Network Abstraction Layer 622
7.1.2 Video Coding Layer 623
7.2 MPEG-2 Video 624
7.2.1 Technical Solution 624
7.3 VC-1 video 625
7.3.1 Explanation of VC-1 Profiles and Levels 626
7.4 AVS Video 627
7.4.1 AVS encoding tools 627
Appendix I – Technical Aspects of Toolbox Codecs and Content Coding 628
Appendix II – List of some additional content related standards 635
Bibliography 637

Toolbox for content coding

1 Scope

This document addresses the use of audio and video coding in services delivered over Internet Protocols (IP). It describes the use of audio and video codecs as specified in standards.

This document adopts a "toolbox" approach for the general case of IPTV applications delivered directly over IP and MPEG-2 TS. This document is not a specification for the use of audio and video codecs for use in IPTV Services.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.264] ITU-T Recommendation H.264 (2005), *Advanced video coding for generic audiovisual services*

[ISO/IEC 14496-3] ISO/IEC 14496-3 (2007), *Information technology – Coding of audio-visual objects – Part 3: Audio*

[ISO/IEC 14496-10] ISO/IEC 14496-10 (2005), *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding*

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP, A Transport Protocol for Real-Time Applications*

[IETF RFC 3640] IETF RFC 3640 (2003), *RTP payload for transport of generic MPEG-4 elementary streams*

[ETSI TS 126 290] ETSI TS 126 290 V7.0.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Audio codec processing functions; Extended Adaptive Multi-Rate – Wideband (AMR-WB+) codec*

[IETF RFC 4352] IETF RFC 4352 (2006), *RTP Payload Format for the Extended Adaptive Multi-Rate Wideband (AMR-WB+) Audio Codec*

[ETSI TS 126 273] ETSI TS 126 273 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); ANSI-C code for the fixed-point Extended Adaptive Multi-Rate – Wideband (AMR-WB+) speech codec (3GPP TS 26.273 version 6.5.0 Release 6)*

[ETSI TS 126 304] ETSI TS 126 304 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Extended Adaptive Multi-Rate – Wideband (AMR-WB+) codec; Floating-point ANSI-C code (3GPP TS 26.304 version 6.6.0 Release 6)*

[SMPTE 421M] SMPTE 421M (2006), *Television – VC-1 Compressed Video Bitstream Format and Decoding Process*

[IETF RFC 4184] IETF RFC 4184 (2005), *RTP Payload Format for AC-3 Audio*

[IETF RFC 4598] IETF RFC 4598 (2006), *RTP Payload Format for Enhanced AC-3 (E-AC-3) Audio*

[GB/T20090.2] GB/T20090.2 (2006), *Information technology – Advanced coding of audio and video – Part 2: Video*

[ISO/IEC 13818-1] ISO/IEC 13818-1(2000), *Information technology — Generic coding of moving pictures and associated audio information: Systems*

[ITU-T G.722.1] ITU-T Recommendation G.722.1 (2005), *Coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss*

[IETF RFC 4749] IETF RFC 4749 (2006), *RTP payload format for G.729.1 Audio codec*

[IETF RFC 2250] IETF RFC 2250 (1998), *RTP Payload Format for MPEG1/MPEG2 Video*

[ISO/IEC 11172-3] ISO/IEC 14496-3 (1993), *Information technology — Coding of moving picture and associated audio for digital storage media at up to about 1.5 Mbit/s — Part 3: Audio, 1993*

[ISO/IEC 13818-7] ISO/IEC 13818-7 (2006), *Information technology Generic coding of moving picture and associated audio information – Part 7: Advanced Audio Coding (AAC)*

3 Definitions

3.1 Terms defined elsewhere

This clause is intentionally left blank.

3.2 Terms defined in this document

3.2.1 Bitstream: Coded representation of a video or audio signal

3.2.2 Multi-channel audio: Audio signal with more than two channels

4 Abbreviations and acronyms

This working document uses the following abbreviations and acronyms:

AAC Advanced Audio Coding

AC-3 Dolby AC-3 audio coding

AMR-WB+ Extended AMR-WB

AOT Audio Object Type

ASO Arbitrary Slice Ordering

AU Access Unit

AVS Audio and Video coding Standard

DRC Dynamic Range Control

E-AC-3 Dolby Enhanced AC-3 audio coding

IRD Integrated Receiver-Decoder

H.264/AVC	H.264/Advanced Video Coding
HDTV	High Definition Television
HE AAC	High-Efficiency Advanced Audio Coding
IP	Internet Protocol
IP-IRD	Internet Protocol Integrated Receiver-Decoder.
LC	Low Complexity
LATM	Low Overhead Audio Transport Multiplex
MBMS	Multimedia Broadcast/Multicast Service
MPEG	Moving Pictures Experts Group (ISO/IEC JTC 1/SC 29/WG 11)
MPEG-2 TS	MPEG-2 Transport Stream
NAL	Network Abstraction Layer
NTP	Network Time Protocol
PS	Parametric Stereo
PSS	Packet switched Streaming Service
QCIF	Quarter Common Interchange Format
QMF	Quadrature Mirror Filter
SBR	Spectral Band Replication
RTP	Real-time Transport Protocol
RTCP	Real-time Transport Control Protocol
RTSP	Real Time Streaming Protocol
S/PDIF	Sony/Philips Digital Interconnect Format
SBR	Spectral Band Replication
SMPTE	Society of Motion Picture and Television Engineers
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VCL	Video Coding Layer
VUI	Video Usability Information

5 Available Codecs

Table 0-1 lists a number of currently available codecs without implying any individual preference. However in the spirit of unification and harmonization the FG IPTV encourages the ITU-T to use its best efforts to reduce duplication or proliferation in its recommendations for codecs use in IPTV Services.

Table 0-1: Available Codecs

	Codec	Delivery directly over IP	MPEG-2 TS
Audio	MPEG-1 Layer II	✓	✓
	AC-3	✓	✓
	MPEG Surround	✓	✓
	MPEG-2 AAC	✓	✓
	MPEG-4 HE AAC	✓	✓
	MPEG-4 HE AAC v2	✓	✓
	Enhanced AC-3	✓	✓
	AMR-WB+	✓	X
	G.722	✓	X
	G.722.1	✓	X
	G.722.1.C	✓	X
	G.722.2	✓	X
	G.729.1	✓	X
Video	MPEG-2	✓	✓
	H.264 / AVC	✓	✓
	VC-1	✓	✓
	AVS	✓	✓

NOTE – Symbols ✓ and X indicate "Yes" and "No" respectively

6 Audio Codecs

6.1 AC-3 (Dolby Digital)

The AC-3 digital compression algorithm can encode from 1 to 5.1 channels of source audio from a PCM representation into a serial bit stream, at data rates from 32 kbit/s to 640 kbit/s. The 0.1 channel refers to a fractional bandwidth channel intended to convey only low frequency signals.

The AC-3 audio codec is specified in [ETSI TS 102 366].

6.2 Overview of AC-3

The AC-3 algorithm achieves high coding gain by coarsely quantizing a frequency domain representation of the audio signal. Figure 6-1 and Figure 6-2 respectively show block diagrams of the AC-3 encoder and decoder. The first step in the encoding process is to transform the representation of audio from a sequence of pulse code modulation (PCM) time samples into a sequence of blocks of frequency coefficients. This is done in the analysis filter bank. Overlapping blocks of 512 time samples are multiplied by a time window and transformed into the frequency domain. Due to the overlapping blocks, each PCM input sample is represented in two sequential transformed blocks. The frequency domain representation may then be decimated by a factor of two so that each block contains 256 frequency coefficients. The individual frequency coefficients are represented in binary exponential notation as a binary exponent and a mantissa. The set of exponents is encoded into a coarse representation of the signal spectrum which is referred to as the spectral envelope. This spectral envelope is used by the core bit allocation routine which determines how

many bits to use to encode each individual mantissa. The spectral envelope and the coarsely quantized mantissas for 6 audio blocks (1536 audio samples per channel) are formatted into an AC-3 frame. The AC-3 bit stream is a sequence of AC-3 frames.

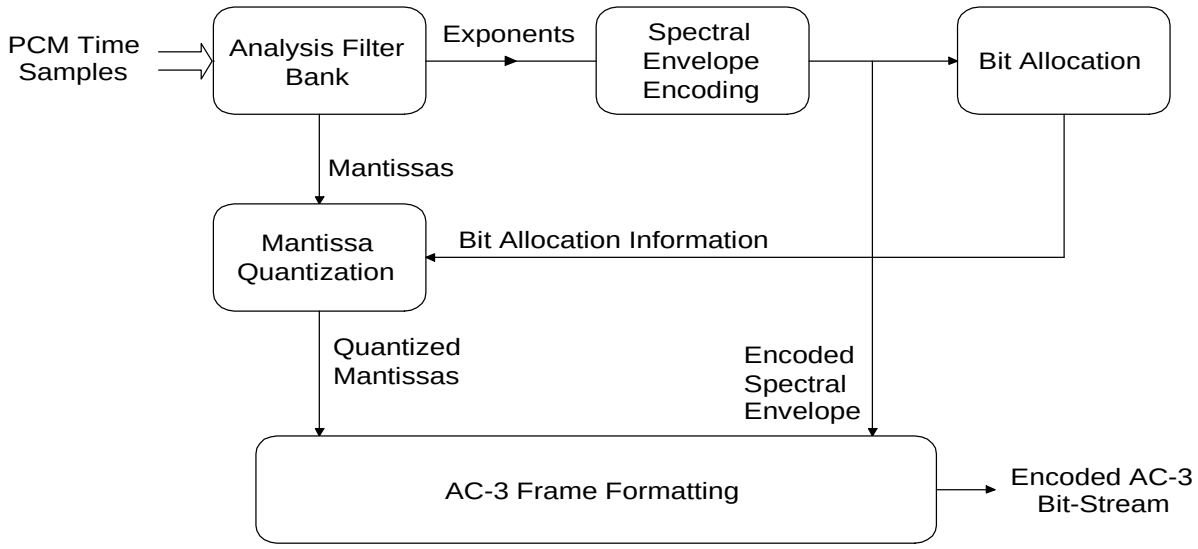


Figure 6-1: The AC-3 encoder

The actual AC-3 encoder is more complex than indicated in Figure 6-1. The following functions not shown above are also included:

1 A frame header is attached which contains information (bit-rate, sample rate, number of encoded channels, etc.) required to synchronize to and decode the encoded bit stream.

2 Error detection codes are inserted in order to allow the decoder to verify that a received frame of data is error free.

3 The analysis filter bank spectral resolution may be dynamically altered so as to better match the time/frequency characteristic of each audio block.

4 The spectral envelope may be encoded with variable time/frequency resolution.

5 A more complex bit allocation may be performed, and parameters of the core bit allocation routine modified so as to produce a more optimum bit allocation.

6 The channels may be coupled together at high frequencies in order to achieve higher coding gain for operation at lower bit-rates.

7 In the two-channel mode, a rematrixing process may be selectively performed in order to provide additional coding gain, and to allow improved results to be obtained in the event that the two-channel signal is decoded with a matrix surround decoder.

The decoding process is basically the inverse of the encoding process. The decoder, shown in Figure 6-2, must synchronize to the encoded bit stream, check for errors, and de-format the various types of data such as the encoded spectral envelope and the quantized mantissas. The bit allocation routine is run and the results used to unpack and de-quantize the mantissas. The spectral envelope is decoded to produce the exponents. The exponents and mantissas are transformed back into the time domain to produce the decoded PCM time samples.

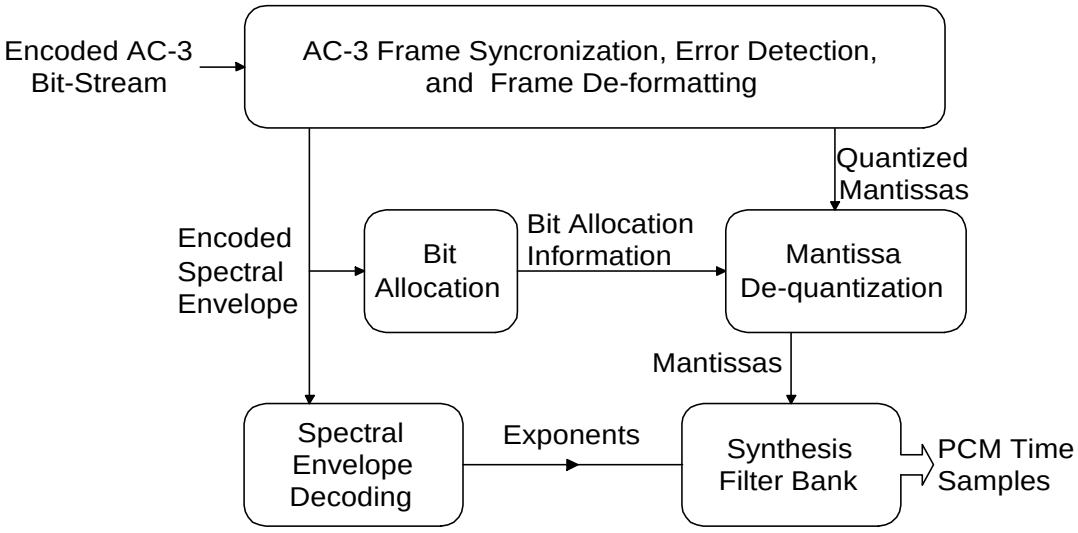


Figure 6-2: The AC-3 decoder

The actual AC-3 decoder is more complex than indicated in Figure 6-2. The following decoder operations not shown above are included:

- Error concealment or muting may be applied in case a data error is detected.
- Channels which have had their high-frequency content coupled together must be de-coupled.
- Dematrixing must be applied (in the 2-channel mode) whenever the channels have been rematrixed.
- The synthesis filter bank resolution must be dynamically altered in the same manner as the encoder analysis filter bank had been during the encoding process.

6.1.2 Transport of AC-3

To transport AC-3 audio, over RTP [IETF RFC 3550], the RTP payload [IETF RFC 4184] is used. Carriage of multiple AC-3 frames in one RTP packet, as well as fragmentation of AC-3 frames in cases where the frame exceeds the Maximum Transmission Unit (MTU) of the network, is supported. Fragmentation may take into account the partial frame decoding capabilities of AC-3 to achieve higher resilience to packet loss by setting the fragmentation boundary at the "5/8ths point" of the frame.

6.2 Enhanced AC-3 (Dolby Digital Plus)

Enhanced AC-3 is an evolution of the AC-3 coding system. The addition of a number of low data rate coding tools enables use of Enhanced AC-3 at a lower bit rate than AC-3 for high quality, and use at much lower bit rates than AC-3 for medium quality.

The Enhanced AC-3 audio codec is specified in [ETSI TS 102 366].

6.2.1 Overview of Enhanced AC-3

Enhanced AC-3 uses an expanded and more flexible bitstream syntax which enables a number of advanced features, including expanded data rate flexibility and support for variable bit rate (VBR) coding. A bitstream structure based on sub-streams allows delivery of programs containing more than 5.1 channels of audio to support next-generation content formats, supporting channel configuration standards developed for digital cinema (D-Cinema) and support for multiple audio programs carried within a single bit-stream, suitable for deployment of services such as Hearing Impaired/Visual Impaired. To control the combination of audio programs carried in separate sub-streams or bit streams, Enhanced AC-3 includes comprehensive mixing

metadata, enabling a content creator to control the mixing of two audio streams in an IP-IRD (Internet Protocol Integrated Receiver-Decoder.). To ensure compatibility of the most complex bit stream configuration with even the simplest Enhanced AC-3 decoder, the bit stream structure is hierarchical – decoders will accept any Enhanced AC-3 bit stream and will extract only the portions that are supported by that decoder without requiring additional processing. To address the need to connect IP-IRDs that include Enhanced AC-3 to the millions of home theatre systems that feature legacy AC-3 decoders via S/PDIF, it is possible to perform a modest complexity conversion of an Enhanced AC-3 bit stream to an AC-3 bit stream.

Enhanced AC-3 includes the following coding tools that improve coding efficiency when compared to AC-3.

- Spectral Extension: recreates a signal's high frequency amplitude spectrum from side data transmitted in the bit stream. This tool offers improvements in reproduction of high frequency signal content at low data rates.
- Transient Pre-Noise Processing: synthesizes a section of PCM data just prior to a transient. This feature improves low data rate performance for transient signals.
- Adaptive Hybrid Transform Processing: improves coding efficiency and quality by increasing the length of the transform. This feature improves low data rate performance for signals with primarily tonal content.
- Enhanced Coupling: improves on traditional coupling techniques by allowing the technique to be used at lower frequencies than conventional coupling, thus increasing coder efficiency.

6.2.2 Transport of Enhanced AC-3

To transport Enhanced AC-3 audio over RTP [IETF RFC 3550], the RTP payload [IETF RFC 4598] is used. Carriage of multiple Enhanced AC-3 frames in one RTP packet, as well as fragmentation of Enhanced AC-3 frames in cases where the frame exceeds the MTU of the network, is supported. Recommendations for concatenation decisions which reduce the impact of packet loss by taking into account the configuration of multiple channels and programs present in the Enhanced AC-3 bit stream are provided.

6.2.3 Storage of AC-3 and Enhanced AC-3 Bitstreams

This section describes the necessary structures for the integration of AC-3 and Enhanced AC-3 bitstreams in a file format that is compliant with the ISO Base Media File Format. Examples of file formats that are derived from the ISO Base Media File Format include the MP4 file format and the 3GPP file format.

6.2.4 AC-3 and Enhanced AC-3 Track definition

In the terminology of the ISO Base Media File Format specification (ISO/IEC 14496-12), AC-3 and Enhanced AC-3 tracks are audio tracks. It therefore follows that these rules apply to the media box in the AC-3 or Enhanced AC-3 track:

- In the Handler Reference Box, the handler_type field shall be set to "soun".
- The Media Information Header Box shall contain a Sound Media Header Box.
- The Sample Description Box shall contain a box derived from AudioSampleEntry. For AC-3 tracks, this box is called AC3SampleEntry, and has a box type designated "ac-3". For Enhanced AC-3 tracks, this box is called EC3SampleEntry, and has box type designated "ec-3". The layout of the AC3SampleEntry and EC3SampleEntry boxes is identical to that of AudioSampleEntry defined in ISO/IEC 14496-12 (including the reserved fields and their values), except that AC3SampleEntry ends with a box containing AC-3 bitstream information called AC3SpecificBox, and EC3SampleEntry ends with a box containing Enhanced AC-3 information called EC3SpecificBox.
- The value of the timescale parameter in the Media Header Box, and the value of the SamplingRate parameter in the AC3SampleEntry Box or EC3SampleEntry Box shall be equal to the sample rate (in Hz) of the AC-3 or Enhanced AC-3 bitstream respectively.

6.2.5 AC-3 and Enhanced AC-3 Sample definition

An AC-3 Sample is defined as follows:

- Exactly one AC-3 syncframe, as defined in [ETSI TS 102 366].

An Enhanced AC-3 Sample is defined as follows:

- The number of Enhanced AC-3 syncframes required to deliver six blocks of audio data from each substream present in the Enhanced AC-3 bitstream, beginning with independent substream 0.

An AC-3 or Enhanced AC-3 Sample is equivalent in duration to 1536 samples of PCM audio data. Consequently the value of the sample_delta field in the Decoding Time to Sample Box shall be 1536.

AC-3 and Enhanced AC-3 Samples shall be byte-aligned. If necessary, up to 7 zero-valued padding bits shall be added to the end of an AC-3 or Enhanced AC-3 Sample to achieve byte-alignment. The Padding Bits Box (defined in section 8.23 of ISO/IEC 14496-12) need not be used to record padding bits that are added to a Sample to align its size to the nearest byte boundary.

6.2.6 AC3SpecificBox

The AC3SpecificBox is defined as follows in Table 6-1:

Table 6-1: AC3SpecificBox

Syntax	No. of bits	Identifier
AC3SpecificBox (){		
BoxHeader.Size	32	uimsbf
BoxHeader.Type	32	uimsbf
fscod	2	uimsbf
bsid	5	uimsbf
bsmod	3	uimsbf
acmod	3	uimbsf
lfeon	1	uimsbf
bit_rate_code	5	uimsbf
reserved	5	uimbsf
}		

Semantics

BoxHeader.Type: The value of the Box Header Type for the AC3SpecificBox shall be "dac3".

Fscod: This field has the same meaning and is set to the same value as the fscod field in the AC-3 bitstream.

bsid: This field has the same meaning and is set to the same value as the bsid field in the AC-3 bitstream.

bsmod: This field has the same meaning and is set to the same value as the bsmod field in the AC-3 bitstream.

acmod: This field has the same meaning and is set to the same value as the acmod field in the AC-3 bitstream.

lfeon: This field has the same meaning and is set to the same value as the lfeon field in the AC-3 bitstream.

bit_rate_code: This field indicates the data rate of the AC-3 bitstream in kbit/s, as shown in Table 6-2.

Table 6-2: bit_rate_code

bit_rate_code	Nominal bit rate (kbit/s)
00000	32
00001	40
00010	48
00011	56
00100	64
00101	80
00110	96
00111	112
01000	128
01001	160
01010	192
01011	224
01 100	256
01101	320
01110	384
01111	448
10000	512
10001	576
10010	640

6.2.7 EC3SpecificBox

The EC3SpecificBox is defined as in Table 6-3:

Table 6-3: EC3SpecificBox

Syntax	No. of bits	Identifier
EC3SpecificBox (){		
BoxHeader.Size	32	uimsbf
BoxHeader.Type	32	uimsbf
data_rate	13	uimsbf
num_ind_sub	3	uimsbf
for(I = 0; i < num_ind_sub; i++)		
{		
fscod	2	uimsbf
bsid	5	uimsbf
bsmod	5	uimsbf
acmod	3	uimsbf
lfeon	1	uimbsf
reserved	3	uimsbf
num_dep_sub	4	uimbsf
if num_dep_sub > 0		
{		
chan_loc	9	uimsbf
}		
else		
{		
reserved	1	uimsbf
}		
}		
}		

Semantics

BoxHeader.Type: The value of the Box Header Type for the EC3SpecificBox shall be "dec3".

data_rate: This value indicates the data rate of the Enhanced AC-3 bitstream in kbit/s. If the Enhanced AC-3 stream is variable bit rate, then this value indicates the maximum data rate of the stream.

num_ind_sub: This field indicates the number of independent substreams that are present in the Enhanced AC-3 bitstream. The value of this field is one less than the number of independent substreams present.

fscod: This field has the same meaning and is set to the same value as the fscod field in the independent substream.

bsid: This field has the same meaning and is set to the same value as the bsid field in the independent substream.

bsmod: This field has the same meaning and is set to the same value as the bsmod field in the independent substream.

acmod: This field has the same meaning and is set to the same value as the acmod field in the independent substream.

lfeon: This field has the same meaning and is set to the same value as the lfeon field in the independent substream.

num_dep_sub: This field indicates the number of dependent substreams that are associated with the independent substream.

chan_loc: If there are one or more dependent substreams associated with the independent substream, this bit field is used to identify channel locations beyond those identified using the acmod field that are present in the bitstream. For each channel location or pair of channel locations present, the corresponding bit in the chan_loc bit field is set to "1", according to Table 6-4. This information is extracted from the chanmap field of each dependent substream.

Table 6-4: chan_loc field bit assignments

Bit	Location
0	Lc/Rc pair
1	Lrs/Rrs pair
2	Cs
3	Ts
4	Lsd/Rsd pair
5	Lw/Rw pair
6	Lvh/Rvh pair
7	Cvh
8	LFE2

6.3 Extended AMR-WB (AMR-WB+)

The AMR-WB+ audio codec can encode mono and stereo content, up to 48 kbit/s for stereo. It supports also downmixing to mono at a decoder. The AMR-WB+ codec has been specified in [ETSI TS 126 290] and includes error concealment and also contains a user's guide. The source code for both encoder and decoder has been fully specified in [ETSI TS 126 304] and [ETSI TS 126 273]. The transport has been specified in [IETF RFC 4352].

6.3.1 Overview of AMR-WB+ codec

The input signal is separated in two bands. The first band is the low-frequency (LF) signal, which is critically sampled at Fs/2. The second band is the high-frequency (HF) signal, which is also down sampled to obtain a critically sampled signal. The LF and HF signals are then encoded using two different approaches: the LF signal is encoded and decoded using the “"cor"” encoder/decoder, based on switched ACELP and Transform Coded eXcitation (TCX). In ACELP mode, the standard AMR-WB codec is used. The HF signal is encoded with relatively few bits using a Band Width Extension (BWE) method.

The parameters transmitted from encoder to decoder are the mode selection bits, the LF parameters and the HF parameters. The codec operates in super frames of 1 024-samples. The parameters for each of them are decomposed into four packets of identical size.

When the input signal is stereo, the left and right channels are combined into mono signal for ACELP/TCX encoding, whereas the stereo encoding receives both input channels.

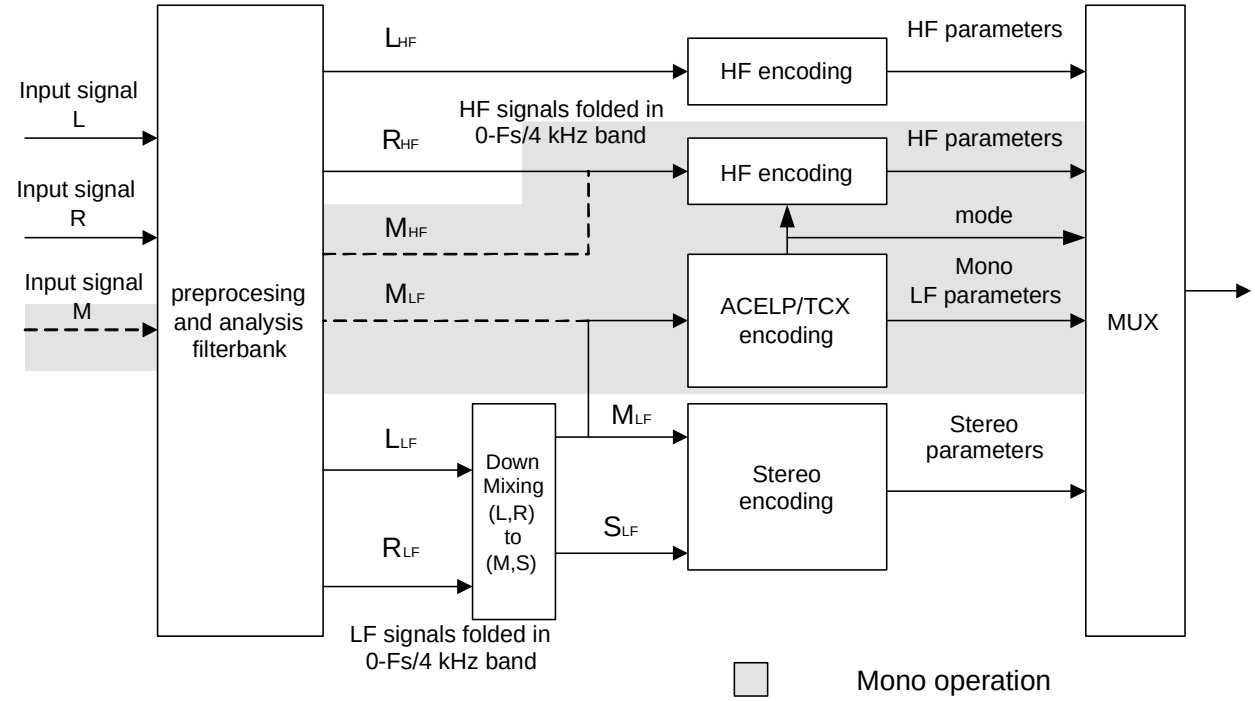


Figure 6-3: High-level structure of AMR-WB+ encoder

Figure 6-4 presents the AMR-WB+ decoder structure. The LF and HF bands are decoded separately after which they are combined in a synthesis filter bank. If the output is restricted to mono only, the stereo parameters are omitted and the decoder operates in mono mode.

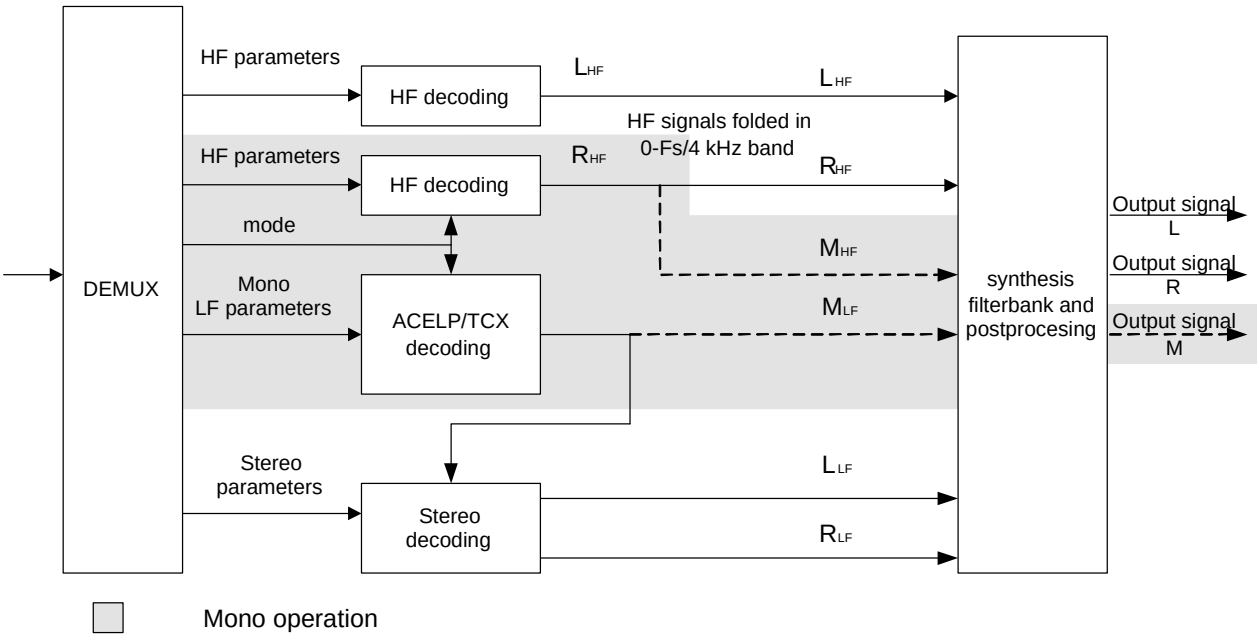


Figure 6-4: High-level structure of AMR-WB+ decoder

6.3.2 Transport and storage of AMR-WB+

To transport AMR-WB+ over RTP [IETF RFC 3550], the RTP payload [IETF RFC 4352] is used. It supports encapsulation of one or multiple AMR-WB+ transport frames per packet, and provides means for redundancy transmission and frame interleaving to improve robustness against possible packet loss. The overhead due to payload starts from three bytes per RTP-packet. The use of interleaving increases the overhead per packet slightly. That payload format includes also parameters required for session setup.

In many application scenarios there is the probability that packets will be lost due to network problems. Because the RTP is running over User Datagram Protocol (UDP), the lost packets are not automatically retransmitted and applications do not need to wait for a retransmission of those lost packets and thus annoying interruptions of the playback is avoided. Instead, applications can utilize forward error correction (FEC) and frame interleaving to improve robustness against possible packet loss. However, doing so increases the bandwidth requirement and increase the signal delay.

The AMR-WB+ RTP payload enables simple FEC functionality with low packetization overhead. In this scheme each packet also carries redundant copy (copies) of the previous frame(s) that can be used to replace possibly lost frames. The cost of this scheme is an increased overall bit rate and additional delay at the receiver to allow the redundant copy to arrive. On the other hand, this approach does not increase the number of transmitted packets, and the redundant frames are also readily available for re-transmission without additional processing. Furthermore, this mechanism does not require signalling at the session setup.

Frame interleaving is another method which may be used to improve the perceptual performance of the receiver by spreading consecutive frames into different RTP-packets. This means that even if a packet is lost then is only lost frames that are not time-wise consecutive to each other that are lost and thus a decoder may be able to reconstruct the lost frames using one of a number of possible error concealment algorithms. The interleaving scheme provided by the AMR-WB+ RTP payload allows any interleaving pattern, as long as the distance in decoding order between any two adjacent frames is not more than 256 frames. If the increases end-to-end delay and higher buffering requirements in the receiver are acceptable then interleaving is useful in IPTV applications.

The AMR-WB+ audio can be stored into a file using the ISO-based 3GP file format defined in [ETSI TS 126 244], which has the media type "audio/3GPP". Note that the 3GP structure also supports the storage of many other multimedia formats, thereby allowing synchronized playback.

6.4 MPEG-4 High Efficiency AAC v2 (HE AAC v2)

The MPEG-4 High Efficiency AAC v2 audio codec is specified in [ISO/IEC 14496-3].

The transport has been specified in [ISO/IEC 14496-3].

6.4.1 Overview of HE AAC v2

The principle problem with traditional perceptual audio codecs operating at low bit rates is, that they would need more bits to encode the whole spectrum accurately than there are available. The results are either coding artefacts or the transmission of a reduced bandwidth audio signal. To resolve this problem, MPEG decided to add a bandwidth extension technology as a new tool to the MPEG-4 audio toolbox. With SBR the higher frequency components of the audio signal are reconstructed at the decoder based on transposition and additional helper information. This method allows an accurate reproduction of the higher frequency components with a much higher coding efficiency compared to a traditional perceptual audio codecs. Within MPEG the resulting audio codec is called MPEG-4 High Efficiency AAC (HE AAC) and is the combination

of the MPEG-4 Audio Object Types AAC-Low Complexity (LC) and Spectral Band Replication (SBR). It is not a replacement for AAC, but rather a superset which extends the reach of high-quality MPEG-4 Audio to much lower bitrates. HE AAC decoders will decode both, plain AAC and the enhanced AAC plus SBR. The result is a backward compatible extension of the standard.

The basic idea behind SBR is the observation that usually there is a strong correlation between the characteristics of the high frequency range of a signal (further referred to as “"highban"”) and the characteristics of the low frequency range (further referred to as “"lowban"”) of the same signal is present. Thus, a good approximation of the representation of the original input signal highband can be achieved by a transposition from the lowband to the highband. In addition to the transposition, the reconstruction of the highband incorporates shaping of the spectral envelope. This process is controlled by transmission of the highband spectral envelope of the original input signal. Additional guidance information for the transposing process is sent from the encoder, which controls means, such as inverse filtering, noise and sine addition. This transmitted side information is further referred to as SBR data.

In June 2004 MPEG extended its toolbox with the Audio Object Type Parametric Stereo (PS), which enables stereo coding at very low bitrates. The principle behind the PS tool is to transmit a mono signal coded in HE AAC format together with a description of the stereo image. The PS tool is used at bit rates in the low bit rate range. The resulting MPEG profile is called MPEG-4 HE AAC v2. Figure 6-5 shows the different MPEG tools used in the MPEG-4 HE AAC v2 profile. A HE AAC v2 decoder will decode all three profiles, AAC-LC, HE AAC and HE AAC v2.

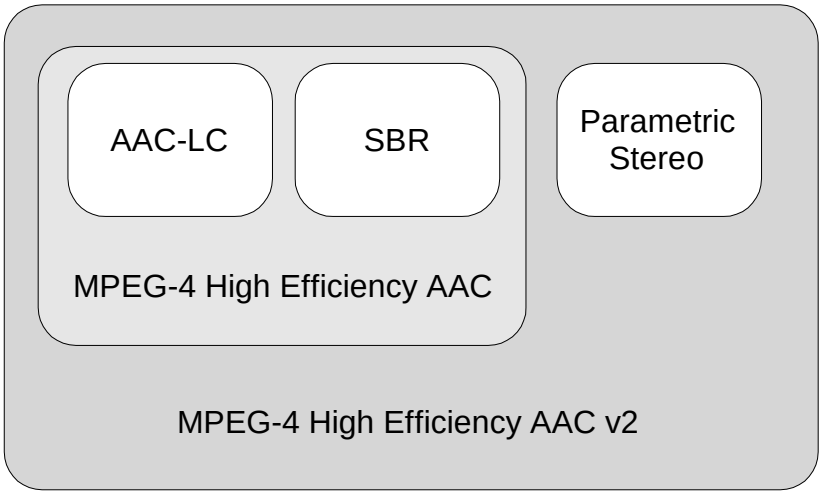


Figure 6-5: MPEG Tools used in the HE AAC v2 Profile

Figure 6-6 shows a block diagram of a HE AAC v2 Encoder. At the lowest bitrates the PS tool is used. At higher bitrates, normal stereo operation is performed. The PS encoding tool estimates the parameters characterizing the perceived stereo image of the input signal. These parameters are embedded in the SBR data. If the PS tool is used, a stereo to mono downmix of the input signal is applied, which is then fed into the aacPlus encoder operating in mono. SBR data is embedded into the AAC bitstream by means of the extension_payload() element Two types of SBR extension data can be signalled through the extension_type field of the extension_payload(). For compatibility reasons with existing AAC only decoders, two different methods for signalling the existence of an SBR payload can be selected. Both methods are described below.

