



Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks

EBU
OPERATING EUROVISION

DVB
Digital Video
Broadcasting

Reference

RTS/JTC-DVB-356

Keywords

broadcasting, digital, DVB, IP, satellite, TV, video

ETSI

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

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

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

Important notice

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
© European Broadcasting Union 2016.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	15
Foreword.....	15
Modal verbs terminology.....	15
1 Scope	16
1.0 General	16
1.1 Scope of the present document.....	16
1.1.1 What is within the scope	16
1.1.2 What is out of the scope.....	18
1.1.3 Additional Specifications for Home Network.....	18
1.1.4 DTDs and XML Schemas.....	18
2 References	18
2.1 Normative references	18
2.2 Informative references.....	23
3 Definitions, abbreviations and notations	24
3.1 Definitions.....	24
3.2 Abbreviations	27
3.3 Notations	30
3.3.1 Augmented Backus-Naur Form (ABNF)	30
3.3.1.1 General rules	30
3.3.1.2 Core rules	31
4 Architecture	31
4.1 Introduction	31
4.1.0 Overview	31
4.1.1 Domains and Actors in an IPTV system.....	32
4.1.2 The Home Network Domain.....	33
4.1.2.1 HNED as end point	33
4.1.2.2 DVB Home Network (DVB HN) content sharing	34
4.1.2a High-level Service Flows in a DVB IPTV network.....	34
4.1.3 Diagram of the DVB-IPTV Protocol Stack	35
4.2 Void.....	37
5 Service discovery	38
5.1 Overview	38
5.2 Service Metadata	38
5.2.1 Service Identification.....	38
5.2.1.0 Introduction	38
5.2.1.1 Service Provider (SP).....	38
5.2.1.2 Service name or service ID	38
5.2.2 Fragmentation of SD&S Records	39
5.2.3 Steps in service discovery (informative).....	39
5.2.4 Service discovery entry points	41
5.2.5 SP discovery information.....	42
5.2.6 DVB-IPTV service discovery information	42
5.2.7 Data Model (Informative).....	43
5.2.8 Metadata Namespace	45
5.2.8.0 General rules	45
5.2.8.1 Current version.....	46
5.2.8.2 Backwards compatibility.....	46
5.2.9 Legend and Syntax of XML diagrams (Informative)	46
5.2.10 XML Basic Types.....	48
5.2.11 XML Complex Types - Attribute Groups.....	51
5.2.11.1 BasicMulticastAddressAttributesType.....	51
5.2.11.2 CommonCastRETTType	52
5.2.11.3 FECAttributeGroupType.....	54
5.2.11.4 MulticastAddressAttribute	54

5.2.12	XML Complex Types - Element Groups	55
5.2.12.1	AnnouncementSupport.....	55
5.2.12.1a	ciAncillaryDataType	56
5.2.12.2	CDSDownloadSessionDescriptionLocationType	57
5.2.12.3	Cell	58
5.2.12.4	CivicAddress	58
5.2.12.5	CountryAvailabilty.....	59
5.2.12.6	DescriptionLocationBCG.....	59
5.2.12.6a	DSMMType	60
5.2.12.7	DVBSTPTransportModeType	61
5.2.12.8	DVBTriplet	62
5.2.12.9	FECInfoType	63
5.2.12.10	FECLayerAddressType.....	63
5.2.12.11	FUSAnnouncementType	65
5.2.12.12	FUSType	66
5.2.12.13	HTTPTransportModeType.....	67
5.2.12.14	McastType.....	68
5.2.12.15	MosaicDescription	69
5.2.12.16	MulticastRETTType	71
5.2.12.17	MultilingualType	72
5.2.12.18	OfferingBase	72
5.2.12.19	OfferingListType	73
5.2.12.20	PackageAvailabilityCountryCodeType.....	74
5.2.12.21	PackagedServiceType	75
5.2.12.22	PayloadList.....	75
5.2.12.23	PayloadListSegmentType	76
5.2.12.24	ReferencedServiceProviderType	77
5.2.12.25	ReplacementService	77
5.2.12.26	RETInfoType	78
5.2.12.27	RMSFUSMulticastAddressType.....	79
5.2.12.28	RMSType	79
5.2.12.29	RTCPReportingType	80
5.2.12.30	RTSPURLType	82
5.2.12.31	ServerBasedEnhancementServiceInfoType	83
5.2.12.32	ServiceAvailabilityType	84
5.2.12.33	ServiceLocation	85
5.2.12.34	SI	85
5.2.12.35	SRMAnnouncementModeType	87
5.2.12.36	SRMAnnouncementModeSAPType	88
5.2.12.37	SRMAnnouncementServiceType	88
5.2.12.38	SRMDownloadServiceFLUTEType	89
5.2.12.39	SRMDownloadServiceHTTPType	90
5.2.12.40	SRMDownloadServiceType	90
5.2.12.41	SRMIDType	91
5.2.12.42	SRMIDVerMType	91
5.2.12.43	SRMIDVerUType	92
5.2.12.44	TargetPackageType	92
5.2.12.45	TextualIdentifier	93
5.2.12.46	TransportModeType	94
5.2.12.47	UnicastRETTType	94
5.2.12.47a	URILinkage	95
5.2.12.48	PackageTextualIdentifier	96
5.2.13	XML Main Types	97
5.2.13.0	Introduction	97
5.2.13.1	Broadband Content Guide Record: BCGOffering	97
5.2.13.2	Broadcast Discovery Record: BroadcastOffering	99
5.2.13.3	Content on Demand Offering Record: CoDOffering	102
5.2.13.4	Packaged Services: PackagedServices	103
5.2.13.5	Referenced Services Offering: ReferencedServices	106
5.2.13.6	RMS Offering: RMSFUSDDiscoveryType	107
5.2.13.7	Service Provider Discovery: ServiceProviderListType	108
5.2.13.8	Regionalization Discovery Information	109

5.2.13.8.1	Regionalization Offering	109
5.2.13.8.2	Example Regionalization Information (Informative)	110
5.2.13.9	SRM Offering Record	111
5.2.13.10	CoD Announce Describe Record	112
5.2.13.11	SRM Download Record	113
5.2.13.12	Cell Request Record	114
5.2.14	XML Schema.....	114
5.3	Service Selection	116
5.4	Transport mechanisms.....	117
5.4.0	Overview	117
5.4.1	Protocol for multicast delivery of SD&S information	117
5.4.1.0	General rules	117
5.4.1.1	Datagram Syntax	118
5.4.1.2	Semantics	118
5.4.1.3	Usage.....	120
5.4.1.3.0	Introduction	120
5.4.1.3.1	Use of sections.....	120
5.4.1.3.2	Maximum section size	121
5.4.1.3.3	Use of ServiceProviderID field	121
5.4.1.3.4	Repetition rates.....	121
5.4.2	Protocol for unicast delivery of SD&S Information	122
5.4.2.0	General rules	122
5.4.2.1	SP Discovery request	122
5.4.2.2	Service Discovery request.....	123
5.4.2.3	Obtaining the Cell ID via HTTP (Pull mode)	124
5.4.3	Signalling of changes.....	125
5.4.4	Fragmentation of SD&S Records	125
5.4.4.1	SD&S Information data types	125
5.4.4.2	Fragmentation of SD&S records.....	126
5.4.4.3	Maximum cycle time of multicast delivery.....	127
5.4.5	XML records and payload ID	127
5.4.6	Segmentation of XML records.....	127
5.5	Encoding.....	128
5.5.1	Introduction.....	128
5.5.2	Usage of BiM.....	128
5.5.2.1	Introduction.....	128
5.5.2.2	DVB-TVA-Init and InitialDescription	128
5.5.2.3	BiM Access Unit.....	128
5.5.2.4	Codec	128
6	RTSP Client.....	129
6.1	Usage of RTSP in DVB.....	129
6.1.0	Introduction.....	129
6.1.1	Service selection	129
6.1.2	Session transport	129
6.1.3	Service information.....	130
6.1.4	Security considerations	130
6.2	Profiles	130
6.2.1	Profile definitions	130
6.2.2	Live media broadcast	130
6.2.3	Media broadcast with trick modes	131
6.2.4	Content on Demand (CoD)	131
6.3	RTSP methods.....	131
6.3.0	List of supported RTSP methods	131
6.3.1	DVB specific usage of RTSP methods	131
6.3.1.1	ANNOUNCE	131
6.3.1.2	DESCRIBE	133
6.3.1.3	GET_PARAMETER.....	133
6.3.1.4	SETUP	133
6.3.2	Headers	134
6.3.2.1	RTSP request header fields	134
6.3.2.2	Transport Header parameters required for direct UDP encapsulation.....	136

6.4	Status codes in response to requests	136
6.5	The use of RTSP with multicast	137
7	Transport of MPEG-2 TS for real-time services	138
7.0	Overview	138
7.1	Transport stream encapsulation	139
7.1.0	General rules	139
7.1.1	Real-time Transport Protocol (RTP) encapsulation	139
7.1.1.0	Real-time Transport Protocol (RTP)	139
7.1.1.1	Real-time Transport Control Protocol (RTCP)	140
7.1.2	Direct User Datagram Protocol (UDP) encapsulation	141
7.1.3	Detection and Usage of RTP and direct UDP encapsulation (Informative)	142
7.1.4	Embedded Service Information (SI)	142
7.2	Network requirements	142
7.2.0	General rules	142
7.2.1	Mandatory constraints	142
7.2.1.1	Packet Jitter	142
7.2.1.2	Direct User Datagram Protocol (UDP) Packet Reordering	142
7.2.2	Recommended constraints	142
7.2.2.0	Introduction	142
7.2.2.1	Packet loss	142
7.2.2.2	Multicast timing	143
7.3	Service initiation and control	143
7.3.0	Introduction	143
7.3.1	Multicast services	143
7.3.2	Unicast services	143
7.4	Quality of Service	143
8	IP Address allocation and network time services	144
8.1	IP Addressing and routing	144
8.1.1	IP Address assignment using IPv4 methods	144
8.1.1.0	Introduction	144
8.1.1.1	Dynamic Addressing only	144
8.1.1.2	Dynamic Host Configuration Protocol (DHCP)	144
8.1.1.3	DHCP messages	144
8.1.1.4	DHCP options	144
8.1.1.4.0	List of (public) DHCP options	144
8.1.1.4.1	Max DHCP message size	147
8.1.1.4.2	NetBIOS over TCP/IP options	147
8.1.1.4.3	DHCP user class option (RFC 3004 [43])	147
8.1.1.4.4	DHCP relay agent information	147
8.1.1.5	DHCP server unavailable	147
8.1.1.6	Multiple DHCP servers	147
8.1.1.7	DNS Server allocation and default gateway	147
8.1.1.8	Universal plug and play	148
8.1.1.9	Server Implementation	148
8.1.1.10	RTP Retransmission Server Address and future DVB DHCP Extensions	148
8.1.1.11	Location Parameter for CellID	148
8.1.2	IP address assignment using IPv6 methods	149
8.1.2.0	Introduction	149
8.1.2.1	Dynamic addressing only	149
8.1.2.2	Unicast IP address assignment using SLAAC	149
8.1.2.3	IP address assignment using Dynamic Host Configuration Protocol Version 6 (DHCPv6)	149
8.1.2.4	Implementation details for IPv6 functionalities	152
8.1.2.4.0	Introduction	152
8.1.2.4.1	Maximum DHCP message size	152
8.1.2.4.2	NetBIOS over TCP/IP options	152
8.1.2.4.3	DHCP user class option (IETF RFC 3315 [122])	152
8.1.2.4.4	DHCP relay agent information	152
8.1.2.4.5	DHCP server unavailable	153
8.1.2.4.6	Multiple DHCP servers	153
8.1.2.4.7	DNS Server allocation and default gateway	153

8.1.2.4.8	Universal plug and play	153
8.1.2.4.9	Server implementation.....	153
8.1.2.4.10	RTP Retransmission Server address and future DVB DHCP extensions	153
8.1.2.4.11	Location parameter for CellID	153
8.2	Network time services	154
8.2.0	Network time services types	154
8.2.1	Real-Time Clock or other applications with an accuracy of 100 ms	154
8.2.2	Accurate time services	154
8.2.3	Time server address discovery.....	155
9	File Upload System Stub (FUSS) to Enable Optional Updates of the System Software of an HNED.....	155
9.0	Introduction	155
9.1	Obtaining the Stub File.....	155
9.1.0	Acquiring Stub File location.....	155
9.1.1	Using DVBSTP to Obtain the Stub File via Multicast	156
9.1.2	Using HTTP(S) to Obtain the Stub File via Unicast.....	156
9.1.2.0	HTTP(S) mechanism.....	156
9.1.2.1	HTTP Congestion avoidance mechanism	156
9.2	Stub File Format.....	157
10	Content Download Service (CDS)	159
10.1	Overview	159
10.2	Functional Architecture	160
10.2.0	CDS Functional Architecture Diagram.....	160
10.2.1	CDS Functional Components	161
10.2.2	CDS Interfaces.....	163
10.2.3	CDS Protocol Stack	163
10.3	CDS Announcement through BCG	163
10.3.0	Introduction.....	163
10.3.1	Usage of SD&S, BCG and TVA for CDS	164
10.3.2	URIs for Download Session Description	164
10.3.2.0	Overview.....	164
10.3.2.1	CDS XML Multicast Locator.....	165
10.3.2.2	CDS XML Unicast Locator	165
10.3.2.3	CDS SDP Multicast Locator	166
10.3.2.4	CDS SDP Unicast Locator	166
10.3.3	URI for files on the CDS HNED storage	167
10.4	CDS Content Item and File Formats	167
10.4.1	General.....	167
10.4.2	File Formats and Media types.....	167
10.4.2.1	MPEG-2 Transport Stream file format.....	167
10.4.2.2	BCG Metadata file format.....	168
10.4.2.3	DVB File Format	168
10.4.3	Content Item Formats	168
10.5	CDS Download Session Description	169
10.5.1	Overview	169
10.5.2	Referencing file locations for download.....	169
10.5.3	Download Session Description Parameters	170
10.5.3.0	Introduction.....	170
10.5.3.1	General Parameters	170
10.5.3.2	Unicast Download Related Parameters	171
10.5.3.3	Multicast Download Related Parameters	172
10.5.4	Download session Modes	173
10.5.5	Transport of download session descriptions	174
10.5.5.0	Introduction.....	174
10.5.5.1	Multicast transport of XML-based download session descriptions.....	175
10.5.5.2	Unicast transport of XML-based download session descriptions	175
10.5.5.3	Multicast transport of SDP-based download session descriptions	176
10.5.5.4	Unicast transport of SDP-based download session descriptions	176
10.6	CDS Content Item Download.....	176
10.6.1	Overview	176

10.6.2	Multicast Content Download	177
10.6.2.1	Overview	177
10.6.2.2	FLUTE Transport Protocol in CDS	178
10.6.2.2.0	General rules.....	178
10.6.2.2.1	Segmentation of files.....	178
10.6.2.2.2	Symbol Encoding Algorithm.....	179
10.6.2.2.3	Use of multiple FLUTE channels	179
10.6.2.2.4	Blocking Algorithm.....	179
10.6.2.2.5	Congestion Control.....	179
10.6.2.2.6	Content encoding of files for transport.....	179
10.6.2.2.7	Further Considerations	179
10.6.2.2.8	Signalling of Parameters with FLUTE	180
10.6.2.2.9	FDT Structure	182
10.6.2.3	Multicast Rate Adaptation.....	182
10.6.2.3.0	General rules.....	182
10.6.2.3.1	CDS network procedures.....	182
10.6.2.3.2	CDS HNED procedures.....	183
10.6.2.4	File download from the FLUTE session	183
10.6.2.5	CDS Network-based Session Completeness	184
10.6.2.5.1	Basic Principle	184
10.6.2.5.2	Message formats	184
10.6.2.5.3	CDS network procedures.....	186
10.6.2.5.4	CDS HNED procedures.....	186
10.6.2.6	File Repair Procedure.....	187
10.6.2.6.1	General Procedure	187
10.6.2.6.2	Identification of file repair needs.....	188
10.6.2.6.3	Distribution of Recovery requests over time	188
10.6.3	Unicast Content Download	189
10.6.3.1	General	189
10.6.3.2	Single server unicast download.....	189
10.6.3.3	Multiple server unicast download	190
10.6.3.4	Redirection	191
10.6.3.4.0	Types of redirection.....	191
10.6.3.4.1	Alternative single server redirection.....	191
10.6.3.4.2	Multiple server redirection	191
10.6.3.4.3	Multicast download redirection	192
10.6.3.4.4	Interpretation of redirection information	192
10.6.4	Parallel downloads	193
10.6.5	Reception Reporting	193
10.6.5.1	General	193
10.6.5.2	Distribution of Reception reporting request over time	194
10.6.5.3	Reception reporting message	194
10.6.5.4	Reception report response message.....	195
10.6.6	Content Version Numbering	195
10.6.7	Priority settings	196
10.7	CDS HNED Storage Management	196
11	Quality of Service.....	196
11.0	Classification	196
11.1	DSCP packet marking	197
11.2	Ethernet Priority	197
12	SRM delivery over IP networks	198
12.1	Overview	198
12.2	Functional Architecture	198
12.3	SRM specific identifiers	199
12.3.0	General.....	199
12.3.1	CP System ID	199
12.3.2	CP System SRM ID	199
12.4	SRM Announcement Services.....	199
12.4.0	General rules	199
12.4.1	SD&S SRM Announcements (SRM-1 interface)	200