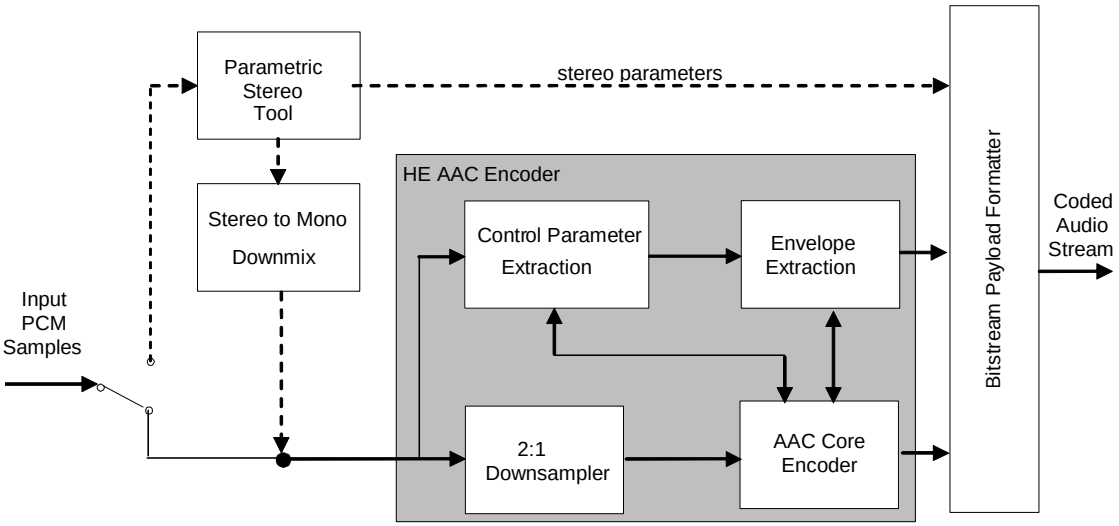


Figure 6-6: HE AAC v2 Encoder

The HE AAC v2 decoder is depicted in Figure 6-7. The coded audio stream is fed into a demultiplexing unit prior to the AAC decoder and the SBR decoder. The AAC decoder reproduces the lower frequency part of the audio spectrum. The time domain output signal from the underlying AAC decoder at the sampling rate fs_{AAC} is first fed into a 32 channel Quadrature Mirror Filter (QMF) analysis filter bank. Secondly, the high frequency generator module recreates the highband by patching QMF subbands from the existing low band to the high band. Furthermore, inverse filtering is applied on a per QMF subband basis, based on the control data obtained from the bit stream. The envelope adjuster modifies the spectral envelope of the regenerated highband, and adds additional components such as noise and sinusoids, all according to the control data in the bit stream. In case of a stream using Parametric Stereo, the mono output signal from the underlying HE AAC decoder is converted into a stereo signal. This processing is carried out in the QMF domain and is controlled by the Parametric Stereo parameters embedded in the SBR data. Finally a 64 channel QMF synthesis filter bank is applied to retain a time-domain output signal at twice the sampling rate, i.e. $fs_{out} = fs_{SBR} = 2 \times fs_{AAC}$.

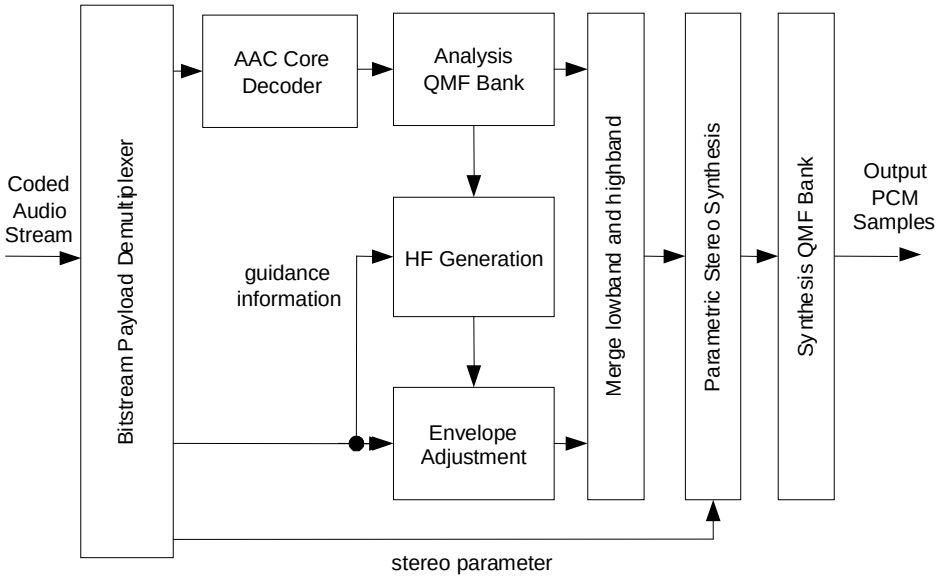


Figure 6-7: HE AAC v2 Decoder

6.4.2 Transport and storage of HE AAC v2

To transport HE AAC v2 audio over RTP [IETF RFC 3550], the RTP payload [IETF RFC 3640] is used. [IETF RFC 3640] supports both implicit signalling as well as explicit signalling by means of conveying the AudioSpecificConfig() as the required MIME parameter “"confi"”, as defined in [IETF RFC 3640]]. The framing structure defined in [IETF RFC 3640] does support carriage of multiple AAC frames in one RTP packet with optional interleaving to improve error resiliency in packet loss. For example, if each RTP packet carries three AAC frames, then with interleaving the RTP packets may carry the AAC frames as given in Figure 6-8.

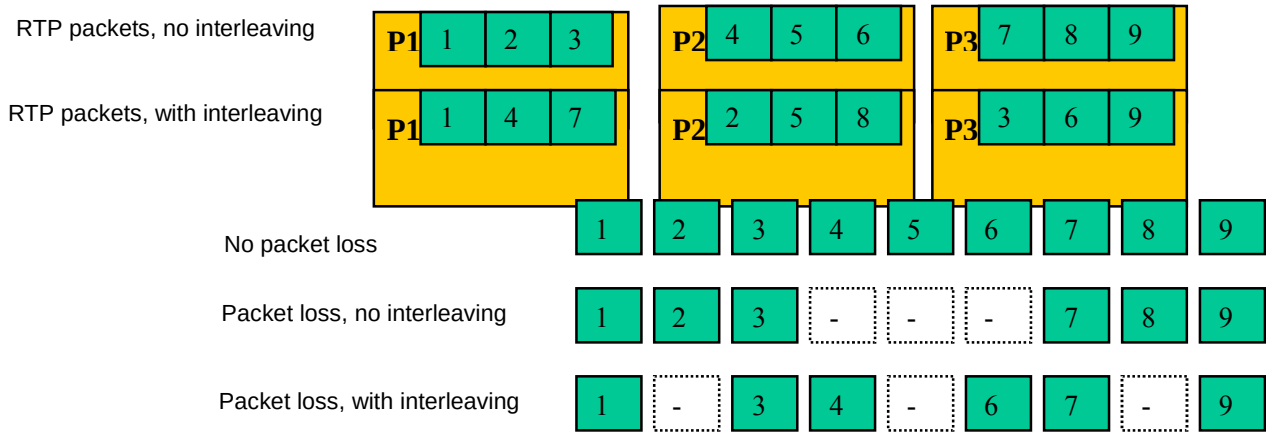


Figure 6-8: Interleaving of AAC frames

Without interleaving, then RTP packet P1 carries the AAC frames 1, 2 and 3, while packet P2 and P3 carry the frames 4, 5 and 6 and the frames 7, 8 and 9, respectively. When P2 gets lost, then AAC frames 4, 5 and 6 get lost, and hence the decoder needs to reconstruct three missing AAC frames that are contiguous. In this example, interleaving is applied so that P1 carries 1, 4 and 7, P2 carries 2, 5 and 8, and P3 carries 3, 6 and 9. When P2 gets lost in this case, again three frames get lost, but due to the interleaving, the frames that are immediately adjacent to each lost frame are received and can be used by the decoder to reconstruct the lost frames, thereby exploiting the typical temporal redundancy between adjacent frames to improve the perceptual performance of the receiver.

6.4.3 HE AAC v2 Levels and Main Parameters for DVB

MPEG-4 provides a huge toolset for the coding of audio objects. In order to allow effective implementations of the standard, subsets of this toolset have been identified that can be used for specific applications. The function of these subsets, called “"Profiles"” is to limit the toolset a conforming decoder must implement. For each of these Profiles, one or more Levels have been specified, thus restricting the computational complexity.

The HE AAC v2 Profile is introduced as a superset of the AAC Profile. Besides the Audio Object Type (AOT) AAC LC (which is present in the AAC Profile), it includes the AOT SBR and the AOT PS. Levels are introduced within these Profiles in such a way, that a decoder supporting the HE AAC v2 Profile at a given level can decode an AAC Profile and an HE AAC Profile stream at the same or lower level.

Table 6-5: Levels within the HE AAC v2 Profile

Level	Max. channels/object	Max. AAC sampling rate, SBR not present [kHz]	Max. AAC sampling rate, SBR present [kHz]	Max. SBR sampling rate, [kHz] (in/out)
1	NA	NA	NA	NA
2	2	48	24	24/48 (see note 1)
3	2	48	48 (see note 3)	48/48 (see note 2)
4	5	48	24/48 (see note 4)	48/48 (see note 2)
5	5	96	48	48/96

NOTE 1: A level 2 HE-AAC v2 Profile decoder implements the baseline version of the parametric stereo tool. Higher level decoders are not be limited to the baseline version of the parametric stereo tool.

NOTE 2: For level 3 and level 4 decoders, it is mandatory to operate SBR in a downsampled mode if the sampling rate of the AAC core is higher than 24 kHz. Hence, if SBR operates on a 48 kHz AAC signal, the internal sampling rate of SBR will be 96 kHz; however, the output signal will be downsampled by SBR to 48 kHz.

NOTE 3: If Parametric Stereo data is present, the maximum AAC sampling rate is 24 kHz; if Parametric stereo data is not present, the maximum AAC sampling rate is 48 kHz.

NOTE 4: For one or two channels, the maximum AAC sampling rate, with SBR present, is 48 kHz. For more than two channels, the maximum AAC sampling rate, with SBR present, is 24 kHz.

For DVB the level 2 for mono and stereo as well as the level 4 multichannel audio signals are supported. The Low Frequency Enhancement channel of a 5.1 audio signal is included in the level 4 definition of the number of channels.

6.4.4 Methods for signalling of SBR and/or PS

In case of usage of SBR and/or PS several ways how to signal the presence of SBR and/or PS data are possible [ISO/IEC 14496-3]. Within the context of DVB services over IP it is recommended to use backward compatible explicit signalling. Here the respective extension Audio Object Type is signalled at the end of the AudioSpecificConfig().

6.5 MPEG-1 Layer 2 Audio

MPEG-1 Layer I or II Audio is a generic subband coder operating at bit rates in the range of 32 to 448 kbit/s and supporting sampling frequencies of 32, 44.1 and 48 kHz. Typical bit rates for Layer II are in the range of 128-256 kbit/s, and 384 kbit/s for professional applications. MPEG-1 Layer I and II audio has been specified in [ISO/IEC 11172-3]. The transport of MPEG-1 Layer I and II audio using RTP over IP has been specified in [IETF RFC 2250]. Furthermore, MPEG-1 Layer II audio is the recommended audio coding system in DVB broadcasting applications as specified in [ETSI TS 101 154].

MPEG-1 Layers I and II (MP1 or MP2) are perceptual audio coders for 1- or 2-channel audio content. Layer I has been designed for applications that require both low complexity decoding and encoding. Layer II provides for a higher compression efficiency for a slightly higher complexity. Using MPEG-1 Layer I one can compress high quality audio CD data at a typical bitrate of 384 kbit/s while maintaining a high audio quality after decoding. Layer II requires bit rates in the range of 192 to 256 kbit/s for near CD quality. A Layer II decoder can also decode Layer I bitstreams.

Thanks to its low complexity decoding combined with high robustness against cascaded encoding/decoding and transmission errors, MPEG-1 Layer II is used in digital audio and video broadcast applications (DVB and DAB). It is also used in Video CD, as well as in a variety of studio applications.

Figure 6-9 shows a high level overview of the MPEG-1 Layers I and II coders. The input signal is transformed into 32 subband signals that are uniformly distributed over frequency by means of a critically sampled QMF filter bank. The critically down sampled subband signals are grouped in a so called allocation frame (384 and 1152 subband samples for Layer I and II respectively). By means of Adaptive PCM, these allocation frames are subsequently quantized and coded into an MPEG-1 bitstream. At the decoder side, the bitstream is decoded into the subband samples which are subsequently fed into the inverse QMF filter bank.

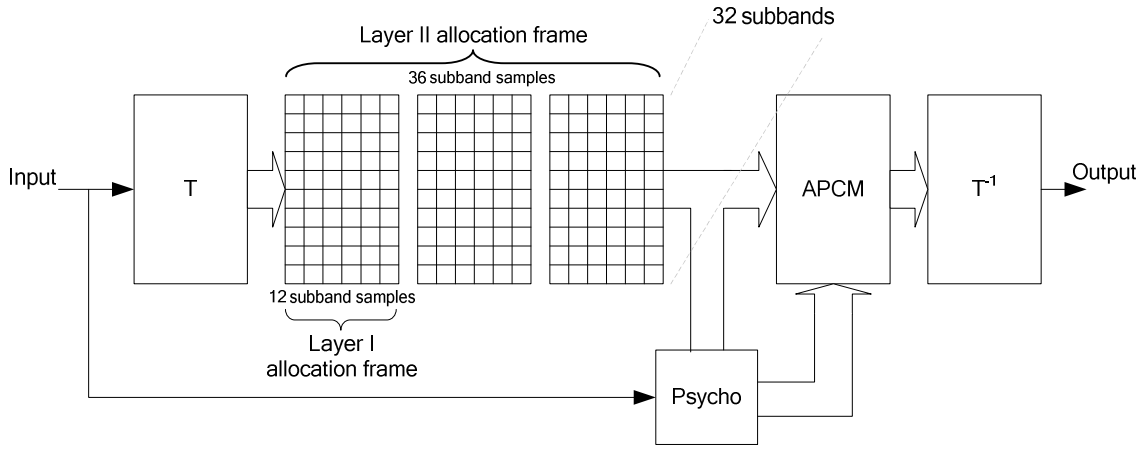


Figure 6-9: High level overview of MPEG-1 Layers II coder

Next to coding of mono and independent coding of stereo signals, also joint coding of stereo signals is supported by applying a technology called intensity stereo coding. Intensity coding exploits the property of the human auditory system that at high frequencies the perceived stereo image depends on intensity level differences.

6.6 MPEG-2 AAC

The MPEG-2 AAC audio codec is specified in ISO/IEC 13818-7:2007 "Information technology – Generic coding of moving picture and associated audio information – Part 7: Advanced Audio Coding (AAC)" [ISO/IEC 13818-7].

6.6.1 Overview of MPEG-2 AAC

[ISO/IEC 13818-7] describes the MPEG-2 audio non-backwards compatible standards called MPEG-2 Advanced Audio Coding (AAC), a higher quality multichannel standard than achievable while requiring MPEG-1 backwards compatibility.

The AAC system consists of three profiles in order to allow a trade-off between the required memory and processing power, and audio quality: *Main profile*

Main profile provides the highest audio quality at any given data rate. All tools except the gain control may be used to provide high audio quality. The required memory and processing power are higher than the LC profile. A main profile decoder can decode an LC-profile encoded bit stream. *Low complexity (LC) profile*

The required processing power and memory of the LC profile are smaller than the main profile, while the quality performance keeps high. The LC profile is without predictor and the gain control tool, but with temporal noise shaping (TNS) order limited. *Scalable sampling rate (SSR) profile*

The SSR profile can provide a frequency scalable signal with gain control tool. It can choose frequency bands to decode, so the decoder requires less hardware. To decode the only lowest frequency band at the 48 kHz sampling frequency, for instance, the decoder can reproduce 6 kHz bandwidth audio signal with minimum decoding complexity.

AAC system supports 12 types of sampling frequencies ranging from 8 to 96 kHz, as shown in Table 6-6, and up to 48 audio channels.

Table 6-6: Supported sampling frequencies

Sampling frequency (Hz)
96 000
88 200
64 000
48 000
44 100
32 000
24 000
22 050
16 000
12 000
11 025
8 000

Table 6-7 shows default channel configurations, which include mono, two-channel, five-channel (three front/two rear channels) and five-channel plus low-frequency effects (LFE) channel (bandwidth < 200 Hz), etc. In addition to the default configurations, it is possible to specify the number of loudspeakers at each position (front, side, and back), allowing flexible multichannel loudspeaker arrangement. Down-mix capability is also supported. The user can designate a coefficient to down-mix multichannel audio signals into two-channel. Sound quality can therefore be controlled using a playback device with only two channels.

Table 6-7: Default channel configurations

Number of speakers	Audio syntactic elements, listed in order received	Default element to speaker mapping
1	single_channel_element	Centre front speaker
2	channel_pair_element	Left and right front speakers
3	single_channel_element()	Centre front speaker
	channel_pair_element()	Left and right front speakers
4	single_channel_element()	Centre front speaker
	channel_pair_element(),	Left and right front speakers
	single_channel_element()	Rear surround speaker
5	single_channel_element()	Centre front speaker
	channel_pair_element()	Left and right front speakers
	channel_pair_element()	Left surround and right surround rear speakers
5+1	single_channel_element()	Centre front speaker
	channel_pair_element()	Left and right front speakers
	channel_pair_element()	Left surround and right surround rear speakers
	Lfe_element()	Low frequency effects speaker
7+1	single_channel_element()	Centre front speaker
	channel_pair_element(),	Left and right centre front speakers
	channel_pair_element()	Left and right outside front speakers
	channel_pair_element()	Left surround and right surround rear speakers
	lfe_element()	Low frequency effects speaker

6.6.2 Overview of Encoder

The basic structure of the MPEG-2 AAC encoder is shown in Figure 6-10. The AAC system consists of the following coding tools: *Gain control*: A gain control splits the input signal into four equally spaced frequency bands. The gain control is used for SSR profile. *Filter bank*: A filter bank modified discrete cosine transform (MDCT) decomposes the input signal into sub-sampled spectral components with frequency resolution of 23 Hz and time resolution of 21.3 ms (128 spectral components) or with frequency resolution of 187 Hz and time resolution of 2.6 ms (1 024 spectral components) at 48 kHz sampling. The window shape is selected between two alternative window shapes. *Temporal noise shaping (TNS)*: After the analysis filter bank, TNS operation is performed. The TNS technique permits the encoder to have control over the temporal fine structure of the quantization noise. *Mid/side (M/S) stereo coding and intensity stereo coding*: For multichannel audio signals, intensity stereo coding and M/S stereo coding may be applied. In intensity stereo coding only the energy envelope is transmitted to reduce the transmitted directional information. In M/S stereo coding, the normalized sum (M as in middle) and difference signals (S as in side) may be transmitted instead of transmitting the original left and right signals. *Prediction*: To reduce the redundancy for stationary signals, the time-domain prediction between sub-sampled spectral components of subsequent frames is performed. *Quantization and noiseless coding*: In the quantization tool, a non-uniform quantizer is used with a step size of 1.5 dB. Huffman coding is applied for quantized spectrum, the different scale factors, and directional information. *Bit-stream formatter*: Finally a bit-stream formatter is used to multiplex the bit stream, which consists of the quantized and coded spectral coefficients and some additional information from each tool. *Psychoacoustic model*: The current masking threshold is computed using a psychoacoustic model from the input signal. A psychoacoustic model similar to [ISO/IEC 11172-3] psychoacoustic model 2 is employed. A signal-to-mask ratio, which is derived from the masking threshold and input signal level, is used during the quantization process in order to minimize the audible quantization noise and additionally for the selection of adequate coding tool.

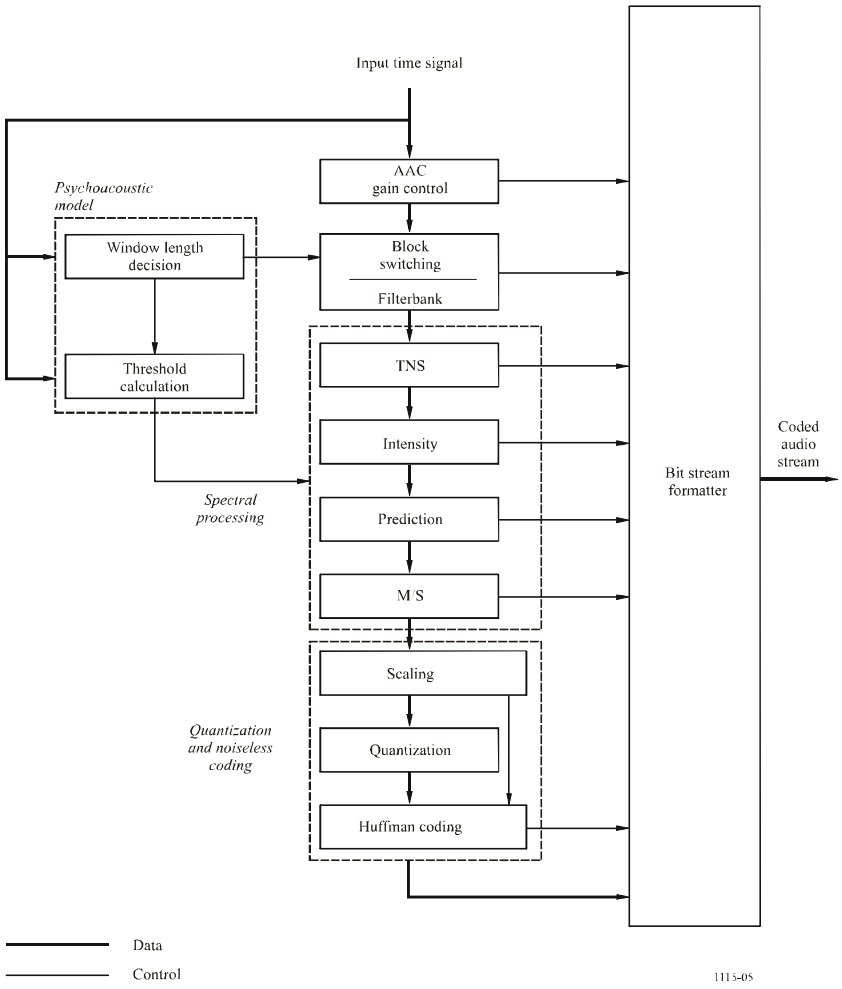


Figure 6-10: MPEG-2 AAC encoder block diagram

6.6.3 Overview of decoder

The basic structure of the MPEG-2 AAC decoder is shown in Figure 6-11. The decoding process is basically the inverse of the encoding process.

The functions of the decoder are to find the description of the quantized audio spectra in the bit stream, decode the quantized values and other reconstruction information, reconstruct the quantized spectra, process the reconstructed spectra through whatever tools are active in the bit stream in order to arrive at the actual signal spectra as described by the input bit stream, and finally convert the frequency domain spectra to the time domain, with or without an optional gain control tool. Following the initial reconstruction and scaling of the spectrum reconstruction, there are many optional tools that modify one or more of the spectra in order to provide more efficient coding. For each of the optional tools that operate in the spectral domain, the option to "pass through" is retained, and in all cases where a spectral operation is omitted, the spectra at its input are passed directly through the tool without modification.

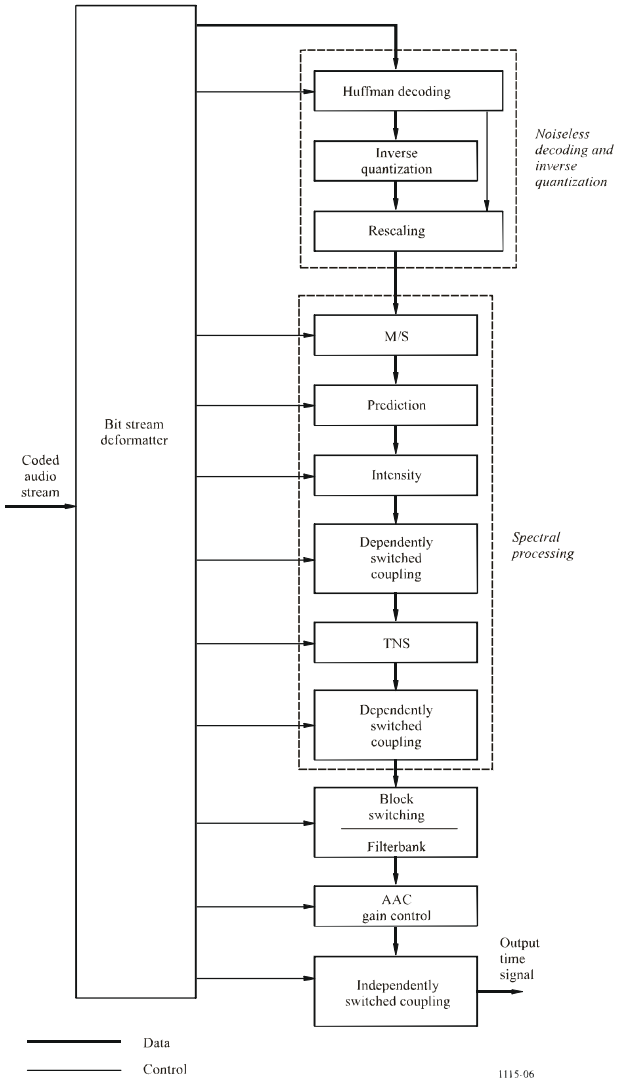


Figure 6-11: MPEG-2 AAC decoder block diagram

6.7 MPEG Surround

6.7.1 Introduction

MPEG Surround adds multichannel capabilities to the audio codec families like MPEG-1 Layer II and MPEG-4 AAC/HE-AAC/HE-AACv2. Operating on top of a core audio codec the system provides a set of features including full backward compatibility to stereo and mono equipment and a broad range of scalability in terms of bit rate used for describing the surround sound image. Conventional audio decoders will decode a stereo or mono signal while based on the same audio stream a decoder supporting the MPEG Surround extension will provide a high quality multichannel signal.

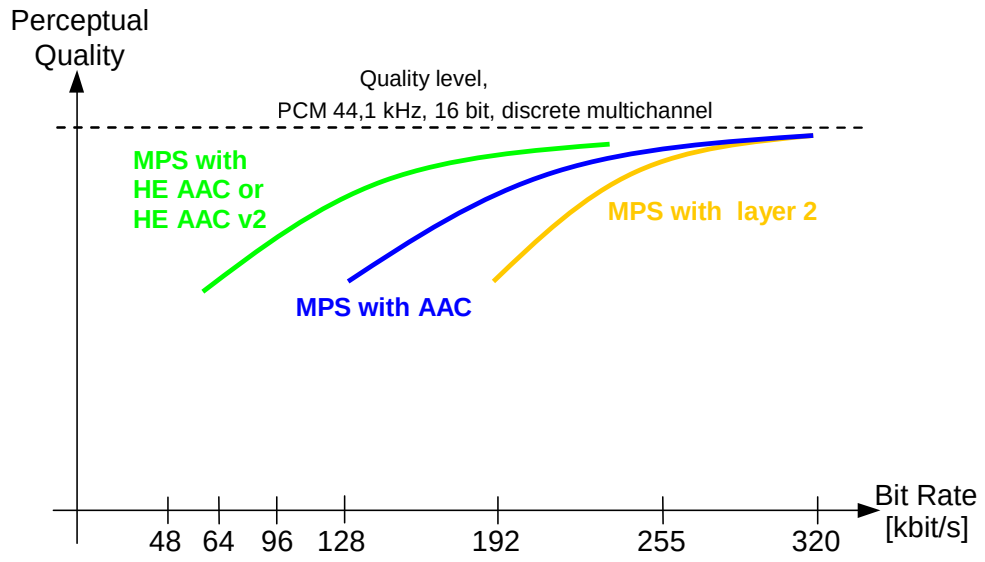


Figure 6-12: Stylistic representation of quality of MPEG Surround (MPS) versus bit rate combined with different core codecs

Figure indicates the typical total bit rate ranges for the use of MPEG Surround in combination with the audio codecs MPEG-1 Layer II (stereo and mono), MPEG 4 AAC (stereo and mono), MPEG 4 HE AAC (stereo and mono), MPEG 4 HE AAC v2 (parametric stereo, only the mono AAC signal is used in combination with MPEG Surround) on the encoder side.

MPEG Surround creates a (mono or stereo) downmix from the multichannel audio input signal. This downmix is encoded using a core audio codec. In addition, MPEG Surround generates a spatial image parameter description of the multichannel audio that is added as an ancillary data stream to the core audio codec. Legacy mono or stereo decoders simply ignore the ancillary data and playback a stereo respectively mono audio signal. MPEG Surround capable decoders will first decode the mono or stereo core codec audio signal and then use the spatial image parameters extracted from the ancillary data stream to generate a high quality multichannel audio signal.

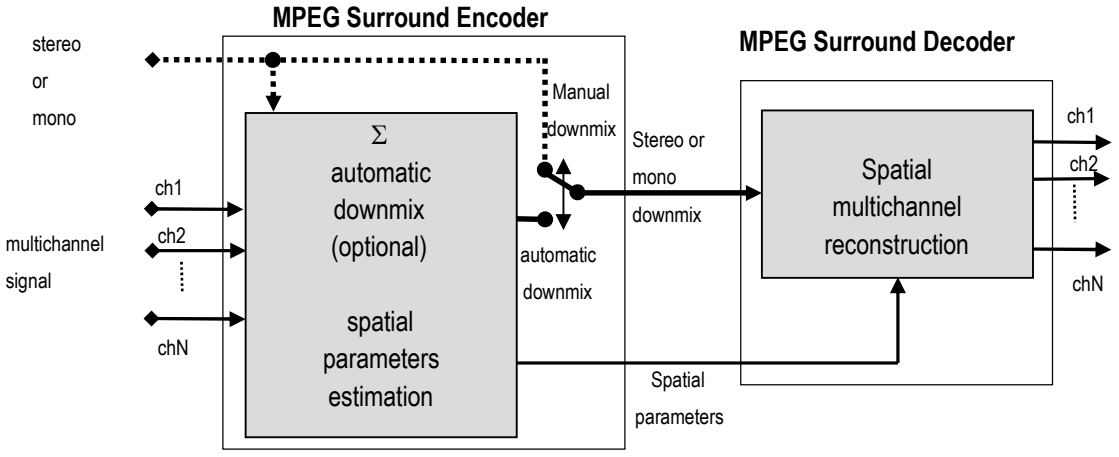


Figure 6-13: Principle of MPEG Surround

6.7.2 MPEG Surround features

In addition to the normal mode of operation in the MPEG Surround Baseline Profile, MPEG Surround supports an additional set of features. These are Binaural Decoding, External Stereo Mix, and Enhanced Matrix Mode, see below.

6.7.3 Introduction to MPEG Surround Baseline profile

The MPEG Surround Baseline Profile is defined in ISO/IEC 23003-1:2007 together with the different levels. In this profile the distinguishing factor between the different levels 1 to 4 is the number of output channels and the use of the coding tool residual coding, which if used allows for higher audio quality but adds computational complexity, hence the bitstream is such that lower level decoders can ignore the residual data. Table 6-8 below summarizes the different levels defined in ISO/IEC 23003-1:2007.

Table 6-8 MPEG Surround level overview

Decoder level	Number of output channels	Residual data
1	2, Stereo and Binaural	Ignores residual data
2	5.1 and Binaural	Ignores residual data
3	5.1 and Binaural	Utilizes residual data
4	7.1 and Binaural	Utilizes residual data

6.7.4 Binaural Decoding

MPEG Surround Binaural Decoding utilizes the downmix, the spatial parameters, and HRTFs supplied to the decoder to create a surround sound audio experience over headphones. There are two modes of operation, a parametric approach, for lowest complexity, and a filtering approach for highest quality. Since both of these methods process the downmix into a 3D audio signal for headphones without first up mixing to the multichannel audio signal, the limited complexity additions allows for portable device usage.

6.7.5 External stereo mix

The MPEG Surround system supports the use of external downmixes. The MPEG Surround encoder analyzes the difference between the internal downmix created by the MPEG Surround encoder and the external downmix. The difference is compensated for at the MPEG Surround decoder side. This allows the broadcaster to have full control of the sound of the transmitted mono or stereo mix. The basic principle is outlined in Figure 6-14.

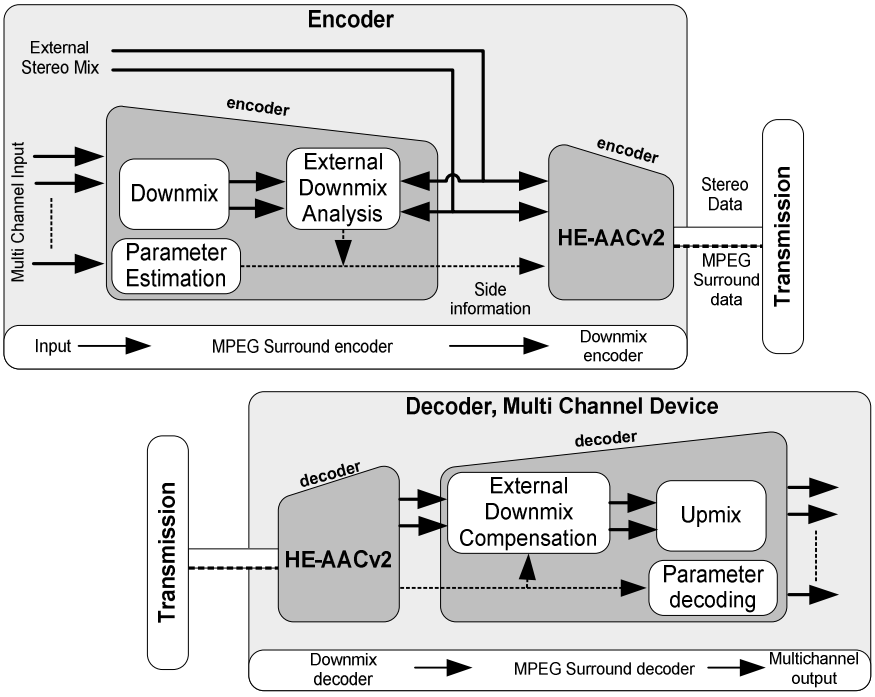


Figure 6-14: MPEG Surround support for external stereo mix

6.7.6 Enhanced Matrix Mode

The MPEG Surround decoder includes Enhanced Matrixed mode that creates a multichannel signal based on the downmix without the transmission of MPEG Surround side information. The parameters required in the MPEG Surround decoder are estimated from the received downmix signal; this tool can also be combined with Binaural Decoding. The basic principle is outlined in Figure 6-15.

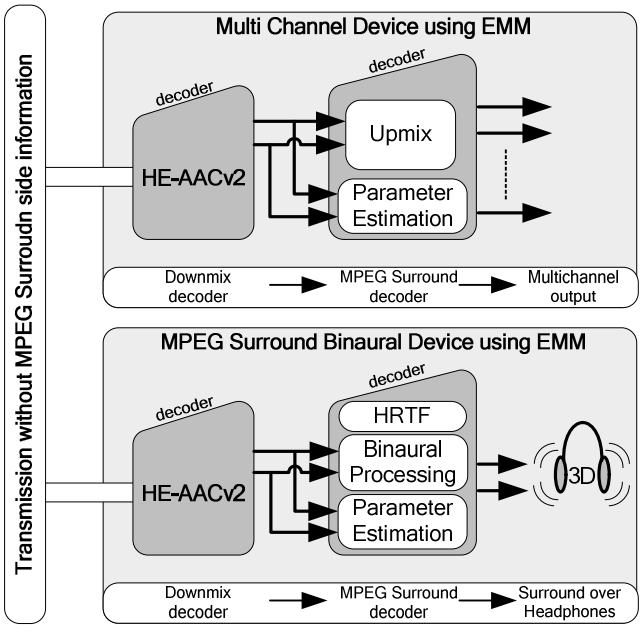


Figure 6-15: Overview diagram for Enhance Matrix Mode decoding mode

6.7.7 MPEG Surround for MPEG-1 Layer II–- Baseline Profile

Encoding and Formatting

The MPEG Surround spatial audio bitstream will be embedded into the ancillary data portion of the MPEG-1 Layer II bitstream as defined in ISO/IEC 11172-3. The actual embedding of the MPEG Surround bitstream into the MPEG-1 Layer II bitstream is specified in ISO/IEC 23003-1.

Configurations, Profiles and Levels

The Baseline MPEG Surround Profile is defined in ISO/IEC 23003-1. For the combination of MPEG Surround with MPEG-1 Layer II, the Baseline MPEG Surround profile shall be used together with the restrictions defined.

The MPEG Surround bitstream payload shall comply with level 3 or 4 of the Baseline MPEG Surround profile.

6.7.8 MPEG Surround for MPEG 4 AAC, HE AAC and HE AAC v2 – Baseline Profile

Encoding and Formatting

The combination of MPEG Surround as specified in ISO/IEC 23003-1 with MPEG-4 AAC, MPEG-4 HE AAC or MPEG-4 HE AAC v2 as specified in ISO/IEC 14496-3 is transmitted using LOAS/LATM, being also specified in ISO/IEC 14496-3. First, the combined MPEG-4 AAC/MPEG Surround, MPEG-4 HE AAC/MPEG Surround or MPEG-4 HE AAC v2/MPEG Surround is formatted using the LATM multiplex format. Specifically, the AudioMuxElement multiplex element shall be used. This LATM multiplex formatted stream is then embedded in the LOAS transmission format for which the AudioSyncStream shall be employed. AudioSyncStream adds a sync word to the audio stream to allow for synchronization. The semantics of the AudioMuxElement and AudioSyncStream formatting are described in ISO/IEC 14496-3.

Configurations, Profiles and Levels

The Baseline MPEG Surround Profile is defined in ISO/IEC 23003-1.

For the combination of MPEG Surround with MPEG-4 AAC, MPEG-4 HE AAC or MPEG-4 HE AAC v2, the Baseline MPEG Surround Profile will be employed together with the AAC Profile, HE AAC profile or HE AAC v2 Profile respectively. The AAC, HE AAC or HE AAC v2 bitstream payloads shall comply with level 2 or level 4 of the respective profile. The MPEG Surround bitstream payload shall comply with level 3, 4 or 5 of the Baseline MPEG Surround profile.

6.8 ITU-T G.722.1 and G.722.1 Annex C

The main body of [ITU-T G.722.1] describes a wideband coding algorithm that provides an audio bandwidth of 50 Hz to 7 kHz, operating at a bit rate of 24 kbit/s or 32 kbit/s. Annex C of [ITU-T G.722.1] is a doubled form of the G.722.1 main body to permit 14 kHz audio bandwidth using a 32 kHz audio sample rate, at 24, 32, and 48 kbit/s. Both G.722.1 and G.722.1 Annex C codecs feature very high audio quality, extremely low computational complexity, and low algorithmic delay compared to other state-of-the-art audio coding algorithms.

The G.722.1 algorithm is based on transform coding, using a Modulated Lapped Transform (MLT) and operates on frames of 20 ms corresponding to 320 samples at a 16 kHz sampling rate. Because the transform window length is 640 samples and a 50 percent overlap is used between frames, the effective look-ahead buffer size is 320 samples. Hence the total algorithmic delay of the coder is 40 ms. Figure 6-16 shows a block diagram of the encoder.

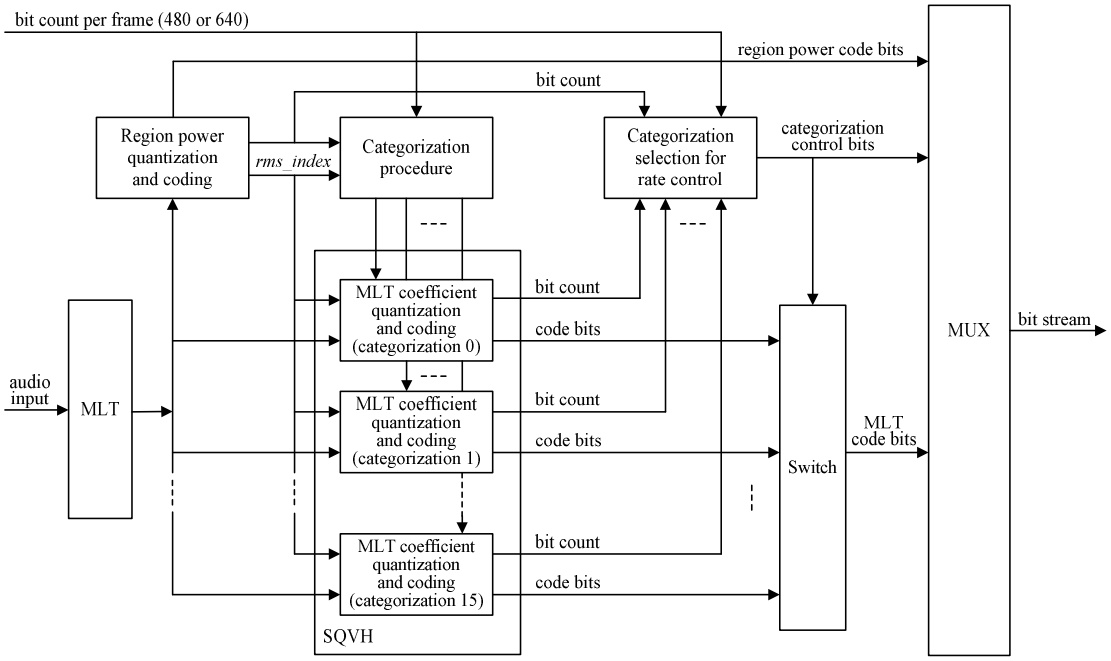


Figure 6-16: Block diagram of the G.722.1 encoder

The MLT performs a frequency spectrum analysis on audio samples and converts the samples from the time domain into a frequency domain representation. Every 20 ms the most recent 640 audio samples are fed to the MLT and transformed into a frame of 320 transform coefficients centered at 25 Hz intervals. In each frame the MLT transform coefficients are divided into 16 regions, each having 20 transform coefficients and representing a bandwidth of 500 Hz. As the bandwidth is 7 kHz, only the 14 lowest regions are used. For each region the region power or the root-mean-square (*rms*) value of the MLT transform coefficients in the region is computed and scalar quantized with a logarithmic quantizer The obtained quantization indices are differentially coded and then Huffman coded with a variable number of bits. Using the quantized region power indices and the number of bits remaining in the frame, the categorization procedure generates 16 possible categorizations to determine the parameters used to quantize and code the MLT transform coefficients. Then, the MLT transform coefficients are normalized, scalar quantized, combined into vectors, and Huffman coded. The bit stream is transmitted on the channel in 3 parts: region power code bits, 4 categorization control bits, and then code bits for MLT transform coefficients.

G.722.1 Annex C has the same algorithmic steps as the G.722.1 main body, except that the algorithm is doubled to accommodate the 14 kHz audio bandwidth. G.722.1 Annex C still operates on frames of 20 ms and has an algorithmic delay of 40 ms, but due to the higher sampling frequency the frame length is doubled to 640 samples from 320 samples and the transform window size increases to 1280 samples from 640 samples. Compared to the G.722.1 main body, the specific differences in the G.722.1 Annex C encoder are as follows:

- Double the MLT transform length from 320 to 640 samples
- Double the number of frequency regions from 14 to 28
- Double the sizes of Huffman coding tables for encoding quantized region power indices
- Double the threshold for adjusting the number of available bits from 320 to 640

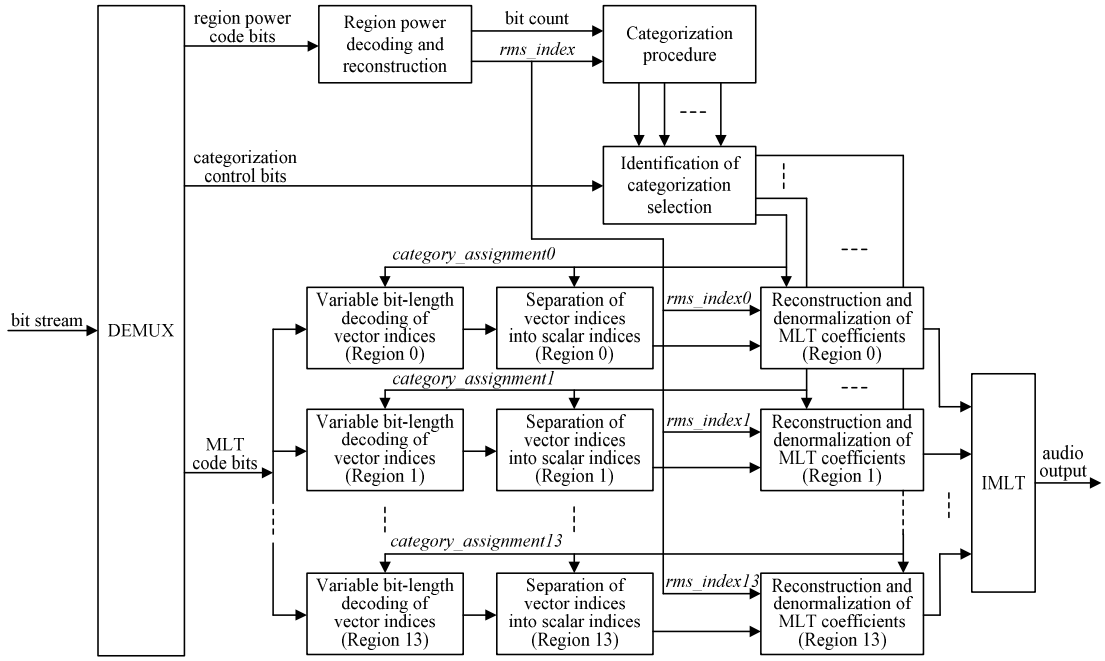


Figure 6-17: Block diagram of the G.722.1 decoder

Figure 6-17 shows a block diagram of the decoder. In each frame the region power code bits are first extracted from the received data and then decoded to obtain the quantization indices for the region powers. Using the same categorization procedure as the encoder, the set of 16 possible categorizations computed by the encoder are recovered and the categorization used to encode MLT transform coefficients is found with the received 4 categorization control bits. For each region the variable bit-length codes for MLT transform coefficients are decoded with the appropriate category and the MLT transform coefficients are reconstructed. The reconstructed MLT transform coefficients are converted into time domain audio samples by an Inverse MLT (IMLT). Each IMLT operation takes in 320 MLT transform coefficients to produce 320 audio samples.

Following are the main changes in the G.722.1Annex C decoder when compared to G.722.1:

- Double the number of frequency regions from 14 to 28
- Double the threshold for adjusting the number of available bits from 320 to 640
- Extend the centroid table used for reconstruction of MLT transform coefficients
- Double the IMLT transform length from 320 to 640 samples

Low complexity is a major technical advantage of G.722.1 and G.722.1 Annex C compared to other codecs with similar performance in this bit-rate range. Table 6-9 and Table 6-10 present the computational complexity in units of Weighted Million Operations Per Second (WMOPS) and memory requirements in bytes of G.722.1 and G.722.1 Annex C, respectively.

Table 6-9: Computational complexity in WMOPS

Codec	Bit rate (kbit/s)	Encoder (WMOPS)	Decoder (WMOPS)	Encoder+Decoder (WMOPS)
G.722.1	24	2.3	2.7	5.0
	32	2.4	2.9	5.3
G.722.1 Annex C	24	4.5	5.3	9.7
	32	4.8	5.5	10.3
	48	5.1	5.9	10.9

Table 6-10: Memory requirements in Bytes

Codec	RAM	Data-ROM
G.722.1	11 K	20 K
G.722.1C	18 K	30 K

In March 2005, as a part of the G.722.1 Annex C development process in ITU-T, subjective characterization tests were performed on G.722.1C by an independent listening lab according to a test plan designed by the ITU-T Q7/SG12 Speech Quality Experts Group (SQEG. A well-known MPEG audio codec was used as the reference codec in the tests. Statistical analysis of the test results showed that G.722.1C met all performance requirements. For speech signal, G.722.1C was better than the reference codec at 24 and 32 kbit/s and G.722.1C at 48 kbit/s was not worse than the reference codec operating at either 48 or 64 kbit/s. For music and mixed content such as film trailers, news, jingles and advertisement, G.722.1C was better than the reference codec at all bit rates and G.722.1C at 48 kbit/s was also better than the reference codec operating at 64 kbit/s.

The RTP payload for G.722.1 and G.722.1C is specified in ITU-T Recommendation G.722.1 Annex A, and also specified in [IETF RFC 3047] and draft-ietf-avt-rfc3047-bis-04 which updates RFC 3047 adding support for G.722.1 Annex C.

6.9 ITU-T G.729.1 – An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729

The G.729.1 coder is an 8-32 kbit/s scalable wideband extension of G.729. The output of G.729.1 has a bandwidth of 50-4000 Hz at 8 and 12 kbit/s and 50-7000 Hz from 14 to 32 kbit/s. At 8 kbit/s, G.729.1 is fully interoperable with G.729, G.729 Annex A, and G.729 Annex B.

G.729.1 is recommended as optional codec for NG-DECT to provide high wideband voice quality in current “"32 kbit/"” DECT channel. The main specific features are the interoperability with widely deployed G.729 based VoIP systems and the specific design for usage over packetized networks (high robustness to packet losses). Scalability can be also identified as a specific feature to easily and efficiently quality/bandwidth usage tradeoff.

The encoder produces an embedded bitstream structured in 12 layers corresponding to 12 available bit rates from 8 to 32 kbit/s. The bitstream can be truncated at the decoder side or by any component of the communication systems to adjust “"on the fl"” the bit rate to the desired value with no need for outband signalling. Figure 6-18 shows the G.729.1 bitstream format.

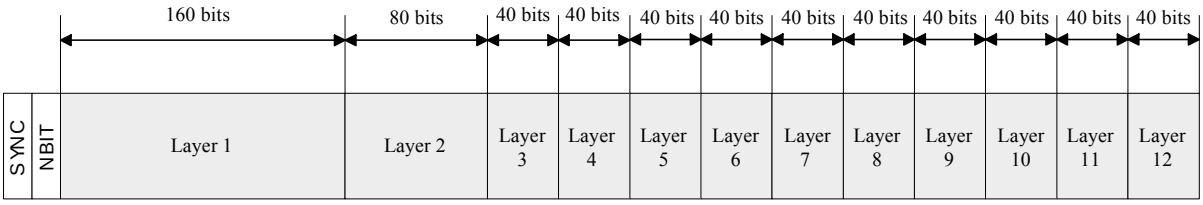


Figure 6-18: G.729.1 bitstream format (compliant with G.192)

The underlying algorithm of the G.729.1 coder is based on a three-stage coding structure: embedded Code-Excited Linear Predictive (CELP) coding of the lower band (50-4000 Hz), parametric coding of the higher band (4000-7000 Hz) by Time Domain Bandwidth Extension (TDBWE), and enhancement of the full band (50-7000Hz) by a predictive transform coding technique referred to as Time-Domain Aliasing Cancellation (TDAC).

6.9.1 Overview of Encoder

The G.729.1 encoder structure is shown in Figure 6-19. The coder operates on 20 ms frame and the default sampling rate is 16000 Hz. However, the 8000 Hz sampling frequency is also supported.

The input signal is first split into two subbands using a QMF filter bank and then decimated. The high-pass filtered lower band signal is coded by the 8-12 kbit/s narrowband embedded CELP encoder. The difference between the input and local synthesis signal of the CELP encoder at 12 kbit/s is processed by the perceptual weighting filter. The weighted difference signal is then transformed into frequency domain by MDCT.

The spectral folded higher band signal is pre-processed by a low-pass filter with 3000 Hz cutoff frequency. The resulting signal is coded by the TDBWE encoder and the signal is also transformed into frequency domain by MDCT. The MDCT coefficients of lower band and higher band signal are finally coded by the TDAC encoder.

In addition, some parameters are transmitted by the frame erasure concealment (FEC) encoder in order to introduce parameter-level redundancy in the bitstream. This redundancy allows improving quality in the presence of erased frames.

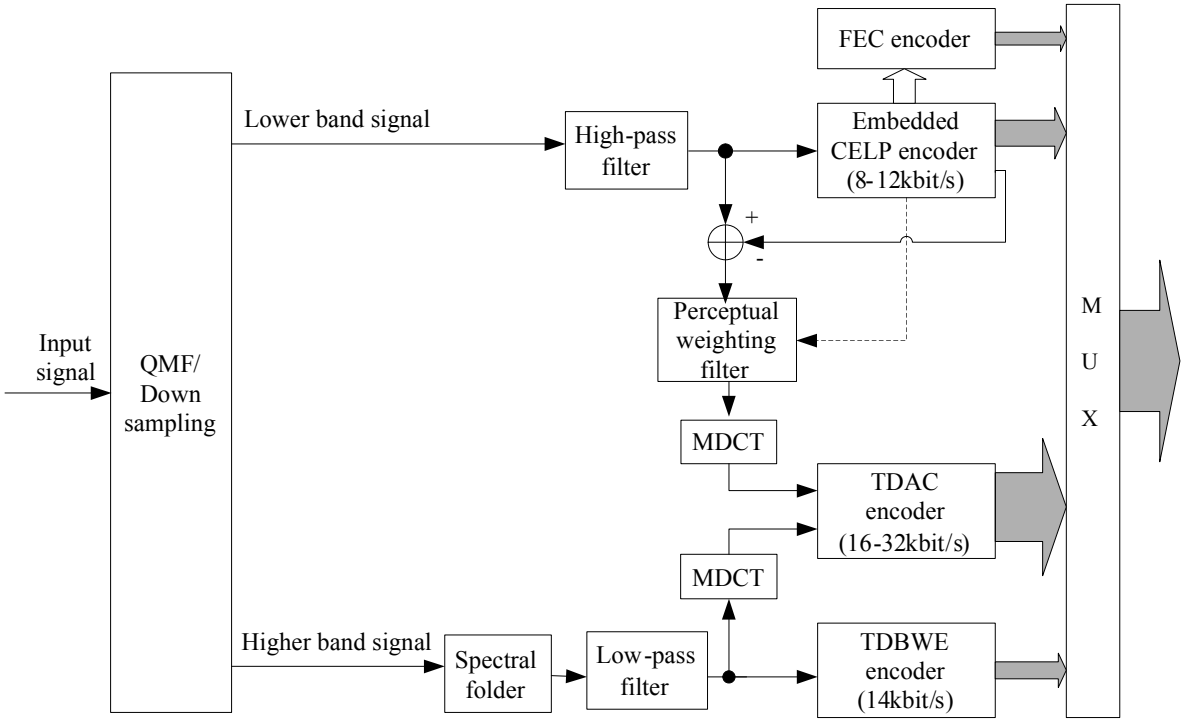


Figure 6-19: High-level block diagram of the encoder

6.9.2 Overview of Decoder

A functional diagram of the decoder is presented in Figure 6-20. The decoding depends on the actual number of received layers or equivalently on the received bit rate.

If the received bit rate is:

- **8 kbit/s (Layer 1):** The layer 1 is decoded by the embedded CELP decoder. Then the decoded signal is post-filtered and post-processed by a high-pass filter. The QMF synthesis filter bank generates the output with a high-frequency synthesis set to zero.
- **12 kbit/s (Layers 1 and 2):** The layer 1 and 2 are decoded by the embedded CELP decoder and the synthesized signal is then post-filtered and high-pass filtered. The QMF synthesis filter bank generates the output with a high-frequency synthesis set to zero.
- **14 kbit/s (Layers 1 to 3):** In addition to the narrowband CELP decoding and lower band adaptive post-filtering, the TDBWE decoder produces a high-frequency synthesis which is then transformed into frequency domain by MDCT so as to zero the frequency band above 3000 Hz in the higher band spectrum. The resulting spectrum is transformed in time domain by inverse MDCT and overlap-add before spectral folding. In the QMF synthesis filter bank the reconstructed higher band signal is combined with the respective lower band signal reconstructed at 12 kbit/s without high-pass filtering.
- **Above 14 kbit/s (Layers 1 to 4+):** In addition to the narrowband CELP and TDBWE decoding, the TDAC decoder reconstructs MDCT coefficients, which correspond to the reconstructed weighted difference in lower band and the reconstructed signal in higher band. In the higher band, the non-received subbands and the subbands with zero bit allocation in TDAC decoding are replaced by the level-adjusted subbands of MDCT coefficients which are produced by TDBWE. The lower band and higher band MDCT coefficients are transformed into time domain by inverse MDCT and overlap-add. The lower band signal is then processed by the inverse perceptual weighting filter. To

attenuate transform coding artefacts pre/post-echoes are detected and reduced in both the lower and higher band signals. The lower band synthesis is post-filtered, while the higher band synthesis is spectrally folded. The lower band and higher band signal are then combined and up-sampled in the QMF synthesis filter bank.

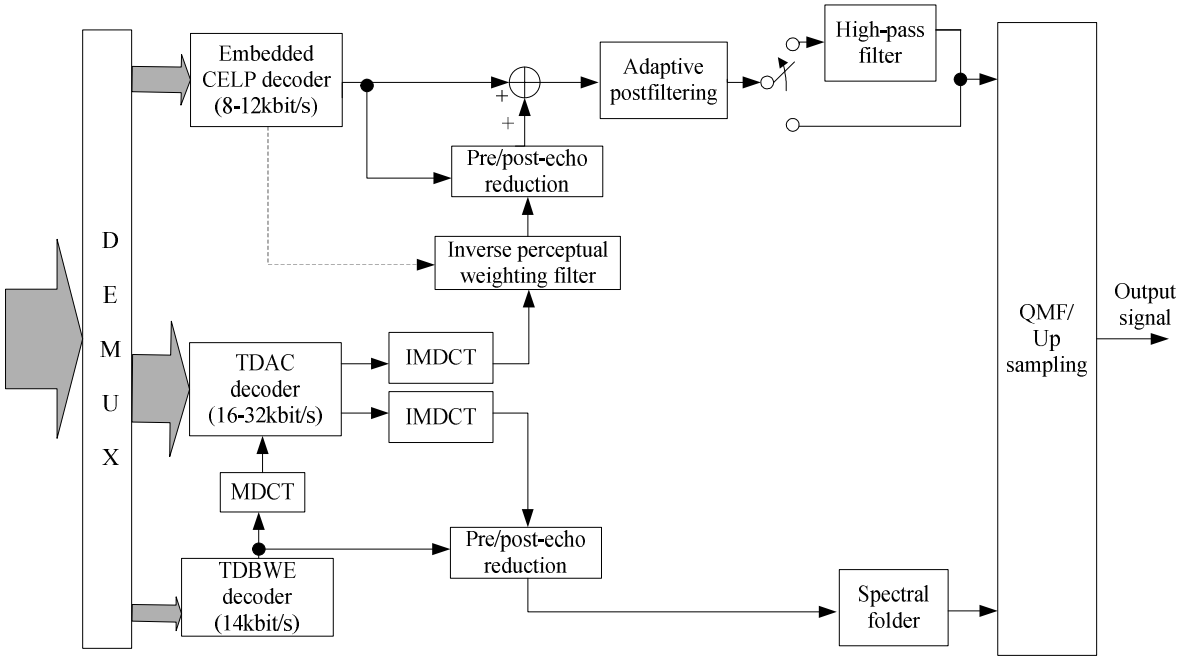


Figure 6-20: High-level block diagram of the decoder

6.9.3 RTP payload

To transmit the G.729.1 bitstream over RTP, the RTP payload format specified in RFC 4749 is used**.** The payload consists of one byte header and zero or more consecutive audio frames at the same bit rate. The payload header consists of two fields: 4 bit MBS and 4 bit FT.

MBS (Maximum Bit rate Supported) indicates a maximum bit rate to the encoder at the receiver site. Because of the embedded property of the G.729.1 coder, the encoder can send frames at the MBS rate or any lower rate. Also, as long as it does not exceed the MBS, the encoder can change its bit rate at any time without previous notice. The MBS values from 0 to 11 represent the bit rate from 8 to 32 kbit/s, respectively. And the MBS value 15 assigned to a multicast group application.

FT (Frame Type) indicates the encoding rate of the frames in the packet. The FT values from 0 to 11, like a MBS, indicate the bit rate from 8 to 32 kbit/s. The FT value 15 indicates that there is no audio data in the payload.

Audio data of a payload contains one or more consecutive audio frames at the same bit rate. The audio frames are packed in order of time, that is, oldest first.

6.10 ITU-T G.722

[ITU-T G.722] is an audio coding system which may be used for a variety of higher quality wideband (50 to 7000 Hz) speech applications. It has been standardized in 1988 to enhance the audio quality of applications like video and audio conferencing over ISDN networks and has been used for some specific radio broadcast usage as well. G.722 usage has recently strongly increased for VoIP: it has been selected as mandatory codecs for New Generation wideband DECT terminals and is gaining momentum for enhanced wideband

voice services over IP networks thanks to some attractive features like low delay, low complexity and licence free status.

6.10.1 Overview of main functional features

G.722 has three modes of operation corresponding to the bit rates of 64, 56 and 48 kbit/s. The G.722 encoder produces an embedded 64 kbit/s bitstream structured in 3 layers corresponding to these 3 operating modes. The bits corresponding to the last 2 layers can be skipped by the decoder or any other component of the communication systems to dynamically reduce the bit rate to 56 kbit/s or 48 kbit/s which corresponds to 1 or 2 bits “"stole"” from the low band.

Encoding/decoding operations are performed on a sample per sample basis which limits the algorithmic delay to 1,625ms.

Complexity is limited and can be estimated to around 10 MIPS.

Appendix III and IV of [ITU-T G.722] propose two possible standardized packet loss mechanisms to strongly increase G.722 audio quality for usage over IP networks subject to packet losses.

For usage of G.722 over IP networks, format of RTP payload is specified in [IETF RFC 3551].

6.10.2 Overview of G.722 SB-ADPCM encoder

The coding system uses sub-band adaptive differential pulse code modulation (SB-ADPCM). The frequency band of the input signal (sampled at 16 kHz) is split into two sub-bands by two linear-phase non-recursive digital QMF filters (Quadrature Mirror Filtors): [0, 4 kHz] for the lower band and [4, 8 kHz] for the higher band. The signals in each sub-band (now sampled at 8 Khz) are encoded using ADPCM with 6 bits per sample for the lower band and 2 bits for the higher band. The number of bits allocated to the lower band are reduced to 5 bits and 4 bits for the 56 kbit/s and 48 kbit/s modes respectively.

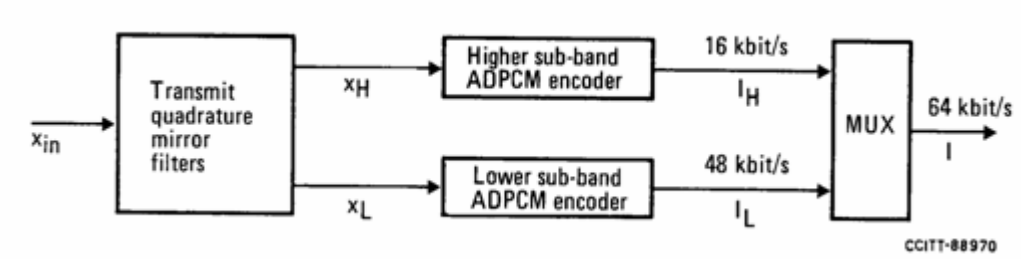


Figure 6-21: Block diagram of the SB-ADPCM encoder

6.10.3 Lower sub-band ADPCM encoder

The lower sub-band input signal, x_L after subtraction of an estimate, s_L, of the input signal produces the difference signal, e_L. An adaptive 60-level non linear quantizer is used to assign six binary digits to the value of the difference signal to produce a 48 kbit/s signal, I_L. In the feedback loop, the two least significant bits of I_L are deleted to produce a 4-bit signal I_{Lt}, which is used for the quantizer adaptation and applied to a 15-level inverse adaptive quantizer to produce a quantized difference signal, d_{Lt}. The signal estimate, s_L is added to this quantized difference signal to produce a reconstructed version, r_{Lt}, of the lower sub-band input signal. Both the reconstructed signal and the quantized difference signal are operated upon by an adaptive predictor which produce the estimate, s_L, of the input signal, thereby completing the feedback loop.

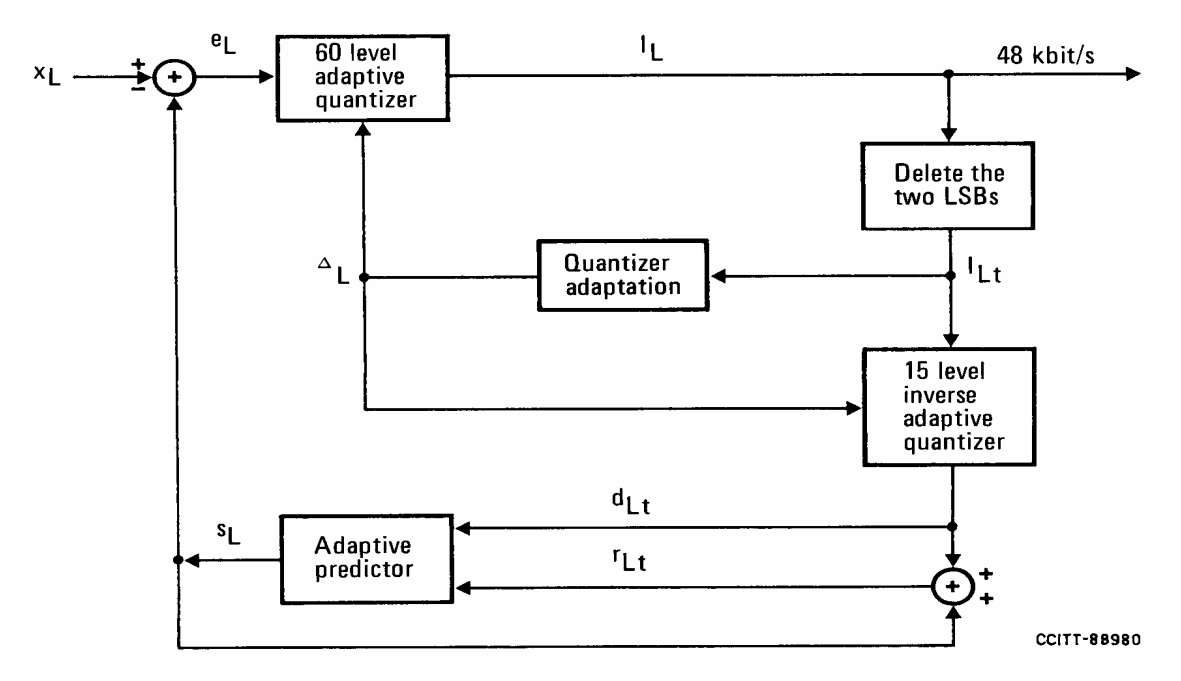


Figure 6-22: Block diagram of the lower sub-band ADPCM encoder

6.10.4 Higher sub-band ADPCM encoder

Same encoding scheme is used for higher sub-band with 4-level non linear quantizer, 4-level inverse adaptive quantizer and no deleted bits.

6.10.5 Overview of G.722 SB-ADPCM decoder

G.722 decoder can operate in any of three possible variants depending on the received indication of the mode of operation as shown in following block diagram Figure 6-23:

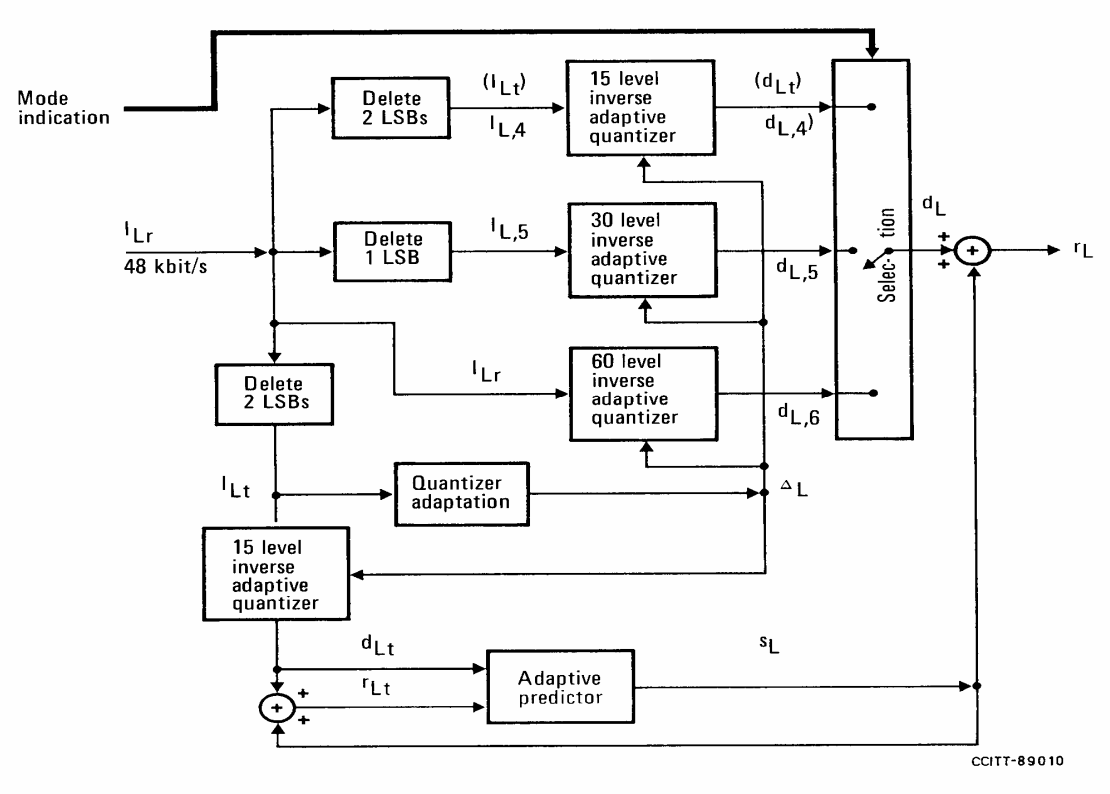


Figure 6-23: Block diagram of the lower sub-band ADPCM decoder

The path which produces the estimate, s_L, of the input signal including the quantizer adaptation, is identical to the feedback portion of the lower sub-band ADPCM encoder. The reconstructed signal, r_L, is produced by adding to the signal estimate one of three possible quantized difference signals, $d_{L,6}$, $d_{L,5}$ or $d_{L,4}$ (= d_{Lt}), selected according to the received indication of the mode of operation.

Upper band decoder has the same structure with a single 4-level inverse adaptive quantizer.

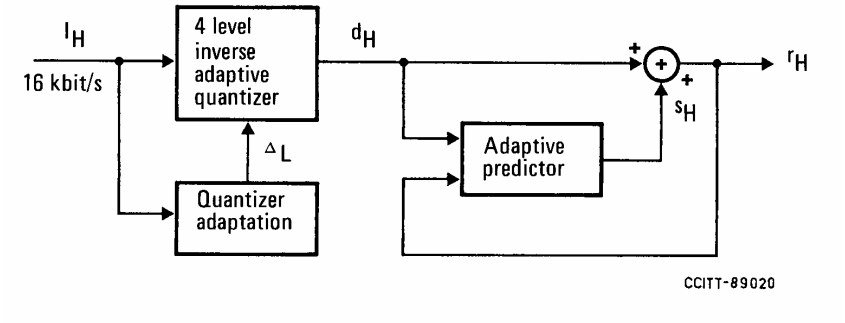


Figure 6-24: Block diagram of the higher sub-band ADPCM decoder

The output decoded signal is then reconstructed by interpolation of the decoded lower band and higher band from 8 kHz to 16 kHz. The combination of the transmit and the receive QMF filters.

6.11 ITU-T G.722.2 (3GPP AMR-WB)

The AMR-WB codec has been standardized by both the ITU-T (as Recommendation G.722.2) and 3GPP. It is a multi-rate codec that encodes wideband audio signals sampled at 16 kHz (with a signal bandwidth of 50-7000 Hz). The AMR-WB codec is also used as a part of the AMR-WB+. However, AMR-WB+ does not work as the AMR-WB codec and has a longer algorithmic delay. For supporting lower delay wideband speech applications, standalone AMR-WB is more suitable. The AMR-WB codec consists of nine modes with bit rates of 23.85, 23.05, 19.85, 18.25, 15.85, 14.25, 12.65, 8.85 and 6.6 kbps. AMR-WB also includes a 1.75 kbps background noise mode that is designed for the Discontinuous Transmission (DTX) operation in GSM and can be used as a low bit rate source-dependent back ground noise mode in other systems.

In 3GPP, the AMR-WB codec has been specified in several specifications. TS 26.171 gives a general overview of the AMR-WB standards. The algorithmic detailed description is given in TS 26.190, and the fixed point and floating point source code are given in TS 26.173 and TS 26.204, respectively. Voice Activity detection is given in TS 26.194 and comfort noise aspects are detailed in TS 26.192. Frame erasure concealment is specified in TS 26.191.

In ITU-T the same specifications are reproduced in Recommendation G.722.2 and its annexes.

In 3GPP, AMR-WB is the mandatory codec for several services when wideband speech sampled at 16 kHz is used. These services include circuit switched and packet-switched telephony, 3G-324H multimedia telephony, Multimedia Messaging Service (MMS), Packet-switched Streaming Service (PSS), Multimedia Broadcast/Multicast Service (MBMS), IP multimedia Subsystem (IMS) Messaging and Presence, and Push-to-talk over Cellular (PoC).

6.11.1 Overview of AMR-WB codec

The codec is based on the code-excited linear predictive (CELP) coding model. The codec operates at an internal sampling frequency of 12.8 kHz. The input signal is processed in 20 ms frames (256 samples).