12.4.2	Dedicated SRM Announcement services.....	200
12.4.2.0	General rules	200
12.4.2.1	HTTP unicast SRM announcement service (SRM-2 interface)	200
12.4.2.2	SAP multicast announcement service (SRM-3 interface)	200
12.5	SRM download services	201
12.5.0	Overview	201
12.5.1	HTTP unicast SRM download service (SRM-4 interface).....	201
12.5.2	FLUTE multicast SRM download service (SRM-5 interface).....	201
12.6	Version Numbers.....	202
12.6.0	Overview of the different types of Version Numbers and their usage	202
12.6.1	SRM File Version Number	203
12.6.2	FLUTE Session Version Number	204
12.6.3	Record Version Number	204
12.6.4	Announcement Service Version Number	204
12.6.5	Segment Version Number.....	204
13	Dynamic Service Management (DSM)	204
13.1	Overview	204
13.2	DSM Functional Architecture	205
13.3	Operating Assumptions	206
13.4	DSM Process.....	207
13.5	Data Model for information stored by the DSM Manager	207
13.5.1	DSM Data Model.....	207
13.5.2	Equivalent Services.....	211
13.6	DSM Message Set	211
13.7	DSM messages	214
13.7.1	Overview	214
13.7.2	Messages at boot time.....	214
13.7.2.1	DSM001 - HNED ID request - HNED to DSM Manager	214
13.7.2.2	DSM002 - Assignment of IDs to HNED - DSM Manager to each HNED	214
13.7.2.3	DSM003 - HNED ID exchange - HNED to DSM Manager	215
13.7.2.4	DSM004 - HNED_ID Confirmation by DSMM - DSM Manager to each HNED.....	215
13.7.3	Status synchronization updates	215
13.7.3.1	DSM101 - Sychronisation of current status - DSM Manager to HNED	215
13.7.4	Messages directly associated with a service selection	216
13.7.4.1	DSM201 - Change request - HNED to DSM Manager	216
13.7.4.2	DSM202 - Change proposal - DSM Manager to HNED	217
13.7.4.3	DSM203 - Change accept/refuse - HNED to DSM Manager	217
13.7.4.4	DSM204 - Change confirmed/cancelled - DSM Manager to HNED	218
13.7.4.5	DSM205 - Service Change Acknowledge - HNED to DSM Manager	218
13.7.4.6	DSM206 - Service Change complete - HNED to DSM Manager	219
13.7.5	Data value messages	219
13.7.5.1	DSM301 - Query value - HNED to DSM Manager	219
13.7.5.2	DSM302 - Return value - DSM Manager to HNED	220
13.7.5.3	DSM303 - Set value - HNED to DSM Manager	220
13.7.5.4	DSM304 - Set value success - DSM Manager to HNED	221
13.7.5.5	DSM305 - Query value - DSM Manager to HNED	221
13.7.5.6	DSM306 - Return value - HNED to DSM Manager	221
13.7.5.7	DSM307 - Set value - DSM Manager to HNED	222
13.7.5.8	DSM308 - Succesfull transaction - HNED to DSM Manager.....	222
13.8	Message Structure and Transport	222
13.8.1	Structure of the messages	222
13.8.2	Transport of the messages.....	223
13.8.3	Message Schema.....	223
13.9	Setting of HNED Identifier (HNED_ID) for each HNED.....	224
Annex A (informative):	MPEG-2 Timing Reconstruction.....	225
A.0	Overview	225
A.1	Clock recovery in a RTP receiver	226
A.2	Recommendation.....	227

Annex B (informative):	SD&S data model.....	228
Annex C (normative):	Schemas	229
C.1	SD&S XML schemas	229
C.1.1	Namespace	229
C.1.2	Simple types	229
C.1.3	Complex types and attribute groups.....	229
C.1.4	Element Types.....	229
C.1.5	Schema	229
C.1.6	Multicasting SD&S XML documents	229
C.2	CDS XML Schemas	229
C.2.0	Introduction	229
C.2.1	Namespace	229
C.2.2	Basic schema definitions	229
C.2.3	Download session description	230
C.2.4	Reception reporting message.....	236
C.3	FLUTE FDT XML Schema for SRM	239
Annex D (informative):	Void	243
Annex E (normative):	Application Layer Forward Error Correction.....	244
E.1	Introduction	244
E.2	Terms and Acronyms	244
E.3	SMPTE 2022-1-based code.....	245
E.4	Raptor code	246
E.4.1	Introduction	246
E.4.2	FEC Streaming Framework.....	246
E.4.2.1	Introduction.....	246
E.4.2.2	Procedural overview	247
E.4.2.2.1	General	247
E.4.2.2.2	Sender Operation.....	248
E.4.2.2.3	Receiver Operation.....	249
E.4.2.3	Protocol Specification.....	249
E.4.2.3.1	General	249
E.4.2.3.2	Structure of Source Block	249
E.4.2.3.3	Packet format for FEC Source packets.....	250
E.4.2.3.4	Packet Format for FEC Repair packets	251
E.4.2.3.5	FEC Streaming Configuration Information.....	251
E.4.2.3.6	FEC Scheme requirements	252
E.4.3	FEC Schemes for streaming	252
E.4.3.1	Raptor FEC Scheme for arbitrary packet flows	252
E.4.3.1.0	Introduction	252
E.4.3.1.1	Formats and Codes	252
E.4.3.1.1.1	FEC Object Transmission Information.....	252
E.4.3.1.1.2	FEC Payload ID.....	253
E.4.3.1.2	Procedures.....	253
E.4.3.1.3	FEC Code specification.....	253
E.4.3.1.4	Encoding packet construction	254
E.4.3.1.5	Transport.....	254
E.4.3.1.6	Example parameters	255
E.4.3.1.6.1	Parameter derivation algorithm	255
E.4.3.1.6.2	Examples	255
E.4.3.2	Raptor FEC Scheme for a single sequenced packet flow.....	255
E.4.3.2.0	General	255
E.4.3.2.1	Formats and Codes	256
E.4.3.2.1.1	FEC Object Transmission Information.....	256
E.4.3.2.1.2	FEC Payload ID.....	256
E.4.3.2.2	Procedures.....	257

E.4.3.2.2.0	General	257
E.4.3.2.2.1	Derivation of Source FEC Packet Identification Information	257
E.4.3.2.2.2	Derivation of repair packet ESIs.....	258
E.4.3.2.2.3	Procedures for RTP flows.....	258
E.4.3.2.3	FEC Code specification.....	258
E.4.3.2.4	Example parameters	258
E.4.3.2.4.1	Parameter derivation algorithm	258
E.4.3.2.4.2	Examples	258
E.5	FEC decoder	259
E.5.1	Decoder requirements (normative).....	259
E.5.1.1	Minimum decoder requirements	259
E.5.1.2	Enhanced decoder requirements	259
E.5.2	Hybrid decoding procedures (informative)	259
E.5.2.1	Outline	259
E.5.2.2	Conversion of SMPTE 2022-1 packets.....	260
E.5.2.3	Extension of Raptor decoding.....	261
E.6	FEC Content Delivery Protocols	261
E.6.0	Introduction	261
E.6.1	Multicast MPEG-2 Transport Stream over RTP	261
E.6.1.0	Introduction.....	261
E.6.1.1	Control protocols	261
E.6.1.2	Transport protocol	262
E.6.2	Unicast MPEG-2 Transport Stream over RTP	262
E.6.2.0	Introduction.....	262
E.6.2.1	Control protocols	262
E.6.2.2	Transport protocol	262
E.6.3	Generic multicast video (informative).....	262
E.6.3.0	Introduction.....	262
E.6.3.1	Control protocols	262
E.6.3.2	Transport protocols	262
E.6.4	Generic unicast video (informative)	262
E.6.4.0	Introduction.....	262
E.6.4.1	Control protocols	263
E.6.4.2	Transport protocols	263
E.6.5	MIME Types definitions for AL-FEC	263
E.7	Raptor explicit encoding sequences	263
Annex F (normative):	RTP Retransmission Solution.....	265
F.1	Introduction	265
F.2	Terms and Acronyms	265
F.3	Retransmission (RET) architecture	265
F.3.0	Introduction	265
F.3.1	RET for CoD/MBwTM service.....	265
F.3.2	RET for LMB service.....	266
F.3.2.0	RET architecture for LMB service	266
F.3.2.1	RTP Sessions for the RET Enabled LMB service	268
F.4	RTCP signalling by RET-enabled HNEDs	268
F.4.0	RTCP reports.....	268
F.4.1	RTCP FB message.....	268
F.4.2	RTCP RR, RTCP SDES and RTCP BYE packets	269
F.4.2.0	Introduction.....	269
F.4.2.1	RTCP SDES Packet	269
F.4.2.2	RTCP RR Packet	269
F.4.2.3	RTCP BYE packet.....	270
F.4.3	RTCP messaging types.....	270
F.5	RTCP signalling towards RET-enabled HNEDs.....	270
F.5.0	Introduction	270

F.5.1	The RTCP SDES/SR packets	270
F.5.2	The RTCP Feed Forward (FF) message (LMB service only)	270
F.5.3	The RTCP Receiver Summary Information (RSI) packets(LMB service only)	271
F.6	Retransmission Format and RTP Retransmission Session SSRC and transport address	274
F.6.1	Retransmission Format.....	274
F.6.2	Some Observations on Retransmission Transport Addresses and SSRC Identifiers	275
F.6.2.1	Unicast services (CoD and MBwTM)	275
F.6.2.2	LMB service	275
F.7	Retransmission Requesting Behaviour of RET-enabled HNED	276
F.7.0	General	276
F.7.1	CoD/MBwTM RET (requesting) Timing Parameters	276
F.7.2	LMB RET (requesting) Timing Parameters	277
F.8	Configuration method and configuration parameters.....	278
F.9	QoS Priority settings	278
F.10	DVB RET and AL-FEC services combined.....	279
F.11	Mapping of DVB-specific RET attributes and parameters in SDP	279
Annex G (normative):	CDS Related Information	280
G.1	CDS Related Extensions to Other Specifications.....	280
G.1.0	Introduction	280
G.1.1	Usage and Extensions of OnDemandProgramType for pull download service.....	280
G.1.1.0	Introduction.....	280
G.1.1.1	Delivery Mode Extension	280
G.1.1.2	Usage of TVA OnDemandProgramType attributes for CDS pull download	280
G.1.1.3	Content Version Number Extension	281
G.1.1.4	Expiry Time Extension	281
G.1.1.5	Early Play Out Indication Extension.....	281
G.1.1.6	Extended OnDemandProgramType XML Schema.....	282
G.1.2	PushDownloadType for CDS push download service.....	282
G.1.2.1	Background and Semantics.....	282
G.1.2.2	PushDownloadType XML Schema	283
G.1.3	Extended ProgramLocationTableType.....	283
G.1.3.0	Introduction.....	283
G.1.3.1	PushDownloadProgram Extension	283
G.1.3.2	Extended ProgramLocationTableType XML Schema.....	284
G.1.4	Extended On-demand decomposed binary locator	284
G.1.5	ProgramURL and Locator URIs for files located on CDS HNED storage.....	286
G.2	SDP syntax	286
G.2.0	General	286
G.2.1	SDP message structure	286
G.2.2	General parameters.....	286
G.2.3.0	Mapping to standard SDP parameters.....	286
G.2.3.1	SP domain, download session ID and download session version	287
G.2.3.2	Content item format	287
G.2.3.3	Download session mode	288
G.2.3.4	Download session time information	288
G.2.3.5	Reception reporting server.....	288
G.2.3.6	Reception reporting mode	288
G.2.3.7	Reception reporting offset time and random time period	289
G.2.4	Unicast download parameters.....	289
G.2.4.0	Introduction.....	289
G.2.4.1	File Reference	289
G.2.4.2	File Length.....	289
G.2.4.3	File Digest.....	289
G.2.4.4	Chunk Length	290
G.2.4.5	Chunk Digest	290
G.2.4.6	Server Base URI and File Content Type.....	290

G.2.4.7	Available Chunk List	291
G.2.4.8	Grouping of media lines	291
G.2.4.9	SDP message structure for unicast download session.....	291
G.2.5	Multicast download parameters.....	293
G.2.5.0	Introduction.....	293
G.2.5.1	File Reference	293
G.2.5.2	Multicast channel source address.....	293
G.2.5.3	Transport Session Identifier	293
G.2.5.4	FEC Encoding ID	293
G.2.5.5	Numbers of channels	293
G.2.5.6	Multicast Address	294
G.2.5.7	Multicast Port Number.....	294
G.2.5.8	Maximum bandwidth.....	294
G.2.5.9	Completion poll response server address and port number.....	294
G.2.5.10	Recovery server base URI	294
G.2.5.11	Recovery mode	294
G.2.5.12	Recovery offset time and random time period.....	295
G.2.5.13	SDP message structure for multicast download session	295
G.3	DVB-MCAST URI scheme.....	296
G.3.0	Overview	296
G.3.1	Basic DVB-MCAST URI scheme.....	296
G.3.2	DVB-MCAST URI scheme for DVBSTP.....	297
G.3.3	DVB-MCAST URI scheme for SAP	297
Annex H (normative):	SDP syntax for SRM announcement services	299
H.0	General	299
H.1	SDP message structure	299
H.2	General Parameters.....	299
H.2.0	Mapping to standard SDP parameters	299
H.2.1	Domain name and Record version number	300
H.2.2	SRM ID	300
H.3	HTTP unicast SRM download service parameters.....	301
H.3.0	Introduction	301
H.3.1	HTTP URI	301
H.3.2	Complete SDP syntax for HTTP unicast SRM Download Service	301
H.4	FLUTE multicast SRM download service parameters	302
H.4.0	Introduction	302
H.4.1	FLUTE Session Version.....	302
H.4.2	FLUTE Session parameters.....	302
H.4.3	Complete SDP syntax for FLUTE multicast SRM Download Service	302
Annex I (normative):	Server-based Fast Channel Change for DVB-IPTV Systems	304
I.1	Scope	304
I.2	Server-based FCC: detailed specification	304
I.2.1	Introduction	304
I.2.2	DVB server-based FCC solution principle	304
I.2.3	DVB server-based FCC and DVB LMB RET	305
I.2.4	Server-based FCC architecture and terminology	306
I.2.4.1	Server-based FCC architecture	306
I.2.4.2	IETF and DVB terminology	306
I.2.5	FCC/ (LMB RET) unicast repair RTP sessions.....	307
I.2.6	RAMS RTCP FB signalling for DVB FCC	307
I.2.7	RAMS RTCP FB message formats	309
I.2.7.1	RAMS RTCP FB message format	309
I.2.7.2	Feedback Control Information for RAMS-R	310
I.2.7.3	Feedback Control Information for RAMS-I	311
I.2.7.4	Feedback Control Information for RAMS-T	312

I.2.8	HNED RTCP reporting for DVB FCC (/LMB RET)	312
I.2.9	FCC RTP burst	312
I.2.9.0	General.....	312
I.2.9.1	Terminating the burst.....	313
I.2.9.2	Burst packet loss recovery	313
I.2.10	Retransmission session transport address and SSRC identifiers	313
I.2.11	RTSP and FCC	314
I.2.12	QoS Priority settings	314
I.2.13	FCC (/LMB RET) Service discovery	314
I.2.14	SD&S FCC (/LMB RET) parameters overview.....	315

Annex J (normative): Companion stream Fast Channel Change for DVB-IPTV Systems.....317

J.1	Scope	317
J.2	Overview	317
J.3	Principles and examples (Informative).....	318
J.3.0	Introduction	318
J.3.1	Normal channel change, RAP and buffer filling delays	318
J.3.2	Channel change with companion stream, RAP delay-only improvement	319
J.3.3	Channel Change with companion stream, RAP and buffer delay improvements.....	320
J.4	HNED behaviour.....	322
J.5	Companion Stream Encoding and HNED requirements (Normative)	322
J.6	Companion stream-based FCC: Extension of the SD&S Broadcast Discovery Record (Normative)..322	

Annex K (informative): Dynamic Service Management Use Cases324

K.1	Example Use Cases and the Associated Message Sequences for Dynamic Service Management Service.....	324
K.1.0	Assumptions	324
K.1.1	Use Case UC1 - Switching on from Standby and requesting a first service with sufficient bandwidth.....	324
K.1.2	Use Case UC2 - change of service, sufficient bandwidth.....	325
K.1.3	Use Case UC3 - HNED2 Requesting a service - DSM negotiation needed	326
K.1.4	Use Case UC4 - HNED1 Requesting a service - DSM negotiation needed	327
K.1.5	Use Case UC5 - HNED2 queries data value from DSMM.....	327

K.2	Example implementation XML Schema for DSM Datamodel	328
-----	---	-----

Annex L (informative): Bibliography.....330

History	331
---------------	-----

Intellectual Property Rights

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

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

Foreword

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

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

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

Founded in September 1993, the DVB Project is a market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcast industry.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

1.0 General

The present document is an updated release of ETSI TS 102 034 "Transport of MPEG-2 TS Based DVB Services over IP Based Networks"; it is referred to as DVB-IPTV phase 1.6 and provides extensions to the set of standardized specifications published by DVB for deployments of DVB services over bi-directional IP networks.

Specifically, it adds support for the following new features:

- Dynamic Service Management (DSM) for enabling more effective usage of the limited access network bandwidth by smart selection of TV services at the appropriate bitrate
- IPv6 technologies
- DVB Companion Screens and Streams specification [125]
- BCGOffering extension to align with UK DTG D-Book 7 Part A v4 [i.11].

As in previous releases of the present document, the DVB-IPTV phase 1.6 work is limited to DVB services [1] encapsulated in MPEG-2 TS [52] covering Live Media Broadcast services (i.e. TV or radio styles), Media Broadcast with Trick Modes, Content on Demand services (CoD) and Content Download Services (CDS). These specifications define the mechanisms required in order for a consumer to be able to buy a standard DVB Home Network End Device (HNED), take it home, plug it into an IP network, choose and consume DVB services available over the IP network.

The interface to the HNED defined as IPI-1 in clause 4 represents the end-terminal interface for a DVB-IPTV service. This IPTV ecosystem can be extended with a home network content sharing model as defined in the DVB Home Network specification (DVB-HN) ETSI TS 102 905 [114], which uses the DLNA Guidelines [i.4] as its foundation.

Clause 4 describes the architectural framework defined for the present document and introduces a Home Network reference model. The content of the remaining clauses are described below.

1.1 Scope of the present document

1.1.1 What is within the scope

The present document provides specifications to be supported on the interface to the HNED defined as IPI-1 in clause 4 and supports both IP version 4 and IP version 6.

It provides a set of technical specifications which covers the following areas:

- The delivery of DVB MPEG-2 TS based services over bi-directional IP networks, both for Live Media Broadcast services (i.e. TV or radio styles) and Content on Demand services. Clause 7 on transport covers the encapsulation of MPEG-2 TS services for streaming delivery over IP and the protocols to be used to access such services. Quality of Service is covered in clause 11 and is based on Differentiated Services (DiffServ).
- The Service Discovery and Selection (SD&S) mechanism for DVB based A/V services over bi-directional IP networks. Clause 5 on SD&S defines the service discovery information, its data format and the protocols to use for carriage of this information. Both push and pull models of delivery are supported. Binarisation encoding of SD&S information is specified and can optionally be used if required. Support for advanced codecs, logical channel numbering and signalling regional DVB-IPTV services is provided.
- The use of command and control application-level protocol RTSP to control CoD services and optionally to join multicast services. This is covered in clause 6.
- Clause 8 deals with the assignment of an IP Address to a Home Network End Device (HNED) to get onto the network. The specification is based on DHCP and is restricted to the scenarios where an HNED has a single interface onto the home network and there is a single DNG per home network segment.
- The identification agent for the HNED specified in clause 9 of versions prior to release 1.4.1 of the present document, is deprecated and has been deleted.