The signal flow at the encoder is shown in Figure 6-25. After decimation, high-pass and pre-emphasis filtering is performed. LP analysis is performed once per frame. The set of LP parameters is converted to immittance spectrum pairs (ISP) and vector quantized using split-multistage vector quantization (S-MSVQ). The speech frame is divided into 4 subframes of 5 ms each (64 samples). The adaptive and fixed codebook parameters are transmitted every subframe. The quantized and unquantized LP parameters or their interpolated versions are used depending on the subframe. An open-loop pitch lag is estimated in every other subframe or once per frame based on the perceptually weighted speech signal.

Then the following operations are repeated for each subframe:

- The target signal *x(n)* is computed by filtering the LP residual through the weighted synthesis filter $W(z)H(z)$ with the initial states of the filters having been updated by filtering the error between LP residual and.
- The impulse response, *h(n)* of the weighted synthesis filter is computed.
- Closed-loop pitch analysis is then performed (to find the pitch lag and gain), using the target *x(n)* and impulse response *h(n)*, by searching around the open-loop pitch lag. Fractional pitch with 1/4th or 1/2nd of a sample resolution (depending on the mode and the pitch lag value) is used. The interpolating filter in fractional pitch search has low pass frequency response. Further, there are two potential low-pass characteristics in the adaptive codebook and this information is encoded with 1 bit.
- The target signal *x(n)* is updated by removing the adaptive codebook contribution (filtered adaptive codevector), and this new target, $x_2(n)$, is used in the fixed algebraic codebook search (to find the optimum innovation).

- The gains of the adaptive and fixed codebook are vector quantified with 6 or 7 bits (with moving average (MA) prediction applied to the fixed codebook gain).

- Finally, the filter memories are updated (using the determined excitation signal) for finding the target signal in the next subframe.

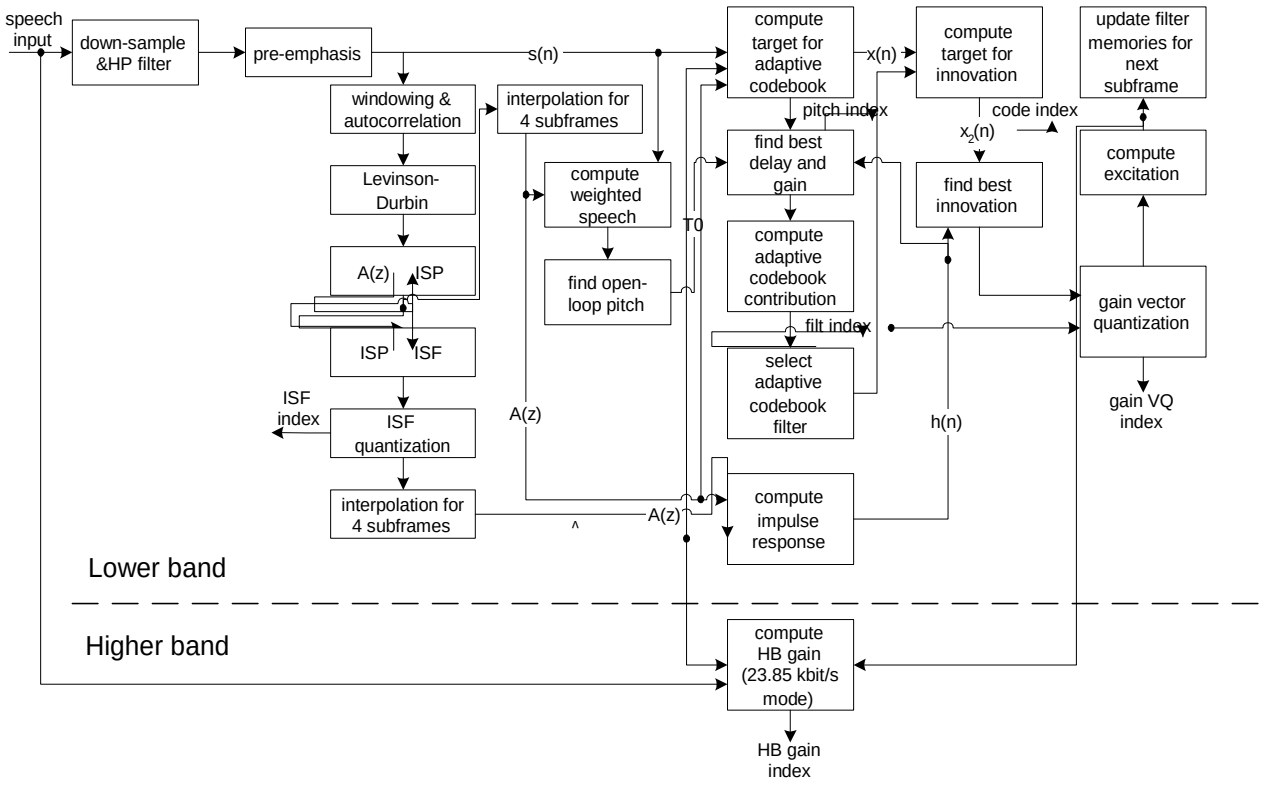


Figure 6-25: Detailed block diagram of the ACELP encoder

The signal flow at the decoder is shown in Figure 6-26. At the decoder, the transmitted indices are extracted from the received bitstream. The indices are decoded to obtain the coder parameters at each transmission frame. These parameters are the ISP vector, the 4 fractional pitch lags, the 4 LTP filtering parameters, the 4 innovative codevectors, and the 4 sets of vector quantized pitch and innovative gains. In the 23.85 kbit/s mode, also the high-band gain index is decoded. The ISP vector is converted to LP filter coefficients and interpolated to obtain LP filters at each subframe. Then, at each 64-sample subframe:

- The excitation is constructed by adding the adaptive and innovative codevectors scaled by their respective gains.

- The 12.8 kHz speech is reconstructed by filtering the excitation through the LP synthesis filter.

- The reconstructed speech is de-emphasized.

Finally, the reconstructed speech is upsampled to 16 kHz and high-band speech signal is added to the frequency band from 6 kHz to 7 kHz.

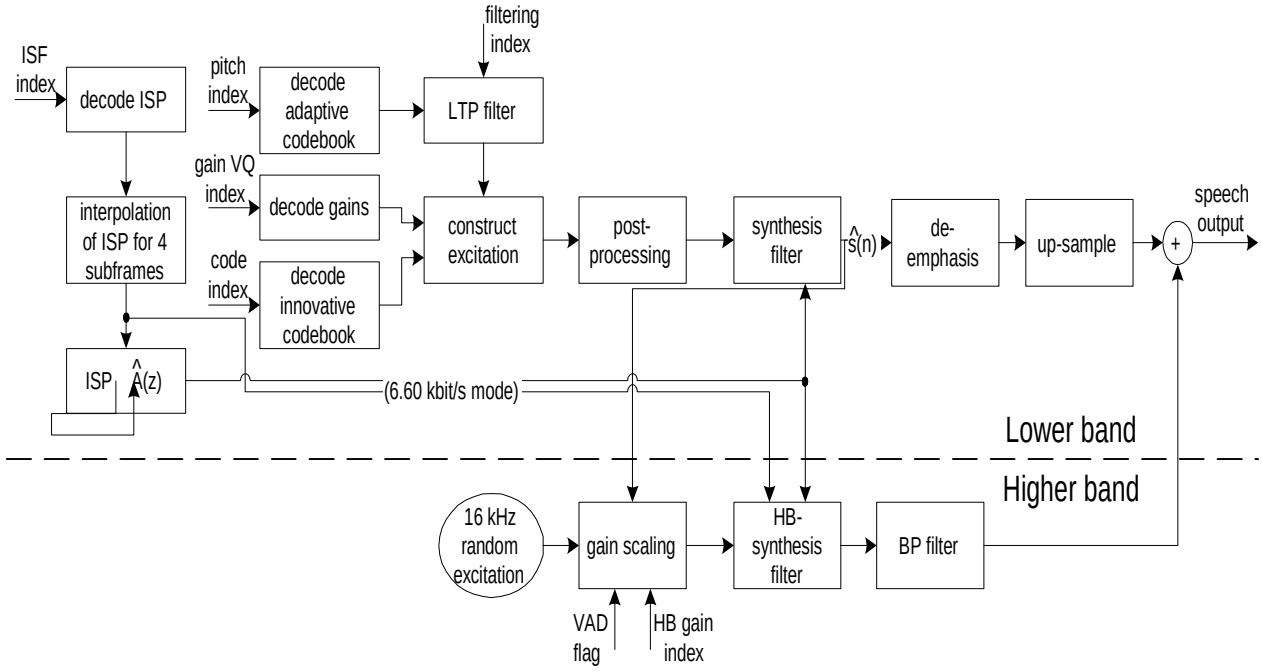


Figure 6-26: Detailed block diagram of the ACELP decoder

6.11.2 Transport and storage of AMR-WB

The RTP payload for AMR-WB is specified in RFC 3267 . It supports encapsulation of one or multiple AMR-WB transport frames per packet, and provides means for redundancy transmission and frame interleaving to improve robustness against possible packet loss. The payload supports two formats, bandwidth-efficient and octet-aligned. The minimum payload overhead is 9 bits per RTP-packet in bandwidth-efficient mode and 2 bytes per RTP-packet in octet aligned mode. The use of interleaving increases the overhead per packet slightly. The payload also supports CRC and includes parameters required for session setup. 3GPP TS 126 234 (PSS) and TS 126 346 (MBMS) use this payload.

The AMR-WB ISO-based 3GP file format is defined in 3GPP TS 26.244, with the media type "audio/3GPP". Note that the 3GP structure also supports the storage of other multimedia formats, thereby allowing synchronized playback. In addition, an additional file format is specified in RFC 3267 for transport of AMR-WB speech data in storage mode applications such as email. The AMR-WB MIME type registration specifies the use of both the RTP payload and storage formats.

7 Video codecs

7.1 H.264/AVC Video

The part of the H.264/AVC standard referenced in the present document specifies the coding of video (in 4:2:0 chroma format) that contains either progressive or interlaced frames, which may be mixed together in the same sequence. Generally, a frame of video contains two interleaved fields, the top and the bottom field. The two fields of an interlaced frame, which are separated in time by a field period (half the time of a frame period), may be coded separately as two fields or together as a frame. A progressive frame should always be coded as a single frame; however, it can still be considered to consist of two fields at the same instant of

time. H.264/AVC covers a Video Coding Layer (VCL), which is designed to efficiently represent the video content, and a Network Abstraction Layer (NAL), which formats the VCL representation of the video and provides header information in a manner appropriate for conveyance by a variety of transport layers or storage media. The structure of H.264/AVC video encoder is shown in Figure 7-1.

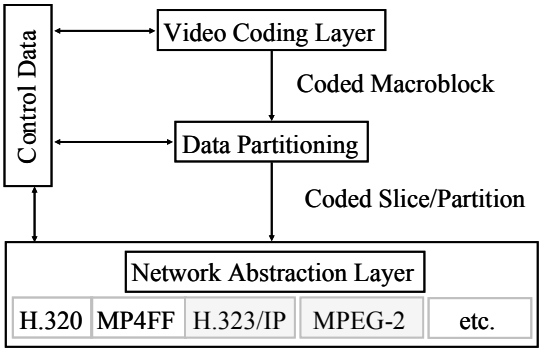


Figure 7-1: Structure of H.264/AVC video encoder

7.1.1 Network Abstraction Layer

The Video Coding Layer (VCL), which is described below, is specified to efficiently represent the content of the video data. The Network Abstraction Layer (NAL) is specified to format that data and provide header information in a manner appropriate for conveyance by the transport layers or storage media. All data are contained in NAL units, each of which contains an integer number of bytes. A NAL unit specifies a generic format for use in both packet-oriented and bit stream systems. The format of NAL units for both packet-oriented transport and bit stream is identical except that each NAL unit can be preceded by a start code prefix in a bit stream-oriented transport layer. The NAL facilitates the ability to map H.264/AVC VCL data to transport layers such as:

- RTP/IP for any kind of real-time wire-line and wireless Internet services (conversational and streaming);
- File formats, e.g. ISO "MP4" for storage and MMS;
- H.32X for wireline and wireless conversational services;
- MPEG-2 systems for broadcasting services, etc.

The full degree of customization of the video content to fit the needs of each particular application was outside the scope of the H.264/AVC standardization effort, but the design of the NAL anticipates a variety of such mappings.

One key concept of the NAL is parameter sets. A parameter set is supposed to contain information that is expected to rarely change over time. There are two types of parameter sets:

- sequence parameter sets, which apply to a series of consecutive coded video pictures; and
- picture parameter sets, which apply to the decoding of one or more individual pictures.

The sequence and picture parameter set mechanism decouples the transmission of infrequently changing information from the transmission of coded representations of the values of the samples in the video pictures. Each VCL NAL unit contains an identifier that refers to the content of the relevant picture parameter set, and each picture parameter set contains an identifier that refers to the content of the relevant sequence parameter set. In this manner, a small amount of data (the identifier) can be used to refer to a larger amount of information (the parameter set) without repeating that information within each VCL NAL unit.

7.1.2 Video Coding Layer

The video coding layer of H.264/AVC is similar in spirit to other standards such as MPEG-2 Video. It consists of a hybrid of temporal and spatial prediction in conjunction with transform coding. Figure 7-2 shows a block diagram of the video coding layer for a macroblock, which consists of a 16x6 luma block and two 8x8 chroma blocks.

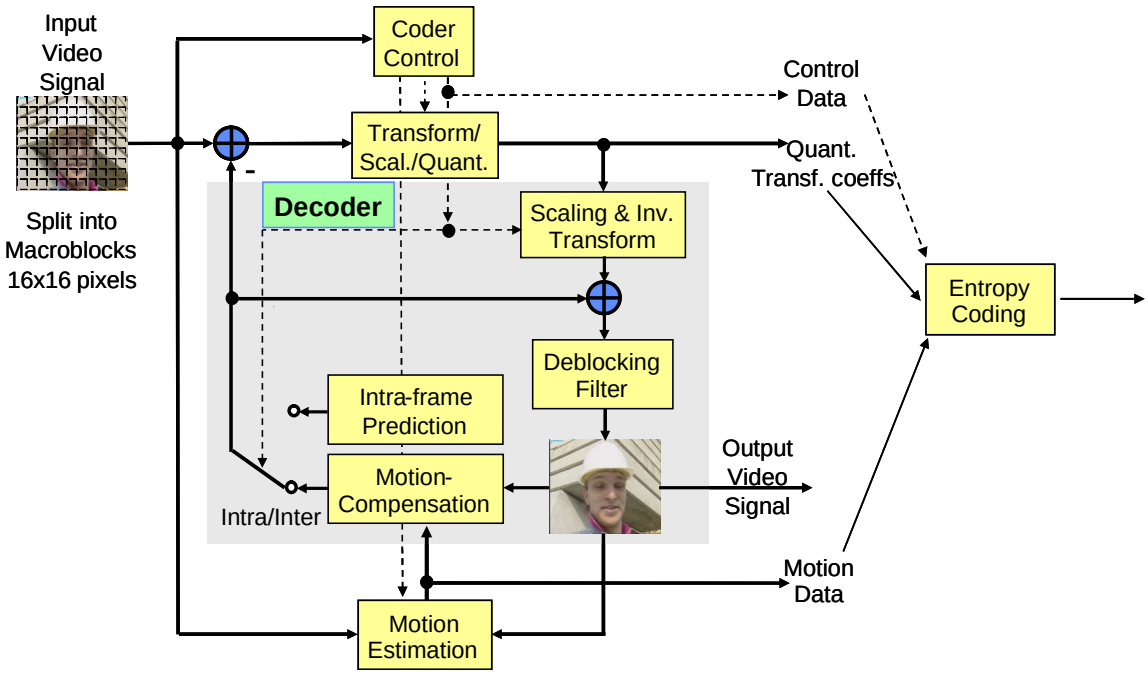


Figure 7-2: Basic coding structure for H.264/AVC for a macroblock

In summary, the picture is split into macroblocks. The first picture of a sequence or a random access point is typically coded in Intra, i.e., without using other information than the information contained in the picture itself. Each sample of a luma or chroma block of a macroblock in such an Intra frame is predicted using spatially neighbouring samples of previously coded blocks. The encoding process is required to choose which and how neighbouring samples are used for Intra prediction which is simultaneously conducted at encoder and decoder using the transmitted Intra prediction side information.

For all remaining pictures of a sequence or between random access points, typically Inter coding is utilized. Inter coding employs prediction (motion compensation) from other previously decoded pictures. The encoding process for Inter prediction (motion estimation) consists of choosing motion data comprising the reference picture and a spatial displacement that is applied to all samples of the macroblock. The motion data which are transmitted as side information are used by encoder and decoder to simultaneously provide the inter prediction signal.

The residual of the prediction (either Intra or Inter) which is the difference between the original and the predicted macroblock is transformed. The transform coefficients are scaled and quantized. The quantized transform coefficients are entropy coded and transmitted together with the side information for either Intra-frame or Inter-frame prediction.

The encoder contains the decoder to conduct prediction for the next blocks or next picture. Therefore, the quantized transform coefficients are inverse scaled and inverse transformed in the same way as at the decoder side resulting in the decoded prediction residual. The decoded prediction residual is added to the prediction. The result of that addition is fed into a deblocking filter which provides the decoded video as its output.

The new features of H.264/AVC compared to MPEG-2 Video are listed as follows: variable block-size motion compensation with small block sizes from 16x16 luma samples down to 4x4 luma samples per block, quarter-sample-accurate motion compensation, motion vectors pointing over picture boundaries, multiple reference picture motion compensation, decoupling of referencing order from display order, decoupling of picture representation methods from picture referencing capability, weighted prediction, improved “"skippe"” and “"direc"” motion inference, directional spatial prediction for intra coding, in-the-loop deblocking filtering, 4x4 block-size transform, hierarchical block transform, short word-length/exact-match inverse transform, context-adaptive binary arithmetic entropy coding, flexible slice size, FMO, ASO, redundant pictures, data partitioning, SP/SI synchronization/switching pictures.

7.2 MPEG-2 Video

ISO/IEC 13818-2 extends the specifications of MPEG-1 Video for more generic classes of video sources and applications. It supports interlaced video and more rigid display timing constraints. Encoded data rates can be up to about 40 Mbit/s for storage and transmission, or even higher for professional applications in video production. Larger frame sizes of up to HD resolution are supported.

7.2.1 Technical Solution

MPEG-2 is forward compatible with MPEG-1 (which means that MPEG-1 streams observing typical constraints e.g. in frame sizes and data rates can be decoded by MPEG-2 decoders). In terms of video encoding tools, specific provisions are made for interlaced video. Further, MPEG-2 defines tools for scalable video coding, e.g. to embed streams which can be used to either decode with CIF+SD, SD+HD resolution. The main technical extensions as compared to MPEG-1 can hence be summarized as follows:

- To support the properties of interlaced video, different methods for field/frame adaptive motion compensation (*frame based*, *field based* and *dual prime* prediction modes), as well as switching between field-/frame-wise DCT are specified. Further, it is possible to switch into a 16x8 prediction mode, where separate motion vectors can be defined for the top and bottom halves of a macroblock.
- The variable-length coding (VLC) tables were extended for better compression performance in higher data rates and resolutions.
- Methods of *scalable* coding are defined, which provide SNR scalability and spatial scalability over a limited number of layers each. In this context, the bitstream is sub-divided into two or three parts, which means that by retaining or receiving only core parts of the stream, it is e.g. possible to reconstruct frames at lower resolution. To encode DCT coefficients related to the different resolution levels, differently optimized variable length codes are provided in the spatial scalable mode.
- Methods to encode sequences with 4:2:2 chrominance sampling are defined by allowing additional 8x8 transform blocks to be subsumed within a macroblock.
- A method of temporal scalability is defined, which allows prediction of additional inserted frames either from a base-layer sequence or from another frame of the enhancement layer sequence. This method can also be used for encoding of stereoscopic sequences with an LRLRLR… interleaving of left and right pictures, as e.g. required for shutter-glass display.
- All scalability modes can also be used to achieve a forward and backward compatible combination of MPEG-1 and MPEG-2, when MPEG-1 syntax is exclusively used in the base layer.
- Methods of data partitioning for DCT coefficients are defined, which can improve the error resilience of video streams.

The number of application domains and necessary combinations of elementary tools is manifold for the case of MPEG-2. As it appears not to be useful for any MPEG-2 device to support *all* elements of the standard, MPEG-2 defines different *profiles*. Further, within each *profile*, *levels* are specified, which describe

maximum sizes or image formats which must be decodable. Each bitstream carries information indicating which profile capability is required at the decoder, as well as the level of required support in the profile, to identify the requirements of decoder capability for the bitstream. From this information, any conforming MPEG-2 decoder can decide immediately whether it will be able to process the bitstream. Within certain application domains, specific ‘'profile @ leve'’ configurations have been established as mandatory, e.g. ‘'Main Profile @ Main Leve'’ is typically required for digital TV broadcast or DVD storage applications. Four levels are defined: ‘'Lo'’, ‘'Mai'’ (SD), ‘'High-144'’ and ‘'Hig'’ (HD), where however not each level is combinable with each profile. The profiles defined by MPEG-2 video are as follows:

- *Simple profile*: This is for *low cost* and *low delay* applications, allowing frame sizes up to SD resolution (ITU-R Rec. BT.601) and frame rates up to 30 *Hz*. Usage of *B* frames is not allowed.
- *Main profil*e: This is the most widely used MPEG-2 profile, defined for SD and HD resolution applications in storage and transmission, without providing compatible decoding of different resolutions. All interlaced-specific prediction modes as well as *B* frames are supported.
- *SNR scalable profil*e: Similar to Main profile, but allows in addition SNR scalability invoking drift at the base layer; resolutions up to SD are supported.
- *Spatial scalable profil*e: Allows usage of (drift free) spatial scalability, also in combination with SNR scalability.
- *High profil*e: Similar to Spatial Scalable profile, but supporting a wider range of levels, and allowing 4:2:2 chrominance sampling additionally. This profile was primarily defined for upward/downward compatible coding between SD and HD resolutions, allowing embedded bitstreams for up to 3 layers with a maximum of two different spatial resolutions.
- *4:2:2 profile*: This profile extends the Main profile by allowing encoding of 4:2:2 chrominance sampling, and allows larger picture sizes and higher data rates.
- *Multiview profil*e: This allows encoding of stereoscopic sequences provided in a left-right interleaved multiplex, using the tool of temporal scalability for exploitation of left-right redundancies. The displacement between left and right pictures is estimated and used for *disparity compensated prediction*, which follows the same principles as motion-compensated prediction. In addition, camera parameters can be conveyed in the stream.

The text of the MPEG-2 Video standard is common with ITU-T Rec. H.262. Subsequent to the second edition of the standard text which was published in 2000, the following corrigenda and amendments are integral part of the MPEG-2 Video specification:

- ITU-T Rec.H.262(2000)/Cor.1 (2002)|ISO/IEC 13818- 2:2000/Cor. 1:2002
- ITU-T Rec. H.262(2000)/Amd.1(2000)|ISO/IEC 13818- 2:2000/Amd. 1:2001
- ITU-T Rec.H.262(2000)/Cor.2 (200X)|ISO/IEC 13818- 2:2000/Cor. 2:200X (in preparation)

7.3 VC-1 video

The VC-1 bit stream is defined as a hierarchy of layers. This is conceptually similar to the notion of a protocol stack of networking protocols. The outermost layer is called the sequence layer. The other layers are entry-point, picture, slice, macroblock and block. In the Simple and Main profiles, a sequence in the sequence layer consists of a series of one or more coded pictures. In the Advanced profile, a sequence consists of one or more entry-point segments, where each entry-point segment consists of a series of one or more pictures, and where the first picture in each entry-point segment provides random access.

In the VC-1 Advanced Profile, the sequence layer header contains the parameters required to initialize the VC-1 decoder. These parameters apply to all entry-point segments until the next occurrence of a sequence layer header in the coded bit stream. For Simple and Main Profiles, the decoder initialization parameters are conveyed as Decoder Initialization Metadata structures (see Annex J of [SMPTE 421M]) carried in the SDP

datagrams signalling the VC-1-based session, rather than via a sequence layer header and an entry-point segment header. Therefore, all IP IRDs supporting VC-1 must be capable of extracting this data from the SDP datagrams.

7.3.1 Explanation of VC-1 Profiles and Levels

As with MPEG-2 and H.264/AVC, Profiles and Levels are used to specify conformance points for VC-1. A profile defines a sub-set of the VC-1 standard which include a specific set of coding tools and syntax. A level is a defined set of constraints on the values which can be taken by key parameters (such as bit rate or video resolution) within a particular profile. A decoder claiming conformance to a specific profile must support all features in that profile. Encoders are not required to make use of any particular set of features supported in a profile but have to provide conforming bit streams, i.e. bit streams that can be decoded by conforming decoders.

Three profiles have been specified: Simple, Main and Advanced. For each profile a number of levels have been defined: two levels with Simple Profile, three levels with Main Profile and five levels with Advanced Profile. Note that VC-1 levels have been defined to be specific to particular profiles; this is in contrast with MPEG-2 and H.264/AVC where levels are largely independent of profiles.

Table summarizes the coding tools that are included in each profile.

Table 7-1: coding tools in each profile

Feature	Simple Profile	Main Profile	Advanced Profile
Baseline intra frame compression	✓	✓	✓
Variable-sized transform	✓	✓	✓
16-bit transform	✓	✓	✓
Overlapped transform	✓	✓	✓
4 motion vector per macroblock	✓	✓	✓
¼ pixel luminance motion compensation	✓	✓	✓
¼ pixel chrominance motion compensation	X	✓	✓
Start codes	X	✓	✓
Extended motion vectors	X	✓	✓
Loop filter	X	✓	✓
Dynamic resolution change	X	✓	✓
Adaptive macroblock quantization	X	✓	✓
B frames	X	✓	✓
Intensity compensation	X	✓	✓
Range adjustment	X	✓	✓
Field and frame coding modes	X	X	✓
GOP Layer	X	X	✓
Display metadata	X	X	✓

NOTE – Symbols ✓ and X indicate "Yes" and "No" respectively.

The Advanced Profile bit stream includes a number of fields which provide information useful to the post-decode display process. This information, collectively known as “"display metadat"” is output by the decoding process. Its use in the display process is optional, but recommended.

7.4 AVS Video

AVS video (Part 2) [GB/T20090.2] is a hybrid coding based on spatial and temporal prediction, integer transform and entropy coding. It has one profile, Jizhun profile. In this profile, there are 4 levels, which are level 4.0 and 4.2 for Standard Definition (SD) video with 4:2:0 and 4:2:2, level 6.0 and 6.2 for HD video with 4:2:0 and 4:2:2, respectively. The basic unit for encoding/decoding in this standard is a Macro-block, which consists of one 16x16 luma block and two 8x8 chroma blocks (for 4:2:0 format). The AVS-P2 bit stream is also defined as a hierarchy of layers. Generally a sequence consists of several GOP (group of pictures, leading by an I picture), which could be a random access point. The other layers between a GOP and a Macro-block are picture and slice. AVS-P2 has many coding tools, which are deblocking, interlace coding, forward, backward and symmetrical prediction using up to two reference pictures, or four reference fields, variable block size motion compensation down to 8x8 block size, intra prediction with 5 directions, 2D-CAVLC entropy coding, 8x8 integer transformation, as well as weighted prediction, etc.

AVS-P8.2 describes an RTP Payload format for the AVS video codec specified by AVS-P2(abbreviation for AVS video (part 2)). In essence, this packetization scheme is based on the one for H.264 in order to reuse its well-defined features and to enable a unified transport platform for AVS-P2. To encapsulate an AVS-P2 syntax unit with the NALU structure, the corresponding start code prefix will be replaced by a NALU header whose fields are valued according to the start code followed. Thus, an AVS-P2 bitstream is formatted as a series of NALUs and could be further packetized or stored by using the methods proposed for H.264. AVS streams can be transported over TS by using a similar system as that of ISO/IEC 13818-1. The differences between the two systems are mainly for specifying the AVS video/audio streams.

7.4.1 AVS encoding tools

The system architecture is illustrated in Figure 7-3.

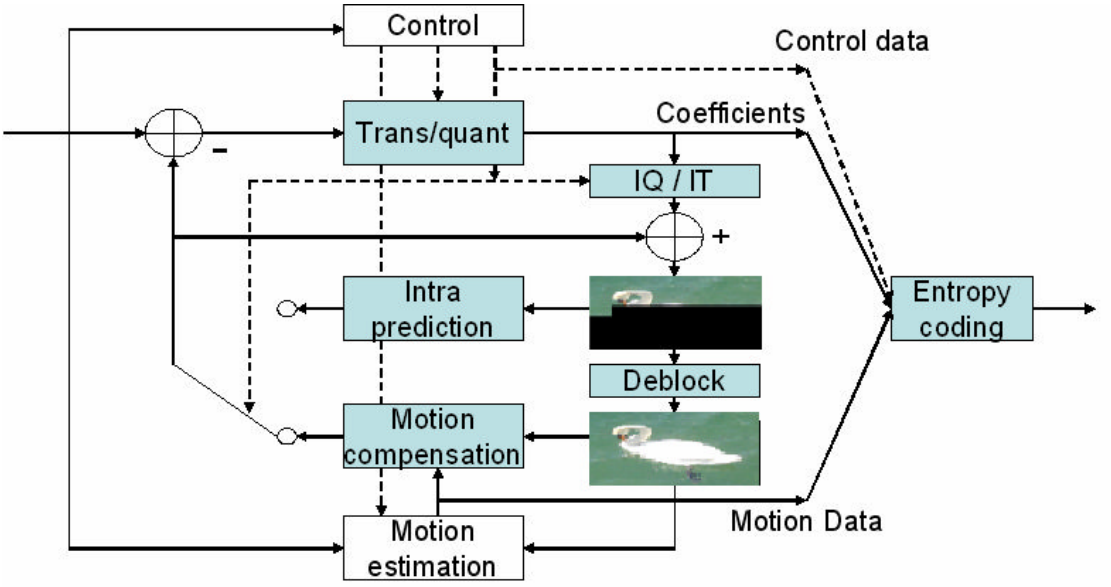


Figure 7-3: AVS video coding structure

Compared with the MPEG-2, AVS video introduces the following new features:

8x8 integer transform; 8x8 intra/inter prediction; Symmetric-prediction and direct-prediction in bi-predictive pictures; In-loop deblocking filtering; Quarter-sample-accurate interpolation and compensation; 2D-CAVLC; Up to 2 reference pictures for both P and B frames.

Appendix I

Technical Aspects of Toolbox Codecs and Content Coding

(This Appendix does not form an integral part of this document.)

Video

The following sections describe the currently use profiles and formats of video encoding for informational purposes only.

Formats and Resolution

Input formats and resolutions which a terminal device may need to cope with are listed in Table I-1:

Table I-1: Input Formats and Resolutions

Vertical size	Horizontal size	Aspect ratio	Interlaced/Progressive	Frame rate (Hz)	Note
1080	1920	16:9	P	50, 59.94, 60	1
1080	1920	16:9	I	24, 25, 30	1
1080	1440	16:9	I	25, 30	
720	1280	16:9	P	25, 50, 60	2
576	720	16:9	P	25, 50	3
576	720	4:3	P	25, 50	3
480	720	16:9	P	60	4
480	720	4:3	P	60	4
480	720	4:3	I	30	4
240	320	4:3	P	30	5

NOTE 1 – [ITU-R BT.709], Under a certain condition, translating high resolution video such as 1920x1080 to lower resolution format, such as 720x483, can optionally be restricted or prohibited.

NOTE 2 – [ITU-R BT.1543]

NOTE 3 – [ITU-R BT.1358]

NOTE 4 – [ITU-R BT.601]

NOTE 5 – Video signal with resolution of 240/320 is for common for wireless devices. Video format for mobile device is for further study.

Terminal devices that support high definition outputs may need to be capable of displaying video and graphics output at the resolutions listed in Table I-2 on Component and HDMI outputs.

Table I-2: Output Formats and Resolutions

Vertical size	Horizontal size	Aspect ratio	Interlaced/Progressive	Frame rate (Hz)
1080	1920	16:9	I	25, 30
1080	1440	16:9	I	25, 30
720	1280	16:9	P	25, 60
576	720	16:9	P	25, 50
576	720	4:3	P	25, 50
480	720	16:9	P	60
480	720	4:3	P	60
480	720	4:3	I	30
240	320	4:3	P	30

In addition to the formats covered here, [SCTE43] and [ETSI TR 101 154 v1.7.1] provide comprehensive lists of video formats.

The following Table I-3 shows picture formats proposed for AVS.

Table I-3: AVS Formats and Resolutions

Maximum resolution supported by the level	Display aspect ratio	P/I	asp_ ratio _idc	Frame rate (Hz)	Level
1920x1152	4:3 16:9 2.21:1	P	2 3 4	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	6.0, 6.1, 6.2
1920x1152	4:3 16:9 2.21:1	I	2 3 4	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	6.0, 6.1, 6.2
720x576	4:3 16:9 2.21:1	P	2 3 4	23.976, 24, 25, 29.97, 30,	4.0, 4.2
720x576	4:3 16:9 2.21:1	I	2 3 4	23.976, 24, 25, 29.97, 30,	4.0, 4.2
352x288	4:3 16:9 2.21:1	P	2 3 4	23.976, 24, 25, 29.97, 30,	2.0, 2.1
352x288	4:3 16:9 2.21:1	I	2 3 4	23.976, 24, 25, 29.97, 30,	2.0, 2.1

The following tables present the encoding formats in SCTE, DVB and Japan IPTV Forum.

Profile for H.264

SCTE: High Profile for both HDTV and SDTV

DVB: High Profile for HDTV, Main Profile for SDTV

Japan: High Profile for HDTV, Main for SDTV (High can be used for SDTV)

Table I-4: Picture encoding format for H.264

			US (SCTE)			Europe (DVB)			Japan (ARIB)		
	Display aspect ratio	**P /I**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**
1920 x 1080	16:9	P	1	23.976, 24, 29.97, 30	4	1	23.976, 24, 25	4			
1920 x 1080	16:9	I	1	29.97, 30	4	1	25, 29.97, 30	4	1	29.97	4
1440 x 1080	16:9	P	14	23.976, 24, 29.97, 30	4	14	23.976, 24, 25	4			
1440 x 1080	16:9	I	14	29.97, 30	4	14	25, 29.97, 30	4	255 or 14	29.97	4
1280 x 1080	16:9	P				15	23.976, 24, 25	4			
1280 x 1080	16:9	I				15	25, 29.97, 30	4			
960 x 1080	16:9	P				16	23.976, 24, 25	4			
960 x 1080	16:9	I				16	25, 29.97, 30	4			
1280 x 720	16:9	P	1	23.976, 24, 29.97, 30, 59.94, 60	4	1	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	4	1	59.94	4
960 x 720	16:9	P				14	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	4			
640 x 720	16:9	P				16	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	4			

Table I-5: Picture encoding format for H.264 SDTV in 30 Hz system

			US (SCTE)			Europe (DVB)			Japan (ARIB)		
	Display aspect ratio	**P /I**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**
720 x 480*	4:3 16:9	P	3 5	23.976, 24, 29.97, 30, 59.94, 60,	4 3	3 5	23.976, 24, 29.97, 30	3			
720 x 480*	4:3 16:9	I	3 5	29.97, 30	3	3 5	29.97, 30	3	3 5	29.97	3 or 3.1 or 3.2
640 x 480	4:3 16:9	P	1	23.976, 24, 29.97, 30, 59.94, 60	4 3	1 11	23.976, 24, 29.97, 30	3			
640 x 480	4:3 16:9	I	1	29.97, 30	3	1 11	29.97, 30	3			
544 x 480**	4:3 16:9	P	5	23.976	3	5 13	23.976, 24, 29.97, 30	3			
544 x 480**	4:3 16:9	I	5	29.97	3	5 13	29.97, 30	3			
480 x 480	4:3 16:9	P				11 7	23.976, 24, 29.97, 30	3			
480 x 480	4:3 16:9	I				11 7	29.97, 30	3			
352 x 480	4:3 16:9	P	7	23.976	3	7 9	23.976, 24, 29.97, 30	3			
352 x 480	4:3 16:9	I	7	29.97	3	7 9	29.97, 30	3			
352 x 240	4:3 16:9	P				3 5	23.976, 24, 29.97, 30, 59.94, 60	3			
352 x 240	4:3 16:9	I				3 5	29.97, 30	3			

*704 x 480 is also included in SCTE definition.