- Clause 9 now specifies the File Upload System Stub (FUSS) which is mandatory and allows the system software of an HNED to be updated on a power-cycle or reboot. The sending of the system software will be handled by the mechanisms in the optional Remote Management and Firmware Update System for DVB-IPTV Services (RMS-FUS) specification [78].
- Network provisioning specified in clause 10 of versions prior to release 1.4.1 of the present document, is deprecated and has been deleted. This functionality is now provided by the Remote Management and Firmware Update Services (RMS-FUS) specification [78].
- Clause 10 now specifies Content Download Services (CDSs). CDSs provide the download of content items to a local storage of the HNED via a broadband IP connection. CDSs can be used to provide IPTV services in areas where a broadband connection suitable for streaming services is not available or prone to errors, for simultaneous delivery of multiple content items to HNEDs or for reduced cost offers as the bandwidth consumption may be limited compared to streaming services. Two types of services are supported: push download services where the distribution decision is taken by the service provider (without explicit request from the user) and pull download services where the download is requested by the user. Annex G provides CDS related information, that is expected to be part of other specifications in the future or that is optional for the present document.
- Clause 12 specifies SRM delivery over IP networks. SRMs are messages issued by the administrator of a Content Protection (CP) System that, when sent to devices that use that CP System, can revoke permission of certain devices or groups of devices to obtain content protected by that CP System. Clause 12 defines the announcement and download mechanisms for the delivery of SRMs to HNEDs over IP networks. Annex H defines the SDP syntax for SRM announcement services.
- Clause 13 specifies Dynamic Service Management. Dynamic Service Management is a feature to enable the HNED and/or user to make smarter decisions about which service to select out of a group of equivalent DVB services in order to provide an optimum service when multiple DVB services are offered to users' home.
- Discovery of Broadband Content Guides (inc. third party). The Broadband Content Guide itself is provided as a separate specification [62].
- Annex E defines an optional protocol for Application Layer FEC (AL-FEC) protection of streaming media for DVB-IPTV services carried over RTP transport. This AL-FEC protocol is a layered protocol with a base layer and zero, one or more optional enhancement layer(s). The base layer is a simple packet-based interleaved parity code based on a subset of [66]. The base layer is mandatory wherever AL-FEC is used. The enhancement layer is a Raptor code, as defined in [64] and [65] and may optionally be used to provide further packet loss protection.
- Annex F defines an optional retransmission mechanism (RET) to provide for protection against packet loss of DVB-IPTV services carried over RTP transport. It specifies the mechanism to provide immediate FeedBack (FB) towards the network using RTCP and how to retransmit the missing packets.

NOTE 1: Packet loss repair can be achieved using the optional AL-FEC solution, the optional retransmission solution or a combination of both solutions.

- Annex I defines an optional server-based Fast Channel Change (FCC) mechanism to reduce the Live Media Broadcast service switching response time. Similar to the RET solution, this FCC mechanism relies on a server that caches the recent content of the LMB service. The LMB service is carried over RTP transport, and RTCP is leveraged for control interaction between the HNED and the FCC server.
- Annex J defines an alternative optional Fast Channel Change (FCC) mechanism to reduce the Live Media Broadcast service switching response time, based on the provisioning of a multicast companion stream. This FCC solution is server-less, but has some impact on the quality of the displayed content during a transition period.

NOTE 2: Fast Channel Change for LMB can be realized either by the server-based FCC mechanism, or by the companion stream approach but not a combination of both.

- Annex K describes a number of use cases to explain the behaviour of DSM server change requests and other DSM Manager interactions. In addition, annex K contains a datamodel for the DSM Manager.

1.1.2 What is out of the scope

Amongst others, the following subjects are *not* covered in the present document:

- Support for non MPEG-2 TS based services.
- Specific support for Conditional Access or Content Protection.
- Network security and authentication.
- Trick modes (i.e. Pause, Fast Forward, etc.) for Live Media Broadcast services over multicast, e.g. network PVR services.
- Configuration of current retail routers and DNGs.

1.1.3 Additional Specifications for Home Network

The present document does not cover home networking. DVB has developed a separate specification for home networking published as ETSI TS 102 905 [114]. Clause 4 introduces a Home Network Reference Model.

1.1.4 DTDs and XML Schemas

The normative DTDs and XML schemas referenced by the present document are attached as separate files contained in archive ts_102034v020101p0.zip which accompanies the present document. The DTDs and XML schemas included in the present document are informative.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

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

The following referenced documents are necessary for the application of the present document.

- [1] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
- [2] ETSI TS 101 162: "Digital Video Broadcasting (DVB); Allocation of identifiers and codes for Digital Video Broadcasting (DVB) systems".
- [3] ETSI TS 101 812 (V1.3.2): "Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.0.3".
- [4] Void.
- [5] IEEE 802.1QTM-2005: "IEEE standard for Local and metropolitan area networks: Virtual Bridged Local Area Networks".
- [6] IEEE 802.2TM-1989: "Information Processing Systems - Local Area Networks - Part 2: Logic link control".

- [7] IEEE 802.3TM-2005/Cor 2-2007: "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 - Corrigendum 2: IEEE Std 802.3an-2006 10GBASE-T Correction".
- [8] IEEE P802.11TM-2012: "IEEE Standard for Information Technology- Telecommunications and information exchange between systems- Local and metropolitan area network- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".
- [9] IEEE 802.1DTM (2004): "IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges".
- [10] IETF RFC 768: "User Datagram Protocol".
- [11] IETF RFC 791: "Internet Protocol; DARPA internet protocol; Protocol specification".
- [12] Void.
- [13] IETF RFC 1034: "Domain names - concepts and facilities".
- [14] IETF RFC 1035: "Domain names - Implementation and specification".
- [15] Void.
- [16] IETF RFC 1101: "DNS Encoding of Network Names and Other Types".
- [17] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".
- [18] IETF RFC 1305: "Network Time Protocol (Version 3) Specification, Implementation and Analysis".
- [19] IETF RFC 1738: "Uniform Resource Locators (URL)".
- [20] IETF RFC 1630: "Universal Resource Identifiers in WWW".
- [21] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".
- [22] IETF RFC 1890: "RTP Profile for Audio and Video Conferences with Minimal Control".
- [23] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".
- [24] IETF RFC 2131: "Dynamic Host Configuration Protocol".
- [25] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".
- [26] IETF RFC 2181: "Clarifications to the DNS Specification".
- [27] IETF RFC 5234: "Augmented BNF for Syntax Specifications: ABNF".
- [28] IETF RFC 2241: "DHCP Options for Novell Directory Services".
- [29] IETF RFC 2250: "RTP Payload Format for MPEG1/MPEG2 Video".
- [30] IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".
- [31] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".
- [32] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".
- [33] IETF RFC 2475: "An Architecture for Differentiated Services".
- [34] IETF RFC 2485: "DHCP Option for The Open Group's User Authentication Protocol".
- [35] IETF RFC 2486: "The Network Access Identifier".

- [36] IETF RFC 2508: "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links".
- [37] IETF RFC 2563: "DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients".
- [38] IETF RFC 2610: "DHCP Options for Service Location Protocol".
- [39] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".
- [40] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".
- [41] IETF RFC 2937: "The Name Service Search Option for DHCP".
- [42] IETF RFC 2998: "A Framework for Integrated Services Operation over DiffServ Networks".
- [43] IETF RFC 3004: "The User Class Option for DHCP".
- [44] IETF RFC 3011: "The IPv4 Subnet Selection Option for DHCP".
- [45] IETF RFC 3023: "XML Media Types".
- [46] IETF RFC 3046: "DHCP Relay Agent Information Option".
- [47] IETF RFC 3376: "Internet Group Management Protocol, Version 3".
- [48] IETF RFC 5052: "Forward Error Correction (FEC) Building Block".
- [49] IETF RFC 3927: "Dynamic Configuration of IPv4 Link-Local Addresses".
- [50] ISO 3166 (all parts): "Codes for the representation of names of countries and their subdivisions".
- [51] ISO 639-2: "Codes for the representation of names of languages -- Part 2: Alpha-3 code".
- [52] ISO/IEC 13818-1 (1996): "Information technology -- Generic coding of moving pictures and associated audio information: Systems".
- [53] ISO/IEC 13818-9 (1996): "Information technology -- Generic coding of moving pictures and associated audio information -- Part 9: Extension for real time interface for systems decoders".
- [54] "Extensible Markup Language (XML) 1.0 (Fourth Edition)"; First published 4 February 2004, revised 16 August 2006, Jean Paoli, Tim Bray, François Yergeau, C. M. Sperberg-McQueen, Eve Maler.
- [55] "XML Schema Part 0: Primer Second Edition"; First published 2 May 2001, revised 28 October 2004, Priscilla Walmsley, David C. Fallside.
- [56] "XML Schema Part 1: Structures Second Edition"; First published 2 May 2001, revised 28 October 2004, David Beech, Henry S. Thompson, Murray Maloney, Noah Mendelsohn.
- [57] "XML Schema Part 2: Datatypes Second Edition"; First published 2 May 2001, revised 28 October 2004, Ashok Malhotra, Paul V. Biron.
- [58] ETSI TS 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".

NOTE: The support of Scalable Video Codec (SVC) is not defined in the present document.

- [59] ETSI TS 102 323: "Digital Video Broadcasting (DVB); Carriage and signalling of TV-Anytime information in DVB transport streams".
- [60] ETSI TS 102 822-3-1: "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".
- [61] ISO/IEC 23001-1 (MPEG-B): "Information technology -- MPEG systems technologies -- Binary MPEG format for XML".

- [62] ETSI TS 102 539: "Digital Video Broadcasting (DVB); Carriage of Broadband Content Guide (BCG) information over Internet Protocol (IP)".
- [63] Void.
- [64] ETSI TS 126 346: "Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs; (3GPP TS 26.346 Release 6)".
- [65] ETSI TS 102 472: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Content Delivery Protocols".
- [66] SMPTE specification 2022-1 (2007): "Forward Error Correction for Real-time Video/Audio Transport Over IP Networks".
- [67] SMPTE specification 2022-2 (2007): "Unidirectional Transport of Constant Bit Rate MPEG-2 Transport Streams on IP Networks".
- [68] Recommendation ITU-T H.610 (07/2003): "Full service VDSL - System architecture and customer premises equipment".
- [69] 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".
- [70] IETF RFC 3926: "FLUTE - File Delivery over Unidirectional Transport".
- [71] IETF RFC 5651: "Layered Coding Transport (LCT) Building Block".
- [72] IETF RFC 5775: "Asynchronous Layered Coding (ALC) Protocol Instantiation".
- [73] IETF RFC 3695: "Compact Forward Error Correction (FEC) Schemes".
- [74] IETF RFC 1952: "GZIP file format specification version 4.3".
- [75] IETF RFC 4566: "SDP - Session Description Protocol".
- [76] IETF RFC 2974: "SAP - Session Announcement Protocol".
- [77] IETF RFC 5053: "Raptor Forward Error Correction Scheme for Object Delivery".
- [78] ETSI TS 102 824: "Digital Video Broadcasting (DVB); Remote Management and Firmware Update System for DVB IPTV Services (Phase 2)".
- [79] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".
- [80] IETF RFC 3890: "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)".
- [81] IETF RFC 3388: "Grouping of Media Lines in SDP".
- [82] IETF RFC 3555: "MIME Type Registration of RTP Payload Formats".
- [83] IETF RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".
- [84] IETF RFC 4585 (July 2006): "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)".
- [85] IETF RFC 4588 (July 2006): "RTP Retransmission Payload Format".
- [86] IETF RFC 3489 (March 2003): "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)".
- [87] IETF RFC 3361 (August 2002): "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

- [88] IETF RFC 3397 (November 2002): "Dynamic Host Configuration Protocol (DHCP) Domain Search Option".
- [89] IETF RFC 3118 (June 2001): "Authentication for DHCP Messages".
- [90] IETF RFC 3442 (December 2002): "The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 2".
- [91] IETF RFC 3495 (March 2003): "Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration".
- [92] IETF RFC 3825 (July 2004): "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information".
- [93] IETF RFC 3925 (October 2004): "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)".
- [94] IETF RFC 4280 (November 2005): "Dynamic Host Configuration Protocol (DHCP) Option for Broadcast and Multicast Control Servers".
- [95] IETF RFC 4388 (February 2006): "Dynamic Host Configuration Protocol (DHCP) Leasequery".
- [96] IETF RFC 4578 (November 2006): "Dynamic Host Configuration Protocol Options for the Intel Preboot eXecution Environment (PXE)".
- [97] IETF RFC 4676 (October 2006): "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".
- [98] IETF RFC 4833 (April 2007): "Timezone Options for DHCP".
- [99] DSL Forum TR-069: "CPE WAN Management Protocol".
- [100] IETF RFC 3679 (January 2004): "Unused Dynamic Host Configuration Protocol (DHCP) Option Codes".
- [101] IETF RFC 4039 (March 2005): "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".
- [102] IETF RFC 4702 (October 2006): "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option".
- [103] ETSI TS 102 825-4: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification".
- [104] IETF RFC 4607 (August 2006): "Source-Specific Multicast for IP".
- [105] ETSI TS 102 006 (V1.3.2): "Digital Video Broadcasting (DVB); Specification for System Software Update in DVB Systems".
- [106] IETF RFC 2246: "The TLS Protocol Version 1.0".
- [107] IETF RFC 2818: "HTTP Over TLS".
- [108] IANA: "SMI Network Management Private Enterprise Codes".
- [109] ETSI TS 102 833: "Digital Video Broadcasting (DVB); File Format Specification for the Storage and Playback of DVB Services".
- [110] ETSI TS 102 770: "Digital Video Broadcasting (DVB); System Renewability Messages (SRM) in DVB Systems".
- [111] IETF RFC 5760: "RTP Control Protocol (RTCP) Extensions for Single-Source Multicast Sessions with Unicast Feedback".
- [112] IETF RFC 5506: "Support for Reduced-Size Real-Time Transport Control Protocol (RTCP): Opportunities and Consequences".

- [113] IETF RFC 5761: "Multiplexing RTP Data and Control Packets on a Single Port".
- [114] ETSI TS 102 905: "Digital Video Broadcasting (DVB); Technical Specification for DVB Services in the Home Network Phase 1".
- [115] ETSI TS 102 851: "Digital Video Broadcasting (DVB); Uniform Resource Identifiers (URI) for DVB Systems".
- [116] IETF RFC 6285: "Unicast-Based Rapid Acquisition of Multicast RTP Sessions".
- [117] IEEE 1003.1™: "IEEE Standard for Information Technology - Portable Operating System Interface (POSIX(R))".
- [118] IETF RFC 3810: "Multicast Listener Discovery Version 2 (MLDv2) for IPv6".
- [119] IETF RFC 4291: "IP Version 6 Addressing Architecture"
- [120] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration"
- [121] IETF RFC 4861: "Neighbor Discovery for IP Version 6 (IPv6)"
- [122] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"
- [123] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information"
- [124] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"
- [125] ETSI TS 103 286-2: "Digital Video Broadcasting (DVB); Companion Screens and Streams; Part 2: Content Identification and Media Synchronisation".
- [126] IETF RFC 950: "Internet Standard Subnetting Procedure".
- [127] IETF RFC 3633: "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".
- [128] IETF RFC 5970: "DHCPv6 Options for Network Boot".
- [129] IETF RFC 3513: "Internet Protocol Version 6 (IPv6) Addressing Architecture".
- [130] IETF RFC 5908: "Network Time Protocol (NTP) Server Option for DHCPv6".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI TR 101 211: "Digital Video Broadcasting (DVB); Guidelines on implementation and usage of Service Information (SI)".
- [i.2] Void.
- [i.3] IETF RFC 3171: "IANA Guidelines for IPv4 Multicast Address Assignments".
- [i.4] IEC 62481-1: "Digital Living Network Alliance (DLNA) Home Networked Device Interoperability Guidelines - Part 1: Architecture and Protocols".
- [i.5] ETSI TS 102 542 (all parts): "Digital Video Broadcasting (DVB); Guidelines for the implementation of DVB-IPTV Phase 1 specifications".

- [i.6] DVB BlueBook A128: "DVB-IP Phase 1.3 in the context of ETSI TISPAN NGN".
- NOTE: Available at http://www.dvb.org/technology/standards/a128.ipi2480r9.DVB-IP1.3_in_ETSI_TISPAN_NGN.pdf.
- [i.7] ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture".
- [i.8] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".
- [i.9] ETSI TS 102 826: "Digital Video Broadcasting (DVB); DVB-IPTV Profiles for TS 102 034".
- [i.10] IETF RFC 3306: "Unicast-Prefix-based IPv6 Multicast Addresses".
- [i.11] UK DTG "D-Book 7 Part A" Version 4 (May 2014).

3 Definitions, abbreviations and notations

3.1 Definitions

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

bridge component: OSI layer 2 connecting component, that connects two or more link layer components, not necessarily using different technologies

NOTE: A bridge is usually called either a hub or a (layer 2) switch, where a hub typically forwards all the data coming in on one of the ports to all the other ports and a switch provides some additional functionality such as forwarding packets only to a specific port.

CDS HNED storage: storage on the HNED dedicated to CDSs of a single service provider

component: specific set of functionalities

NOTE: It can offer this functionality to other components in the same device.

connecting component: component which is used to connect link layer components with each other

Content Download Service (CDS): service that provides download delivery of content items to the local storage of the HNED

NOTE: The consumption is independent of the delivery.

content item: editorially coherent grouping of one or more audiovisual or generic data files which are intended to be consumed in conjunction with each other

content provider: entity that owns or is licensed to sell content or content assets

Content on Demand (CoD): program provided at the request of the end user for direct consumption (real-time streaming)

Content Service Provider (CSP): entity which acquires/licenses content from Content Providers and packages this into a service

customer: person(s) contracted to receive IPTV services delivered on the access network and responsible for administering that connection

NOTE: The terms "home" and "customer" are synonymous in the context of the present document.

Delivery Network (DN): network connecting the Delivery Network Gateway (DNG) and service providers

Delivery Network Gateway (DNG): device that is connected to one or multiple delivery networks and one or multiple home network segments

Destination Transport address: combination of the IP destination address and destination UDP port

Download Session Description: collection of parameters that describe how a content item can be downloaded within a download session using the DVB-IPTV CDS

DSM Manager: function to provide information to HNEDs about equivalent services

DSM Service: service to provide the feature defined under "Dynamic Service Management"

DVB CoD RET server: interacts with the RET clients by responding to RET requests with RET packets

DVB-IPTV service: one or more programmes under the control of a service provider delivered over IP

NOTE: The programmes can be made available either as part of a schedule or on demand and either for direct consumption (Live Media Broadcast or Content on Demand Services) or for local storage (CDSs).

DVB FCC client: part of the HNED that makes use of the RAMS protocol to request, receive and control a burst of unicast RTP packets from a DVB FCC server, a process that is initiated before the normal LMB connection process

DVB FCC server: interacts with the DVB FCC client through RAMS and provides the RTP burst from its cache

DVB LMB RET server: interacts with RET clients, mainly by responding to RET requests with RET packets

DVB RET client: part of the HNED that makes use of the RET protocol to request and receive RET packets from a DVB (CoD/LMB) RET server when it detects packet loss

Dynamic Service Management: feature to enable more efficient use of bandwidth and media services in a home by providing a message set to signal equivalent services

event: grouping of elementary broadcast data streams with a defined start and end time belonging to a common service

EXAMPLE: First half of a football match, News Flash, first part of an entertainment show.

Feed Forward (FF): RTCP FB message relayed by an LMB RET server to DVB RET clients

gateway component: connecting component that connects two or more link layer components of typically different technologies together (it can function at OSI layers 4 through 7)

headend: functionality upstream from the DNG responsible for managing the HNEDs in a home and serving content and metadata to those HNEDs

home: 'location' where the access network is terminated (IPI-1), and where the connection into the complete combination of equipment is located

NOTE 1: The "location" is used in a logical way.

NOTE 2: The terms "home" and "customer" are synonymous in the context of this clause.

Home Network End Device (HNED): device that is connected to the IP network via the IPI-1 interface through which DVB-IPTV services are consumed, and that provides the functionality for DVB-IPTV content navigation and rendering

NOTE: HNED and IPI-1 are one-to-one associated with each other: an HNED per definition exhibits an IPI-1 logical interface, and vice versa, an IPI-1 interface is terminated by an HNED.

Home Network Segment (HNS): consists of a single link layer technology and provides a layer 2 connection between home network end devices and/or connecting components

Internet Service Provider (ISP): party offering an Internet access service to the end-user

link layer component: OSI layer 2 component consisting of link layer technology and which is used to provide connectivity between devices

EXAMPLES: Ethernet, DVB-RC, IEEE 802.11 [8].

MPEG-2: Refers to ISO/IEC 13818-1 [52].

NOTE: Systems coding is defined in ISO/IEC 13818-1 [52]. The real time interface specification is defined in ISO/IEC 13818-9 [53].

original RTP session: RTP session where the RTP packets are original packets (not retransmitted)

package: collection of DVB services marketed as a single entity

primary multicast session: SSM session which RTP receivers can join at a random point in time

program: collection of program elements

NOTE: Program elements may be elementary streams. Program elements need not have any defined time base; those that do, have a common time base and are intended for synchronized presentation. Taken from ISO/IEC 13818-1 [52].

pull download service: Content Download initiated by the user

push download service: Content Download initiated by the service provider without explicit request by the user

Random Access Point (RAP): represents an Intra-encoded (I)-frame

Rapid Acquisition of Multicast RTP sessions (RAMS): RTCP FB messages and protocol as defined in IETF RFC 6285 [116], for rapid acquisition of RTP multicast session

RET-enabled CoD/LMB: CoD/LMB service where RET-enabled HNED can make use of DVB RET protocols for packet loss repair

RET-enabled HNED: HNED that has a DVB RET client

router component: OSI layer 3 connecting component which connects two or more link layer components to each other, not necessarily of the same type

NOTE: A router is able to select among multiple paths to route packets through the network based on a destination address available in the packet. The only OSI layer 3 type considered is IP.

RTP session: As defined in clause 3 of IETF RFC 3550 [21].

Service Provider (SP): entity providing a service to the end-user

NOTE: See clause 4 on architecture. In the context of the present document, SP will mean a Service Provider providing DVB-IPTV services.

session multiplexing: scheme by which the original stream and the retransmission stream are sent in different RTP sessions

source transport address: combination of the IP source address and source UDP port

SP offering: set of streams or services a Service Provider proposes to the end-user

SSRC multiplexing: scheme by which the original stream and the retransmission stream are sent in the same RTP session with different SSRC values

transport stream: data structure defined in ISO/IEC 13818-1 [52]

TS Full SI: transport stream with embedded service information as defined by DVB in ETSI EN 300 468 [1] with the exception of the network information table NIT

NOTE: The NIT table may be omitted as it has no meaning in the context of IP services.

TS - Optional SI: transport stream with MPEG PSI (PAT and PMT tables) as defined in ISO/IEC 13818-1 [52], all other MPEG-2 and DVB tables are optional

3.2 Abbreviations

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

A/V	Audio/Video
ABNF	Augmented Backus-Naur Form
ALC	Asynchronous Layered Coding
AL-FEC	Application Layer Forward Error Correction
ARP	Address Resolution Protocol
ASM	Any Source Multicast
AV	Audio Video
AVPF	Audio-Visual Profile Feedback
BCG	Broadband Content Guide
BCMCS	3GPP2 BroadCast MultiCast Service
BGD	Broadband Gateway Device
BiM	Binary MPEG format for XML
BLP	Bitmask Lost Packet
BNF	Backus-Naur Form
BW	BandWidth
CA	Civic Address
CCI	Congestion Control Identifier
CDP	Content Delivery Protocol
CDS	Content Download Service
CI	Content Identifier
CMD	Carousel Multicast Download
CoD	Content on Demand
CoS	Class of Service
CP	Content Protection
CPCM	Content Protection and Copy Management
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
CRID	Content Reference IDentifier
CSP	Content Service Provider
CSRC	Contributing SouRCe
DF	Do not Fragment
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DLNA	Digital Living Network Alliance
DNG	Delivery Network Gateway
DNS	Domain Name System
DSCP	Differentiated Services CodePoint
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSM	Dynamic Service Management
DSM-CC	Digital Storage Media - Command and Control
DSMCC	Digital Storage Media Command and Control
DSMM	Dynamic Service Management Manager
DTD	Document Type Declaration
DTG	Digital TV Group
DTH	Direct To Home
DTV	Digital Television
DUID	DHCP Unique IDentifier
DVB SI	DVB Service Information
DVB	Digital Video Broadcasting
DVB-RC	Digital Video Broadcasting - Return Channel
DVB-S	Digital Video Broadcasting - Satellite
DVBSTP	DVB SD&S Transport Protocol
EBU	European Broadcasting Union
ECM	Entitlement Control Message
EMM	Entitlement Management Message
ESI	Encoding Symbol ID

EUI	Extended Unique Identifier
FB	FeedBack

NOTE: Typically including negative acknowledgements, i.e. NACK.

FCC	Fast Channel Change
FCI	Feedback Control Information
FDT	File Delivery Table
FEC	Forward Error Correction
FEC-SF	FEC Streaming Framework
FF	Feed Forward
FLUTE	File Delivery over Unidirectional Transport
FMT	Feedback Message Type
FQDN	Fully Qualified Domain Name
FUS	Firmware Update Service
FUSS	File Upload System Stub
GOP	Group of Pictures
GZIP	GnuZIP
HD	High Definition
HE	Head End
HEL	Header Extension Length
HET	Header Extension Type
HN	Home Network
HNED	Home Network End Device
HNS	Home Network Segment
HTC	Head-end Time Clock
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	IDentifier
IDF	Ile De France
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPDC	Internet Protocol DataCasting
IPI	Internet Protocol Infrastructure
IPTV	Internet Protocol TeleVision
IPv4	Internet Protocol version 4
IRC	Internet Relay Chat
ISDB	Integrated Services Digital Broadcasting
ISN	Initial Sequence Number
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union-Telecommunication
JTC	Joint Technical Committee
LCT	Layered Coding Transport
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
LMB	Live Media Broadcast
LPR	Liner PRinter
MAC	Media Access Control
MBwTM	Media Broadcast with Trick Modes
MC	MultiCast
MHP	Multimedia Home Platform
MIME	Multipurpose Internet Mail Extension
MLD	Multicast Listener Discovery
MP@ML	Main Profile at Main Level
MPEG	Moving Pictures Expert Group
MPTS	Multiple Program Transport Stream
MS	Multiple Server

MSN	Message Sequence Number
MTS	MPEG-2 Transport Stream
MTU	Maximum Transmission Unit
NACK	Negative ACKnowledgement
NAT	Network Address Translation
NDS	Novell Directory Services
NENA	National Emergency Number Association
NIT	Network Information Table
NNTP	Network News Transport Protocol
NPT	Normal Play Time
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSN	Original Sequence Number
OTI	Object Transmission Information
OUI	Organizational Unique Identifier
PAT	Program Association Table
PCR	(MPEG-2) Program Clock Reference
PHY	PHYSical
PID	Packet ID
PIDF	Presence Information Data Format
PiP	Picture-in-Picture
PLL	Phased Locked Loop
PMT	Program Map Table
PSI	Program Specific Information
PT	Payload Type
PTS	Presentation Time Stamp
PVR	Personal Video Recording
PXE	Preboot eXecution Environment
QoS	Quality of Service
QRC	Query-Response Channel
RAM	Random Access Memory
RAMS	Rapid Acquisition of Multicast RTP Sessions
RAP	Random Access Point
RET	RETransmission
RFC	Request For Comments
RMS	Remote Management and Firmware
RR	Receiver Report
RS	Retransmission Server
RSI	Receiver Summary Information
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
RTT	Round Trip Time
RW	Read Write
SAP	Session Announcement Protocol
SBL	Source Block Length
SBN	Source Block Number
SD	Standard Definition
SD&S	Service Discovery and Selection
SDES	Source DEscription
SDP	Session Description Protocol
SDT	Service Description Table
SFMT	Sub Feedback Message Type
SI	Service Information
SIP	Session Initiation Protocol
SLAAC	StateLess Address AutoConfiguration
SLP	Service Location Protocol
SMD	Scheduled Multicast Download
SMPTE	Society of Motion Picture and Television Engineers
SMTP	Simple Mail Transport Protocol
SN	Sequence Number
SNTP	Simple Network Time Protocol

SOAP	Simple Object Access Protocol
SP	Service Provider
SPI	Source Packet Information
SPIIL	Source Packet Information Length
SR	Sender Report
SRBT	Sub-Report Block Type
SRM	System Renewability Message
SRMID	SRM IDentifier
SRV	SeRVice, specific DNS RR
SS	Single Server
SSL	Secure Socket Layer
SSM	Source Specific Multicast
SSRC	Synchronization Source
STC	(MPEG-2) System Time Clock
STS	
SW	
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIAS	Transport Independent Application Specific maximum bandwidth
TLS	Transaction Layer Security
TLV	Type Length Value
TOI	Transport Object Identifier
ToS	Type of Service
TS	Transport Stream
TSI	Transport Session Identifier
T-STD	(MPEG-2) Transport Stream System Target Decoder
TTL	Time To Live
TV	TeleVision
TVA	TV Anytime
TZ	Time Zone
UD	Unicast Download
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
UTF	Unicode Transformation Format
VCR	Video Cassette Recorder
VOD	Video On Demand
WWW	World Wide Web
XML	eXtensible Markup Language
XOR	eXclusive OR
XSD	XML Schema Document
ZIP	Zoning Improvement Plan

3.3 Notations

3.3.1 Augmented Backus-Naur Form (ABNF)

3.3.1.1 General rules

The present document uses the Augmented Backus-Naur Form (ABNF) conform to IETF RFC 5234 [27], for syntax specification.

The following general rules are defined:

```

host          = domainName / ipAddress
domainName   = *(domainNameLabel '.') topLabel ['.']
domainNameLabel = label / aceLabel
label         = ALPHANUM *('-' / ALPHA) ALPHA
topLabel      = ALPHA *('-' / ALPHA) ALPHA
name          = ALPHA *(( '-' ALPHA) / ALPHA)
aceLabel      = acePrefix punnyCode
                                         ; E.g. www.example.org
                                         ; E.g. legal-label6
                                         ; E.g. com
                                         ; E.g. legal-name6
                                         ; Internationalized Domain Name

```

```

acePrefix      = 'x' 'n' '-' '-'
               ; E.g. 'xn--' or 'XN--'
punyCode      = *('-' / ALPHANUM)
ipAddress     = dottedDecimal / 1*10(DIGIT)           ; E.g. 80.78.123.11 or 1347320587
dottedDecimal = 1*3(DIGIT) '.' 1*3(DIGIT) '.' 1*3(DIGIT) '.' 1*3(DIGIT)
version       = 1*3(DIGIT) '.' 1*3(ALPHANUM)          ; E.g. 1.2A
version       = / 1*3(DIGIT) '.' 1*3(ALPHANUM) '.' 1*3(ALPHANUM) ; E.g. 1.11C.32

```

3.3.1.2 Core rules

The following set of ABNF core rules derived from [27] are defined:

```

ALPHA   = %x41-5A / %x61-7A ; A-Z / a-z
BIT     = "0" / "1"
CHAR    = %x01-7F ; any 7-bit US-ASCII character, excl. NUL
CR      = %x0D ; carriage return
CRLF   = CR LF ; Internet standard newline
CTL     = %x00-1F / %x7F ; control characters
DIGIT   = %x30-39 ; 0-9
ALPHANUM= ALPHA / DIGIT ; A-Z / a-z / 0-9
DQUOTE  = %x22 ; " (Double Quote)
HEXDIG  = DIGIT / %x41-46 / %x61-66 ;
HTAB    = %x09 ; horizontal tab
LF      = %x0A ; linefeed
LWSP   = *(WSP / CRLF WSP) ; linear white space (past newline)
OCTET  = %x00-FF ; 8 bits of data
SP     = %x20 ; space
VCHAR  = %x21-7E ; visible (printing) characters
WSP    = SP / HTAB ; white space

```

NOTE 1: The rules for constructing domainName are aligned with IETF RFC 1035 [14], IETF RFC 1101 [16] (First mention of labels starting with digits), IETF RFC 1738 [19] (URL), IETF RFC 2181 [26] (Clarifications), IETF RFC 2396 [31] (including the optional trailing dot), IETF RFC 2486 [35] (URI) and ICANN agreements with domain registrars (www.icann.org/tlds/agreements/pro/registry-agmt-appc-26aug03.htm and www.icann.org/tlds/agreements/name/registry-agmt-appc-13-03jul01.htm).

NOTE 2: ABNF is used in several places throughout the present document.

4 Architecture

4.1 Introduction

4.1.0 Overview

The present document addresses the protocols and interactions for the data, management, signalling and control plane between the service provider and a DVB-IPTV end-terminal, referred to as the Home Network End Device (HNED). The prime target for IPTV standardization by DVB is the logical interface of the HNED, referred to as IPI-1, to enable high-volume low-cost equipment.

It shall be noted that an end-to-end IPTV architecture specification is outside the scope of the present document, and work has been done elsewhere to consider it.

NOTE: Other standards development organizations have specified end-to-end IPTV architectures defining both the logical network components and their interfaces, for example ETSI TISPAN. Specifically the DVB blue book A128 [i.6] discusses how the DVB IPI-1 (sub-)interface (elements) fits in with the ETSI TISPAN IPTV architecture specifications [i.7] and [i.8].

The IPI-1 interface can be used to deliver content and metadata into the DVB-HN to be consumed by DVB-HN devices, as defined in [114], with the HNED acting as a DVB HN Broadband Gateway Device (BGD). [114] defines how content sharing and local content management can be implemented in a home network across DVB HN devices.

4.1.1 Domains and Actors in an IPTV system

IPTV is generally deployed as a subscription-based service where several domains are involved. Figure 1 depicts the different IPTV domains and the connectivity relative to the layering model described in the OSI reference model (X.200). The four identified "domains" in Figure 1 can be associated with different "actors" in the IPTV delivery chain as described below.

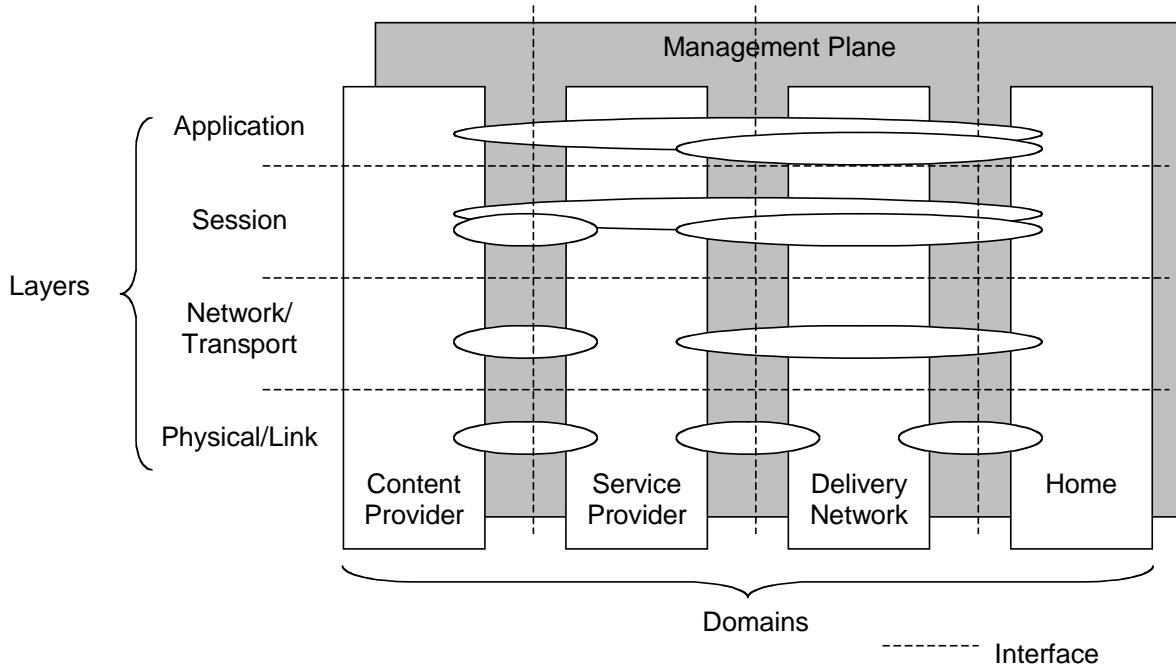


Figure 1: Layer model showing the relationship of the "domains" to the OSI based stack layers

The four communicating network domains are as follows:

- Content Provider: the entity that owns or is licensed to sell content or content assets and provides the original descriptive metadata. Although the Service Provider is probably the actor with which the user will have a commercial agreement in order to access content, a direct logical information flow may be set up between Content Provider and Home client e.g. for rights management and protection. This flow is shown in the layered model.
- Service Provider: the entity providing a service to the end-user. Different types of service provider may be relevant for DVB services on IP, e.g. simple Internet Service Providers (ISPs) and Content Service Providers (CSPs). In the context of DVB services on IP, the CSP acquires/licenses content and metadata from one or more Content Providers and packages this into a service. In this case the service provider is not transparent to the application and content information flow.
- Delivery Network: the entity connecting clients and service providers. The delivery system usually is composed of access networks and core or backbone networks, using a variety of network technologies. The delivery network is transparent to the IP traffic, although there may be timing and packet loss issues relevant for A/V content streamed on IP. The Delivery Network is owned and controlled by a Network Provider.
- Home: the domain where the A/V services are consumed. In the home one or more IPTV end devices (HNEDs) may be used for managed IPTV service consumption, where each HNED acts as the IPTV service consumption end-point. Additionally, there may also be sharing of DVB IPTV delivered content and metadata locally in the home network across devices inside the home network. Such local content sharing system is specified by DVB in DVB HN [114]. See clause 4.1.2.