**528 x 480 is also included in SCTE definition.

Table I-6: Picture encoding format for H.264 SDTV in 25 Hz system

			US (SCTE)			Europe (DVB)			Japan (ARIB)		
	Display aspect ratio	**P /I**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**
720 x 576	4:3 16:9	P				2 4	25	3			
720 x 576	4:3 16:9	I				2 4	25	3			
544 x 576	4:3 16:9	P				4 12	25	3			
544 x 576	4:3 16:9	I				4 12	25	3			
480 x 576	4:3 16:9	P				10 6	25	3			
480 x 576	4:3 16:9	I				10 6	25	3			
352 x 576	4:3 16:9	P				6 8	25	3			
352 x 576	4:3 16:9	I				6 8	25	3			
352 x 288	4:3 16:9	P				2 4	25, 50	3			
352 x 288	4:3 16:9	I				2 4	25	3			

Profile for MPEG-2 video

SCTE: Main Profile for HDTV and SDTV

DVB: Main Profile for HDTV and SDTV

ARIB: Main Profile for HDTV and SDTV

Table I-7: Picture encoding format for MPEG-2 HDTV

			US (SCTE)			Europe (DVB)			Japan (ARIB)		
	Display aspect ratio	**P /I**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**
1920 x 1080	16:9	P	1,3	23.976, 24, 29.97, 30	HL	3	23.976, 24, 29.97, 30	HL			
1920 x 1080	16:9	I	1,3	29.97, 30	HL	3	29.97, 30	HL	3	29.97	HL
1440 x 1080	16:9	P	3	23.976, 24, 29.97, 30	HL						
1440 x 1080	16:9	I	3	29.97, 30	HL				3	29.97	HL
1280 x 720	16:9	P	1,3	23.976, 24, 29.97, 30, 59.94, 60	HL	3	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	HL	3	59.94	HL

Table I-8: Picture encoding format for MPEG-2 SDTV in 30 Hz system

			US (SCTE)			Europe (DVB)			Japan (ARIB)		
	Display aspect ratio	**P /I**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**
720 x 480*	4:3 16:9	P	2 3	23.976, 24, 29.97, 30, 59.94, 60	H14L	2 3	23.976, 24, 29.97, 30, 59.94, 60	H14L	N.A. 3	59.94	H14L
720 x 480*	4:3 16:9	I	2 3	29.97, 30	ML	2 3	29.97,30	ML	2 3	29.97	ML
640 x 480	4:3	P	1,2	23.976, 24, 29.97, 30, 59.94, 60	ML	2	23.976, 24, 29.97, 30	ML			
640 x 480	4:3	I	1,2	29.97, 30	ML	2	29.97, 30	ML			
544 x 480**	4:3 16:9	P	2	23.976	ML	2 3	23.976, 29.97	ML			
544 x 480**	4:3 16:9	I	2	29.97	ML	2 3	29.97	ML	2 3	29.97	ML
480 x 480	4:3 16:9	P				2 3	23.976, 29.97	ML			
480 x 480	4:3 16:9	I				2 3	29.97	ML	2 3	29.97	ML
352 x 480	4:3 16:9	P	2	23.976	ML	2 3	23.976, 29.97	ML			
352 x 480	4:3 16:9	I	2	29.97	ML	2 3	29.97	ML			
352 x 240	4:3 16:9	P				2 3	23.976, 29.97	ML	2 3	29.97	LL

*704 x 480 is also included in SCTE definition.

**528 x 480 is also included in SCTE definition.

Table I-9: Picture encoding format for MPEG-2 SDTV in 30 Hz system

			US (SCTE)			Europe (DVB)			Japan (ARIB)		
	Display aspect ratio	**P /I**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**	**asp _idc**	**Frame rate (Hz)**	**Level**
720 x 576	4:3 16:9	P				2 3	25, 50	H14L			
720 x 576	4:3 16:9	I				2 3	25	ML			
544 x 576	4:3 16:9	P				2 3	25	ML			
544 x 576	4:3 16:9	I				2 3	25	ML			
480 x 576	4:3 16:9	P				2 3	25	ML			
480 x 576	4:3 16:9	I				2 3	25	ML			
352 x 576	4:3 16:9	P				2 3	25	ML			
352 x 576	4:3 16:9	I				2 3	25	ML			
352 x 288	4:3 16:9	P				2 3	25	ML			

Appendix II

List of some additional content related standards

(This Appendix does not form an integral part of this document.)

Introduction

The IPTV Services Requirements Document [FG IPTV-DOC-0147] contains several requirements related to closed captioning, subtitles and descriptive audio. This Appendix lists some standards which deal with these features.

It should be noted that this is not an exhaustive list.

Relevant requirements

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

- The IPTV architecture is required to support the end-user with the ability to choose a preferred language option (audio, subtitle, captioning, supplementary video and supplementary descriptive audio) from various languages that the content provider pre-defined and the service provider delivered.

- The IPTV architecture is recommended to support multiple languages audio, multiple language subtitles, multiple languages captioning, multiple language supplementary video and multiple language descriptive audio.
- The IPTV architecture is recommended to support the capability for the end-user to watch with the preferred audio, subtitle, and captioning, supplementary video or descriptive audio.
- If the end-user's option can not match with the pre-defined content languages, the IPTV architecture is recommended to support the capability for the IPTV terminal device to present the content with default audio, default subtitle and captioning, default supplementary video and default descriptive audio.
- The IPTV architecture is recommended to support the capability for the end-user to switch audio, subtitles and captioning, supplementary video and descriptive audio back and forth when the user is watching the program without having to change his or her preferred language settings.
- The IPTV architecture is required to support the ability for the end-user to turn on and off the audio, the subtitle and captioning, supplementary video and descriptive audio at anytime without altering any of the default setting options.
- The IPTV architecture is recommended to support the ability to independently select a default language for each of the following: audio, subtitle, captioning, supplementary video and supplementary descriptive audio.
- The IPTV architecture is required to support the ability for the IPTV terminal device to decode video, audio, subtitles, captioning, supplementary video and descriptive audio and present them to the end-user.
- The IPTV terminal device is recommended to allow the user the selection of subtitles or captions being displayed with a solid background or a transparent one.

Coding and carriage of closed caption information

CEA-708-C: "Digital Television (DTV) Closed Captioning", 30 July 2006, Consumer Electronics Association specifies the encoding of closed caption information in multiple languages, colors and fonts. It also specifies rendering of the information based on user preference and user specified data (such as location, size, etc.). All DTV receivers, set top units (including IPTV receivers) and Cable ready receivers are mandated to support this standard within the US since July 2002. This standard is also adopted by Canada and Mexico.

Additionally, the following standards specify the carriage of closed caption information in MPEG-2, AVC/H.264 and VC-1/SMPTE 421M:

1. ATSC Standard A/53 Part 1:2007, "ATSC Digital Television Standard, Digital Television System" (carriage of closed captions in the user_data part of MPEG-2).

2. ETSI TS 101 154 V1.8.1, Digital Video Broadcasting (DVB): Implementation Guidelines for the use of MPEG-2 Systems, Video and Audio in Satellite, Cable and Terrestrial Broadcasting Applications, Annex B, June 2007 (carriage of closed captions for AVC/H.264 and VC-1/SMPTE 421M).

3. SCTE DVS 683: AVC video systems and transport constraints for Cable television, Oct 2007 (Carriage of closed captions for H.264/AVC using registered user data SEI).

As closed caption information is tightly synchronized with video frames and is required to add very little overhead, this is usually carried as part of each picture and hence the carriage is codec-centric.

4. ARIB STD-B24 Ver.5.1 (2007), Data Coding and Transmission Specification for Digital Broadcasting, Volume 3 Data Transmission Specification: This provides a carriage of closed captions using an independent PES. Synchronization of closed captions with video is made by Presentation Time Stamp (PTS).

Subtitles

ANSI/SCTE 27: Subtitling methods for broadcast Cable, 2003, provides a scheme for coding and transmission of subtitles in multiple languages. This scheme has been in wide use in both US and Central America for several years.

ARIB STD-B24 Ver.5.1 (2007), "Data Coding and Transmission Specification for Digital Broadcasting, Volume 1 Data Coding, Part 3 Coding of Captions and Superimposing".

Descriptive Audio

ISO/IEC 13818-1 | ITU-T Rec H.222.0 provides the mechanism in the ISO-639 language descriptor (audio_type value of 0x03) to signal "descriptive audio" as a complete stream.

ARIB STD-B32 Ver.2.1 (2007), Video Coding, Audio Coding and Multiplexing specifications for Digital Broadcasting provides MPEG-2 AAC ADTS parameters to carry descriptive audio.

ARIB STD-B10 Ver.4.4 (2007), Service Information for Digital Broadcasting System provides the mechanism to identify descriptive audio and ISO_639 code based language identification

Some audio compression standards such as Dolby AC-3 and E-AC-3 support transmission of descriptive audio as "associated service" to decoders that have the ability to combine the "main" audio information with the associated information. This type of usage reduces the channel bandwidth to transmit both "main" and "descriptive audio". However, it does require terminal devices with the capability to decode two audio streams and mix them.

Other audio compression standards like MPEG-4 LC_AAC and MPEG-4 HE-AAC implement descriptive audio as an additional audio bitstream which in the linear domain is mixed together with the "main audio", provided that the terminal device implements the required capability.

Bibliography

[b_ITU-T G.722.2] ITU-T Recommendation G.722.2 (2003): *Wideband coding of speech at around 16 kbit/s using Adaptive Multi-rate Wideband (AMR-WB)*

[b_IETF RFC 3267] IETF RFC 3267 (2002), *Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codec*

II.6.3 IPTV middleware

Summary

The document identifies those aspects of architecture specific to IPTV middleware and describes the various functions with explanatory definitions where appropriate.

Keywords

API, IPTV, middleware, service platform

Current status

This document is complete.

Dependency on or relationship to other FG IPTV documents:

- IPTV service requirements document

CONTENTS

		Page
1	Scope	641
2	References	641
3	Definitions	641
	3.1 This working document uses the following terms defined elsewhere	641
	3.2 This working document defines the following terms	641
4	Abbreviations and acronyms	641
5	IPTV middleware architecture	642
6	IPTV Terminal middleware architecture	643
	6.1 IPTV terminal middleware components and APIs	644
	6.1.1 System and resource management component	644
	6.1.2 Media management component	646
	6.1.3 Communication component	646
	6.1.4 Security component	646
	6.1.5 Metadata access component	647
	6.1.6 User interaction component	647
	6.2 Classification of IPTV terminal middleware components APIs	648
7	Service platform middleware	648
	7.1 IPTV service platform middleware components and APIs	649
	7.1.1 Application management component	649
	7.1.2 Content delivery and control component	649
	7.1.3 Service control component	650
	7.1.4 Monitoring and configuration component	650
	7.1.5 Content access component	651
	7.1.6 Resource management component	651
	7.2 Classification of IPTV service platform middleware components APIs	651

IPTV middleware

1 Scope

This document identifies those aspects of architecture specific to IPTV middleware and describes the various functions with explanatory definitions where appropriate. It also describes the application programming interfaces (APIs) between the IPTV applications and the IPTV middleware.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this working document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this working document 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 working document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.200] ITU-T Recommendation J.200 (2001), *Worldwide common core – Application environment for digital interactive television services*

3 Definitions

3.1 This working document uses the following terms defined elsewhere:

None

3.2 This working document defines the following terms:

3.2.1 **Resource Abstraction Interface (Layer):** an interface layer between resource and middleware service which encapsulates OS operations and resources layer and provide abstract view for resource layer.

3.2.2 **Resources (Layer):** the native hardware and software resources that provide middleware services component of certain functionality through resource abstraction layer, and middleware service functions are provided to application layer through the API of the middleware services.

3.2.3 **Service Components (Layer):** the pure native components that offer functionalities to application layers regardless of type of software and hardware in the resource layer.

4 Abbreviations and acronyms

This working document uses the following abbreviations and acronyms:

API Application Programming Interface

DRM Digital Rights Management

EPG Electronic Program Guide

GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HW	Hardware
OS	Operating System
PVR	Personal Video Recorder
RAL	Resource Abstraction Layer
RAM	Random Access Memory
RTSP	Real Time Streaming Protocol
SW	Software
VoD	Video on Demand

5 IPTV middleware architecture

The IPTV middleware supports the variety of functionalities (e.g. EPG, PVR, gaming, etc.) provided by the IPTV architecture to the IPTV terminal devices. Figure 5-1 provides an overview of the IPTV middleware architecture.

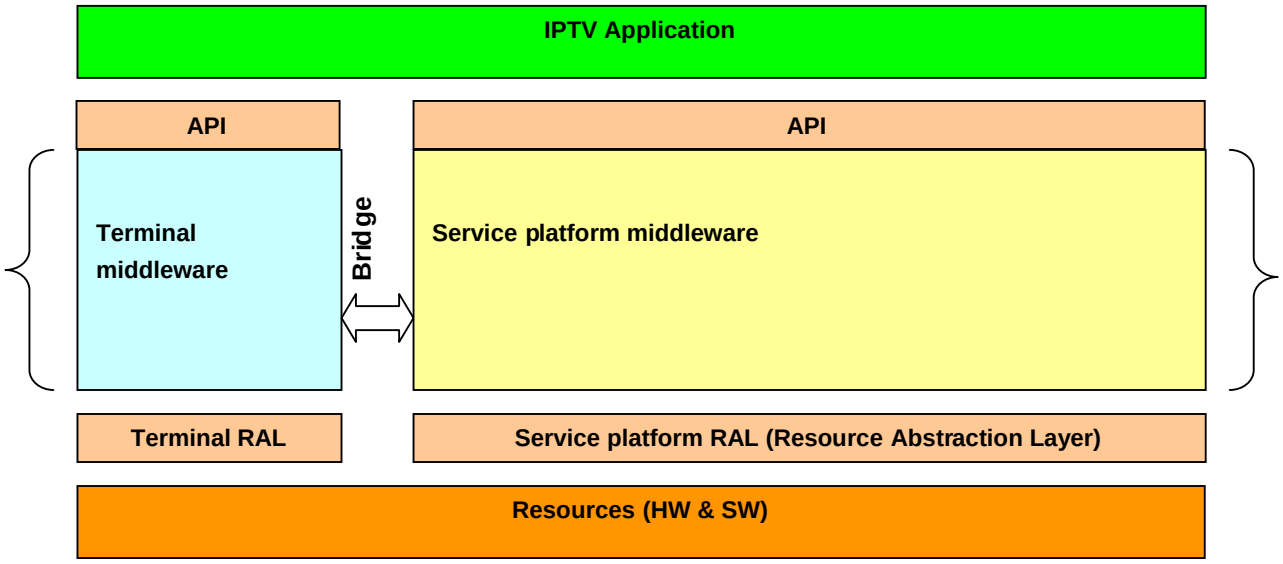


Figure 5-1: IPTV middleware architecture

The following provides description of IPTV middleware architecture components.

(1) IPTV application layer

Application layer is the layer where operators and 3rd parties provide services and applications. These services and applications include EPG applications, VOD, linear TV streams, PVR, games, Internet applications as well as other value-added services.

(2) API layer

A set of interfaces for service providers or manufacturers to build specific applications and be presented on a granular basis for a variety of purposes.

(3) IPTV middleware

The IPTV middleware is divided into a service platform middleware and a terminal middleware linked through a Bridge.

The IPTV middleware invokes the lower layer resources (e.g. network interfaces) to control them, and provides APIs for upper layers.

It is recommended that the IPTV middleware implement the relevant functional modules and end-user functions described in the "IPTV architecture" document [FG IPTV-DOC-0181].

The IPTV middleware also provides some specific functions:

- Resource management function, a functional module to manage system resources in IPTV terminal devices and servers.
- Application management function, a functional module to manage the life cycle of the applications and interaction operations between them.

Optionally, the terminal middleware implements a multimedia application platform and a presentation engine.

(4) Resource abstraction layers

Resource abstraction layer (RAL) is to make the middleware independent of lower software and hardware layers.

The resources abstracted in RAL include:

- Software resources, such as drivers and OS
- Hardware resources, such as computing devices, CPU, storage devices, firmware (e.g. codec), rendering devices (e.g. display, speaker), IO devices.

6 IPTV Terminal middleware architecture

Figure 6-1 shows IPTV terminal middleware architecture (note that this architecture is compatible with the architecture shown in Figure 1/J.200).

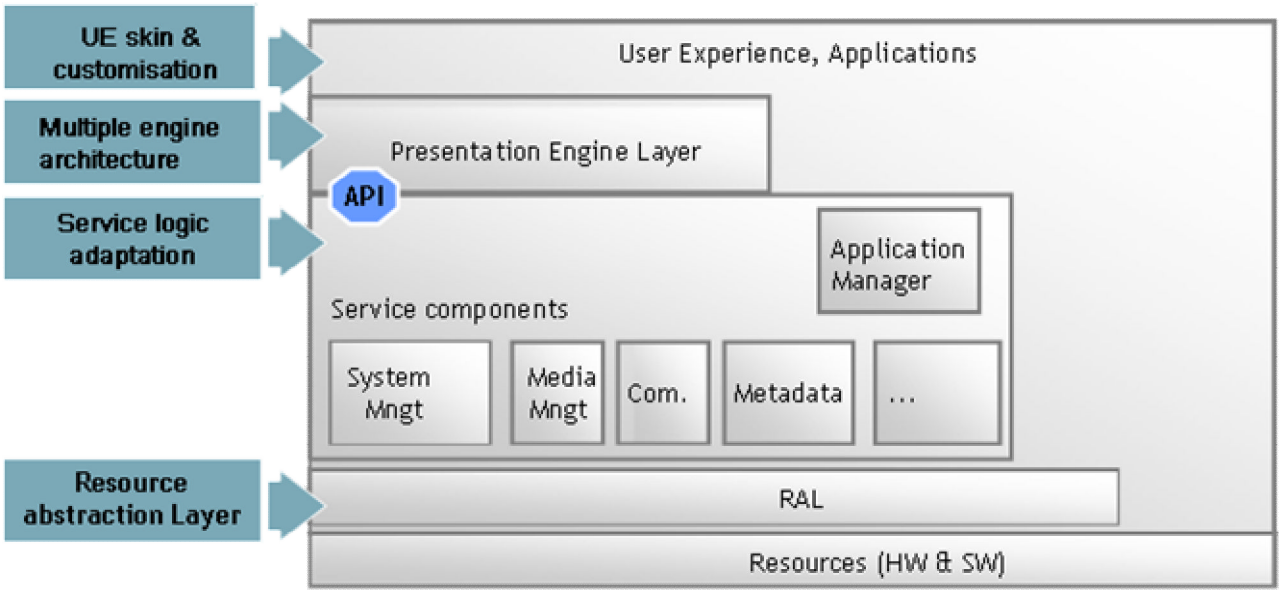


Figure 6-1: IPTV terminal middleware architecture – overview

Resource abstraction layer (RAL)

The IPTV terminal middleware is hardware-agnostic. A specific resource abstraction layer (RAL) exists for each specific hardware and operating system – this provides the necessary interface to the lower layers (e.g. RAM, network access, hard drive, USB port, etc.). The RAL interface is designed so that device drivers can be written irrespective of the service logic adaptation layer.

Service logic adaptation layer

The service logic adaptation layer is made of service components. The service components are pure native components that offer functionalities common to all middleware implementations (e.g. service selection & presentation, service information management, PVR, security system). They are used and enriched by the application services in order to simplify the development of service components and applications above it.

The definition and the scope of services depend on the concrete functionalities deployed in the IPTV system.

Nevertheless, some service components can be defined that are generic in nature:

- System and resource management component.
- Media management component.
- Communication component.
- Security component.
- Metadata access component.
- User interaction component.

All this components can optionally use the functions available on the network.

Presentation engine layer

The presentation engine layer may include various engines along with a set of high-level services. This layer is built on top of the service logic adaptation layer.

In some implementation this layer may not exist.

User experience and application layer

The applications are either downloaded or resident. In particular, an application is powered by a presentation engine (e.g. HTML Browser). An application can either have full or restricted access to the presentation engine layer features. Moreover some applications may directly access the service logic adaptation layer without using a presentation engine.

6.1 IPTV terminal middleware components and APIs

This chapter describes the functionalities of the IPTV terminal middleware components and identifies their APIs

6.1.1 System and resource management component

System and resource management component is used to manage IPTV terminal device resources, and provide software Initialization API, upgrade and download API, system resources management API, and terminal management API to the upper application layer.

Software Initialize and Diagnosis API: an IPTV Terminal Middleware API that is responsible to initial IPTV terminal device, prepare running environment and provide diagnostic capabilities to IPTV terminal device.

- Configure IPTV terminal device;
- Task initialization, such as application management, DRM task, subscriber authentication process, etc.;
- Network connection initialization, such as, to get network parameter, configure access mode, and etc.;
- Resource initialization, such as memory, timer, I/O equipment, A/V decoder and other system resource;
- Coordinate with other IPTV terminal device APIs, such as, to work with Security and Authentication API to start user authentication procedure, to work together with Upgrade and Download API to check software version and perform software upgrade procedure;
- Diagnosis for IPTV terminal device.

Upgrade and download API: an IPTV terminal middleware API that is responsible for dynamic downloading or upgrading software for IPTV terminal device.

- Software upgrade and download for application layer
- Software upgrade and download for middleware service
- Software upgrade and download for resource layer
- Coordination with security and authentication API to check validity of software and data

Terminal Management API: an IPTV terminal middleware API that is responsible to provides IPTV terminal management and configuration function.

- Remote management
- Log management
- Software version management
- Server parameter configuration, such as server address configuration
- Access mode and parameter configuration
- Media device parameter configuration, such decoder
- Subscriber configuration, such access account, service account

System resource management API: an IPTV terminal middleware API that is responsible to schedule resource used by application and manage their status.

- Status registration of resource usage by application
- Allocation and scheduling of resource to application
- Resource release management

Removable storage API: an IPTV terminal middleware API that is responsible to access information available in a removable storage device (e.g. smartcard, USB key)

- Access user information, such as user authentication, user ID, network access authority
- Access service information, such as service profile authorized by service providers
- Access billing information, such as prepaid account, fees consumed
- Access user preferences such as accessibility features and display settings

6.1.2 Media management component

Media management component is responsible for managing media streaming, media presentation and media storage, and provide media service API to the up layer application.

Media service API: an IPTV terminal middleware API that is responsible to manage media streaming, media presentation and media storage.

- Media streaming management, such as media streaming session set up and control for VoD, multicast linear TV, unicast linear TV, and time shift.
- Media decoding management.
- Media rendering and trick mode management, such as play, stop, pause, and resume.
- Caption presentation.
- Trigger of DRM process.
- Media buffer management.
- PVR and storage management.

6.1.3 Communication component

Communication component is responsible for IPTV terminal device communications, which including the following functionalities:

- Communication management
- Communication protocol management (HTTP, RTSP, etc.)
- Internet access

IPTV communication API: an IPTV terminal middleware API that is responsible for the communications between terminal device and service platform.

Internet access API: an IPTV terminal middleware API that is responsible to control and manage the basic operations of open Internet resident clients.

- Internet client management, such as web browser, e-mail and news client
- Internet client control

6.1.4 Security component

Security component is responsible for security mechanism of whole system, including subscriber authentication, media authorization, network security, software upgrade security, and service application security. This middleware service component provides security and authentication API and DRM API to the upper application layer.

Security and authentication API: an IPTV terminal middleware API that is responsible for security mechanism of whole system, including subscriber authentication, network security, software upgrade, and service application security, etc.

- Subscriber authentication and identification information management
- Service application authorization
- Software upgrade and download authentication
- Network security policy management
- Key, token and registration information management
- Parental control related information management
- Content purchasing information management

DRM API: an IPTV terminal middleware API that is responsible to process right control messages, process right management messages, and enable upper application layer to access the right DRM system.

- Licence management
- Right management
- Key management
- Decryption of media stream and data stream

6.1.5 Metadata access component

Metadata access component is responsible for metadata system access, the metadata presentation and service selection management, and provides metadata access API to the upper application layer.

Metadata API: an IPTV terminal middleware API that is responsible for metadata system access, the metadata presentation and service selection management.

- Metadata system access
- Metadata delivery management
- Metadata presentation, such as program scheduler and event catalogue
- Service selection management
- Metadata compression and decompression

6.1.6 User interaction component

User interaction component is responsible for interacting with end-users, and dispatch events originated by end user to application layer user interaction API to the upper application layer.

End user interaction API: an IPTV terminal middleware API that is responsible to interact with end users, and dispatch events originated by end user to application layer.

- Interaction with end user, via keyboard, or mouse, or remote controller
- Receiving and dispatching event from end user to application layer
- Service provider's terms and conditions notification to end user
- Display of service provider logo

Graphical user interface API: an IPTV terminal middleware API that is responsible to provide GUI engine to upper application to implement graph design, display and control function.

- Graph design and display function;
- User interface control interface design and display function;
- Set image and video attribute.

6.2 Classification of IPTV terminal middleware components APIs

Table 6-1 provides the list of recommended and optional APIs.

Table 6-1: IPTV terminal middleware components API classification

API	Recommended	Optional
Software initialize and diagnosis	X	
Upgrade and download	X	
Terminal management		X
System resource management		X
Removable storage		X
Media service	X	
IPTV communication	X	
Internet access		X
Security and authentication	X	
DRM	X	
Metadata	X	
End user interaction	X	
Graphical user interface		X

7 Service platform middleware

The IPTV service platform middleware components are classified as following:

- Application management component,
- Content delivery and control component,
- Service control component,
- Monitoring and configuration component,
- Content access component,
- Resource management component.

These components are shown in Figure 7-1 below:

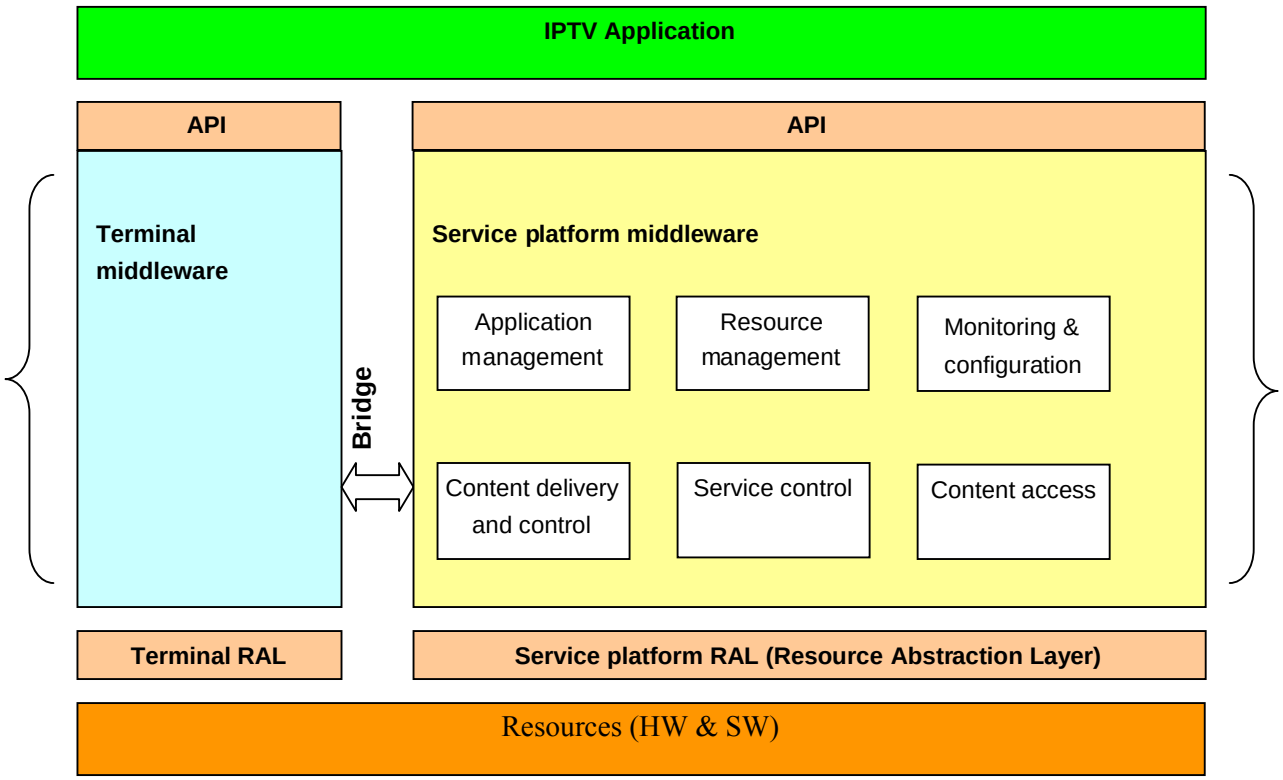


Figure 7-1: IPTV service platform middleware architecture – overview

7.1 IPTV service platform middleware components and APIs

7.1.1 Application management component

Application management component is responsible for the management of the life cycle of the applications and interaction operations between them.

Application management API: an IPTV service platform middleware API that is responsible for allowing service providers to:

- Manage the lifecycle of application.
- Maintain application status.
- Manage application according to control information from user or application providers.
- Manage the resources for applications.

7.1.2 Content delivery and control component

The content delivery and control component is responsible for the delivery of content to the end-user IPTV terminal device.

Content distribution API: an IPTV service platform middleware API that is responsible for controlling the content delivery between the content provider and the service provider.

- Content distribution policy management
- Distribute the content according to service provider rules
- Copy and caches the content
- Retrieve content
- Bandwidth and congestion control

- Scheduled distribution
- On demand distribution

Content streaming API: an IPTV service platform middleware API that is responsible for the streaming content to IPTV terminal devices. The media service API of IPTV terminal middleware is a client of this service platform middleware API.

- Media streaming control,
- Media trick mode management,
- Network PVR and storage management.

7.1.3 Service control component

The service control component is responsible for providing the functions to request and release the network and service resources.

Service management API: an IPTV service platform middleware API that is responsible for managing IPTV services offered to end users.

- Service profile management
- Service package management
- Service pricing policies management
- Statistics and usage management

Service navigation API: an IPTV service platform middleware API that is responsible for producing IPTV service navigation logic as described in section "Service navigation systems" of the "IPTV Middleware, Application and Content Platforms" document [FG IPTV-DOC-0194].

7.1.4 Monitoring and configuration component

The monitoring and configuration component is responsible for overall system management, status monitoring and configuration.

End user management API: an IPTV service platform middleware API that is responsible for the end users management.

- End users profile management
- Statistics and usage management
- Subscriber management
- End user account management
- Registration, authentication and authorization for the end user

Monitoring and configuration API: an IPTV service platform middleware API that is responsible for overall system management, status monitoring and configuration.

- IPTV terminal device management
- Software upgrade and download management
- Charging information management

7.1.5 Content access component

Content access component is responsible for providing content information coming from a content provider to a service provider.

Content access API: an IPTV service platform middleware API that is responsible for providing content information to upper layer applications.

- Provide the location and the description metadata of the content
- Provide pricing information of the content
- Content usage rules management

7.1.6 Resource management component

Resource management component is used to manage service platform resources.

Resource management API: an IPTV service platform middleware API that is responsible for managing resources used by applications.

- Monitoring resource usage by applications
- Allocation, scheduling and release of resources for applications

7.2 Classification of IPTV service platform middleware components APIs

Table 7-1 provides the list of recommended and optional APIs.

Table 7-1: IPTV service platform middleware components API classification

API	Recommended	Optional
Application management	X	
Content distribution		X
Content streaming	X	
Service management	X	
Service navigation		X
End user management	X	
Monitoring and configuration	X	
Content access	X	
Resource management	X	

II.6.4 IPTV metadata

Summary

The present document gives the overview of the metadata for IPTV services and describes its elements and delivery protocols, identifying relevant standards.

The IPTV metadata, the information on services and contents processed by the service and content delivery infrastructure, provides descriptive and structural framework for managing IPTV services.

Aspects of transport, representation, content provisioning, and security of metadata are covered.

Keywords

IPTV metadata

Current status

This document is complete.

Dependency on or relationship to other FG IPTV documents:

- IPTV service requirements document
- Service Security and Content Protection Aspects for IPTV
- IPTV protocols

CONTENTS

		Page
1	Scope	655
2	References	655
3	Definitions	656
	3.1 Terms defined elsewhere	656
	3.2 Terms defined in this Recommendation	656
4	Abbreviations and acronyms	657
5	Conventions	657
6	IPTV Metadata service overview	657
7	Metadata service discovery	658
	7.1 Service provider metadata	659
8	Metadata delivery method	659
	8.1 Updating method	659
	8.1.1 Metadata fragments	660
	8.2 Metadata transport container	660
	8.3 Metadata change notification	661
9	Metadata representation	661
10	Metadata elements	661
	10.1 Service and content metadata	661
	10.2 User metadata	667
11	Metadata for content provisioning	669
12	Metadata aggregation management	669
13	User metadata security	670
14	Classification scheme	670
15	Identity management	670
16	Metadata API	670
17	Metadata framework	670

IPTV metadata

1 Scope

The present document gives the overview of the metadata for IPTV services, and describes its elements and delivery protocols, identifying relevant standards.

The IPTV metadata provides a descriptive and structural framework for managing IPTV services. The IPTV metadata is the information on services and contents processed by service and content delivery infrastructure.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this document 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 document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.750] ITU-T Recommendation F.750 (2004), *Metadata Framework Recommendation*

[ISO/IEC 15706] ISO 15706 (2002), *Information and documentation – International Standard Audiovisual Number (ISAN)*

[ISO/IEC 15938-5] ISO/IEC 15938-5(2003), *Information technology – Multimedia content description interface – Part 5: Multimedia description schemes*

[ISO/IEC 21000-7] ISO/IEC 21000-7(2003), *Information technology – Multimedia framework (MPEG-21) – Part 7: Digital Item Adaptation*

[ETSI TS 102 034] ETSI TS 102 034 V1.2.1 (2006), *Digital Video Broadcasting: Transport of MPEG-2 Based DVB Services over IP Based Networks*

[ETSI TS 102 323] ETSI TS 102 323 V1.2.1 (2006), *Digital Video Broadcasting (DVB); Carriage and signalling of TV-Anytime information in DVB transport streams*

[ETSI TS 102 471] ETSI TS 102 471 V1.2.1 (2006), *Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Electronic Service Guide (ESG)*

[ETSI TS 102 472] ETSI TS 102 472 V1.2.1 (2006), *Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Content Delivery Protocols*

[ETSI TS 102 539] ETSI TS 102 539 V1.1.1 (2006), *Digital Video Broadcasting: Carriage of Broadband Content Guide (BCG) information over Internet Protocol*

[ETSI TS 102 822-3-1] ETSI TS 102 822-3-1 V1.3.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 1: Phase 1 – Metadata schemas*

[ETSI TS 102 822-3-2] ETSI TS 102 822-3-2 V1.3.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 2: System aspects in a uni-directional environment*

[ETSI TS 102 822-3-3] ETSI TS 102 822-3-3 V1.1.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 3: Phase 2 – Extended Metadata Schema*

[ETSI TS 102 822-3-4] ETSI TS 102 822-3-4 V1.1.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 3: Phase 2 – Interstitial metadata*

[ETSI TS 102 822-5-1] ETSI TS 102 822-5-1 V1.2.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 5: Rights Management and Protection (RMP) Sub-part 1: Information for Broadcast Applications*

[ETSI TS 102 822-6-1] ETSI TS 102 822-6-1 V1.3.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network; Sub-part 1: Service and transport*

[ETSI TS 102 822-6-3] ETSI TS 102 822-6-3 V1.1.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network; Sub-part 3: Phase 2 – Exchange of Personal Profile*

[ETSI TS 102 822-8] ETSI TS 102 822-8 V1.1.1 (2006), *Broadcast and On-line Services: Search, select and rightful use of content on personal storage systems ("TV-Anytime"); Part 8: Phase 2 – Interchange Data Format*

[IETF RFC 3265] IETFRFC 3265 (2002), *Session Initiation Protocol (SIP) – Specific Event Notification*

[IETF RFC 4287] IETFRFC 4287 (2005), *The Atom Syndication Format*

[OASIS SOAP-MS] OASIS 200401 (2004), *Web Services Security: SOAP Message Security 1.0*

[OASIS WSBN] OASIS (2006), *Web Services Base Notification 1.3 (WS-BaseNotification)*

[OMA-REL] Open Mobile Alliance (2005), *DRM Rights Expression Language, Candidate Version 2.0*

[SMPTE 380M] SMPTE 380M-2004, *Material Exchange Format (MXF) Descriptive Metadata. Scheme – 1*

3 Definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Metadata: Structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities. [FG-IPTV-DOC-0194]

3.2 Terms defined in this Recommendation

This document defines the following terms:

3.2.1 Metadata fragments: A metadata fragment is a self-consistent atomic portion of a metadata instance. In this context, self-consistency means that fragments can be obtained in a random order and each fragment can be transmitted and updated independently.

3.2.2 Metadata instance: A metadata instance is the data instance describing the instance of content or user, etc. A metadata instance has its data-model defined by corresponding metadata schema.

3.2.3 Metadata schema: A metadata schema is the representation format for specifying data-model describing target instance.