In any specific business case a single organization may fulfil several of the network functions described above.

As mentioned above the Service Provider entity covers various kinds of Service Provider types, especially broadband ISPs and CSPs. It should be noted that although we treat these two business roles separately, a single company could very well act in both roles. In such a case the end user could be offered a single subscription covering both the ISP and the CSP service offerings (see below).

It is noted that today's Internet business models often involve so called virtual SPs, which means that the SP relies on some other party, typically a wholesale IP network operator, to implement and run all (or parts) of the service production platform. However, in the present document we do not distinguish any virtual SP roles - whether the SP owns the service production platform or "out-sources" the platform is irrelevant for this model since we simply look at the services and functions of each domain. It is also noted that in some countries, the access provider and the ISP may be different parties. In this context, however, those are not treated separately, but the ISP is the only party covered.

The "access provider" could for example provide the end device with the IP address. However, in order to simplify the description we cover such potential access provider services/functions under the ISP role.

4.1.2 The Home Network Domain

4.1.2.1 HNED as end point

In the context of the present document, the concept of home network domain is confined to the physical home network that interconnects an HNED with the broadband access network through the Delivery Network Gateway (DNG) function, and where the HNED is considered the end-point in the IPTV ecosystem. There may be multiple HNEDs connected to the same DNG. The detailed functionality of the DNG is not defined in the present document, and the basic architecture is shown in Figure 2.

The DVB HNED device is logically connected to the network by means of the IPI-1 interface over which the network/transport, session and application layer protocol interactions occur for each of the various IPTV service functions considered in the present document.

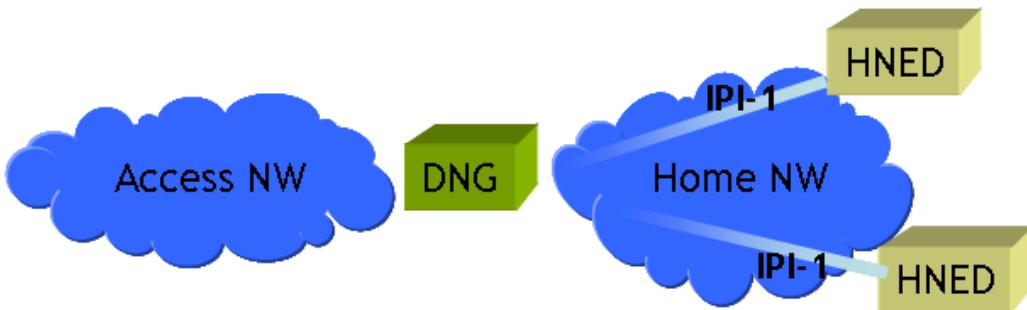


Figure 2: DVB HNEDs and associated IPI-1 interfaces in a home network

The DNG and HNED can be described as follows:

- **Delivery Network Gateway (DNG):** the device that connects the home network domain with the broadband access network. It can be a so-called "null" device, a wire interconnecting the networks on OSI layer 1 or it can function as a bridge or router interconnecting different link layer technologies. It may also act as a gateway also providing functionality on the OSI layer 4 and above but that may be specific to the DNG or service provider.
- **Home Network End Device (HNED):** as defined in clause 3.1, the device that is connected to the IP network via the IPI-1 interface through which DVB IPTV services are consumed, and that provides the functionality for DVB-IPTV content navigation and rendering.

NOTE: HNED and IPI-1 are one-to-one associated with each other: an HNED per definition exhibits an IPI-1 logical interface, and vice versa, an IPI-1 interface is terminated by an HNED.

The following high-level characteristics apply to the Home Network domain consisting of DNG and HNED(s), with respect to the DVB IPTV service architecture:

- 1) A home network can be simultaneously connected to multiple and heterogeneous delivery networks, but can only be connected to a broadband access network by means of a single DNG.
As an example, in a typical scenario xDSL and DVB-S2 connectivity may both be available at the home.
- 2) End users may be able to choose the IPTV service provider based on the available connectivity and hence the metadata (SD&S as described in clause 5), subject to contractual restrictions which may apply.
As an example, the ISPs and the CSPs may be independent from each other.

- 3) Different end users in the same home network may be able to select different IPTV service providers subject to the available metadata (SD&S).
- 4) End users may be able to access DVB content from a DVB IPTV delivery network using multiple HNEDs in the home, subject to contractual restrictions which may apply.

Figure 2a: Void

Figure 2b: Void

4.1.2.2 DVB Home Network (DVB HN) content sharing

The DVB IPTV service offerings and consumption, for which the protocols on the IPI-1 interface are defined in the present document can be extended with a home network content sharing model as defined in the DVB Home Network (DVB-HN) specification ETSI TS 102 905 [114], which uses the DLNA Guidelines [i.4] as its foundation.

This enables a device hosting the DVB IPTV HNED functionality, to act as a contribution channel providing the necessary translation methods to expose content and metadata on the DVB-HN home network, therefore making it possible to view the DVB IPTV content on the DVB-HN players subject to restrictions where they apply.

ETSI TS 102 905 [114] specifies how DVB content can be shared between logical devices within the home domain, by defining DVB Home Network (DVB HN) logical functions, HN device classes and the associated DVB IPI-HN interfaces. The basic architecture is depicted in Figure 2c. Note that this is a logical representation, and multiple logical devices may be combined into a single physical device, e.g. a single physical device incorporating server and player connected through a DVB IPI-HN interface.

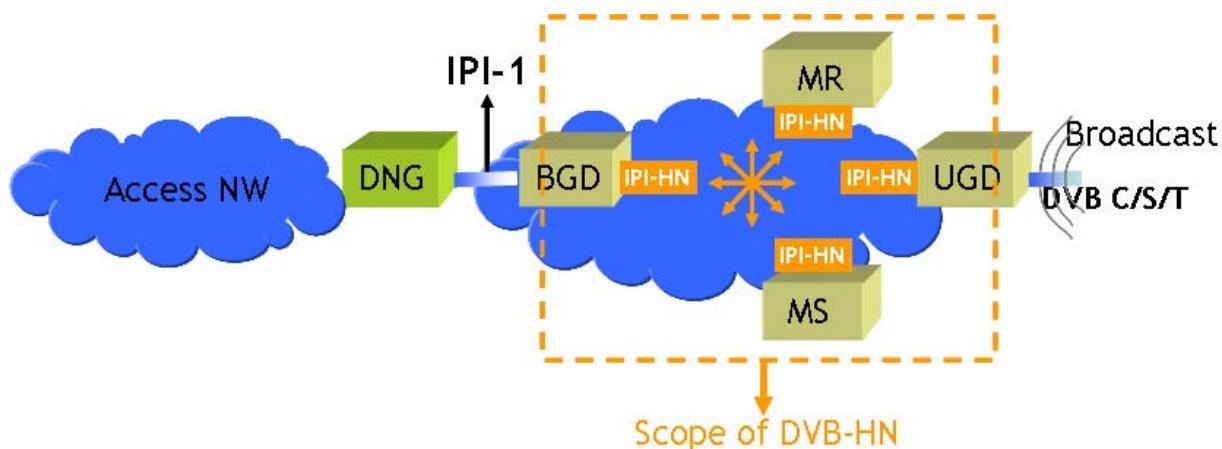


Figure 2c: DVB IPI-HN architecture and scope

The DVB IPI-1 interface is independent of the DVB IPI- HN interface, although both can co-exist within the same physical home network domain, and DVB IPI-1 and DVB IPI-HN interface can be simultaneously present on the same PHY interface of a device connected to the home network. Physical devices may combine DVB HNED function and any DVB HN logical function.

4.1.2a High-level Service Flows in a DVB IPTV network

Figure 2d is an expansion of Figure 2 and schematically depicts the service flows on the IPI-1 interface related to the main services specified in the present document.

The main services are:

- Service and Service Provider Discovery.
- Live Media Broadcast (LMB) Service connection and streaming.
- Content-on-Demand (CoD) and Live Media Broadcast with Trick Mode (LMBwTM) Service Selection, streaming and streaming control.
- Content Download Service (CDS) selection and download.

Once the HNED is equipped with an IP address, the HNED engages in the following steps:

- Step 0: Through RMS-FUS, the HNED can be provided with the right configuration (e.g. at boot-up).
- Step 1: The DVB HNED first performs service provider discovery (e.g. through SD&S or via DHCP) and hence connects to an SD&S entry point.
- Steps 2 & 3: The DVB HNED discovers services by connecting to the SD&S server of a specific Service Provider and/or by receiving information from the Broadband Content Guide (optional) delivery server.

After having received all necessary metadata, the HNED can start consuming other services from the DVB IPTV Service Provider of its choice as exemplified through flows 4, 5 and 6 in Figure 2d.

Flow 4 in Figure 2d involves the connection to a Live Media Broadcast Service transported over multicast and subsequent streaming whereas flow 5 depicts the connection of an HNED to a Content-on-Demand Server (using RTSP) and subsequent consumption of the unicast content. Flow 6 depicts the connection to and consumption of the Content Download Service (unicast or multicast).

It shall be noted that not all services defined in the present document need to be implemented in an IPTV system or need to be supported by an HNED on the IPI-1 interface to claim compliance to the present document. In order to facilitate and maximize the stepwise deployment of IPTV services, [i.9] defines a set of service oriented profiles. Examples are LMB profile, CoD profile, etc.

Clause 4.1.3 provides an overview of all protocols that have been defined in the present document for the IPI-1 interface in order to support the services described herein.

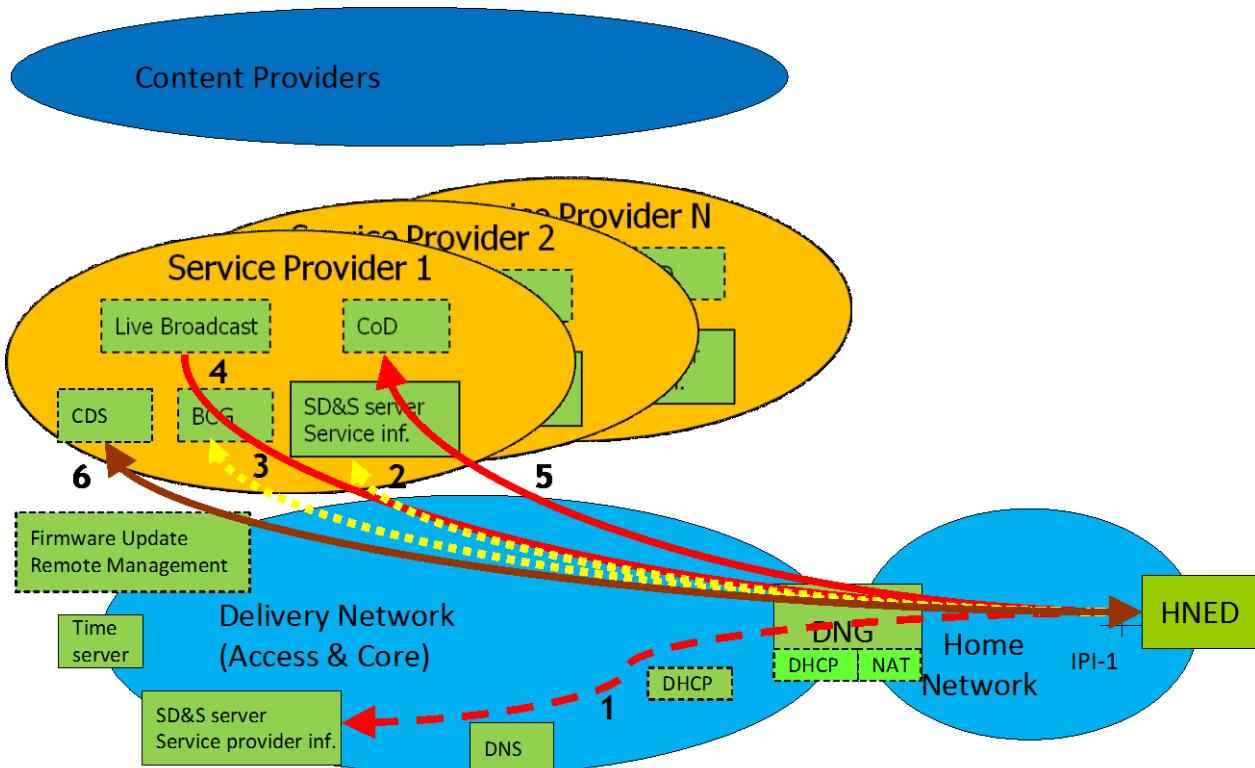


Figure 2d: Schematic overview of the main service flow interactions in a DVB IPTV network

4.1.3 Diagram of the DVB-IPTV Protocol Stack

Figure 3 is a logical diagram of the high-level protocols on the IPI-1 interface, specified in the present document for enabling DVB services over IP-based networks and the associated delivery and network support services. The organization of this protocol stack is based on the hierarchical structure frequently applied in equipment design, i.e. service offering and applications, middleware and functions, IP protocols and transport, and phy/MAC/link layers. This follows the ISO/OSI layering convention in general terms.

The top layer of this stack signifies the service offering intended by the Service Provider. This consists of programs, information about programs, multicast- and/or unicast IP addresses; in short, the essential items needed to enable a DVB service over an IP network.

The middleware and functions layer includes those functions described in the present document and other DVB supporting documents, the text colours are unique to the functions or groups of functions and those colours map down to the IP protocol and transport layer of the diagram.

The colour coding used is:

- QoS = red.
- Multicast service connection and management = black.
- Reliability of delivery/LMB Fast Channel Change = green.
- DVB AV and data services and metadata = blue.
- Remote management and firmware update = yellow.
- Content Download Service (CDS) = brown.
- HNED provisioning and boot procedures = purple.

The IP protocol and transport layer attempts to identify which protocols and transports are required and map the usage of those protocols and transports to the functions of the layers above using the colour coding. Where the protocol is shown in black it indicates that it is required by multiple functions, e.g. DVBSTP, HTTP, etc.

In principle the protocols required for transport of elements of the service offering via IP networking are independent of the physical layers below the IP networking layer and the present document is generally agnostic to the physical layer technology.

The software stack diagram is shown for information only and is not normative.

The HNED is an IP compliant device; on its IPI-1 interface it supports the requirements laid down in IETF RFC 1122 [17]. HTTP, TCP, UDP and IP are available to the HNED as networking and transport protocols.

The following clauses mention the protocols and protocol-related markings, usage of which is specified in the clauses of the present document.

Information for service discovery and selection services is assembled according to the SD&S protocol, specified in clause 5. The SD&S protocol for multicast (push) services is transported in IP packets according to the DVBSTP transport protocol, also specified in clause 5. For unicast (pull) services the SD&S information is transported via HTTP. An SD&S entry point can be implemented using a DNS mechanism, specified in clause 5.

The Real-Time Streaming Protocol (RTSP) is used for delivery and control of content on-demand services and optionally can also be used for control of the delivery of Live Media Broadcast services, e.g. TV and audio (radio) programs. The specification of this usage can be found in clause 6.

The Audio and Video streams and the Service Information are multiplexed into a valid MPEG-2 Transport Stream, according to [52]. The resulting MPEG-2 packets are encapsulated directly in UDP or in RTP/UDP for streaming delivery, with DSCP packet markings for quality of service. Streaming delivery of MPEG-2 TS on IP is specified in clause 7. The use of RTCP, e.g. to send information to receivers about transmission statistics, and of IGMP and MLD to join and leave multicast streams, is also specified in clause 7.

DSCP packet markings and Ethernet priority setting for quality of service are specified in clause 11.

The DHCP protocol is used to configure the HNED with an IP address. The detailed mechanisms and the options for this and related other functions are specified in clause 8. Real time clock services or accurate network time services are implemented using respectively SNTP or NTP protocol.

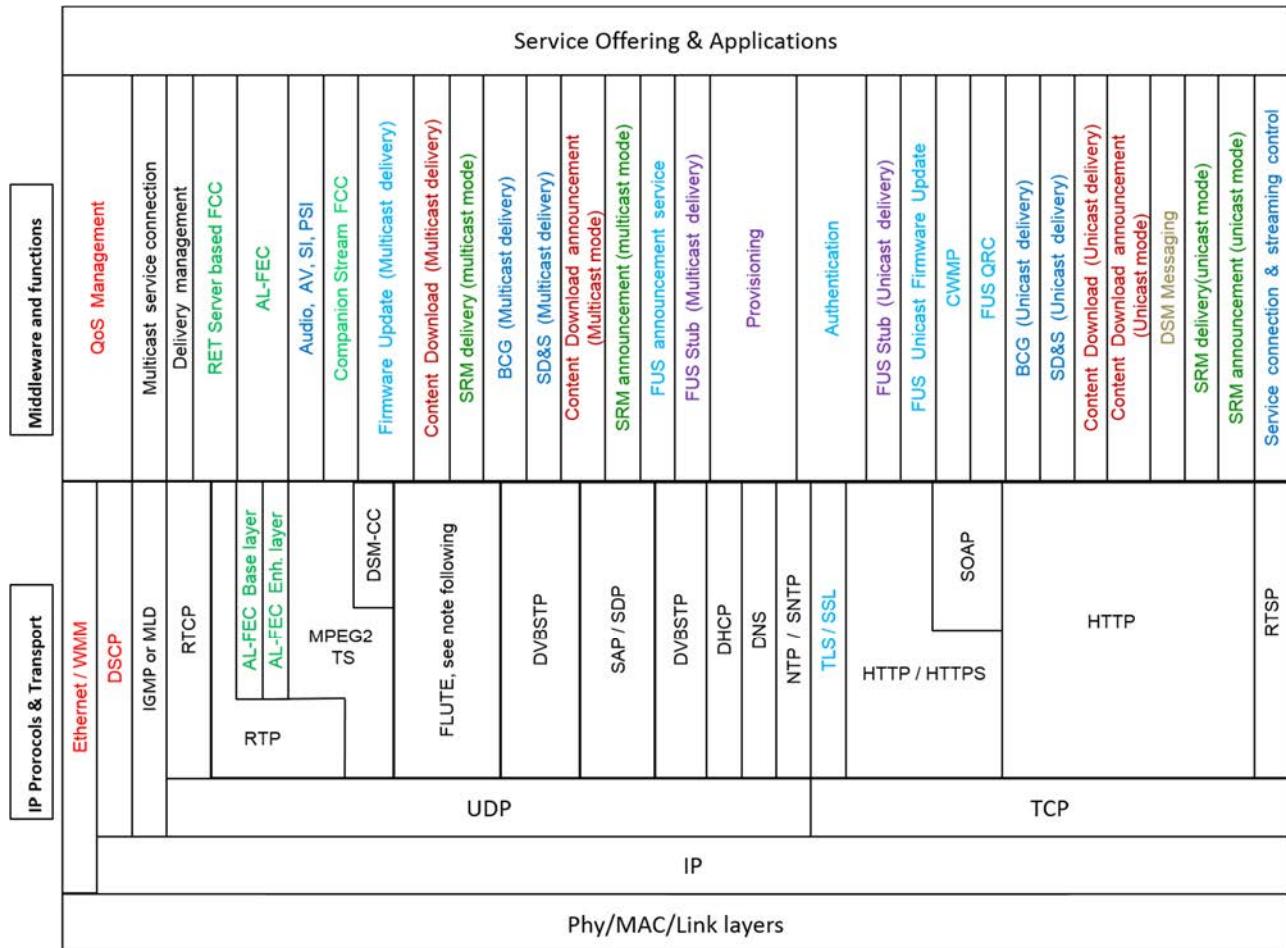
The initial boot procedure uses a stub file (FUSStub) downloaded over HTTP for unicast or acquired from a multicast DVBSTP service, this stub file mechanism replaces the identification agent method defined in versions prior to release 1.4.1 of the present document.

For Content Download Services (CDSs) the HTTP protocol is used for unicast delivery and the FLUTE protocol for multicast delivery.

Content download sessions are described in XML or SDP syntax and delivery is via HTTP (unicast) or SAP (multicast for SDP data) or DVBSTP (multicast for XML data). The mechanisms and protocols are specified in clause 10.

For System Renewability Message (SRM) delivery over IP the HTTP protocol is used for unicast download and the FLUTE protocol for multicast download. HTTP (unicast) and SAP (multicast) are used for SRM announcements. The mechanisms are specified in clause 12.

Annexes E and F describe two optional ways to enhance the reliability of delivery for RTP transport using AL-FEC or Retransmissions and annexes H and I two mechanisms to reduce the response time when switching LMB services (using Server-based Fast Channel Change or Companion Stream FCC).



NOTE 1: The profile of DSM-CC used for firmware delivery for RMS-FUS is as specified in ETSI TS 102 006 [105] (V1.3.2).

NOTE 2: The information exchanged in RTSP may be conveyed in an XML or SDP format.

NOTE 3: TLS/SSL indicates that either TLS or SSL can be used.

NOTE 4: HTTP/HTTPS indicates that either HTTP or HTTPS can be used.

NOTE 5: DSM-CC is the transport protocol used for SRM and RMS-FUS but has no relationship with Dynamic Service Management.

Figure 3: Diagram of the protocol stack for DVB-IPTV services

4.2 Void

Figure 4: Void

Figure 5: Void

5 Service discovery

5.1 Overview

The present document covers the mechanisms used for service discovery, service selection and the delivery of service discovery information.

Service discovery is the mechanism enabling the discovery of DVB-IPTV services available over bi-directional IP network. The service discovery results in the presentation of a list of services with sufficient information for the user to make a choice and access the chosen service. Selection takes place after the user has made a choice about which service to view.

Live Media Broadcast, CoD and CDSs are covered by the present document. Two types of Live Media broadcast services have been identified: broadcast services with DVB SI [1] embedded in the stream (referenced as "TS Full SI") and broadcast services without in-band SI except for MPEG PSI (referenced as "TS optional SI").

"TS Full SI" is intended for the case where the Service Provider selects traditional DVB broadcast digital TV streams (from different sources) and provides them as they are over IP to the end-user, in the same way that DTV operators aggregate satellite-received streams over cable. In such a case, the minimum amount of information that the Service Provider has to generate specifically for IP delivery is the information needed at the receiver end to be able to locate the different transport streams (similar to the information needed for the scanning phase in cable, satellite or terrestrial networks). Information on individual services is afterwards acquired from the transport stream itself through classical use of service information as defined in DVB SI [1].

"TS - Optional SI" is intended for the more advanced situation where the Service Provider wants to present its offering but where it cannot afford or does not want to use bandwidth for usual DVB service description information. In that case, the service discovery information has to give the location of the service as well as relevant service information about each service.

The Broadband Content Guide [62] provides CoD and CDS information and program schedule information for Live Media Broadcast services.

CDSs use the BCG for service announcement. Service announcement for CDS is introduced in clause 10.3.

Two transport mechanisms are defined to support both push and pull models of delivery for the service discovery information. Both unicast and multicast modes are supported and the same information can be carried over both modes.

The service discovery information shall be represented with and carried as XML records [54] and the XML schemas [55], [56] and [57] describing their syntax and grammar are specified in clause 5.2.

5.2 Service Metadata

5.2.1 Service Identification

5.2.1.0 Introduction

This clause defines the mechanisms used to identify service providers and services in the context of service discovery.

5.2.1.1 Service Provider (SP)

A SP shall be identified uniquely by the name of the DNS Domain it has registered and controls. The organizations administrating the Internet DNS domain names shall be used as a globally unique registration mechanism that allows these textual SP identifiers to be globally unique names.

5.2.1.2 Service name or service ID

Each service shall be assigned one textual identifier that takes the form of an Internet DNS host name under the DNS domain that the SP controls. Thus a service can be uniquely identified by a concatenation of a service name (managed uniquely by the SP) and the SP's domain name.

The syntax of a textual service identifier is as defined in MHP (clause 14.9 [3]):

```
<service_name>."<service_provider_domain_name>
```

where <service_name> is a unique name for the service within the SP's domain and <service_provider_domain_name> is an Internet DNS domain name that the SP has rights to control. The <service_name> field shall follow the rules defined for Internet DNS names so that the whole textual service identifier is a valid host name to be used in the Internet DNS as defined in IETF RFC 1035 [14].

There are two basic mechanisms for uniquely identifying a service:

- the triplet of numeric identifiers: original_network_id, transport_stream_id and service_id as defined in DVB SI [1];
- a textual service identifier, as defined above.

Either form can be used for identifying a service globally and uniquely.

It should be noted that the DVB triplet (original_network_id, transport_stream_id and service_id) distinguishes between the same service carried by different networks. For example the triplet would consider the channel BBC1 carried by BskyB and by Freeview as two separate services.

For example, the SP CANAL+ is identified by the domain name "canal-plus.com" and a service can be assigned the name "canalplussport.canal-plus.com".

5.2.2 Fragmentation of SD&S Records

Following restructuring, the text for this clause can now be found in clause 5.4.4.

Table 1: Void (see Table 12a)

Figure 6: Void (see Figure 9a)

5.2.3 Steps in service discovery (informative)

Figure 7 summarizes the steps of the Service Discovery process. Each step is further described in separate clauses below however, to help further understand the process, some more detailed informative text follows figure 7.

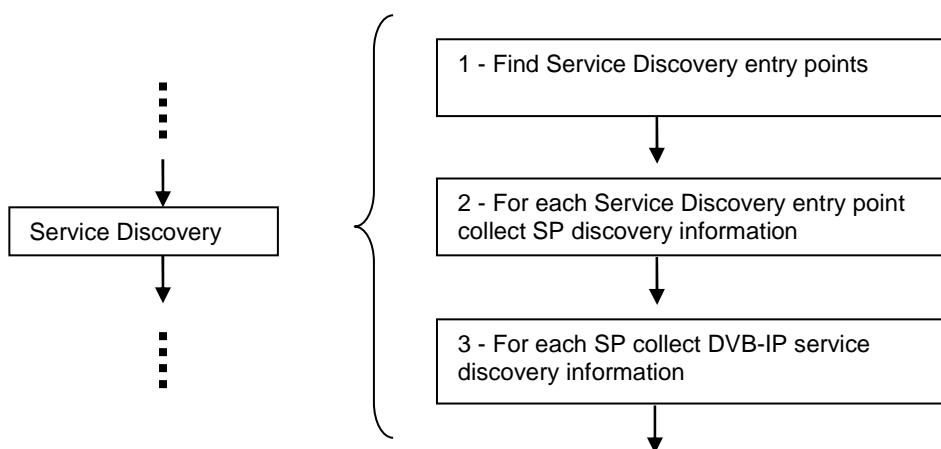


Figure 7: Steps in service discovery

The service discovery process begins with the discovery of SPs offering DVB-IPTV services over the IP network and continues with the discovery of available services from each SP.

The service discovery process bootstraps itself by determining the entry point(s) of the discovery information. This is specified in clause 5.2.4.

The discovery of SPs offering DVB-IPTV services is done via the acquisition of the SP Discovery Information specified in clause 5.2.5. SPs publish their offering via the service discovery information as specified in clause 5.2.6.

There are many different ways of finding the Service Discovery entry points. This discussion assumes that the HNED acquires them through DNS using DHCP Option 15. The steps for finding the Service Discovery Entry points are:

- 1) The IP address is obtained through DHCP in the normal manner (see clause 8.1.1). This will result in DHCP option 15 being filled in with a domain name called "*DNS_DomainName*".
- 2) A DNS lookup (Query message) is then performed with the QNAME being _dvbservdsc.tcp.
DNS_DomainName, and the lookup should specify SRV. The return answer should be what is in the RR record for the QNAME, for example "SD&S1_DomainName A IP_SD&S1" and "SD&S2_DomainName A IP_SD&S2" where "SD&S1_DomainName" and "SD&S2_DomainName" are the domain names, "A" is the type of the record (for simplicity, there is no recursion, so this is a host) and "IP_SD&S1" and "IP_SD&S2" are the IP addresses.

The HNED has now found the Service Discovery Entry points from (2) so it can now collect the SP discovery information for each of the two entry points "SD&S1_DomainName" and "SD&S2_DomainName". This is done using either multicast or unicast, but for this example unicast is assumed which uses an HTTP GET to obtain the SP Discovery XML record. There are two types of GET that can be used: the first obtains the information for a specific SP via a specific domain name, whilst the other obtains the information for all SPs in a single piece of XML. In the latter case, a single SP Discovery request is assumed.

For this example, the HNED could issue an HTTP GET like the following to the IP address of SD&S1_DomainName.

```
GET /dvb/sdns/sp_discovery?id=ALL HTTP/1.1 CRLF
Host: SD&S1_DomainName CRLF
```

The SD&S Server should return XML similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceDiscovery xmlns="urn:dvb:metadata:iptv:sdns:2008-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ServiceProviderDiscovery>
        <ServiceProvider DomainName="SP1_DomainName" Version="1">
            <Name Language="ENG">SP1_name</Name>
            <Offering>
                <Pull Location="http://sdns.SP1.com/dvb/sdns">
                    <PayloadID Id="2">
                        <Segment ID="0" />
                        <Segment ID="1" />
                        <Segment ID="2" />
                        ...
                    </PayloadID>
                </Pull>
            </Offering>
        </ServiceProvider>

        <ServiceProvider DomainName="SP2_DomainName" Version="1">
            <Name Language="ENG">SP2_name</Name>
            <Offering>
                <Pull Location="http://sdns.SP2.com/dvb/sdns">
                    <PayloadID Id="2">
                        <Segment ID="0" />
                        <Segment ID="1" />
                        <Segment ID="2" />
                        ...
                    </PayloadID>
                </Pull>
            </Offering>
        </ServiceProvider>
    </ServiceProviderDiscovery>
</ServiceDiscovery>
```

The HNED now has all the information for all the Service Providers "SP1 Name" and "SP2 Name" providing DVB-IPTV services, so it can now discover the services each one provides. This needs a similar HTTP GET as used to pull the Service Provider Discovery information, for each of the Service Providers, but this time for each of the segments provided in the Service Provider Discovery record. The record lists 3 segments: 0, 1 and 2 that will result in 3 GETs each returning the corresponding XML, for example:

```
GET /dvb/sdns/service_discovery?id=SP1_DomainName&Payload=02&Segment=0000 HTTP/1.1 CRLF
Host: sdns.SP1.com CRLF
```

```
GET /dvb/sdns/service_discovery?id=SP1_DomainName&Payload=02&Segment=0001 HTTP/1.1 CRLF
Host: sdns.SP1.com CRLF
```

```
GET /dvb/sdns/service_discovery?id=SP1_DomainName&Payload=02&Segment=0002 HTTP/1.1 CRLF
Host= sdns.SP1.com CRLF
```

The XML returned should be similar to the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceDiscovery xmlns="urn:dvb:metadata:iptv:sdns:2008-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <BroadcastDiscovery DomainName="SP1_DomainName">
        <ServiceList>
            <SingleService>
                <ServiceLocation>
                    <IPMulticastAddress..Address="IP_MulticastAddress1" Port="port_value" />
                </ServiceLocation>
                <TextualIdentifier DomainName="SP1_DomainName" ServiceName="SvceName1" />
                <DVBTriplet OrigNetID= "ON_id_value1" TSID= "TS_ID_value1" ServiceID="S_ID_value1" />
                ...
            </SingleService>
            ...
        </ServiceList>
    </Broadcast Discovery>
</ServiceDiscovery>
```

5.2.4 Service discovery entry points

The service discovery process shall bootstrap itself by determining the entry point(s) of the discovery information. The SD&S entry points can be one of the following:

- A well known multicast address registered with IANA that is 224.0.23.14 (DvbServDisc).
- A list of SD&S entry points addresses may be acquired via DNS according to the service location IETF RFC 2782 [40]. The service name is _dvbservdsc, the protocol may be tcp or udp, while the rest of the name is the domain name maintained by DVB for service discovery; this domain name is set to services.dvb.org. So the lookup shall be either _dvbservdsc._tcp.services.dvb.org or _dvbservdsc._udp.services.dvb.org. This requires that the HNED support an SRV cognizant DNS client and according to the specification in IETF RFC 2782 [40]. The DVB organization will maintain the services.dvb.org domain name for service discovery and new SPs should register with DVB to add them to the DNS SRV list. HTTP servers will be found via the tcp protocol method whilst the multicast addresses will be found via the udp protocol method.
- When the HNED connects to the network to request its own address (e.g. during DHCP) it may be provided with domain names via DHCPv4 option 15 [25] or DHCPv6 option 24 [124] depending on whether IPv4 or IPv6 will be used. A list of SD&S entry points addresses is then acquired via DNS according to the service location IETF RFC 2782 [40] as described above. The service name is _dvbservdsc, the protocol may be tcp or udp, while the rest of the name is the domain name provided via DHCP Option 15 or DHCPv6 option 24. For example the lookup could be _dvbservdsc._tcp.example.com. This requires that the HNED support an SRV cognizant DNS client according to the specification in IETF RFC 2782 [40].

NOTE: The DNS mechanism as described in IETF RFC 2782 [40] may be used in a recursive fashion, i.e. the domain names returned can include ones starting with _dvbservdsc in which case further DNS SRV methods are required to locate the final domain names.

If no portnumber is specified, the default portnumber shall be 3937 (dvbservdsc) as assigned by IANA.

The HNED shall look for SD&S entry points in the priority order defined below. When one of the steps below provides at least one entry point then the HNED shall stop searching for new entry points:

- 1) The domain names returned by DHCPv4 option 15 or DHCPv6 option 24 shall be used in conjunction with the DNS mechanism defined above. If the method does not resolve to one or more valid domain names or returns an error, then the HNED shall go to the next step.
- 2) The HNED joins the IANA registered multicast address; if no valid DVBTSP packets are received within a minimum period of 2 cycles of SD&S Information delivery (maximum cycle period specified in clause 5.4.4.3) then the HNED shall go to the next step.

- 3) The DVB constructed DNS method defined above shall be used, if it does not resolve to one or more valid domain names or returns an error, then the HNED shall go to the next step.
- 4) If no entry point has been found through the steps above there shall be the option for the user to enter the URL [19] or an IP address and optional portnumber of an entry point manually.

5.2.5 SP discovery information

Following restructuring, the text for this clause can now be found in clause 5.2.13.7: "ServiceProvider Discovery: ServiceProviderListType".

Table 2: Void (see Table 11ck)

5.2.6 DVB-IPTV service discovery information

Following restructuring, the text for this clause can now be found in clause 5.2.13: "XML Main Types" of the present document.

The following clauses also contained in clause 5.2.6 of ETSI TS 102 034 V1.4.1 and V1.5.2 have been restructured as follows:

- The text for clause 5.2.6.1 "DVB-IPTV Offering Record" can now be found in clause 5.2.12.18: "OfferingBase" of the present document.
 - Table 3 is void and replaced by Table 11az.
- The text for clause 5.2.6.2 "Broadcast discovery record" can now be found in clause 5.2.13.2: "Broadcast Discovery Record: BroadcastOffering" of the present document.
- The text for clause 5.2.6.2.1 "Broadcast discovery record - TS Full SI" can now be found in clause 5.2.13.2: "Broadcast Discovery Record: BroadcastOffering" of the present document.
 - Table 4 is void and replaced by Table 11cf.
- The text for clause 5.2.6.2.2 "Broadcast discovery record - TS Optional SI" can now be found in clause 5.2.13.2: "Broadcast Discovery Record: BroadcastOffering" of the present document.
 - Table 5 is void and replaced by Table 11cf.
- The text for clause 5.2.6.3 "Content on Demand (CoD) discovery record" can now be found in clause 5.2.13.3: "Content on Demand Offering Record: CoDOffering" of the present document.
 - Table 6 is void and replaced by Table 11cg.
- The text for clause 5.2.6.4 "Service From other Services Providers record" can now be found in clause 5.2.13.5: "Referenced Services Offering: ReferencedServices" of the present document.
 - Table 7 is void and replaced by Table 11ci.
- The text for clause 5.2.6.5 "Package discovery record" can now be found in clause 5.2.13.4: "Packaged Services: PackagedServices" of the present document.
 - Table 8 is void and replaced by Table 11ch.
- The text for clause 5.2.6.6 "Broadband Content Guide record" can now be found in clause 5.2.13.1: "Broadband Content Guide Record: BCGOffering" of the present document.
 - Table 9 is void and replaced by Table 11ce.
- The text for clause 5.2.6.7 "HNED Cell ID Discovery - Regionalization Discovery Record" can now be found in clause 5.2.13.8: "Regionalization Discovery Information" of the present document.
- The text for clause 5.2.6.7.1 "Obtaining the Cell ID via HTTP (Pull mode)" can now be found in clause 5.4.2.3: "Obtaining the Cell ID via HTTP (Pull mode)" of the present document.