3.2.4 **Usage environment:** The usage environment is described by user characteristics, terminal capabilities, network characteristics and natural environment characteristics, where the contents being consumed.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

CS	Classification Scheme
EPG	Electronic Program Guide
ESG	Electronic Service Guide
FLUTE	File deLivery over Unidirectional Transport (IETF RFC 3926)
HTTP	Hypertext Transfer Protocol
ISAN	International Standard Audiovisual Number
OASIS	Organization for the Advancement of Structured Information Standards
PPV	Pay-Per View
QoS	Quality of Service
SDO	Standards Development Organization
SIP	Session Initiation Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
VoD	Video-on-Demand
XML	eXtensible Markup Language

5 Conventions

No specific conventions have been used in this document.

6 IPTV Metadata service overview

Figure 6-1 illustrates metadata flows between metadata sources and client side metadata applications, including user navigation methods and interactive program guides.

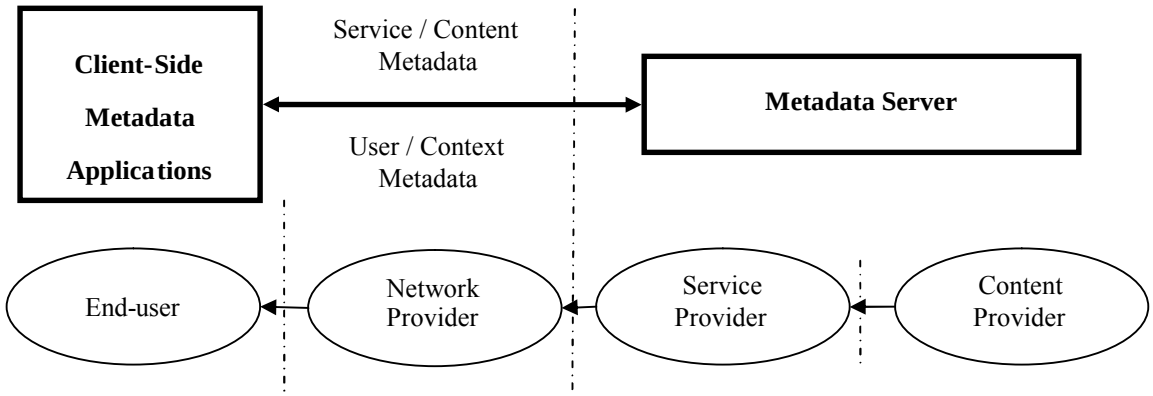


Figure 6-1: IPTV Metadata service overview

The Metadata Server is the entity responsible for aggregating metadata sets produced by Content Providers or Service Providers to describe services and content, as well as metadata sets generated or registered by metadata clients to describe end-user preference or context. These metadata sets are maintained in the database managed by the Metadata Server. The metadata maintained in the Metadata Server's database is accessed by, delivered to or contributed from metadata clients through metadata delivery and exchange protocols. These clients are typically categorized as Web-based navigation servers maintained by the Service Provider or client-side applications running on the IPTV client. The Web servers provide web-pages to the IPTV client through logical interfaces between the Service Provider and end-user domain. These pages are consumed by Web browsers to aid end-users in obtaining their preferred content. Metadata directly consumed by a client-side metadata application is used for providing the network-transparent user interface for navigation, for example, a content overview listing integrated with local content storage management. The Metadata Server also stores and manages end-user profiles or context metadata required to support content or service adaptation.

The following clauses provide summarized requirements for IPTV Metadata with some solutions, elements or attributes defined in those standard specifications as relevant for gap analysis.

Standards references are listed in clause 2 of this document.

7 Metadata service discovery

Locating a particular service in question is provided by the service discovery function. This functionality is implemented by service description metadata and the service discovery protocol. There are already a lot of solutions in this area; however, they usually have a limited scope constrained by the context of the standardization body and are not generally applicable, and not inter-operable. A unified service discovery mechanism is needed for all services defined in IPTV context. Metadata service would be categorized in one of those services. The Metadata Service should be discovered in the same manner as other service attachments.

[ETSI TS 102 539] specifies a mechanism for signalling and carrying metadata over an always-on bi-directional IP network. The specification allows for metadata describing both Content on Demand and live services already defined in [ETSI TS 102 034]. It specifies the mechanisms used for service discovery, service selection and the delivery of service discovery information.

7.1 Service provider metadata

The basic process of how a user starts consuming an IPTV service can be described in the following steps. User finds service provider and registers for the service usage. The entry point for finding service provider of user's preference provides listings of service metadata entry point and their providers. User browses the available detailed offerings by service descriptions provided by those entry points. Then user selects offerings and starts consumption.

The description of the available IPTV service providers may contain the following information for each service provider;

- Unique Service Provider Identifier (e.g. a domain name)
- Service Provider Name in different languages
- Service Provider Description in different languages
- Entry point for subscription
- Entry point to get description of IPTV services offered by this service provider
- Etc.

8 Metadata delivery method

The metadata delivery protocol is implemented on the basis of a common transport stratum. There are several styles of metadata delivery, such as unicast or multicast, subscribe-notify, query-response, or a mixture of those modes. These metadata delivery methods can be implemented on a SIP-based service platform, a WebService based service-oriented architecture (SOA) framework. The delivery protocol should be modular so that different kinds of metadata delivery can be supported by a single protocol suite.

- Push or pull mode of delivery
- Unicast or multicast, ensuring reliability or not.
- Query-response; metadata bi-directional transport, XQuery, etc.

[ETSI TS 102 539] specifies push and pull modes of content description delivery for container-based and query/response-based protocols. DVB adopts the DVB-STP multicast transport protocol for push mode and the HTTP unicast protocol for pull mode as defined in [ETSI TS 102 034]. A profile for unicast query/response delivery using Simple Object Access Protocol (SOAP) over HTTP specified in [ETSI TS 102 822-6-1] is also defined as optional. The query protocol can retrieve any portion of XML instance identified by XPath predefined or dynamically assigned by the content guide service. [ETSI TS 102 822-8] defines the interchange data format for the delivery of metadata and content referencing information from different data sources.

As per clause 8 of [ETSI TS 102 471] Metadata transport containers carrying ESG metadata instances are transported in FLUTE dynamic file delivery carousel sessions as described for file delivery in [ETSI TS 102 472].

8.1 Updating method

Out-dated metadata should be updated automatically if delivered metadata is already cached or stored in the metadata client. The versioning and updating for delivered metadata is managed through a fragment updating method. The metadata consistency and reliability must be guaranteed by this method itself. When changes in the original metadata instance occur, it should be possible to notify clients with replicated instances of this metadata automatically. A mechanism should also be provided for maintaining the atomicity, consistency, isolation and durability of the related Metadata Fragments.

8.1.1 Metadata fragments

A Metadata fragment is a self-consistent atomic portion of a metadata instance sent to the metadata client. In this context, self-consistency means that fragments can be obtained in a random order and each fragment can be transmitted and updated independently. The instance is identified through individual fragment IDs. The fragment can be defined or managed at the transport container level or the metadata representation, schema level.

- Metadata instance identification, versioning and updating
- Fragment definition; scope or unit, layer of schema or transport envelope, etc.

[ETSI TS 102 539] and [ETSI TS 102 471] rely on fragment updating method defined in [ETSI TS 102 822-6-1]. The detail of the metadata fragment structure is in [ETSI TS 102 822-3-2]. This document defines how to split the metadata description into a number of self-contained fragments and how to identify them and mange their versions and expiration periods.

Sub-clause 7.3 "The Fragment Management Information" of [ETSI TS 102 471] provides the encapsulation mechanism for a set of ESG metadata fragments, by providing the ability to assign a unique identifier (fragment ID) for the lifetime of an ESG fragment and indicating the current version of an ESG fragment.

[IETF RFC 4287] 4.2.9 published, 4.2.15 updated.

8.2 Metadata transport container

Metadata must be transport protocol agnostic, thus a generic transport envelope or container format may be required. The transport container contains metadata instances. The header of transport container should contain information about the metadata representation scheme, such as the coding format, whether it is compressed or uncompressed, and the specific compression method used. If the metadata fragment is defined at the transport container level, the fragment should be encapsulated in the container with fragment management information, which allows the metadata client to identify new versions of a fragment without actually reading and comparing the content of the fragments. Fragment management information includes unique identification of the fragment, version of the fragment instance and timing information, such as the start and end time of availability of the instance. The metadata in this container may be secured with cryptographic methods that prevent unauthorized modification by intermediate entities on its distribution path. In this case, security and integrity management parameters may be included in the header of container. In some environment, the transport containers may be multiplexed with content delivery protocol data units, as in-band delivery.

- Generalised metadata envelope
- Fragment encapsulation, filtering information
- Security consideration
- In-band with content delivery

[ETSI TS 102 822-3-2] specifies the structure of the container carrying the metadata fragment. It describes the format of the container and additional requirements on the delivery layer to provide container identification, information about the type of data a container carries and the current version of a container.

Per clauses 6 and 7 of [ETSI TS 102 471] ESG fragments are encapsulated in the ESG Container. The ESG Container provides fragment aggregation, versioning and filtering. ESG fragments may be represented in uncompressed, GZIP-compressed and BiM-compressed forms.

8.3 Metadata change notification

Notification of modifications to metadata within Metadata Server should be propagated to metadata clients. If metadata is pre-cached or stored in a local metadata client database, the Metadata Server must keep track of the most recent versions of the metadata instances already delivered. If the Metadata Server detects a modification, the most current version of those instances must be propagated to the clients and outdated metadata instances should be automatically discarded and updated to the latest version. Notification can be announced at a scheduled time or on demand by a client request. Clients should be able to declare their preferences for filtering the notifications.

- Change notification subscription, delivery
- Reliable transport for notification
- Subscribe-notify; session initiation protocol (SIP) specific event notification, Web service event notification, etc.

Web Services Notification [OASIS WSBN] provides a standardized way for a Web service, or other entity, to disseminate event notification to another set of clients. The SIP-specific framework for event notification [IETF RFC3265] also specifies a flexible way to provide generalized event notification services. Both types of event notification can be applied to the publish/subscribe service model for metadata delivery management systems.

9 Metadata representation

Most of metadata instances which are generated according to industry standards and are compliant to them which are represented in extensible markup language (XML) are not interoperable. There is a strong requirement that the semantics and representation scheme of metadata should be based on a common standardized data model and format. Ideally, names and terms should be selected from a controlled vocabulary or thesaurus so that indexing, search and retrieval are more accurate. Standard representation, registration and maintenance procedures should be specified to ensure interoperability of controlled vocabularies. Existing and mature metadata standards, such as [ISO/IEC 15938-5] or [ETSI TS 102 822-3-1], shall be adopted or integrated to avoid reinvention of new metadata standards.

- Metadata in XML data
- Adopt existing standardized metadata schema as a base for further extension
- Integrated with controlled vocabulary or thesaurus management standard

10 Metadata elements

This clause enumerates typical elements or attributes required for the standardized set of metadata.

10.1 Service and content metadata

Service and content metadata are descriptive information and must be able to be parsed by machines for consumption by user interface. The end-user shall be able to navigate through a variety of service and content offerings in order to select a specific service to acquire the desired contents.

Service metadata includes detail description used for service discovery and selection to activate a specific IPTV service. Content metadata is produced by content providers and service providers. Content providers typically supply title, synopsis, genre, and other descriptive metadata about the content, while service providers assign the time of delivery, cost, and other information about the service.

Elements required in service and content metadata are;

Elements required for content:

- Identifier
  - [ETSI TS 102 822-3-1] 6.3.6 programId, 6.3.7 groupId (Group), 6.4.2 InstanceMetadataId, 6.4.3 serviceId, 6.6.5 segmentId, 6.6.6 groupId (SegmentGroup)
  - [ETSI TS 102 822-3-3] 8.4 item_id, 8.5 component_id, 8.6 crid (Package)
  - [ETSI TS 102 471] 5.4.1 serviceID, 5.5.1 serviceBundleID, 5.6.1 contentID, 5.7.1 scheduleId
  - [b-UPnP CDS2] B.8.3 upnp:programID, B.8.4 upnp:seriesID, B.8.5 upnp:channelID, B.9.1.1 upnp:channelGroupName@id, B.10.2 upnp:radioStationID
  - [IETF RFC 4287] 4.2.6 id
- Title/name (secondary title)
  - [ETSI TS 102 822-3-1] 6.3.4 Title (Program, Group), 6.4.2 Title (ProgramLocation), 6.4.3 Name (ServiceInformaion), 6.6.2 Title (Segment, SegmentGroup)
  - [ETSI TS 102 471] 5.4.1 ServiceName, 5.5.1 ServiceBundleName, 5.6.1 Title (Content)
  - [b-UPnP CDS2] B.8.1 upnp:programTitle, B.8.2 upnp:seriesTitle, B.9.1 upnp:channelGroupName, B.11.2 upnp:channelName
  - [IETF RFC 4287] 4.2.14 title
- Rights or copy rights information (including information about the content owner)
  - [IETF RFC 4287] 4.2.10 rights
- Name of content provider, service provider (e.g. broadcasting organization)
  - [ETSI TS 102 822-3-1] 6.4.3 Owner (brand owner of the service)
  - [ETSI TS 102 471] 5.4.1 ServiceProvider, 5.5.1 ServiceBundleProvider
  - [b-UPnP CDS2] B.9.4 upnp:serviceProvider
  - Primary (, secondary) spoken language
  - [ETSI TS 102 822-3-1] 6.3.4 Language (Program, Group), 6.3.5 AudioLanguage (Program, ProgramLocation) 6.4.3 ServiceLanguage
  - [ETSI TS 102 822-3-3] 6.1.1.1 AudioLanguage (Component)
  - [ETSI TS 102 471] 5.4.1 ServiceLanguage, 5.6.1 Language (Content), 5.10.7.1 Language (Component)
  - [b-UPnP CDS2] B.7.7 dc:language
- Primary (secondary) caption language (with speed parameter)
  - [ETSI TS 102 822-3-1] 6.3.4 CaptionLanguage (Program, Group)
  - [ETSI TS 102 471] 5.6.1 CaptionLanguage (Content), 5.10.7.1 OpenCaptionLanguage (Component)
- Genre
  - [ETSI TS 102 822-3-1] 6.3.4 Genre (Program, Group), 6.4.2 Genre (ProgramLocation), 6.4.3 ServiceGenre, 6.6.2 Genre (Segment, SegmentGroup)
  - [ETSI TS 102 471] 5.4.1 ServiceGenre, 5.5.1 ServiceBundleGenre, 5.6.1 Genre (Content)
  - [UPnP CDS2] B.4.1 upnp:genre
  - [IETF RFC 4287] 4.2.2 Category

- Keywords
  - [ETSI TS102 822-3-1] 6.3.4 Keyword (Program, Group), 6.6.2 Keyword (Segment, SegmentGroup)
  - [ETSI TS102 471] 5.6.1 Keyword (Content)
- Description (synopsis, abstract)
  - [ETSI TS 102 822-3-1] 6.3.4 Synopsis (Program, Group), 6.4.2 Synopsis (ProgramLocation), 6.4.3 ServiceDescription, 6.6.2 Synopsis (Segment, SegmentGroup)
  - [ETSI TS 102 471] 5.4.1 ServiceDescription, 5.5.1 ServiceBundleDescription, 5.6.1 Synopsis (Content)
  - [b-UPnP CDS2] B.7.1 dc:description
  - [IETF RFC 4287] 4.2.13 Summary
- Credits (e.g. actor/actress, director, producer, scenario writer)
  - [ETSI TS 102 822-3-1] 6.3.4 CreditsList (Program, Group), 6.6.2 CreditsList (Segment, SegmentGroup)
  - [ETSI TS 102 471] 5.6.1 CreditsList (Content)
  - [b-UPnP CDS2] B.3.1 upnp:artist, B.3.2 upnp:actor, B.3.3 upnp:author, B.3.4 upnp:producer, B.3.5 upnp:director, B.3.6 dc:publisher, B.3.7 dc:contributor, B.1.7 dc:Title, B.1.8 dc:Creator
  - [IETF RFC 4287] 4.2.1 author, 4.2.3 contributor
- Awards
  - [ETSI TS 102 822-3-1] 6.3.4 AwardsList (Program, Group)
- Location and time of production
  - TSI TS 102 822-3-1] 6.3.4 ProductionLocation, ProductionDate (Program, Group)
  - -UPnP CDS2] B.7.4 upnp:region, B.7.6 dc:date
- Parental guidance or rating (with rating standards identifier)
  - TSI TS 102 822-3-1] 6.3.4 ParentalGuidance (Program, Group)
  - TSI TS 102 471] 5.4.1 ParentalGuidance (Service), 5.5.1 ParentalGuidance (ServiceBundle), 5.6.1 ParentalGuidance (Content)
- Review (with name or reviewing entity)
  - SI TS 102 822-3-1] 6.3.8 Review
  - b-UPnP CDS2] B.8.9 upnp:rating
- Type of contents, like promotional, advertisement
- Encrypted or not
  - TSI TS 102 471] 5.4.1 clearToAir (Service), 5.7.1 clearToAir (ScheduleEvent)
- Preview, supplementary video and descriptive audio
  - TSI TS 102 822-3-1] 6.3.4 RelatedMaterial (Program, Group), 6.6.2 RelatedMaterial (Segment, SegmentGroup)
  - -UPnP CDS2] B.5.4 dc:relation
- Related website
  - TSI TS 102 822-3-1] 6.3.4 RelatedMaterial (Program, Group), 6.6.2 RelatedMaterial (Segment, SegmentGroup)
  - TSI TS 102 471] 5.4.1 RelatedMaterial (Service), 5.5.1 RelatedMaterial (ServiceBundle), 5.6.1 RelatedMaterial (Content)

  - [b-UPnP CDS2] B.5.4 dc:relation, B.2.1.19 res@contentInfoURI
  - [IETF RFC 4287] 4.2.7 link
- Information for invoking value-added applications, associated or un-associated, service provider-managed applications, e.g. news highlights, stock exchange, traffic conditions, sport results, in the form of print text, images and other associated assets as enhancements
  - [ETSI TS 102 822-3-1] 6.3.4 RelatedMaterial (Program, Group), 6.6.2 RelatedMaterial (Segment, SegmentGroup)
- Codec or format
  - [ETSI TS 102 822-3-1] 6.3.5 Coding
  - [ETSI TS 102 822-3-3] 6.1.1.1 Coding (Audio), 6.1.1.2 Coding (Video)
  - [ETSI TS 102 471] 5.10.7.1 Codec, ProfileLevelIndication
- Aspect ratios, resolution, bit rate, frame rate for video
  - [ETSI TS 102 822-3-1] 6.3.5 AspectRatio, HorizontalSize, VerticalSize, Bitrate, FrameRate
  - [ETSI TS 102 822-3-3] 6.1.1.1 BitRate, AspectRatio, HorizontalSize, VerticalSize, FrameRate
  - [ETSI TS 102 471] 5.10.7.1 Bandwidth, FrameRate
  - [ETSI TS 102 822-3-1] B.2.1.10 res@resolution, B.2.1.6 res@bitrate
- Mono, stereo, multi-channel indication for audio
  - [ETSI TS 102 822-3-1] 6.3.5 MixType, NumOfChannels
  - [ETSI TS 102 822-3-3] 6.1.1.1 MixType, NumOfChannels
  - [ETSI TS 102 471] 5.10.7.1 Mode
  - [b-UPnP CDS2] B.2.19 res@nrAudioChannels
- Acquisition or delivery schedule, start/end availability, protocol and address
  - [ETSI TS 102 822-3-1] 6.4.2 PublishedStartTime, PublishedEndTime, StartOfAvailability, EndOfAvailability, ProgramURL
  - [ETSI TS 102 471] 5.7.1 PublishedStartTime, PublishedEndTime
  - [b-UPnP CDS2] B.11.3 upnp:scheduledStartTime, B.11.4 upnp:scheduledEndTime
- First/repeat delivery or live broadcast
  - [ETSI TS 102 822-3-1] 6.4.2 FirstShowing, LastShowing, Repeat, Live
  - [ETSI TS 102 471] 5.7.1 live, repeat
  - [b-UPnP CDS2] B.8.10 upnp:episodeType
- File format, File size
  - [ETSI TS 102 822-3-1] 6.3.5 FileFormat, FileSize
  - [ETSI TS 102 822-3-3] 6.1.3 FileFormat, FileSize
  - [ETSI TS 102 471] 5.10.7.1 FileFormat, Storage
  - [UPnP CDS2] B.2.1.3 res@size
- Duration
  - [ETSI TS 102 822-3-1] 6.3.4 Duration (Program, Group), 6.6.5 SegmentLocator (Segment), 6.6.6 Duration (SegmentGroup)
  - [ETSI TS 102 471] 5.6.1 Duration (Content)
  - [b-UPnP CDS2] B.2.1.4 res@duration

- Content expiration date
- Replacement timing

Elements required for collective content:

In some cases, content needs to be a collection of various kinds of sub-contents. For example, series is a collection of each episode. Previously, group is well known as a collection of same types of contents, and a package is a collection of various types of contents such as main content and related web pages.

Considering the relation between EPG metadata and EPG application, metadata for these collective contents need to be defined separately from the applications for presenting them.

- Total number of sub-contents
  - [ETSI TS 102 822-3-1] 6.3.7 numOfItems (Group), 6.6.6 numberOfSegments (SegmentGroup)
  - [b-UPnP CDS2] B.8.6 upnp:episodeCount
- Ordered flag to indicate whether the sub-contents are ordered or not
  - [ETSI TS 102 822-3-1] 6.3.7 ordered (Group), 6.6.6 ordered (SegmentGroup)
- IDs for sub-contents
  - [ETSI TS 102 822-3-1] 6.3.6 index
  - [ETSI TS 102 822-3-3] 8.4 item_id
  - [b-UPnP CDS2] B.8.7 upnp:episodeNumber
- Price and conditions of availability of a collective content
  - [ETSI TS 102 822-3-1] 6.3.4 PurchaseItem
  - [b-UPnP CDS2] B.9.5 upnp:price
- IDs for other collections of which this collection is a member
  - [ETSI TS 102 822-3-1] 6.3.6 MemberOf (Program), 6.3.7 MemberOf (Group)
    - Descriptions for each sub-content
      - Content Type

        [ETSI TS 102 822-3-3] 6.1.3 ContentType
      - Elements for content

        [ETSI TS 102 822-3-3] 8.4 Item
      - Description of Usage environment where each sub-content is properly consumed

        [102 822-3-3] 6.2.8 TerminalInformation, NetworkInformation, NaturalEnvironmentInformation
      - Description of User Preferences and profile with which a user hopefully wants to consume the sub-content.

        [ETSI TS 102 822-3-3] 6.2.8 TargetUserPreferences, UserInformation
      - Relation information between sub-contents such as one is preceded from other one.

        [ETSI TS 102 822-3-3] 8.4 RelationType

Elements required for optional quality monitoring:

- Video quality scores of compressed video data [J.bitvqm draft]

Elements required for group of segment:

- Play-list for digesting (e.g. highlights)
  - [ETSI TS 102 822-3-1] 6.6.6 SegmentGroupInformationType

– [ETSI TS 102 822-3-3] 8.4 SelectionType, ChoiceType

Elements required for service (or channel):

- Channel Number, Minor Channel Number (the minor channel number is used for two-part channel numbers)
- Service (or channel) logo
  - [ETSI TS 102 822-3-1] 6.4.3 Logo
  - [ETSI TS 102 471] 5.4.1 ServiceLogo
  - [b-UPnP CDS2] B.7.3 upnp:icon
- Type of service, such as video-on-demand (VOD), live streaming.
  - [ETSI TS 102 822-3-1] 6.4.2 live
  - [ETSI TS 102 471] 5.4.1 ServiceType, 5.6.1 ContentType, 5.7.1 live
- Time-table (schedule)
  - [102 822-3-1] 6.7.1 Schedule
  - [102 471] Compilation of 5.7.1 ScheduleEvent
- Near VoD support or not
- Free or subscribed
  - [ETSI TS 102 822-3-1] 6.4.2 Free (indicates free access or not)
  - [ETSI TS 102 471] 5.4.1 freeToAir
- Local Network Affiliate (describes the local network affiliate, such as KNSD is an NBC affiliate in San Diego, California; and KOMO is an ABC affiliate in Seattle, Washington.)
- Channel Content Advisory (used to label channels with adult content, enabling parents to block this content, if desired)

Elements required for describing delivery modes:

- Push or pull
- Caching policy
- Pre-recording (for subtitles, captions, additional textual information, associated application)
- Required quality of service (QoS) level
  - [ETSI TS 102 822-3-3] 6.2.8 NetworkInformation

Elements required for content adaptation:

- Targeting (class of user profile, user preference)
  - [ETSI TS 102 822-3-3] 6.2.8 TargetUserPreferences, TargetUsageHistory, UserInformation
- Interstitials (commercials and promos) replacement, replacement rules
  - [ETSI TS 102 822-3-4] 7.6.1 InterstitialBreakType
- Consumption control parameter, based on usage environment (device, network, etc.)
  - [ETSI TS 102 822-3-3] 6.2.8 TerminalInformation, NetworkInformation, NaturalEnvironmentInformation

Elements required for Usage restrictions, usage rules:

[ETSI TS 102 471] 5.8.1 UsageConstraints

- ValidityPeriod
  - [ETSI TS 102 822-5-1] 5.3 Time Window Start Date & Time Window End Date
  - [b-UPnP CDS2] B.2.1.14 res@validityStart, B2.1.15 res@validityEnd
  - [OMA-REL] 5.5.4 datetime, 5.5.5 interval
- Output control (for display only or recording in storage device)
  - [ETSI TS 102 822-5-1] 5.3 High Definition Digital Export Control, Analogue Export Signalling, Analogue Standard Definition (SD) control, Simultaneous Rendering Counta
  - [UPnP CDS2] B.2.1.13 res@allowedUse (number of plays, copies) B.2.1.17 res@usageInfo
- Trick mode enabled or not
  - [ETSI TS 102 822-5-1] 5.3 Buffer Duration
- Maximum buffering size or duration
  - [102 822-5-1] 5.3 Buffer Duration
- Schedule (, timeslots) for pay-per view (PPV)
- Licensing and subscription information, e.g. retail price, billing models, discount, conditions and licence information
  - [ETSI TS 102 822-3-1] 6.3.4 PurchaseItem
  - [ETSI TS 102 822-3-3] 6.4 ExtendedPurchaseItemType
  - [ETSI TS 102 471] 5.8.1 PurchaseType
  - [b-UPnP CDS2] B.9.5 upnp:price, B.9.6 upnp:payPerView
- DRM type, clearing house or pricing server URL, licence identification
  - [ETSI TS 102 822-3-1] 6.3.4 PricingServerURL
  - [ETSI TS 102 471] 5.8.1 PurchaseRequest, 5.9.1 PortalURL
  - [b-UPnP CDS2] B.2.1.5 res@protection
- Restricted area
  - [ETSI TS 102 822-5-1] 5.3 Geographical Control
- Expiration date or deletion management information
- Recordable or not, in service provider storage or consumer storage
  - [b-UPnP CDS2] B.7.16 upnp:recordable
- Payment models depends on amounts of interstitial content
- Content adaptation allowed or not, i.e. by transcoding

10.2 User metadata

User metadata is shared and a common structure describing profiles or context related to an end-user. It could be represented by end-user preference, usage history, context for contents consuming environment like device and transport capability, such as types of codec, QoS statistic, etc. They can be accessed by several applications over multiple service domains. These data elements are intended to be reusable between different applications. User metadata specifies customer specific information required to support functions such as notification delivery for preferred contents subscription, customization of contents, consumption policy control, interstitial ads insertion, etc.

Elements required in user metadata are;

Elements required for User profile or preference:

- [ETSI TS 102 822-3-3] 9 ExtendedUserDescription

• User identifier
  - [ETSI TS 102 822-3-1] 6.5.2.3 UserIdentifier
• Demographic data
  - [ETSI TS 102 822-3-3] 6.2.1 BioGraphicInformation, 6.2.6 Location
• Favorite channels
  - [ETSI TS 102 822-3-1] 6.5.2.2 UsagePreference ([ISO/IEC 15938-5] 15.2.3.3 PublicationSource)
• Viewing behaviour
  - [ETSI TS 102 822-3-1] 6.5.1.1 UsageHistory
• Multiple personal profiles identification
• Personal profiles, personal preferences exchangeable or not, with other devices, e.g. PDRs
  - [ETSI TS 102 822-6-3] 5 User Profile Message Interface
• Support "personally linked" segments

Elements required for audience measurement metadata:

Audience measurement metadata consists of elements in measurements and context information.

(Measurements)

- Minimum information for channel identification, content identification where the concept of a channel may not exist (e.g. downloads and content-on-request), and platform identification
- Additional information about viewed services and the interactive services
- Other specific measures: e.g. information about receiver configuration, favorite channels, channel availability, quality and availability of services
- Timing

(Context information)

- Identification of users
- State and use of the receiver
- Localization of the user for mobile environments
- User authorization
- Capabilities of the device to receive the AV services, information about the environment

Elements required for device and network description:

• Interface capability, e.g. bit rate, bandwidth restrictions of network interface
  - [ISO/IEC 21000-7] 5.5.3 NetworkCapabilityType
• Presentation capability (e.g. resolution, supported codec or formats, media profile)
  - [ISO/IEC 21000-7] 5.4 TerminalCapabilitiesType

Elements required for EPG UI representation:

- EPG graphical presentation control information like fonts, the icons, the pointer, the background pictures, and the sounds effect, etc.
- Certified skins of EPG appearances

11 Metadata for content provisioning

There are some metadata in the content provisioning phase exchanged across contributing networks that include both content providers and service providers. These descriptive metadata are required to provide details about the production, such as the title and responsible organization, location of the shot or shots, participants, and other annotating information. It is essential for contributors to be consistent in how the metadata is added, terms are used, and rules are followed, so that everyone involved provides information that is useful and understood by all parties within the metadata workflow, with minimal duplication of effort.

The followings are specific set of descriptive metadata expected to be exchanged in content provisioning phase.

- Titles, Group Relation ships, and Branding
- Identification
- Event and Publication
- Award
- Captions Description
- Annotation and Classification
- Setting Period
- Scripting
- Shot and Key Point
- Participant
- Contacts List, Person, Organization, and Location
- Contract and Right
- Image Format
- Device Parameters

A framework of descriptive metadata schemes is defined in DMS-1[SMPTE 380M]. DMS-1 is intended for B2B interchange.

12 Metadata aggregation management

There are some attributes required for managing the instance of metadata. It is likely that metadata from a number of independent content creators and publishers will need to be aggregated in so-called metadata aggregator. The owner information of original metadata should be managed properly during the process of metadata aggregation or delivery.

- Metadata Publisher, Metadata Owner
- Metadata Instance Copyright Line (contains the legal text associated with the metadata copyright)

[IETF RFC 4287] 4.2.1 author, 4.2.3 contributor, 4.2.10 rights

13 User metadata security

The authentication and integrity validation of sub-blocks of the user metadata must be possible where good privacy protection is required. It should be possible to specify access rights of valid user to metadata instances. Metadata servers may be enabled to impose different levels of authorization requirements on metadata.

- Access, privacy control for user profile, user metadata

[ETSI TS 102 822-6-3] 6 Notes on Privacy and Security, Messaging security by [OASIS SOAP-MS]

14 Classification scheme

The classification scheme (CS) is an MPEG-7 tool for the provision of controlled terminology for use in classification and is referred by some standardized metadata. The namespaces for CS extended or originally created for ITU-T IPTV services are specified and maintained with their detail CS definitions.

- Controlled terminology defined by standardized classification scheme (CS)
- CS Namespace maintenance

[ETSI TS 102 822-3-1] Annex A – Classification Scheme

15 Identity management

Identity management ensures uniqueness and integrity of content, service, content or service provider, user and device. It is required to allow service providers to offer service and contents efficiently. Those identifiers may be used for service customization, content adaptation or advertisements targeting. ITU-T should specify the syntax of those identifiers and their encoding restriction within ITU-T IPTV services.

[ISO/IEC 15706] ISAN identifies all types of audiovisual works and their relevant versions. Registrations and allocation are done via Registration Agencies. ISAN permanently identifies an audiovisual work and its versions over its lifecycle.

16 Metadata API

IPTV Middleware may provide the application programming interface (API) to access metadata information.metadata access API has already been standardized in DVB and other SDOs for specific ECG schema set. Careful evaluation is required for deciding which level of API classes should be provided to fulfil generalized application requirements.

17 Metadata framework

A general metadata framework is defined in [ITU-T F.750].

Bibliography

[b_UPnP CDS2] *UPnP Forum (2006), ContentDirectory service:2 Service Template Version 1.01 For UPnP™ Version 1.0, Document version 1.00.*

II.6.5 Standards for IPTV multimedia application platforms

Summary

This document identifies and analyzes the relevant standards for IPTV multimedia application platforms.

Keywords

Application platform, DASE, DDE-T, DOM, IPTV.

Current status

This document is complete.

Dependency on or relationship to other FG IPTV documents

- IPTV service requirements document
- IPTV middleware, applications, and content platforms
- Service navigation system
- IPTV metadata

CONTENTS

			Page
1	Scope		673
2	References		673
3	Definitions		674
	3.1	Terms defined elsewhere	674
	3.2	Terms defined in this document	674
4	Abbreviations and acronyms		675
5	Requirements for IPTV Multimedia Application Platform		676
	5.1	Architecture	676
	5.2	Middleware	676
	5.3	Terminal Device	678
6	Standards for Declarative Application Platforms		678
	6.1	Binary Format for Scene (BIFS)	678
	6.2	Broadcasting Markup language (BML)	680
	6.3	CEA-2014	681
	6.4	Cascading Style Sheet (CSS)	682
	6.5	Document Object Model (DOM)	682
	6.6	Digital Video Broadcasting HyperText Markup Language (DVB-HTML)	682
	6.7	ECMAScript	683
	6.8	Lightweight Application Scene Representation (LASeR) & Simple Aggregation Format (SAF)	684
	6.9	Lua	684
	6.10	MHEG-5	684
	6.11	Nested Context Language (NCL)	685
	6.12	Scalable Vector Graphics (SVG)	685
7	Standards for Procedural Application Platforms		686
	7.1	GEM-based Application Platforms	686
8	Other Related Standards		689
	8.1	MPEG Multimedia Middleware (M3W)	689
Appendix I – Comparison of some multimedia application platforms			692
Appendix II – Worldwide TV Markup Language (WTVML)			693

Standards for IPTV multimedia application platforms

1 Scope

This document identifies and describes the relevant standards for interoperability and harmonization among IPTV multimedia application platforms.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this document 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 document does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-R BT.1699] ITU-R Recommendation BT.1699 (2005), *Harmonization of declarative content format for interactive TV applications*

[ITU-R BT.1722] ITU-R Recommendation BT.1722 (2005), *Harmonization of procedural content formats for interactive TV applications*

[ITU-T J.201] ITU-T Recommendation J.201 (2004), *Harmonization of declarative content format for interactive television applications*

[ITU-T T.170] ITU-T Recommendation T.170 (1998), *Framework of T.170 Series of Recommendation*

[ITU-T T.172] ITU-T Recommendation T.172 (1998), *MHEG-5 – Support for base-level interactive applications*

[ITU-T T.175] ITU-T Recommendation T.175 (1998), *Application Programming Interface (API) for MHEG-5*

[ISO/IEC 13522-5] ISO/IEC 13522-5 (1997), *Information technology – Coding of multimedia and hypermedia information – Part 5: Support for base-level interactive applications*

[ISO/IEC 14496-11] ISO/IEC 14496-11 (2005), *Information technology – Coding of audio-visual objects – Part 11: Scene description and application engine (BIFS)*

[ISO/IEC 14496-20] ISO/IEC 14496-20 (2006), *Information technology – Coding of audio-visual objects – Part 20: Lightweight Scene Representation (LASeR) and Simple Aggregation Format (SAF)*

[ISO/IEC 23004] ISO/IEC 23004 (2007), *Information technology – Multimedia Middleware*

[ETSI TS 102 322] ETSI TS 102 322 (2004), *Specification for a Lightweight Microbrowser for interactive TV applications, based on and compatible with WML V1.1.1*

[ETSI TS 102 819] ETSI TS 102 819 V1.3.1, *Digital Video Broadcasting (DVB); Globally Executable MHP version 1.0.2*

[ETSI TS 102 812] ETSI TS 102 812-v1.2.1 (2000), *Digital Video Broadcasting (DVB) – Multimedia Home Platform (MHP) Specification 1.1.1*

[A/101] ATSC Document A/101, *ATSC Standard: Advanced Common Application (ACAP)*

[ABNT NBR 15606-2] ABNT NBR 15606-2, Ginga-NCL – *Execution Platform for Declarative Applications*

[ABNT NBR 15606-4] ABNT NBR 15606-4, Ginga-J – *Execution Platform for Procedural Applications*

[ANSI/SCTE 90-1] ANSI/SCTE 90-1(2004), *SCTE Application Platform Specification OCAP 1.0 Profile*

[ARIB STD-B23] ARIB STD-B23 ver.1.1, *Application Execution Engine Platform for Digital Broadcasting*

[ARIB STD-B24] ARIB STD-B24 Ver5.1, *Data coding and Transmission Specification for Digital Broadcasting*

[CEA-2014] CEA-2014 (2006), *Web-based Protocol and Framework for Remote User Interface on UPnP™ Networks and the Internet (Web4CE)*

[CSS1] Cascading Style Sheets, level 1 (1996), *W3C Recommendations: CSS, level 1*

[CSS2] Cascading Style Sheets, level 2 CSS2 Specification (1998), *W3C Recommendations: CSS2 Specification*

[CSS TV Profile] CASS TV Profile 1.0 (2003), *W3C Recommendations: CSS TV Profile 1.0*

[DOM2] DOM Level 2 Core Specification, *W3C Recommendation: Document Object Model (DOM) Level 2 Core Specification*

[ECMA-262] Standard ECMA-262 3rd Edition (1999), *ECMA Standardizing Information and Communication Systems*

[SVG 1.1] Scalable Vector Graphics (SVG) 1.1 Specification (2003), *W3C Recommendation: Scalable Vector Graphics (SVC) 1.1 Specification*

[XHTML 1] XHTML™ 1.0 Second Edition, *W3C Recommendation: XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition)*

3 Definitions

3.1 Terms defined elsewhere

This clause is intentionally left blank.

3.2 Terms defined in this document

This clause is intentionally left blank.

4 Abbreviations and acronyms

This document uses the following abbreviations and acronyms:

ABNT	Associação Brasileira de Normas Técnicas
ACAP	Advanced Common Application Platform
API	Application Programming Interface
ARIB	Association of Radio Industries and Businesses (Japan)
BIFS	Binary Format for Scene
BIFS-Anim	BIFS Animation
BML	Broadcast Markup Language
CE	Consumer Electronics
CSS	Contents Scramble System
DASE	Digital television Application Software Environment
DDE-T	Declarative Data Essence-Transitional
DOM	Document Object Model
ECMA	European Computer Manufacturers Association
EE	Execution Engine
FBA	Face and Body Animation
GEM	Globally Executable MHP
ISDB-T	Integrated Services Digital Broadcasting-Terrestrial
LASeR	Lightweight Application Scene Representation
MHEG	Multimedia and Hypermedia information coding Experts Group
MHP	Multimedia Home Platform
M3W	MPEG Multimedia Middleware
NCL	Nested Context Language
OCAP	Open Cable Application Platform
PE	Presentation Engine
SAF	Simple Aggregation Format
SBTVD-T	Sistema Brasileiro de TV Digital – Terrestre
SMIL	Synchronized Multimedia Integration Language
SMPTE	Society of Motion Picture Television Engineers
S&N	Synthetic and Natural
SVG	Scalable Vector Graphics
UI	User Interface
VCR	Video Cassette Recorder
VM	Virtual Machine
XHTML	Extensible HyperText Markup Language
XML	eXtensible Mark-up Language

5 Requirements for IPTV Multimedia Application Platform

The following requirements are duplicates of those identified in IPTV services requirements [FG IPTV-DOC-0147] and should not be modified in any way without consultation with the group (i.e. study group question) which owns [FG IPTV-DOC-0147]. In the case of a discrepancy between the text in this document and that of [FG IPTV-DOC-0147], then the latter text should take precedence.

5.1 Architecture

- The IPTV architecture is required to support the end-user ability to see the associated information (e.g. by pressing a specific remote control key) and to act upon it (e.g. to follow the link, to make a choice, to bet, to return). (6.5.1.8)
- The IPTV architecture is required to support the ability to search for available content [ATIS-0800002]. (6.6.1)
- The IPTV architecture is required to have the capability to support information about the content available to the end user [ATIS-0800002]. (6.6.1)
- The IPTV architecture is recommended to facilitate the acquisition of content – e.g., VOD, Advertising [ATIS-0800002]. (6.6.1)
- The IPTV architecture is not recommended to preclude supporting the requirements related to the retransmission of the existing terrestrial, satellite and cable broadcast such as regional and regulatory. (6.6.1)
- The IPTV architecture is recommended to support middleware transparency aiming to decouple business functionality from middleware-specific functionality which allows developers to change middleware application elements without significantly modifying business functionality for IPTV services. (6.6.2.1)
- The IPTV architecture is recommended to support mechanisms for the end-user to log advertisement information of interest [ATIS-0800002]. (6.6.2.1)
- The IPTV architecture is recommended to support the APIs to manage the resources for applications [ATIS-0800002]. (6.6.2.2)

5.2 Middleware

- The IPTV middleware is required to support terminal device start-up and initialization function. (6.6.2.1)
- The IPTV middleware is required to support server-side device start-up and initialization function. (6.6.2.1)
- The IPTV middleware is required to provide an API for stopping and starting the presentation of video and audio. (6.6.2.2)
- The IPTV middleware is required to provide an API to communicate with IPTV services providers to implement media transmission and media control function. (6.6.2.2)
- The IPTV middleware is required to provide the API to access metadata information. (6.6.2.2)
- The IPTV terminal device is recommended to support remote management. (6.5.2.11)
- The IPTV terminal device is recommended to support log management. (6.5.2.11)

- The IPTV terminal device is recommended to support software version management. (6.5.2.11)
- The IPTV terminal device is recommended to support server parameter configuration. (6.5.2.11)
- The IPTV terminal device is recommended to support access mode and parameter configuration. (6.5.2.11)
- The IPTV terminal device is recommended to support media device parameter configuration, such decoder. (6.5.2.11)
- The IPTV terminal device is recommended to support subscriber configuration, such as access account, service account. (6.5.2.11)
- The IPTV terminal device is recommended to support monitoring and management of terminal resources. (6.5.2.12)
- The IPTV terminal device is recommended to support allocation and scheduling of terminal resource to application. (6.5.2.12)
- The IPTV middleware is recommended to support pause in a DVR capable terminal or system. (6.6.2.1)
- The IPTV middleware is recommended to manage skip forward and skip backward (e.g. by time period, interval, location in content, etc.). (6.6.2.1)
- The IPTV middleware is recommended to support executing of multiple simultaneous applications [DVB-MHP]. (6.6.2.1)
- The IPTV middleware components are recommended to facilitate service processes interaction among one or more IPTV devices (e.g. a server and its clients, such as STB, security system, or VoD server) in an IPTV system. (6.6.2.1)
- The IPTV middleware is recommended to be able to manage the information about the applications. (6.6.2.1)
- The IPTV middleware is recommended to support an API to access information on removable storage device (e.g. USB key). (6.6.2.2)
- The IPTV middleware is recommended to support the API for controlling (e.g. selection, showing and hiding) subtitle and closed captioning display [ATIS-0800002]. (6.6.2.2)
- The IPTV middleware is recommended to provide an API for DRM function to communicate with DRM system. (6.6.2.2)
- The IPTV middleware is recommended to include an API to access user preferences (e.g. accessibility features and display settings) available on a removable storage device (e.g. smartcard). (6.6.2.2)
- The IPTV middleware is recommended to provide service enabling API. (6.6.2.2)
- The IPTV middleware APIs are recommended to be open, flexible, granular, self-contained and components-based. (6.6.2.2)
- The IPTV middleware is recommended to provide an API to support a variety of mixed media formats to be presented together (e.g. an HTML text page embedding a video stream). (6.6.2.2)
- The IPTV middleware is recommended to provide an API to support picture-in-picture. (6.6.2.2)
- The IPTV middleware is recommended to support application management (e.g. applications lifecycles, applications states). (6.6.2.2)

- The IPTV middleware is recommended to be hardware and OS independent. (6.6.2.2)
- The IPTV middleware is recommended to provide an API to manage captioning including the selection from a range of languages, speed and verbosity. (6.6.2.3)
- The IPTV middleware is recommended to support a means to change the style of EPG. (6.6.5)
- The IPTV middleware is recommended to support the ability of the ITF to declare its usage environment description to the service provider. (6.6.6)
- The IPTV middleware is recommended to support the ability of the ITF to obtain the usage environment description from the service provider. (6.6.6)
- The IPTV middleware can optionally support the decoding of SI (Service Information). (6.6.2.1)
- The IPTV middleware can optionally support capabilities to run value-added applications. (6.6.2.1)
- The IPTV middleware can optionally support shortcut mechanism for selection. (6.6.2.1)
- The IPTV middleware can optionally support the presentation engine for the multimedia data (e.g. audio, video, graphics, text and images) providing the browsing, the synchronization, the interaction with the user, of such data. (6.6.2.1)
- The IPTV middleware can optionally support the API to communicate with IPTV services providers [ATIS-0800002]. (6.6.2.2)
- The IPTV middleware can optionally provide an API for recording programs locally. (6.6.2.2)

5.3 Terminal Device

- The IPTV middleware, if trick mode is supported, is required to support play, pause and stop. (6.6.2.1)
- The IPTV terminal device is recommended to offer to the end-user a service navigation capability based on the metadata for the services available through each network e.g. RF tuning information. (6.5.2)
- The IPTV terminal device is recommended to support receiving and dispatching event from end-user to application. (6.5.2.10)

6 Standards for Declarative Application Platforms

This clause describes the standards for declarative application platforms without implying any specific order or preferences but in an alphabetical order.

The declarative application platform is a framework on which applications written by markup language (e.g. HTML) with or without script language (e.g. ECMAScript) can run.

6.1 Binary Format for Scene (BIFS)

BIFS [ISO/IEC 14496-11] is the scene description language standardized by ISO as a part of MPEG-4 standard. It is designed to allow for the efficient representation of dynamic and interactive presentations, comprising two and three dimensional (2D & 3D) graphics, images, text and audiovisual material. The representation of such a presentation includes the description of the spatial and temporal organization of the different scene components as well as user-interaction and animations.

The main features of MPEG-4 BIFS are the following:

- Seamless embedding of audio/video content. MPEG-4 BIFS allows integration and control of different audio/video objects seamlessly in a scene.
- Rich set of 2D/3D graphical constructs: MPEG-4 BIFS provides a rich set of graphical constructs which enable 2D and 3D graphics. BIFS also provides tools that enable easy authoring of complex Face and Body Animation, tools for 3D mesh encoding, and representation of 2D and 3D natural and synthetic sound models.
- Local and Remote Interactivity: BIFS defines elements that can interact with the client-side scene as well as with remote servers. Interactive elements allow for text input, mouse events, and other input devices that can trigger a variety of behaviours.
- Local and Remote Animations: Scene properties, such as object positions, colours, and even shapes, etc., can be animated using either predefined scene descriptions or via streams sent from a server.
- Reuse of Content: MPEG-4 scenes can contain references to streamed sub-scenes. That means that content can easily be reused, a powerful way to create a very rich user experience from relatively simple building blocks.
- Scripted Behaviour: MPEG-4 scenes can have two types of scripted behaviour. A Java API can control and manipulate the scene graph, as well as built-in ECMA script (javascript) support that can be used to create complex behaviours, animations, and interactivity.
- Streamable scene-description: the spatial and temporal graphic layout is carried in a BIFS-Command stream. Such a stream operates on the scene-graph through commands which replace, delete and insert elements in the scene-graph.
- Accurate synchronization. Audio/visual content can be tightly synchronized with other A/V content, client-side, and server-driven scene animation, due to the underlying MPEG-4 Systems layer.
- Compression: the scene description is converted to binary data and compressed in an efficient way.

The diagram below summarizes the different components of BIFS.

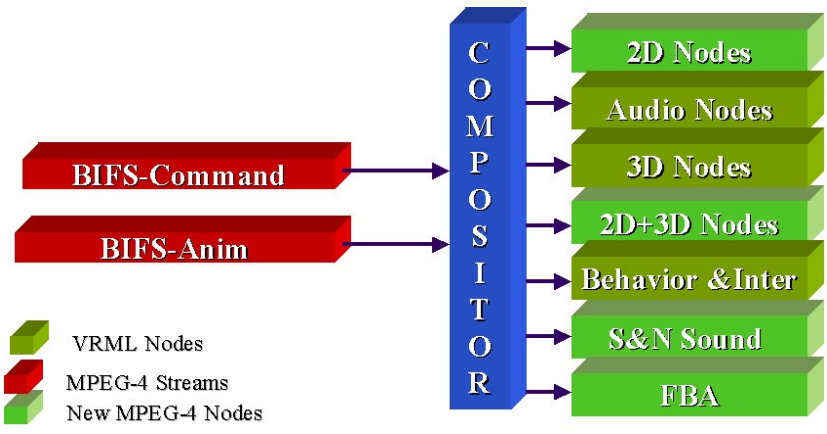


Figure 6-1: MPEG-4 Scene Description

6.2 Broadcasting Markup language (BML)

BML [ARIB STD-B24] [ITU-T J.201] is a declarative application specification for multimedia broadcasting in Japan standardized by Association of Radio Industries and Businesses (ARIB). BML consists of XHTML, CSS, Document Object Model (DOM) and ECMAScript. BML was revised to include additional functionalities for receivers with digital storage and for terrestrial digital broadcasting including mobile reception.

The specification of Terrestrial Integrated Services Digital Broadcasting (ISDB-T) multimedia coding scheme was first based on that of Multimedia and Hypermedia information coding Experts Group (MHEG). But since March 1999, Association of ARIB started developing an XML specification for multimedia coding scheme based on the functionalities of MHEG. This contributed to the development of an XML application language, BML that enables the presentation of an XML file on BML browsers. The ARIB data broadcasting system standards were enacted as BML in October 1999.

BML application can be based on synchronization and spatial-temporal relationships of multiple media formats, structural composition, event-action associations, navigation, and user interaction capabilities just as MHEG. BML defines additional API and object for broadcasting using ECMAScript.

The semantics of BML is based on the following minimum set of MHEG classes:

- Application Class
- Scene Class
- Link Class
- Action Class

BML is applied to reference model for data broadcasting service that is carried out as part of the digital broadcasting. The following figure shows the structure of BML.

- Data Coding
  - Coding mono-media (1): Coding system for character string and bit map, etc. used in multimedia is specified.
  - Coding of subtitle, superimpose (2): Coding system for subtitle and superimpose is specified.
- XML-based Multimedia Coding Scheme
  - Multimedia Coding (3): Coding system of XML based system adopted as multimedia coding system and its profile is specified.
- Data Transmission Specification
  - Content transmission format (4): Content transmission format of data carousel transmission method, etc. to transmit content is specified.
  - Subtitle and superimpose transmission format (5): Independent PES transmission format to transmit subtitle and superimpose is specified.

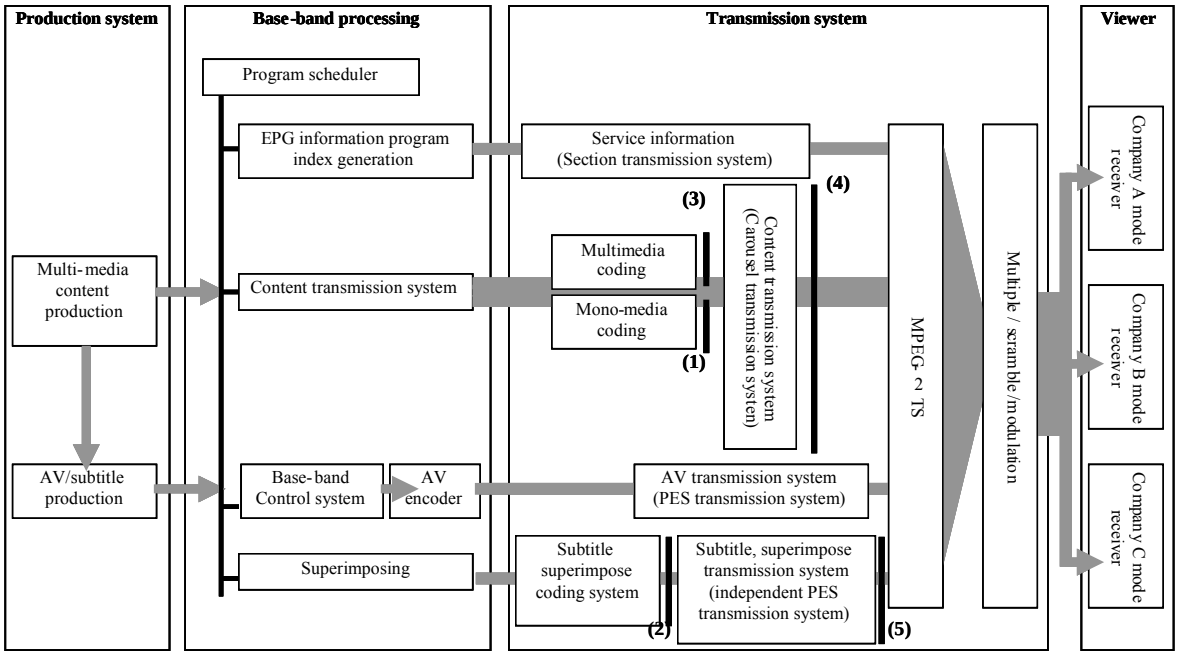


Figure 6-2: System Structure of BML

6.3 CEA-2014

CEA-2014 is a Remote User Interface specification that allows a user interface to be remotely displayed on devices. It is based on existing web rendering technologies for consumer electronics (CE) browser with Worldwide Web Consortium (W3C) tags, XHTML 1, ECMA-262, CSS TV profile and DOM 2. CEA-2014 is a web-based protocol and framework for Remote user interface (UI) on UPnP Home Network and over Internet. It defines two service domains of CEA-2014 as in Figure 6-3.

CEA-2014 defines the mechanisms allowing a user interface to be remotely displayed on and controlled by devices or control points other than the one hosting the logic. The basic device operations are based on the UPnP Device Architecture v1.0 for UPnP networks and UPnP devices in the home. The standard also allows the remote display of user interfaces provided by third party internet services on UPnP devices in the home, and covers UI capabilities for TVs, mobile phones and portable devices.

A major component of CEA-2014 is the CE-HTML profile that uses XHTML content to define user interfaces that can be rendered on screens with different resolutions and sizes ranging from HDTV screens to mobile-phone displays.

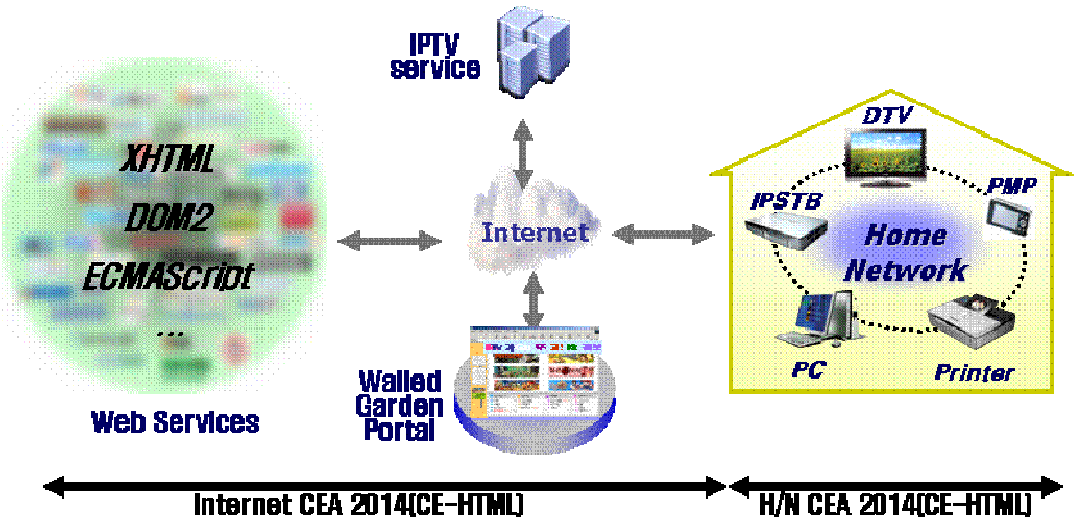


Figure 6-3: Service Model of CEA-2014 (Remote User Interface)

6.4 Cascading Style Sheet (CSS)

CSS is a style sheet language specified by W3C that is used to describe the presentation (e.g. fonts, colours and spacing) of a document written in a markup language. CSS is human readable and writable, and expresses style in common desktop publishing terminology.

CSS has been in use since October 1995 using the Media Type text/css without registration.

A CSS can be either linked to a document through a URI or included in the document.

A superset of [CSS1], [CSS2] includes a number of new capabilities like absolute, relative, and fixed positioning of elements, the concept of media types, support for aural style sheets and bidirectional text, and new font properties such as shadows.

[CSS TV Profile] specification defines a subset of [CSS2]: e.g. colour specifications tailored to TV devices.

6.5 Document Object Model (DOM)

DOM 2.0 [DOM 2] defines the Document Object Model Level 2 Core, a platform- and language-neutral interface that allows programs and scripts to dynamically access and update the content and structure of documents. The Document Object Model Level 2 Core builds on the Document Object Model Level 1 Core.

The DOM Level 2 Core is made of a set of core interfaces to create and manipulate the structure and contents of a document. The Core also contains specialized interfaces dedicated to XML.

6.6 Digital Video Broadcasting HyperText Markup Language (DVB-HTML)

Digital Video Broadcasting HyperText Markup Language (DVB-HTML) [ITU-T J.201] is a standard for allowing digital televisions to access internet content. It is an optional part of the larger MHP1.1 standard of DVB.

The specification is based around a modularized version of XHTML 1.1, and also includes CSS 2.0, DOM 2.0, and ECMAScript (also known as JavaScript).

Among other things, MHP 1.1 specifies the Internet Access profile, in which applications can control the basic operations of Open Internet resident clients (Web browser, e-mail and news client).

The figure below outlines the basic architecture of MHP 1.1 and the relationship between the DVB-HTML optional application type and the DVB-J application type.

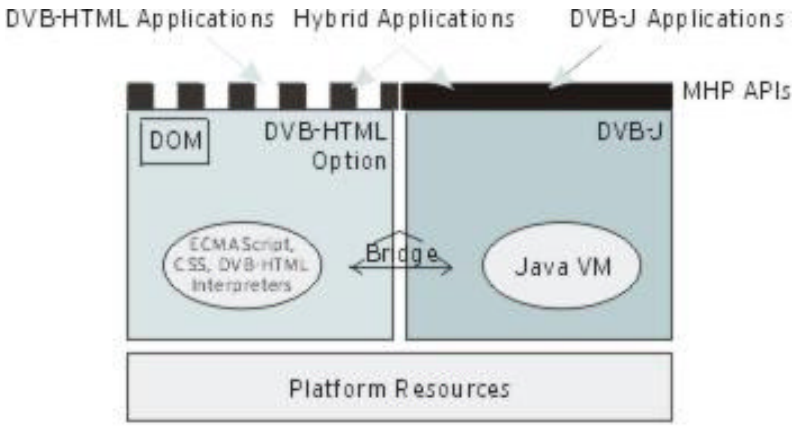


Figure 6-4: MHP 1.1 and DVB-HTML

6.7 ECMAScript

ECMAScript [ECMA-262] is a scripting programming language, standardized by European computer manufacturers association (ECMA) International in the [ECMA-262] specification. The language is used on the Web and is often referred to as JavaScript or JScript, after the two primary implementations of the specification.

ECMAScript is supported in many applications. ECMAScript is also included as a component in many presentation engines (PE) such as BML and DVB-HTML, which are used for digital data broadcasting. Some implementations have a completely different set of libraries; making applications written in one dialect of ECMAScript will not necessarily work in another.

ECMAScript is an object-oriented programming language for performing computations and manipulating computational objects within a host environment. It was originally designed to be a web scripting language, providing a mechanism to enliven web pages in browsers and to perform server computation as part of a web-based client-server architecture.

A web browser provides an ECMAScript host environment for client-side computation including, for example, objects that represent windows, menus, pop-ups, dialog boxes, text areas, anchors, frames, history, cookies, and input/output. Further, the host environment provides a means to attach scripting code to events such as change of focus, page and image loading, unloading, error and abort, selection, form submission, and mouse actions. Scripting code appears within the HTML and the displayed page is a combination of user interface elements and fixed and computed text and images. The scripting code is reactive to user interaction and there is no need for a main program.

A web server provides a different host environment for server-side computation including objects representing requests, clients, and files; and mechanism to lock and share data. By using browser-side and server-side scripting together, it is possible to distribute computation between the client and server while providing a customised user interface for a web-based applications.

6.8 Lightweight Application Scene Representation (LASeR) & Simple Aggregation Format (SAF)

[ISO/IEC 14496-20] (MPEG-4 Part 20) is a specification designed for representing and delivering rich-media services to resource-constrained devices such as mobile phones. It defines two binary formats: LASeR, a binary format for encoding 2D scenes, including vector graphics, and timed modifications of the scene; and SAF, Simple Aggregation Format, a binary format for aggregating in a single stream LASeR content with audio/video streams.

The LASeR specification has been designed to allow the representation of 2D scenes describing rich-media services for constrained devices. A rich-media service features a dynamic and interactive presentation comprising 2D vector graphics, images, text and audiovisual material. The representation of such a presentation includes describing the spatial and temporal organization of its different elements as well as its possible interactions and animations.

The SAF specification defines tools to enable the transport of LASeR content along with its attached audiovisual material according to these requirements. The SAF specification defines a binary format for a SAF stream, made of a LASeR stream with any type of media stream. SAF streams can be delivered using many delivery mechanisms: download-and-play, progressive download, streaming or broadcasting. To achieve reactivity, the SAF specification defines the concept of cache unit which allows sending in advance sub-content which will be used later on in the presentation.

6.9 Lua

The Lua programming language [ABNT NBR 15606-2] is a lightweight, reflective, imperative and procedural language, designed as a scripting language with extensible semantics as a primary goal.

Lua combines simple procedural syntax with powerful data description constructs based on associative arrays and extensible semantics. Lua is dynamically typed, runs by interpreting byte-code for a register-based virtual machine, and has automatic memory management with incremental garbage collection.

Lua has a compiled binary format. It is currently mainly used for gaming development. Lua scripts can also be embedded in NCL applications, supported by Brazilian Terrestrial Digital TV middleware, Ginga.

6.10 MHEG-5

MHEG-5 [ITU-T T.170] [ITU-T T.172] [ITU-T T.175] [ISO/IEC 13522-5] [ETSI ES 202 184] represents an application, as a set of scenes, which contain objects common to all scenes. A multimedia application can be conceived as a set of self-contained objects based on synchronization and spatial-temporal relationships of multiple media formats, structural composition, event-action associations, navigation, and user interaction capabilities. Controlling the playback of time-dependent contents, like streams of multiplexed audiovisual data requires specific support. These streams demand video cassette recorder (VCR) control functions (play, pause, fast forward, and so on), as well as the capability to manage events generated during their presentation. For example, rendering text subtitles can be synchronized with time code events generated during the playback of a stream.

A scene supports the spatially and temporally coordinated presentation of audiovisual content consisting of graphics, bitmaps, text, and streams (based on the multiplex of audio and video components). Interaction can be performed via graphic elements like buttons, sliders, text entry boxes, and hypertext selections. Every scene, as well as an entire application, is a self-contained entity that can represent its localized behaviour by links that are event-action associations. Events can be generated by users, expiration of timers, playback of streams, and other conditions within the run-time environment.

The global scope of MHEG-5 is to define the syntax and semantics of a set of object classes that can be used for interoperability of multimedia applications across minimal-resources platforms. The developed applications will reside on a server, and as portions of the application are needed, they will be downloaded to the client. In a broadcast environment, this download mechanism could rely, for instance, on cyclic rebroadcast of all portions of the application. It is the responsibility of the client to have a runtime that interprets the application parts, presents the application to the user, and handles the local interaction with the user.

6.11 Nested Context Language (NCL)

NCL [ABNT NBR 15606-2] is a declarative language for hypermedia document authoring. Based on an XML application language, it focuses on how media objects are structured and related in time and space. As a glue language, NCL does not restrict or prescribe the media-object content types, and it can include an XHTML-based media object, as defined in other common DTV standards.

An NCL document is represented by a composite node, which can contain a set of media nodes or other composite nodes, recursively. Composite nodes may also contain a set of links relating its component nodes. The composition element, representing a composite node, is defined in the *Basic Composition* module of NCL. In order to allow the creation of links touching node content parts (anchors) or node attributes, the language provides the definition of interface points. For composite nodes, an interface point called *port* can export an interface point of one of its component nodes. Interface point elements are defined in the NCL Interfaces functional area.

Anchors are defined via the area element, which extends the syntax and semantics of the homonym element defined by SMIL and XHTML. Besides allowing the specification of anchors representing spatial portions, through the *coords* attribute (as in XHTML), and the definition of anchors representing temporal portions, through *begin*, *end* and *duration* (as in SMIL), the *area* element permits the definition of textual anchors. NCL links are created by making reference to a hypermedia connector, which defines the relation type without defining the related participants, thus, a link must also define a set of binds associating connector roles to node interface points (the link participants). Since a composite node *port* exports an interface point of an internal node, links among nodes contained in different compositions can be defined.

6.12 Scalable Vector Graphics (SVG)

SVG [SVG 1.1] is a language for describing two-dimensional graphics and graphical applications in XML. SVG allows for three types of graphic objects: vector graphic shapes (e.g., paths consisting of straight lines and curves), images and text. Graphical objects can be grouped, styled, transformed and composited into previously rendered objects. The feature set includes nested transformations, clipping paths, alpha masks, filter effects and template objects.

SVG drawings can be interactive and dynamic. Animations can be defined and triggered either declaratively (i.e., by embedding SVG animation elements in SVG content) or via scripting. Sophisticated applications of SVG are possible by use of a supplemental scripting language which accesses SVG DOM), which provides complete access to all elements, attributes and properties.

SVG Basic and SVG Tiny are targeted to resource-limited devices and are part of the 3GPP platform for third generation mobile phones. SVG Print is a set of guidelines to produce final-form documents in XML suitable for archiving and printing.

7 Standards for Procedural Application Platforms

This clause describes the standards for procedural application platforms without implying any specific order or preferences but in an alphabetical order.

The procedural application platform is a framework on which applications written by APIs based on procedural language (e.g. Java) can run.

7.1 GEM-based Application Platforms

Globally Executable MHP (GEM) [ETSI TS 102 819] specifies the core of Blu-ray's BD-J, OCAP and MHP. For broadcast, it can best be thought of as the overlap between the MHP and OCAP standards for interactive television. It's a formally standardized Java-based platform for interactive content and applications. GEM has been standardized by DVB, and adopted by ETSI, the ITU, CableLabs, ARIB, ACAP, Ginga, and the Blu-ray Disc Association.

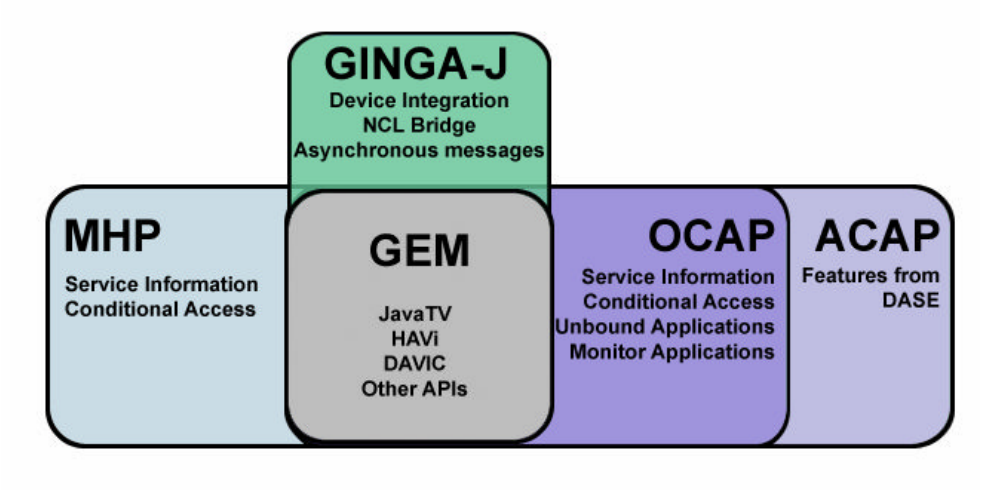


Figure 7-1: GEM-based Standards for Multimedia Application Platforms

Advanced Common Application Platform (ACAP)

ACAP [A/101] [ITU-T J.201] is applicable for specifications and standards based on the ACAP APIs, content formats, and semantic guarantees.

ACAP Applications are classified into two categories depending upon whether the initial application content processed is of a procedural or a declarative nature. These categories of applications are referred to as a procedural (ACAP-J) and declarative (ACAP-X) applications, respectively. An example of an ACAP-J application is a Java TV™ Xlet composed of compiled JavaTM byte code in conjunction with other multimedia content such as graphic, video, and audio. An example of an ACAP-X application is a multimedia document composed of Extensible HyperText Markup Language (XHTML) markup, style rules, scripts, and embedded graphics, video, and audio.

Application environments are similarly classified into two categories depending upon whether they process procedural or declarative applications. These categories are referred to as ACA-J and ACAP-X environments, respectively. An example of an ACAP-J environment is a Java Virtual Machine and its associated API implementation. An example of an ACAP-X environment is an XHTML multimedia document browser, also known as a user agent.

The architecture and facilities of the ACAP standard are intended to apply to broadcast systems and receivers for terrestrial (over-the-air) broadcast and cable TV systems.

ACAP is primarily based on GEM and Digital Television Application Software Environment (DASE), and includes additional functionality from OCAP. The followings are the relevant specifications which ACAP includes:

- Globally Executable MHP (GEM): ACAP includes GEM 1.0.2 in its entirety, except as explicitly modified by the ACAP.
- Open Cable Application Platform (OCAP): ACAP includes OCAP 1.0 in its entirety, except as explicitly modified by the ACAP for ACAP terminal operating in a terrestrial broadcast environment.
- Addition on Non-ACAP Interfaces: Terminal Specifications based on ACAP may add public interfaces, provided that they are added in a namespace that does not conflict with ACAP. ACAP terminal specifications and ACAP terminals shall not require that such extension interfaces be called by ACAP applications in order to enable behaviour that is normatively required by ACAP standard.

GINGA

Brazilian's middleware choice is called Ginga, which is part of *Sistema Brasileiro de TV Digital – Terrestre* (SBTVD-T), (Brazilian Digital TV System – Terrestrial), the Brazilian's official standard for Terrestrial Digital TV. The applications that can be run on Ginga are classified into two categories depending upon whether the initial application content – these two categories of applications are referred to as declarative and procedural applications. Application environments are similarly classified into two categories depending upon whether they process declarative or procedural applications, and are called Ginga-NCL [ABNT NBR 15606-2] and Ginga-J [ABNT NBR 15606-4], which are registered with *Associação Brasileira de Normas Técnicas* (ABNT), Brazilian Association of Technical Standardization.

Ginga-NCL is a logical subsystem of the Ginga System that processes Nested Context Language (NCL) documents, and it is adherent to [ITU J.201] Recommendation. A key component of Ginga-NCL is the declarative content decoding engine (NCL formatter). The NCL Formatter is in charge of receiving an NCL document and controlling its presentation, trying to guarantee that the specified relationships among media objects are respected. The formatter deals with NCL documents that are collected inside a data structure known as private base. Ginga associates a private base with a TV channel. NCL documents in a private base can be started, paused, resumed, stopped, and can reference each other. Other important modules are the XHTML-based user agent, which includes a stylesheet (CSS) and ECMAScript interpreter, and the Lua engine, which is responsible for interpreting Lua scripts.

Ginga-J [ABNT NBR 15606-4] is an application interface that includes all required Java APIs, content and data formats, and protocols up to the application level. Applications developed over the Ginga-J specification are executed and/or displayed on SBTVD-T certified host devices. The Ginga-J specification allows individual terrestrial television operators to deploy their custom applications and services on all SBTVD-T compliant host devices connected to their networks. Ginga-J includes GEM 1.1 specification [ETSI TS 102 819] as its base, and uses the Service Information APIs from [ARIB STD-B23], which was a natural choice, since Brazilian Digital TV system uses the ISDB-T modulation standard. Additionally, it incorporates some APIs providing functionalities for the development of digital TV applications combining resources from other devices such as mobile phones and PDAs.

ITU-R BT.1699

[ITU-R BT.1699] identifies functional commonality among the declarative application environments for interactive TV application specifications ACAP-X, BML and DVB-HTML. Elements which are common to these three standards are identified as a "Common Core". The value of the Common Core is to assist program authors to exchange declarative content internationally using these standards. This Recommendation also notes features outside of the Common Core of the covered standards. The goal of [ITU-R BT.1699] is to note these differences to encourage efforts toward increasing commonality between the standards to further improve functionality and enhance economies of scale.

[ITU-R BT.1699] is intended to harmonize the application environment for declarative content for interactive TV. It specifies common elements, media types and APIs at the syntactic level of the declarative application environment to satisfy regional application requirements for the three standards ACAP-X, BML and DVB-HTML as specified in the normative references. It is noted that there are other declarative formats such as MHEG-5 and Society of Motion Picture Television Engineers (SMPTE) DDE-T, which are not covered in [ITU-R BT.1699].

ITU-R BT.1722

[ITU-R BT.1722] defines APIs, semantic guarantees and system aspects of platform behaviour for the harmonized instruction set for the execution engines for interactive TV applications.