- The text for clause 5.2.6.7.2 "Obtaining the Cell ID via the Regionalization Discovery Record (Push mode)" can now be found in 5.2.13.8: "Regionalization Discovery Information" of the present document.
 - Table 10 is void and replaced by Table 11cl.
- The text for clause 5.2.6.8 "Provision of RMS-FUS Information" can now be found in clause 5.2.13.6: "RMS Offering: RMSFUSDiscoveryType" of the present document.
 - Table 11 is void and replaced by Table 11cj.

5.2.7 Data Model (Informative)

Figure 7aa provides a graphic representation of the DVB-IPTV service discovery model.

The boxes in bold are the components required to establish the list of DVB-IPTV services available from different SPs.

Clause 5.2.13 provides details on the elements that may be contained within the Service Discovery element.

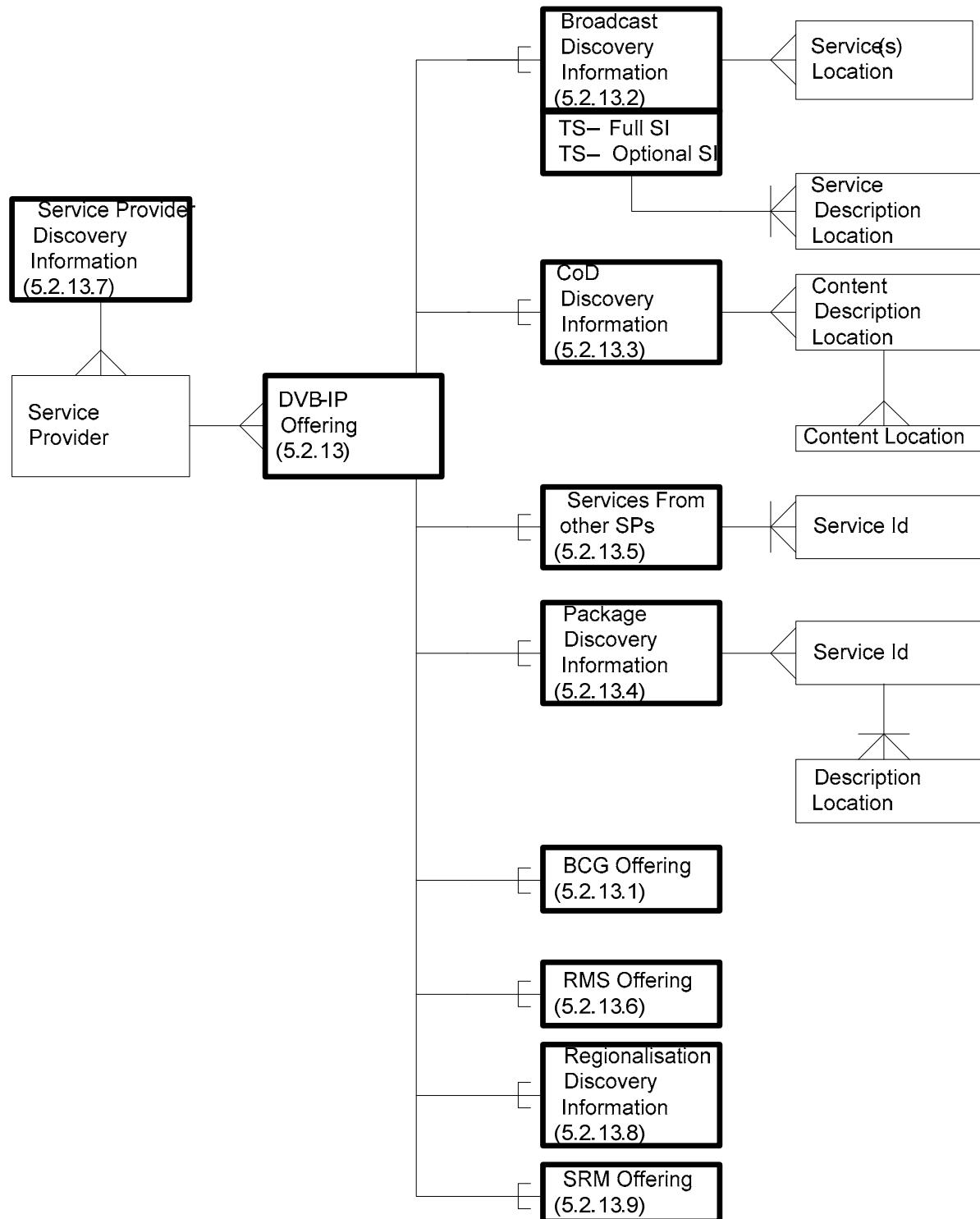


Figure 7aa: Data model for DVB-IPTV service discovery information

Table 11aa: List of Offerings within the DVB IPTV Data Model

Offering	Description
Broadcast Discovery information	The "Broadcast Discovery" information (see clause 5.2.13.2) is provided in two forms: "TS - Full SI broadcast discovery information" is used when full DVB SI is available in-band, this may be indicated by a value of "Stream" for the "PrimarySISource" attribute of "SI" for a "IPService". "TS - Optional SI broadcast discovery information" is used when complete service description is not available in-band, this may be indicated by a value of "XML" for the "PrimarySISource" attribute of "SI" for a "IPService".
CoD Discovery information	The "CoD Discovery" information (see clause 5.2.13.3) is used for SPs that would like to describe their CoD offer (see note).
Services From Other SPs	The "Services From Other SPs" (see clause 5.2.13.5) allow SPs to reference individual services or a complete offering from another SP with which it has a commercial agreement.
Package Discovery information	The "Package Discovery" information (see clause 5.2.13.4) is used by SPs that would like to group several services and present them as a single entity. The package information does not enable the discovery of new services; the package discovery information references services which have to be discovered via the two other components in the model called Broadcast and CoD Discovery Information. Additional information on services can optionally be provided in the context of a package.
Service Provider Discovery information	"Service Provider Discovery" information carries the necessary description of the SPs providing services within the overall offering.
BCG Offering	The "BCG Offering" (see clause 5.2.13.1) provides a means of offering guide data. This guide data may lead to content available either as services resolved via the SP discovery information, or via other mechanisms (such as Cod).
RMS Offering	The "RMS Offering" (see clause 5.2.13.6) provides a means to offer both remote management and firmware update services.
Regionalization Offering	The "Regionalization Offering" (see clause 5.2.13.8.1) provides the information required to offer regionalized services.
SRM Offering	The "SRM Offering" (see clause 5.2.13.9) describes where System Renewability Messages may be found.
NOTE: This now is deprecated, and the BCG Discovery information should be used.	

All the "Discovery" entry points except "ServiceproviderDiscovery" use extended versions of the "dvb:Offeringbase", each extended in an appropriate way to add additional attributes.

"ServiceproviderDiscovery" opens into a list of service providers offering IPTV services.

Using the data model above, the HNED first builds the list of DVB-IPTV SPs operating on the network, then in a second stage the list of DVB-IPTV services is established by acquiring the service discovery information for each SP.

The model allows the entry point to the service discovery and selection mechanism to be a specific SP, in this case the information relating to the SP and the list of services for this SP may be acquired from the same location.

This model is extended by adding new types of discovery information if new types of SP offers are identified.

5.2.8 Metadata Namespace

5.2.8.0 General rules

The namespace root for metadata definitions provided by the present document shall be "urn:dvb:metadata:iptv:sdns".

By inclusion, the present document also makes use of the updated TV-Anytime namespace "urn:tva:metadata:2011", and the base XML schema namespace(s), the text version of the schema header is included below.

Elements which are referenced by an unknown namespace shall be ignored, even if they appear to be known. Additional namespaces are to be expected in the future as new features are introduced.

```

<xsd:schema targetNamespace="urn:dvb:metadata:iptv:sdns:2014-1"
  xmlns:tva="urn:tva:metadata:2011"
  xmlns:dvb12="urn:dvb:metadata:iptv:sdns:2012-1"
  xmlns:dvb14="urn:dvb:metadata:iptv:sdns:2014-1"
  xmlns:dvb="urn:dvb:metadata:iptv:sdns:2008-1"
  xmlns:mpeg7="urn:tva:mpeg7:2008"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xsd:annotation>
    <xsd:documentation>schema to validate the record of the description of the DVB-IP offering of
    a service Provider
      This is the phase 1.6.1 version of the schema.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:import namespace="urn:tva:metadata:2011" schemaLocation=".tva_metadata_3-1_v171.xsd"/>
  <xsd:import namespace="urn:dvb:metadata:iptv:sdns:2008-1" schemaLocations=".sdns_v1.4r13.xsd"/>
  <xsd:import namespace="urn:dvb:metadata:iptv:sdns:2012-1" schemaLocation=".sdns_v1.5r25b.xsd"/>
  <xsd:import namespace="urn:tva:mpeg7:2008" schemaLocation=".tva_mpeg7_2008.xsd"/>

```

5.2.8.1 Current version

This version of the present document uses the version designation "2014-1". Hence metadata definitions that are new, or have been updated in this version, shall use the namespace "urn:dvb:metadata:iptv:sdns:2014-1" and the elements and attributes affected by the update will be pre-fixed by "dvb14".

5.2.8.2 Backwards compatibility

Metadata definitions introduced in previous versions have used different version designations of the form "*year-version*", e.g. "2008-1" (see also clause 5.2.8.1). These definitions remain in effect, unless a definition of the same element, in the same namespace root, but with a newer version designation has been provided, i.e. later updates can effectively override certain elements. Non-overridden element definitions remain in effect, however.

EXAMPLE: Assume that the 2008-1 version has defined elements A and B; assume further that the 2012-1 version re-defines just element B. In this case, for element A the 2008-1 definition applies, and for element B the 2012-1 definition applies. The new definition for element B will be prefixed by "dvb12".

An instance document that uses "dvb12" items is at liberty to use dvb:B (assuming it is not using any of the new features), as might be the case where backwards compatibility over dvb:B is more important than extended functionality of dvb12:B.

NOTE: Care should be taken to ensure that the correct namespace qualifier (e.g. "dvb12") is applied to all items.

5.2.9 Legend and Syntax of XML diagrams (Informative)

The elements shown with bold boundaries are mandatory, and those without a bold boundary are optional. Attribute groups are shown without a bold outline, also the optional attributes, but the mandatory attributes are shown with a bold outline.

Table 11ab: Symbols used in SD&S related XML Schemas

Symbol	Meaning	Comments
	ComplexType	As an example, the name within the item is that of the complex type element ("PayloadList")
 +		

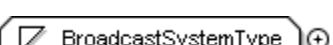
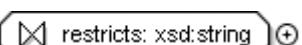
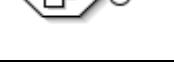
Symbol	Meaning	Comments
	SimpleType	As an example, the name within the item ("BroadcastSystemType") is that of the simple type element
	An Attribute	As an example, the name within the item "Version" is that of the attribute
	Attribute Group	As an example, the name within the item is that of the group
	Choice	
	Restriction Base	The example shows the "string" as the restriction base
	Simple content	
	Annotation	
	Documentation	Usually used with "annotation" symbol
	Complex Content	Often used as qualifier to "ComplexType" definition
	Sequence	
	Unbounded Sequence	

Table 11ac: Meaning of instance indication for elements and attributes

Indication	Meaning
No indication	1 instance only
1..∞	Minimum of 1 instance, but there may be multiple instances
0..∞	May be absent, but there may also be multiple instances

The "@" symbol preceding the name of the attribute or element indicates that the entity is an attribute of the element to which it is attached.

The text version of the detail for any specific element type gives a more complete description of the specific part of the XML Schema (XSD) file.

5.2.10 XML Basic Types

The following basic types represent the building blocks used in the subsequent XML structures.

NOTE: These names are intended to be descriptive and informative, providing simply the XML specification of certain well-known types.

Table 11ad describes the basic types, followed by their XML definitions.

Table 11ad: XML Basic Type Descriptions

Name	Definition
BroadcastSystemType	Identifies the broadcast delivery system. This type can take any of the values ("ANALOG", "ID_DVB_C", "ID_DVB_S", "ID_DVB_T", "ID_DVB_C2", "ID_DVB_S2", "ID_DVB_T2", "ID_ISDB_C", "ID_ISDB_S", "ID_ISDB_T", "ID_ATSC_T").
CPSystemIDType	Identifier (CP System ID) of the Content Protection System as defined in ETSI TS 101 162 [2].
CPSystemSRMID	CP System SRM Identifier of Content Protection System as defined in ETSI TS 101 162 [2].
DomainType	This type describes a "domain name" type. It is recommended that domain names comply with the "preferred name syntax" of clause 3.5, IETF RFC 1034 [13].
EnhancementServiceType	Lists the server-based enhancement service offerings for LMB. Only RET and FCC are defined.
Genre	This type describes the content genre, which is encoded as a number in the range 0 to 15, as detailed in the content_nibble_level_1 field of the content_descriptor, as in table 26 in ETSI EN 300 468 [1].
Hexadecimal3bit	A 3 bit number represented as a single hexadecimal digit, not preceded by "0x".
Hexadecimal4bit	A 4 bit number represented as a single hexadecimal digit, not preceded by "0x".
Hexadecimal8bit	An 8 bit number, represented as one or two hexadecimal digits, not preceded by "0x".
Hexadecimal16bit	A 16 bit number represented as between one and four hexadecimal digits, not preceded by "0x".
Hexadecimal32bit	A 32-bit number represented as 8 hexadecimal digits, not preceded by "0x".
Integer6bit	A 6 bit decimal number in the range 0 to 63, without any number base identifier.
IPorDomainType	A building block type that can hold either an IP address (see IPType), or a domain name (see DomainType), but not both.
IPType	An IPv4 dotted address of the form a.b.c.d (decimal) or an IPv6 colon separated address (hexadecimal) compliant with IETF RFC 4291 [119]. The RegEx expressions of the IPv4 and IPv6 formats are shown in the XML expansions following the present table (see note 1).
ISO-3166-List	A comma separated list of one or more three character country codes. These are intended to be as defined in ISO 3166 [50], however this definition allows more flexibility which may be exploited in some cases to enable the carriage of special values.
ISO 639-2 [51]	A single three letter language code, as defined in ISO 639-2 [51]. This definition allows more flexibility than simply the codes defined in ISO 639-2 [51], and this may be exploited to carry special values.
OrigNetId	The original_network_id, as defined in ETSI TS 101 162 [2], which also specifies the management of this number space. This value shall be in decimal.
PrimarySISource	This type is used to indicate if the primary SI information is contained in the XML (where this type takes the value "XML") or in the stream (where this type takes the value "Stream").
PullURL	This is used to specify the complete URL from which SD&S information can be pulled, including the protocol scheme, authority and path. The HNED shall append to this URL the request as described in clause 5.4.2.
RTSP	This is used where an RTSP URL is required.
Service	This is the name of a service, as specified in ETSI TS 101 812 [3], clause 14.9, and as specified in clause 5.2.1.2 in the present document. It is recommended that this follows the rules for an internet DNS name as specified in IETF RFC 1035 [14] and subsequent updates.
ServiceID	The service_id, as defined in ETSI EN 300 468 [1]. This value shall be in decimal (see note 2).
ServiceType	An eight bit hexadecimal value (see Hexadecimal8bit) encoding the "type" of a service. The values and meanings are defined in ETSI EN 300 468 [1], table entitled "service type coding".