Revision of Recommendation [ITU-R BT.1722] includes the following updated and newly developed instruction set for the execution engines: GEM, MHP 1.0 and 1.1, OCAP 1.0, ARIB-AE and ACAP. Harmonization is based on GEM 1.0.1 which has been developed with contributions from DVB, SCTE, ARIB and ATSC. GEM 1.0.1 is the normative reference in Recommendation [ITU-R BT.1722].

Multimedia Home Platform (MHP)

MHP [ETSI TS 102 812] is the set of specifications for multimedia broadcasting that has been developed by the DVB Project. MHP has two functional categories. The version 1.0 series covers the execution engine (EE) environment and the version 1.1 series covers the presentation engine (PE) environment in addition to version 1.0. The PE portion of the version 1.1 series is not standalone; it mandates the existence of the EE environment. The first release of the DVB MHP version 1.0 series was May 2000. The MHP 1.0 specification employs Java technology for an EE environment.

Open Cable Application Platform (OCAP)

OCAP [ANSI/SCTE 90-1] is the set of specifications for the interactive multimedia services of digital CATV that has been developed by the OpenCable project managed. OCAP 1.0 is based on MHP 1.0.2, and includes the extensions for the cable system in USA.

8 Other Related Standards

8.1 MPEG Multimedia Middleware (M3W)

M3W [ISO/IEC 23004] provides, next to the architecture and component model descriptions and the reference software, two sets of APIs, Multimedia platform APIs, the functional APIs, and Support platform APIs, the non-functional APIs:

- The architecture and component model:
  - Part-1: Architecture
  - Part-3: Component Model
- The functional APIs:
  - Part-2: Multimedia API
- The non-functional APIs:
  - Part-4: Resource and Quality Management
  - Part-5: Component Download
  - Part-6: Fault Management
  - Part-7: System Integrity Management
- The reference software:
  - Part-8: Reference Software

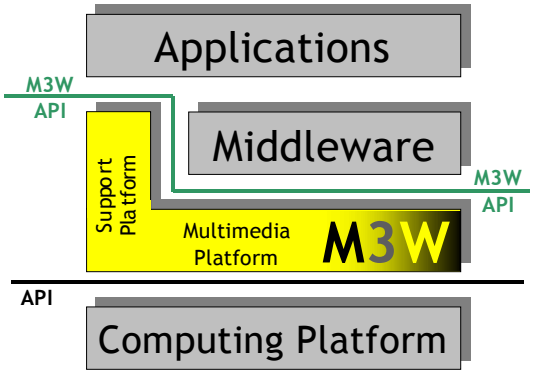


Figure 8-1: The Structure of M3W

M3W Multimedia platform APIs defines mainly audio and video processing APIs handling front-end, decoders and post-processing of A/V and trust management APIs handling Key Management, Signature Management, Licence Management, and Certificate Management. The M3W Multimedia APIs offer a high-level API that is independent of the target hardware. By standardizing things that are common, the Multimedia APIs let developers focus on innovation and reduce time to market without limiting product differentiation. It simplifies the work of middleware and application developers because it is designed from what they need, rather than simply reflecting how a particular product's hardware and software happens to be implemented.

Appendix I

Comparison of some multimedia application platforms

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

Table I-1: Comparison of some multimedia application platforms

	Presentation Engine (PE)		**Execution Engine (EE)**	**Mono-media**			
ARIB-BML	Spec.	BML		Video	Graphics	Audio	Character
	Components	XHTML1.0 CSS1/2 DOM1/2 ECMAScript		MPEG-2 MPEG-1 MPEG-4 H.264	JPEG MPEG-2 I(frame) PNG MNG GIF MPEG-4 I(VOP) H.264 I (Picture)	MPEG-2 AIFF-C MPEG-4	EUC-JP (8bit)
ATSC-ACAP	Spec.	XDML	Java	MPEG-2	JPEG PNG MNG (ACAP-X only)	AC-3 PCM	UTF-8
	Components	XHTML1.0 CSS2 DOM2					
DVB-MHP	Spec.	DVB-HTML	DVB-J	MPEG-2	JPEG MPEG-2 I(Intra) PNG GIF	MPEG-1	UTF-8
	Components	XHTML1.0 CSS2, DOM2 ECMAScript	Java				
OpenCable-OCAP	Spec.	OCAP HTML	Java	MPEG-2	JPEG MPEG-2 I (Intra) PNG, GIF Animated GIF SWF	MPEG-1 AC3 WAVE MS-PCM Format	UTF-8
	Components	HTML1.0 CSS2 DOM1/2 ECMAScript					

Appendix II

Worldwide TV Markup Language (WTVML)

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

Worldwide TV Markup Language (WTVML)

Worldwide TV Mark-up Language (WTVML) [ETSI TS 102 322] is a content format for the delivery of Interactive TV applications using Internet Servers. A WTVML Interactive television technology platform comprises a micro-browser, a markup language, and a significant collection of associated software tools and services. The micro-browser and markup language are both based upon the Open Mobile Alliance WML 1.3 specification. It has all the required elements, attributes and events necessary to describe the user interface and user interaction models for the majority of Interactive TV services.

The format supports key features to enable service-oriented applications and also provides a balance between the explicit layout and design requirements necessary for television and flexibility and dynamic capabilities of the Internet. The format fully describes the rendering and interaction of the Interactive TV service in such a manner as to allow its implementation in a number of different mechanisms and technologies. The format assumes a user agent behaviour that is more sophisticated and more stateful than a standard internet based HTML browser.

The format combines explicit pixel-perfect control required for TV user interfaces, and the dynamic layout and internet compatibility requirements necessary for e-business and dynamic content. It provides a good separation between the layout of high level objects, and the dynamic layout of elements in the main mark-up language. This separation also allows for the default attribute values to be set for a given layout, effectively creating sets of inherited styles. One useful by product of this separation is the ability to deploy the service in a functionally identical way by interoperating differently or replacing the high level layout for different device types.

The format assumes a rich event model, and contains explicit state and variable management, allowing sophisticated user interface effects to be created without the use of scripting.

It is common to implement WTVML functionality by way of a micro-browser and gateway architecture. In this architecture, the gateway processes the raw WTVML and generates compiled byte-code to be passed to the user agent to execute. It is expected that different networks may implement their own output formats from the gateway, consisting of WTVML byte-codes extended from the standard WAP Forum byte codes, HTML and Javascript, Java execution classes or even code that can be run directly on legacy set-top boxes middleware or APIs.

Bibliography

[b-ITU-T J.202] ITU-T Recommendation J.202 Rev. 2 (2007), Harmonization of procedural content format for interactive TV applications.

[b-ETSI TS 102 543] ETSI TS 102 543 (2007), Digital Video Broadcasting (DVB) Globally Executable MHP (GEM).

II.7 IPTV VOCABULARY OF TERMS

IPTV vocabulary of terms

1 Scope

This document provides vocabulary of terms presently used in FG IPTV documents. The main purpose of this document is twofold. First, it is a place holder for all IPTV-related terms and their definition presently under discussion in FG IPTV. Second, it highlights terms, if any, which have been defined differently. This document holds definitions of all terms used in FG IPTV documents which have been approved in the appropriate working group at this FG IPTV meeting. It should be emphasized that the ownership of terms belongs to the working group where the term is defined. That is, any contribution suggesting changes to the definitions shall be addressed against the document which holds the definition of the specific term.

2 References

FG IPTV-DOC-0147 (15-19 October 2007), IPTV services requirements

FG IPTV-DOC-0181 (11-18 December 2007), IPTV architecture

FG IPTV-DOC-0182 (11-18 December 2007), IPTV service scenarios

FG IPTV-DOC-0184 (11-18 December 2007), Quality of experience requirements for IPTV

FG IPTV-DOC-0185 (11-18 December 2007), Traffic Management Mechanisms for the Support of IPTV Services

FG IPTV-DOC-0188 (11-18 December 2007), IPTV security aspects

FG IPTV-DOC-0189 (11-18 December 2007), IPTV Network Control Aspects

FG IPTV-DOC-0190 (11-18 December 2007), IPTV multicast frameworks

FG IPTV-DOC-0192 (11-18 December 2007), Aspects of IPTV end system – Terminal device

FG IPTV-DOC-0193 (11-18 December 2007), Aspects of home network supporting IPTV services

FG IPTV-DOC-0194 (11-18 December 2007), IPTV middleware, application and content platforms

FG IPTV-DOC-0195 (11-18 December 2007), Toolbox for content coding

FG IPTV-DOC-0196 (11-18 December 2007), IPTV middleware

FG IPTV-DOC-0197 (11-18 December 2007), IPTV metadata

3 Conventions

In this document:

[aaa] notation after title of a term indicates source of the definition for that term.

(DOC-xxxx) notation before title of a term indicates the document from which the term and its definition have been obtained. A list of all documents used to compile the terms is provided in clause 2 of this document.

4 Terms and their definitions

(DOC-0188) Access Control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

(DOC-0188) Accessibility [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

(DOC-0147) Accessibility feature: An additional content component that is intended to assist people hindered in their ability to perceive an aspect of the main content. Examples: captions for the hard of hearing, subtitles in various languages, sign-language interpretation video and descriptive audio.

(DOC-0147) and (DOC-0188) Acquisition: The process of obtaining content by the end-user.

NOTE – For content with accessibility features this means that the content will be available in a form that can be used by the end-user.

(DOC-0185) Admission control: The mechanism that controls the traffic to be admitted into the network.

(DOC-0194) Application [ITU-T Y.101]: A functional implementation realized as software running in one or spread over several interplaying hardware entities.

(DOC-0194) Application instance: An occurrence of an application.

(DOC-0194) Application manager [ITU-T J.200]: The entity that is responsible for managing the lifecycle of the applications. It manages applications running in both the Presentation engine and Execution engine if both are present.

(DOC-0194) Application Programming Interface (API): Consists of software libraries that provide uniform access to system services. [ITU-T J.200].

NOTE – In the case of middleware, it is an interface between application layer and middleware service which encapsulates the services offered by the middleware and enable application developer to develop new application.

(DOC-0182) Application provider: The application provider is the entity providing IPTV-related user applications.

(DOC-0147) Aspect ratio [ITU-T T.101]: The ratio of the width to the height of the image rectangular area.

(DOC-0147) Associated information services: TBD, examples of associated information services: links to other websites, betting, voting, etc.

(DOC-0147) Audio description: This service provides a commentary describing the visual events pertinent to the content and augments the dialog in the content.

NOTE – Audio description is primarily intended to assist users who are unable to see the video content clearly. The narrative passages fit between the dialogue and other significant audio content so as not to interfere with it. Ideally the user can control the volume and spatial positioning of the audio or derive it from a separate output.

(DOC-0188) Authentication [ITU-T X.800]: See Data Origin Authentication and Peer-Entity Authentication.

(DOC-0188) Authorization [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

(DOC-0147) and (DOC-0195) Bitstream: Coded representation of a video or audio signal.

(DOC-0147) and (DOC-0190) Broadcast [ITU-T M.60]: One-way transmission from one point to two or more other points.

(DOC-0147) and (DOC-0194) Broadcast TV: One-way transmission of TV signals from one point to two or more other points.

(DOC-0185) Buffer management: Buffer management deals with which packets, awaiting transmission, to store or drop.

(DOC-0147) Captions: Captions provide a real-time on-screen transcript of the dialogue as well as any sound effects.

NOTE – This service can be provided by means of either textual or graphical supplementary content. The captions and the dialogue are usually in the same language. The service is primarily to assist users having difficulty hearing the sound. Ideally, users may have some control over the position and size of the presentation. Different speakers are distinguished, usually by different colours.

(DOC-0147) Channel: Content formatted as a selectable set of data and transported as part of a data stream.

(DOC-0147) Channel changing: The act of changing from one channel to another.

(DOC-0147) and (DOC-0189) Channel zapping: The act of fast changing from one channel to another.

(DOC-0194) Character [ITU-T J.200]: A specific "letter" or other identifiable symbol, e.g. "A".

(DOC-0194) Character encoding [ITU-T J.200]: Mapping between an integer input value, and the textual character that is represented by this mapping, e.g. in ASCII value 65 (decimal) is character "A", or shift-JIS for Japanese characters.

(DOC-0194) Character set: See character encoding.

(DOC-0184) Clean Audio: Audio track of an IPTV Service with background sounds removed.

(DOC-0192) Client PVR (cPVR): An instance of PVR, where the end-user terminal device contains the recording capability that can be solicited and operated by end-users to record and store video, audio, and other associated data locally for subsequent playback.

(DOC-0147) Closed Captions: captions that can be switched on or off by the viewer.

(DOC-0147) Conditional Access: A synonym for Service Protection.

(DOC-0188) Conditional Access: The function served by a Conditional Access System; often used as an abbreviation for Conditional Access System.

(DOC-0188) Conditional Access System: A component of a Service and Content Protection system the purpose of which is to prevent unauthorized (unentitled) access to a service or to content.

(DOC-0188) Confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

(DOC-0189) Connection admission control: The mechanism that controls the traffic to be admitted into the network.

(DOC-0194) Content [ITU-T T.174]: Encoded generic value, media or non-media data.

(DOC-0182) Content aggregator: A player in the IPTV service delivery chain whose role is to aggregate content, e.g. to form a TV bouquet composed of several TV channels.

(DOC-0147) and (DOC-0188) Content protection: Ensuring that an end-user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder.

(DOC-0194) Content protection: Act of preventing unauthorized use of any content.

(DOC-0182) Content provider: The content provider is the entity owning contents or being licensed to sell content assets. Their role is contents delivery.

(DOC-0147), (DOC-0188) and (DOC-0192) Content tracing: A process to enable the identification of the (arbitrary) origin of content, and/or the responsible party (e.g. the end-user), to facilitate subsequent investigation in the event of unauthorized content copying or distribution.

(DOC-0147) Converged services [ITU-T Q.1702]: The integration of Internet, multimedia, e-mail, presence, instant messaging, m-commerce, etc., services with voice service.

(DOC-0185) Cross layer interaction: The ability of one layer adapting its performance based on information received from other layers.

(DOC-0188) Data Origin Authentication [ITU-T X.800]: The corroboration that the source of data received is as claimed.

(DOC-0147), (DOC-0190) and (DOC-0193) Delivery network gateway (DNG) [ATIS-0800002]: A device implementing the DNGF.

NOTE – DNG also is commonly referred to as the Residential Gateway (RG).

(DOC-0147) 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).

(DOC-0188) Denial of Service [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

(DOC-0188) Digital Rights Management: A synonym for Service and Content Protection or Content Protection, depending upon the context of use.

NOTE – In this document, the term Service and Content Protection is used instead of Digital Rights Management.

(DOC-0147) Digital Rights Management: A synonym for SCP.

(DOC-0188) Digital Signature [ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

(DOC-0192) Distributed PVR (dPVR): Multiple instances of PVR, where a combination of cPVRs and nPVRs can be used to record and store video, audio, and other associated data for subsequent playback. For example, this usually occurs within a Home Network containing multiple cPVRs in order to distribute storage of video, audio, and other data.

(DOC-0147), (DOC-0182) and (DOC-0189) Electronic program guide (EPG): A structured set of data, intended to provide information on available content that may be accessed by end-users.

(DOC-0194) Electronic Content Guide (ECG): A service navigation interface used especially for content streaming and download.

NOTE – It is sometimes used synonymously with EPG.

(DOC-0194) Electronic Program Guide (EPG): A service navigation interface which is used especially for programs.

NOTE – In some traditional Broadcast Services, EPG is defined as an on-screen guide used to display information on scheduled live broadcast television programs, allowing a viewer to navigate, select, and discover programs by time, title, channel, genre. This traditional definition does not cover "catalogues" for on-demand and download services (sometimes called ECG) and bi-directional interactive service (sometimes called IPG) for end-user interaction with a server or head-end.

Some EPGs utilize web-pages, or teletext to realize this function.

(DOC-0194) EPG provider [ITU-T J.90]: The entity that collects, collates and assembles the elements of information that constitute the EPG database.

(DOC-0194) Electronic Service Guide (ESG): A service navigation interface used especially for available services and contents.

(DOC-0147), (DOC-0189) and (DOC-0190) End-user [ITU-T J.112]: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

(DOC-0194) Execution engine (EE) [ITU-T J.200]: instructions and associated data and media content. An execution engine may be implemented with an operating system, computer language compilers, interpreters, and Application Interfaces (APIs), which a procedural application may use to present audiovisual content, interact with a user, or execute other tasks, which are not evident to the user. A common example of an execution engine is the JavaTV software environment, using the Java programming language and byte code interpreter, JavaTV APIs, and a Java Virtual Machine for program execution.

(DOC-0194) Extended channel: Means to organize different operation content together, including live channel, TVOD, information service, EPG and so on. For each extended channel, there is a related channel number.

(DOC-0181) Functional architecture [ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE 1 – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

NOTE 2 – This definition is taken from Y.2012 and therefore relates to NGN. However, it is also valid for other networks, e.g. networks supporting IPTV.

(DOC-0181) and Functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

(DOC-0194) Globally Executable MHP (GEM): A terminal specification based on MHP that enables applications to interoperate across OCAP, MHP and other GEM based platforms.

(DOC-0184) Group of Pictures: The Group of Pictures (GOP) is a group of successive pictures within a MPEG-coded film and/or video stream. Each MPEG-coded film and/or video stream consists of successive GOPs. From the MPEG pictures contained in it the visible frames are generated.

(DOC-0185) Home Gateway (HG): The interface of the home network to provider access network.

(DOC-0147), (DOC-0192) and (DOC-0193) Home network (HN): A communication system designed for the residential environment, in which two or more devices exchange information.

(DOC-0194) Home network (HN) [ITU-T J.190]: Short-range communications system designed for the residential environment, in which two or more devices exchange information under some sort of standard control.

(DOC-0192) and (DOC-0160) HN capable IPTV TD: An IPTV TD which has HN capability. This is typically a server and/or a client to HN devices.

(DOC-0192) and (DOC-0160) HN capable TD: A TD which has HN capability. This is typically a server and/or a client to HN devices.

(DOC-0147), (DOC-0192) and (DOC-0193) Hybrid terminal device: An IPTV terminal device that can also receive content from different types of transmission systems (e.g. satellite, cable).

(DOC-0188) Integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

(DOC-0194) Interactive Program Guide (IPG): A service navigation interface used especially for bi-directional interactive service with a server or head-end.

NOTE – It is sometimes used synonymously with EPG.

(DOC-0194) Interactive Television (iTV): A service in which the user can send requests, within a browser environment, to the service provider in order to obtain additional information. This capability requires channels to have what is known as a "return path".

(DOC-0147) Interstitial program: A short program which is shown between events (e.g. between two movies) or embedded during presentation of an event (e.g. advertisement).

(DOC-0185) IP differentiated model: The model that defines a set of edge functions and a number of per-hop behaviour (PHB).

(DOC-0185) IP reservation model: The model that is based on the IP Integrated Services (IntServ) and allows the use of RSVP signalling protocol for bandwidth reservation.

(DOC-0147) IPTV: IPTV is defined as multimedia services such as television/video/audio/text/graphics/ data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

(DOC-0147), (DOC-0192) and (DOC-0193) IPTV End System (IES): A single or set of consumer devices that support IPTV Services (i.e. everything from Gateway to Display).

(DOC-0190) IPTV multicast interoperability: IPTV multicast interoperability is the exchange of IPTV service information amongst multicast based IPTV service providers. And to make the optimal contract and to provide the stable IPTV services amongst multicast based IPTV service providers.

(DOC-0192) IPTV Network: An entity encompassing the full group of IPTV Architecture functions expected to be within the Network Provider and Service Provider functional domains.

(DOC-0190) IPTV Service Exchange Point: IPTV SEP (service exchange point) is identified as a reference point for handling the service brokering function between IPTV SPs enabling the optimal contract between IPTV SPs and providing the stable IPTV services amongst IPTV service providers. IPTV SEP can be located in any peering point.

(DOC-0147) and (DOC-0192) and (DOC-0193) IPTV TD: A terminal device which has ITF functionality, e.g. an STB.

(DOC-0147, (DOC-0189) and (DOC-0192) and (DOC-0193) IPTV terminal function (ITF): The functionality that is responsible for processing the content conveyed by the IP transport.

(DOC-0194) IPTV Terminal Function (ITF)*: The functionality within the home network that is responsible for terminating the IP signal, and converting the content into a renderable [i.e. enabling to be seen and/or heard] format, e.g. a STB.

* Based on [ATIS-0800002] with modification.

(DOC-0188) Key [ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

(DOC-0188) Key Management [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

(DOC-0194) Lifetime/Lifecycle of an application: Characterizes the time from which the application is loaded to the time the application is destroyed.

(DOC-0147), (DOC-0181) and (DOC-0189) Linear TV: A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed.

(DOC-0188) Masquerade [ITU-T X.800]: The pretence by an entity to be a different entity.

(DOC-0192) Metadata: Structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities[1].

---

1 Information obtained from: http://www.libraries.psu.edu/tas/jca/ccda/tf-meta3.html

NOTE – EPG metadata has many applications and may vary in depth from merely identifying the content package title or information to populate an EPG to providing a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold.

(DOC-0194) and (DOC-0197) Metadata [ITU J.98]: Metadata is descriptive data associated with a content asset package or file. It may vary in depth from merely identifying the content package title or information to populate an EPG to providing a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold. Separate uses for metadata have originated from the studios, distribution networks (Cable, Satellite), down to the CPE (STBs, PVRs).

(DOC-0194) Metadata format [ITU-T H.222AMD1]: Identifies the coding format of metadata.

(DOC-0197) Metadata fragments: A metadata fragment is a self-consistent atomic portion of a metadata instance. In this context, self-consistency means that fragments can be obtained in a random order and each fragment can be transmitted and updated independently.

(DOC-0197) Metadata instance: A metadata instance is the data instance describing the instance of content or user, etc. A metadata instance has its data-model defined by corresponding metadata schema.

(DOC-0197) Metadata schema: A metadata schema is the representation format for specifying data-model describing target instance.

(DOC-0194) Metadata service [ITU-T H.222AMD1]: Coherent set of metadata of the same format delivered to a receiver for a specific purpose.

(DOC-0194) Middleware: A layer of software between applications and resources, which consists of a set of service enablers that allow multiple functionalities running on one or more devices in an IPTV system to interact across a network.

(DOC-0147) Mobility: The ability for the end-user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

(DOC-0190) Multicast Access Control Functions: Multicast Access Control Functions is that control a multicast user access to IPTV multicast tree. The IPTV user can join a multicast service using these control functions with proper authentication and authorization of the user.

(DOC-0190) Multicast Delivery Control Functions: Multicast Delivery Control Functions is that can control IPTV multicast delivery among transport functions.

(DOC-0190) Multicast Domain Management: A multicast domain is a set of multicast routing and forwarding instances than can send multicast traffic to each other. These multicast routing and forwarding instances are referred to as IPTV multicast domain. Thus, multicast domains map all of a customer's multicast groups that exist in particular IPTV service members to a single unique global multicast group. This is achieved by existing or specific group routing and forwarding capability in the network.

(DOC-0195) Multi-channel audio: Audio signal with more than two channels.

(DOC-0147) Multicrypt: A mechanism that enables the reception of programmes encrypted according to various encryption systems by means of a Common Interface (CI).

(DOC-0147) Multi-channel audio: Audio signal with more than two channels.

(DOC-0194) Multimedia [ITU-T J.148]: The combination of multiple forms of media such as audio, video, text, graphics, fax, and telephony in the communication of information.

(DOC-0194) Multimedia application [ITU-T T.174]: An application which involves the presentation of multimedia information to the user.

(DOC-0194) Multimedia representation [ITU-T T.171]: The property of handling several types of representation media.

(DOC-0194) Multimedia service [ITU-T Q.1702]: A service in which the interchanged information consists of more than one type, such as text, graphics, sound, image and video.

(DOC-0147) and (DOC-0192) Network personal video recorder (nPVR): Same as PVR except that the recording device is located at the service provider premises.

(DOC-0147), (DOC-0182) and (DOC-0190) Network provider [ITU-T Q.1290]: The organization that maintains and operates the network components required for IPTV functionality. A network provider can optionally also act as service provider.

(DOC-0147) Open Captions: captions that are displayed and cannot be switched off by the viewer.

(DOC-0189) and (DOC-0190) Overlay Multicast Network: One type of overlay network that provides multicast services to end users on top of the general network infrastructure.

(DOC-0189) and (DOC-0190) Overlay Network: A virtual network of nodes and logical links that is built on top of the underlying network infrastructure with the purpose of implement a network service that is not available in the underlying network infrastructure.

(DOC-0147) Package: A collection of content components that in some combination (either all or a subset) together provide an end-user experience and are intended to be used together.

NOTE – A package can be instantiated with or without audio visual content depending on scenarios, in which audio visual content and package can be tightly associated or can be loosely coupled enough to be handled (generation, delivery, consumption) independently.

(DOC-0189) Parental control: Parental Control provides a mechanism for deciding the suitability of particular content for a minor on his/her age.

(DOC-0147) Pay per view (PPV): A TV service where a particular program event (e.g. a hockey match) can be bought separately from any package or subscription. The transmission of the program event is made at the same time to everyone who has ordered it.

(DOC-0188) Peer-Entity Authentication [ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

(DOC-0147) Personal digital recorder (PDR): See PVR.

(DOC-0147) Personal mobility: This is the mobility for those scenarios where the end-user changes the terminal device used for network access at different locations. The ability of a user to access tele-communication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

(DOC-0147) and (DCO-0192) Personal video recorder (PVR): An end-user controlled device that records, stores and plays back multimedia content. PVR is also known as personal digital recorder (PDR).

(DOC-0188) Phishing: Act of acquiring sensitive or personal information such as usernames, date of birth, passwords or credit card details, by masquerading as a trustworthy entity.

(DOC-0194) and (DOC-0164) Presentation [ITU-T T.411]: The operation of rendering the content of a document in a form perceptible to a human being.

(DOC-0194) Presentation engine [ITU-T J.200]: A subsystem in a receiver that evaluates and presents declarative applications consisting of content, such as audio, video, graphics, and text primarily based on presentation rules defined in the presentation engine. A presentation engine also responds to formatting information, or "mark-up", associated with the content, to user inputs, and to script statements, which control presentation behaviour and initiate other processes in response to user input and other events. A common example of a presentation engine is an HTML browser, capable of displaying text and graphic content formatted in HTML, with interactive behaviour programmed in ECMA script.

(DOC-0188) Privacy [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

(DOC-0147) Public Information Services: are specific un-associated Information Services. Examples of un-associated information services: news highlights, stock exchange, traffic conditions, sport results.

(DOC-0147) Push VoD: A TV service where multimedia content is packaged and delivered at the discretion of the service provider to the end-user's storage system.

(DOC-0184) Quality of experience (QoE) [ITU-T P.10/G.100]: The overall acceptability of an application or service, as perceived subjectively by the end-user.

NOTE 1 – Quality of Experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.).

NOTE 2 – Overall acceptability may be influenced by user expectations and context.

(DOC-0185) QoS routing: The mechanism that is used to control network congestion and improve network utilization by selecting an appropriate path.

(DOC-0147) Random access point: A point in the content from which playback can begin. NOTE – For example, in MPEG encoding, this would be an I-frame, as opposed to a P-frame or B-frame.

(DOC-0181) Reference point [ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

NOTE – A reference point may correspond to one or more physical interfaces between pieces of equipment.

(DOC-0188) Repudiation [ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

(DOC-0192) Residential Gateway (RG): A logical element that acts as a bridge between the access network and the home network, providing in premise and aggregated security management, provisioning and addressing services for logical elements within a compliant IPTV Network.

(DOC-0196) Resource Abstraction Interface (Layer): an interface layer between resource and middleware service which encapsulates OS operations and resources layer and provide abstract view for resource layer.

(DOC-0196) Resources (Layer): the native hardware and software resources that provide middleware services component of certain functionality through resource abstraction layer, and middleware service functions are provided to application layer through the API of the middleware services.

(DOC-0147) Re-transmission Broadcast Service: A service in which content is provided from various broadcasting environments including, but not limited to, terrestrial, satellite and cable, and re-transmitted into IP network simultaneously or otherwise.

(DOC-0147) and (DOC-0188) Rights: One or more legal or business entitlements to Use or employ Content, e.g., to view, record, redistribute Content.

(DOC-0147) and (DOC-0188) Rights Expression: The syntactic embodiment of Rights in a concrete form.

(DOC-0147) SCP: A combination of service protection and content protection.

(DOC-0188) SCP Bridge: On a single device, two or more Service and Content Protection systems are operative. Content acquired via one Service and Content Protection system can be accessed via another Service and Content Protection system resident on the same device according to granted rights

(DOC-0188) SCP End-to-End: Using a single Service and Content Protection system, two or more devices exchange and access content according to granted rights. This mode should be the simplest mode to implement since only a single Service and Content Protection system.

(DOC-0188) SCP Interchange: This case is characterized by two or more devices, each device having one or more operative Service and Content Protection systems. The content acquired by one device through one of its Service and Content Protection systems can be securely transferred to and accessed on another device through a different Service and Content Protection system according to granted rights.

(DOC-0188) Scrambling Algorithm: An algorithm used in a scrambling (encryption) or descrambling (decryption) process.

(DOC-0188) Security label [ITU-T X.800]: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

NOTE – The marking and/or binding may be explicit or implicit.

(DOC-0188) Security policy [ITU-T X.800]: The set of criteria for the provision of security services.

(DOC-0194) Segmentation: Division of content into different parts, e.g. scenes and chapters.

(DOC-0188) Service: A set of functionality enabled by a provider for end users; for example, providing IP connectivity with managed quality of service, providing an IPTV Service, providing a content on demand service, etc.

(DOC-0194) and (DOC-0164) Service [ITU-T Y.101]: A structure set of capabilities intended to support applications.

(DOC-0188) Service and Content Protection: A combination of Service Protection and Content Protection, or a system or implementation thereof.

(DOC-0196) Service Components (Layer): the pure native components that offer functionalities to application layers regardless of type of software and hardware in the resource layer.

(DOC-0194) and (DOC-0164) Service Navigation: The presentation of information that allows the end-user to discover, select and consume services.

(DOC-0194) Service Navigation Interface: A user interface which is intended to provide information on available services, including content that may be accessed by end-users for service navigation.

(DOC-0147) Service Protection: Ensuring that an end-user can only acquire content that they are entitled to receive.

NOTE – Service protection is sometimes referred to as conditional access.

(DOC-0188) Service Protection: Ensuring that an end-user can only acquire a service, and, by extension, the content contained therein, that they are entitled to receive.

(DOC-0147), (DOC-0182) and (DOC-0190) Service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider can optionally or can optionally not be a customer of another service provider.

(DOC-0194) Set-top box (STB): A device that contains demodulator, de-multiplexer, decoder, other functionalities and interfaces related to signal reception and presentation of the distributed programme at the subscriber's site.

(DOC-0147) Sign language interpretation: A video service showing an interpreter who uses hand gestures and facial expression to convey the main audio content and dialogue to sign language and lip readers.

NOTE – This service comes in the form of supplementary video content, usually smaller in image size to that the main video content. Ideally the user can control the position, size and background properties (solid or transparent and the colour, if solid). It is of sufficient temporal and spatial quality to enable sign reading and lip reading.

(DOC-0147) SimulCrypt: A mechanism that facilitates using several service protection systems.

(DOC-0147) Skin: A customized graphical appearance (the visual aspect of a graphical user interface (GUI)) applied to certain software and websites for aesthetic reasons or ease of use.

(DOC-0188) Spoofing: An activity in which a forged (spoofed) source (e.g. a person or computer program) successfully masquerades as a legitimate source by falsifying data and for the purpose of obtaining information and/or obscuring the true source to prevent non- repudiation for spreading computer viruses.

(DOC-0194) Stream [ITU-T J.200]: A unidirectional continuous flow of content.

(DOC-0147) and (DOC-0190) Subscriber [ITU-T Q.3050.1]: The subscriber is responsible for concluding contracts for the services subscribed to and for paying for these services.

(DOC-0147) and (DOC-0190) Subscription [ITU-T Q.1741.3]: A subscription describes the commercial relationship between the subscriber and the service provider.

(DOC-0147) Subtitles: Subtitles provide a real-time on-screen transcript of dialogue for the purpose of language translation or to clarify speech that is unclear.

NOTE – This service can be provided by means of either textual or graphical supplementary content. The subtitles and the dialogue are usually in different languages. The assumed audience for subtitling is hearing people who do not understand the language of the dialogue.

(DOC-0147) Supplementary content: This is defined as video, audio, textual, graphical or other forms of content that can be optionally accessed by the end-user and rendered by the terminal. It has the following features:

- It only works in conjunction with the main content.
- It is synchronous with the main content.

(DOC-0194) Telecommunication service [ITU-T F.700]: Set of telecommunication capabilities that work in a complementary and cooperative way in order to let users perform applications.

(DOC-0147), (DOC-0192) and (DOC-0193) Terminal device (TD): A device which typically presents and/or processes the content, such as a personal computer, a computer peripheral, a network appliance, a mobile device, a TV set, a monitor, a VoIP Terminal or an audio-visual media player.

(DOC-0147) Terminal device protection: Ensuring that a terminal device employed by an end-user in the reception of a Service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters not otherwise protected by encryption or watermarking.

(DOC-0188) Terminal Device Protection: Ensuring that a terminal device employed by an end-user in the reception of a Service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters (e.g., saved keys) not otherwise protected.

(DOC-0147) Terminal mobility: This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access IPTV services from different locations and while in motion, and the capability of the network to identify and locate that terminal.

(DOC-0188) Threat [ITU-T X.800]: A potential violation of security.

(DOC-0147) Time shifting: A function which allows playback of content after its initial transmission.

(DOC-0194) Time-shifting: Act of recording of programmed content (i.e. video stream or sound) for the purpose of viewing or listening at other than original scheduled time.

(DOC-0147) and (DOC-0194) Time-shift TV: A TV program that has been time shifted.

(DOC-0185) Transmission Scheduler: The mechanism that controls which packets to select for transmission on an outgoing link.

(DOC-0147) Trick mode functionality: The ability to pause, rewind or forward stored content.

(DOC-0184) Triple Play Services: Services that include IPTV, VoIP, and Internet Access.

(DOC-0147) TV with trick mode: TV service with trick mode functionality.

(DOC-0147) Universal Design: It is the design of the products and environments to be useable by all people, to the greatest extent possible by including accessibility features in the original design to prevent the need for adaptation after deployment.

NOTE – The intent of universal design is to simplify life for everyone by making products, communications, and the built environment more usable by as many people as possible at little or no extra cost. Universal design benefits people of all ages and abilities.

(DOC-0197) Usage environment: The usage environment is described by user characteristics, terminal capabilities, network characteristics and natural environment characteristics, where the contents being consumed.

(DOC-0147) Usage environment description: The usage environment description includes the description of end-user characteristics, terminal capabilities, network characteristics and natural environment characteristics.

NOTE – These various dimensions of the usage environment description, which originate from end-users, can be used for accommodating, for example, the adaptation of contents for transmission, storage and consumption.

(DOC-0147) and (DOC-0188) Use: The purpose(s) for which acquired content is employed.

(DOC-0194) User device [ATIS-0800002]: Also known as Home Network End-Device (HNED), Home Network Device (HND), Consumer Equipment (CE), terminal and physical device. A piece of hardware equipment running its software and attached to a Home Network and being identified by a GUID, e.g. a MAC address. A single device can be used by one or more users.

(DOC-0194) User Interface (UI): Also known as UI, a user interface is the sensory and behavioural aspects of a program that are presented to a user. The term is generally used to denote the menuing and navigational constructs of a program.

(DOC-0147) and (DOC-0188) User Privacy Protection: Ensuring that information considered to be private (or confidential) by an end-user be maintained in confidence, while remaining subject to mandatory disclosure due to legal processes.

(DOC-0181), (DOC-0189) and (DOC-0194) Video-on-Demand (VoD): A service in which the subscriber can view video content whenever desired. The operating assumption is that the content is stored on the provider's VoD server. Subscriber accesses the movie from a library directory which may include search engine that accesses movie description and rating. Subscribers typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time when using this service.

(DOC-0184) VoD Trick Modes: Download and streaming video on demand (VoD) systems provide the user with a large subset of VCR functionality including pause, fast forward, fast rewind, slow forward, slow rewind, jump to previous/future frame, etc. These functions are usually referred to as "trick modes".

(DOC-0192) Watermark: Machine readable data in the form of a signal embedded in a digital media stream so as to be imperceptible to the consumer, but persistent through faithful transformations of the content.

NOTE – that this definition pertains to watermarks in the context of IPTV service and is not a universal definition of a watermark. In the IPTV context, watermarks are used to facilitate Rights Management and media piracy investigation.

(DOC-0147) Web-based EPG: An EPG that can be accessed on a web server by means of a URL.

(DOC-0147) Wireless network characteristics: The characteristics of a wireless network expressed in terms of current available bandwidth, packet loss and possibly other to-be-defined wireless network information parameters for a specific wireless link type e.g. WLAN, Cellular, WPAN or WMAN.

Printed in Switzerland
Geneva, 2008