Name	Definition
StreamingType	This type is used to indicate if RTP (with the value "rtp") or direct UDP (with the value "udp") streaming is used.
TransportProtocolType	A string that may be used to signal the transport and FEC type used for delivery.
TSId	The transport_stream_id as defined in ETSI EN 300 468 [1]. This value shall be in decimal.
Usage	Indicates the usage for the IPService. This element is a string and can be "Main", "SD", HD", "PiP", "FCC", "3D" or DSMService. This element is used to indicate that other IPServices exist for the same content, and that they will be exposed as sub-IPServices within this IPService. The value of DSMService is mandatory for services which are part of a DSM group and where DSM is enabled in the HNED.
Version	A number conveying the version of a table or record. This value will increase with changes to the table or record, modulo 256. This value shall be in hexadecimal.
NOTE 1:	The Regular Expression (RegEx) applied as a pattern match for match for an IPv6 address in the definition of "IPTypE" in the present table and expanded below is capable of validating the options for the 128 bit structure defined in IETF RFC 4291 [119], but not the actual address entered in terms of matching any specific address group mapping.
NOTE 2:	This should not be confused with the definition of a service given in clause 5.2.1.2 of the present document.

```

<xsd:simpleType name="BroadcastSystemType">
  <xsd:restriction base="xsd:string"/>
</xsd:simpleType>
<xsd:simpleType name="CPSysTemIDType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">CP System ID of Content Protection System as defined in TS
101 162</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9a-fA-F]{4}" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="CPSysTemSRMIDType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">CP System SRM ID of Content Protection System as defined in
TS 101 162</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="([0-9a-fA-F][0-9a-fA-F])\{1,256\}" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="DomainType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="((.|\\n|\\r)*)?(\\.(.|\\n|\\r)*)+" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="EnhancementServiceType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="FCC" />
    <xsd:enumeration value="RET" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Genre">
  <xsd:restriction base="xsd:byte">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="15" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Hexadecimal3bit">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-7]" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Hexadecimal4bit">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9a-fA-F]" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Hexadecimal8bit">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9a-fA-F]\{1,2\}" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Hexadecimal16bit">
  <xsd:restriction base="xsd:string">

```

```

<xsd:pattern value="[0-9a-fA-F]{1,4}" />
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Hexadecimal32bit">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9a-fA-F]{8}" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Integer6bit">
  <xsd:restriction base="xsd:unsignedShort">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="63" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="IPOrDomainType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">union of DomainType and IPType</xsd:documentation>
  </xsd:annotation>
  <xsd:union memberTypes="dvb14:IPType dvb:DomainType"/>
</xsd:simpleType>
<xsd:simpleType name="IPType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">union of DomainType and IPType</xsd:documentation>
  </xsd:annotation>
  <xsd:union memberTypes="dvb14:IPv4Type dvb14:IPv6Type"/>
</xsd:simpleType>
<xsd:simpleType name="IPv4Type">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">Regular expressions in pattern values for type define compatible address structures for IPv4 or IPv6 syntax</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="(((1[0-9])|(1[0-9][0-9])|(2[0-4][0-9])|(25[0-5]))\.){3}(([1-9]?[0-9])|(1[0-9][0-9])|(2[0-4][0-9])|(25[0-5]))"/>
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="IPv6Type">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">Regular expressions in pattern values for type define compatible address structures for IPv4 or IPv6 syntax</xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:pattern value=" < Expanded below "Regular Expression for IPv6" for text formatting > "/>
  </xsd:restriction>
</xsd:simpleType>

```

Regular Expression (RegEx) for IPv6:

```

"/^[\s*(((0-9A-Fa-f){1,4}:){7}([0-9A-Fa-f]{1,4}::))|(((0-9A-Fa-f){1,4}:){6}(:0-9A-Fa-f){1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|::))|(((0-9A-Fa-f){1,4}:){5}(((0-9A-Fa-f){1,4}:){1,2})|:(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|(((0-9A-Fa-f){1,4}:){4}(((0-9A-Fa-f){1,4}:){1,3})|((0-9A-Fa-f){1,4}):((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|(((0-9A-Fa-f){1,4}:){3}(((0-9A-Fa-f){1,4}:){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|(((0-9A-Fa-f){1,4}:){2}(((0-9A-Fa-f){1,4}:){1,5})|(((0-9A-Fa-f){1,4}:){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|(((0-9A-Fa-f){1,4}:){1}(((0-9A-Fa-f){1,4}:){1,6})|((0-9A-Fa-f){1,4}:0,4):((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|(((0-9A-Fa-f){1,4}:){1,7})|(((0-9A-Fa-f){1,4}:){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)|(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|::)))(%.)?\s*$/"

```

```

<xsd:simpleType name="ISO-3166-List">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="\c\c\c(\,\c\c\c)*" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="ISO639-2">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="\c\c\c" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="OrigNetId">
  <xsd:restriction base="xsd:unsignedShort" />
</xsd:simpleType>
<xsd:simpleType name="PrimarySISource">

```

```

<xsd:restriction base="xsd:string">
    <xsd:enumeration value="Stream"/>
    <xsd:enumeration value="XML"/>
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="PullURL">
    <xsd:restriction base="xsd:anyURI"/>
</xsd:simpleType>
<xsd:simpleType name="RTSP">
    <xsd:restriction base="xsd:anyURI">
        <xsd:pattern value="rtsp://.*"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Service">
    <xsd:restriction base="xsd:string">
        <xsd:pattern value="(.|\\n|\\r)+"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="ServiceId">
    <xsd:restriction base="xsd:unsignedShort"/>
</xsd:simpleType>
<xsd:simpleType name="ServiceType">
    <xsd:restriction base="dvb:Hexadecimal8bit"/>
</xsd:simpleType>
<xsd:simpleType name="StreamingType">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="rtp"/>
        <xsd:enumeration value="udp"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="TransportProtocolType">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="RTP-AVP"/>
        <xsd:enumeration value="UDP-FEC"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="TSId">
    <xsd:restriction base="xsd:unsignedShort"/>
</xsd:simpleType>
<xsd:simpleType name="Usage">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="FCC"/>
        <xsd:enumeration value="PiP"/>
        <xsd:enumeration value="Main"/>
        <xsd:enumeration value="HD"/>
        <xsd:enumeration value="SD"/>
        <xsd:enumeration value="3D"/>
        <xsd:enumeration value="DSMService"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Version">
    <xsd:restriction base="xsd:string">
        <xsd:pattern value="[0-9a-fA-F]{2}"/>
    </xsd:restriction>
</xsd:simpleType>

```

5.2.11 XML Complex Types - Attribute Groups

5.2.11.1 BasicMulticastAddressAttributesType

This common group of attributes is used to carry the basic multicast address, without any information on FEC or RET channels.

```

<xsd:attributeGroup name="BasicMulticastAddressAttributesType">
    <xsd:attribute name="Source" type="dvb14:IPOrDomainType" use="optional"/>
    <xsd:attribute name="Address" type="dvb14:IPOrDomainType" use="required"/>
    <xsd:attribute name="Port" type="xsd:unsignedShort" use="required"/>
</xsd:attributeGroup>

```

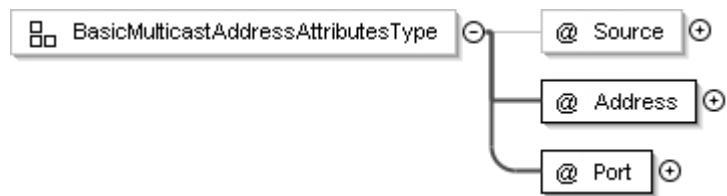


Figure 7ab: BasicMulticastAddressAttributesType

Table 11ae: BasicMulticastAddressAttributesType Fields

Name	Definition	Constraints
Source	The IP unicast address of the source of the TS may be provided. If this attribute is not present, then the multicast shall be ASM (any source). The format of this attribute is defined in clause 5.2.10.	Optional
Address	The multicast group address at which the service may be accessed. The format of this attribute is defined in clause 5.2.10.	Mandatory
Port	The port at which the service may be accessed.	Mandatory

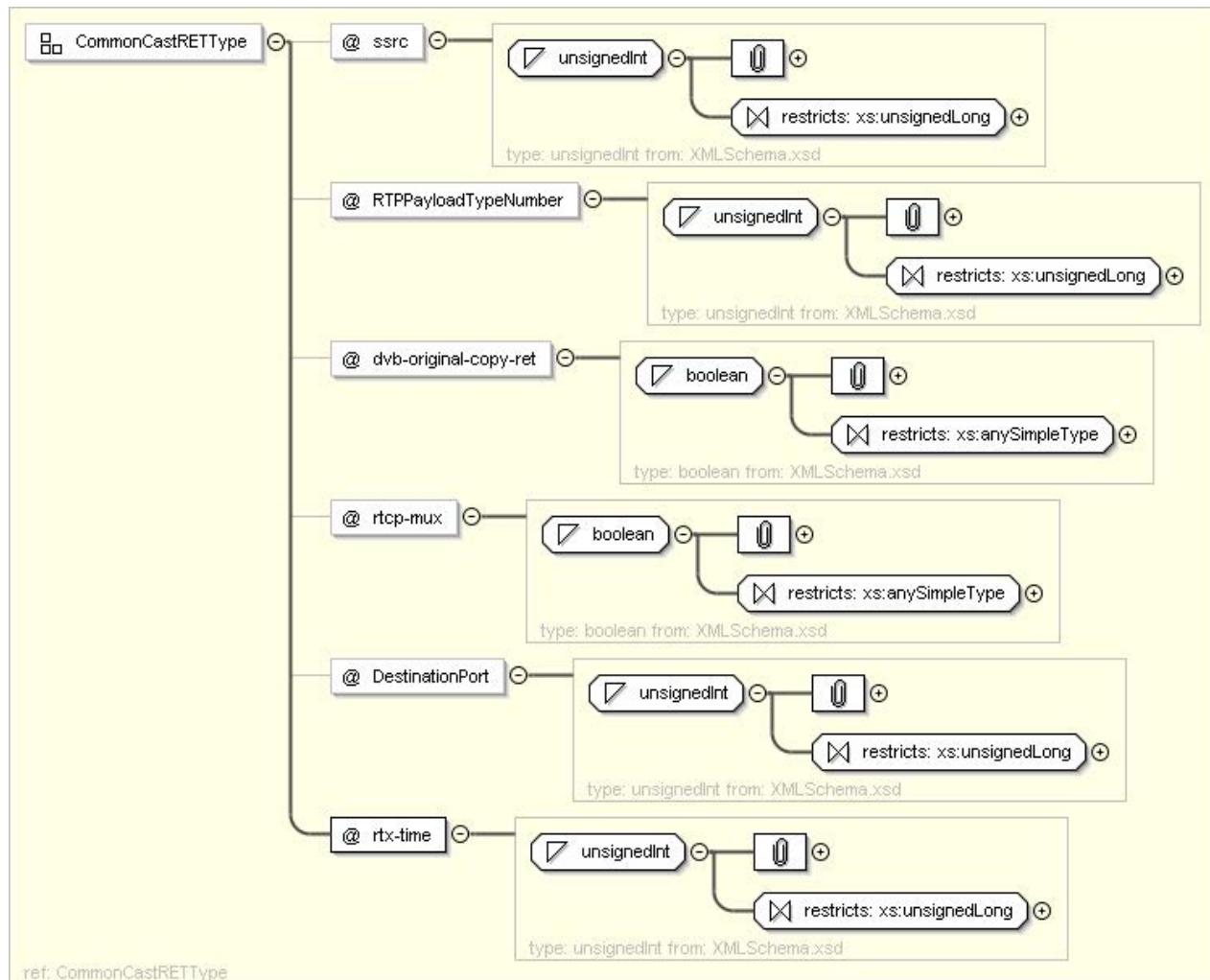
5.2.11.2 CommonCastRETTType

This attribute group is a collection of attributes common across both unicast RET/FCC and multicast RET.

```

<xsd:attributeGroup name="CommonCastRETTType">
    <xsd:attribute name="ssrc" type="xsd:unsignedInt" use="optional"/>
    <xsd:attribute name="RTPPayloadTypeNumber" type="xsd:unsignedInt" use="optional"/>
    <xsd:attribute name="rtcp-mux" type="xsd:boolean" use="optional" default="false"/>
    <xsd:attribute name="DestinationPort" type="xsd:unsignedInt" use="optional"/>
    <xsd:attribute name="rtx-time" type="xsd:unsignedInt" use="required"/>
</xsd:attributeGroup>

```

**Figure 7ac: CommonCastRETTType****Table 11af: CommonCastRETTType attributes**

Name	Definition	Constraints
<code>ssrc</code>	SSRC of the RTP packets in the retransmission session. This shall have the same value as the SSRC of the associated primary multicast, except for Multicast RET when SSRC multiplexing is used.	Optional
<code>RTPPayloadNumber</code>	Dynamic RTP payload type number of the RTP packets in the retransmission session.	Optional
<code>rtcp-mux</code>	If present, this attribute signals that RTCP and RTP retransmission packets are multiplexed on the same destination port in the retransmission session. If not present, then it follows standard definition, i.e. that RTCP packets are carried in the port one above that signalled by <code>DestinationPort</code> attribute.	Optional
<code>DestinationPort</code>	For multicast RET: UDP Destination port of multicast RET RTP Packets. For unicast RET/FCC: UDP Destination Port of unicast RTP retransmission packets. If not present, this port number matches the source port of the RTCP packets issued by the HNED for RTCP reporting in the original session.	Mandatory for multicast RET. Optional for Unicast RET
<code>rtx-time</code>	Amount of time (in milliseconds) an RTP packet payload is available for retransmissions. This attribute is defined only for RET service; the value shall be ignored for FCC.	Mandatory

5.2.11.3 FECAttributeGroupType

This attribute group represents the FEC information used in enhancement layers.

```
<xsd:attributeGroup name="FECAttributeGroupType">
  <xsd:attribute name="FECMaxBlockSize" type="xsd:unsignedShort" use="optional"/>
  <xsd:attribute name="FECMaxBlockTime" type="xsd:unsignedShort" use="optional"/>
  <xsd:attribute name="FECOTI" type="xsd:base64Binary" use="optional"/>
</xsd:attributeGroup>
```

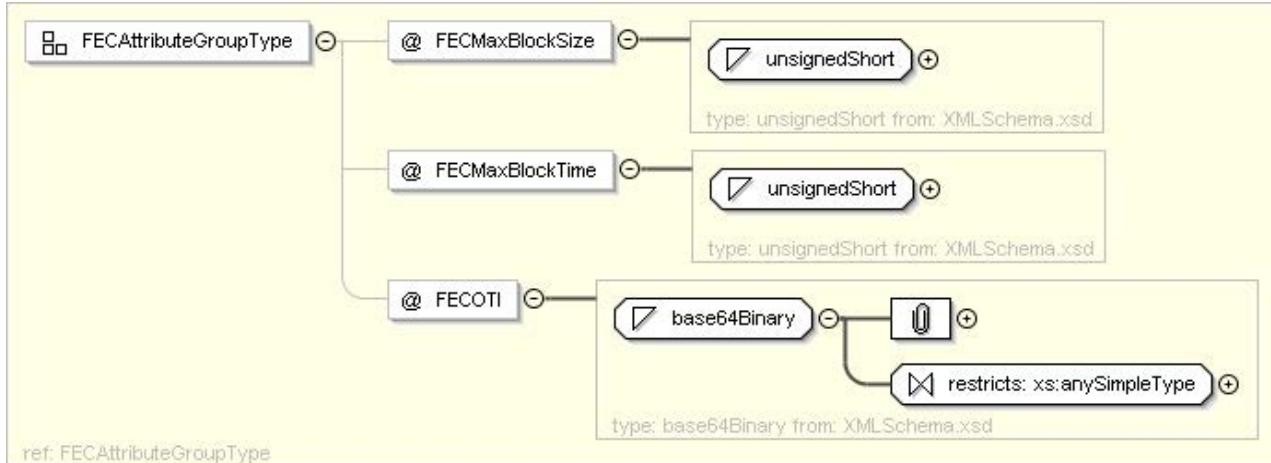


Figure 7ad: FECAttributeGroupType

Table 11ag: FECAttributeGroupType Fields

Name	Definition	Constraints
FECMaxBlockSize	This indicates the maximum number of stream source packets that will occur between the first packet of a source block (which is included) and the last packet for that source block (source or repair).	Optional
FECMaxBlockTime	The maximum transmission duration of any FEC Block in milliseconds (source and repair packets).	Optional
FECOTI	The FEC Object Transmission Information for the Raptor code If a FECEnhancementLayer element is included then this element shall be included.	Mandatory when the attributeGroup is used for a FEC enhancement layer

5.2.11.4 MulticastAddressAttribute

This type conveys the set of parameters needed to support a multicast service. It supports Source Specific Multicast (SSM) addressing if the Source attribute is specified. Otherwise it supports Any Source Multicast (ASM) addresses. It also holds the information required to support and configure the FEC support, if FEC is present.

```
<xsd:attributeGroup name="MulticastAddressAttributes">
  <xsd:attributeGroup ref="dvb14:BasicMulticastAddressAttributesType"/>
  <xsd:attribute name="Streaming" type="dvb:StreamingType" use="optional"/>
  <xsd:attributeGroup ref="dvb:FECAttributeGroupType"/>
</xsd:attributeGroup>
```

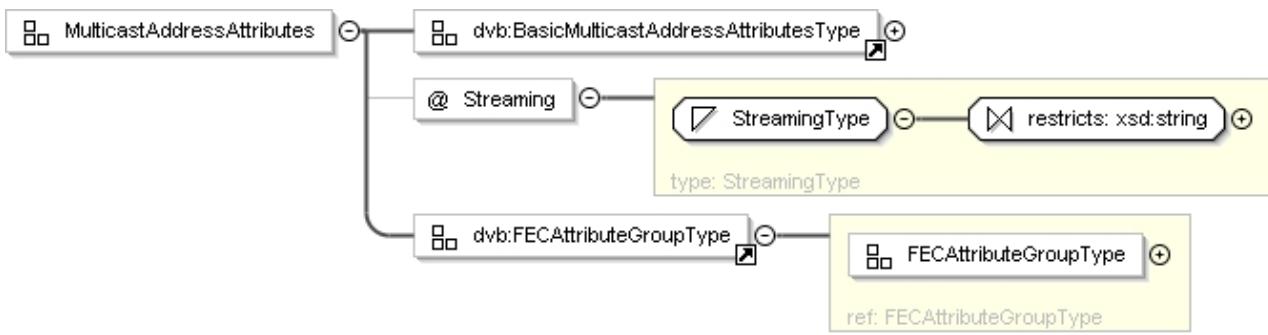


Figure 7ae: MulticastAddressAttribute

Table 11ah: MulticastAddressAttribute Attributes

Name	Definition	Constraints
BasicMulticastAddressAttributesType (included attributeGroup)	The basic multicast address value, and is an inclusion of the group defined in clause 5.2.11.1.	Mandatory
Streaming	Optionally indicates RTP or direct UDP streaming. In case the parameter is not provided, RTP streaming is assumed. This type is defined in clause 5.2.10.	Optional
FECAttributeGroupType (included attributeGroup)	The information required for FEC and conveys the details of the FEC information flow, and is an inclusion of the group defined in clause 5.2.11.3. The appropriate parts of this attribute group shall be present if FEC enhancement layer(s) is used.	Mandatory where FEC enhancement layer(s) is used

5.2.12 XML Complex Types - Element Groups

5.2.12.1 AnnouncementSupport

The announcement support element identifies the type of spoken announcements that are supported by the service (for example emergency flash, road traffic flash, etc.). Furthermore, it informs about the transport method of the announcement and gives the necessary linkage information so that the announcement stream can be monitored.

This is an XML representation of the `announcement_support_descriptor` defined in ETSI EN 300 468 [1]. The meanings and values of attributes and elements are defined in ETSI EN 300 468 [1].

```

<xsd:complexType name="AnnouncementSupport">
    <xsd:sequence>
        <xsd:element name="Announcement" maxOccurs="unbounded">
            <xsd:complexType>
                <xsd:choice minOccurs="0">
                    <xsd:element name="TextualIdentifier" type="dvb:TextualIdentifier"/>
                    <xsd:element name="DVBTriplet" type="dvb:DVBTriplet"/>
                </xsd:choice>
                <xsd:attribute name="Type" type="dvb:Hexadecimal4bit" use="required"/>
                <xsd:attribute name="ReferenceType" type="dvb:Hexadecimal3bit" use="required"/>
                <xsd:attribute name="ComponentTag" type="dvb:Hexadecimal8bit" use="optional"/>
            </xsd:complexType>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="SupportIndicator" type="dvb:Hexadecimal16bit" use="required"/>
</xsd:complexType>
  
```

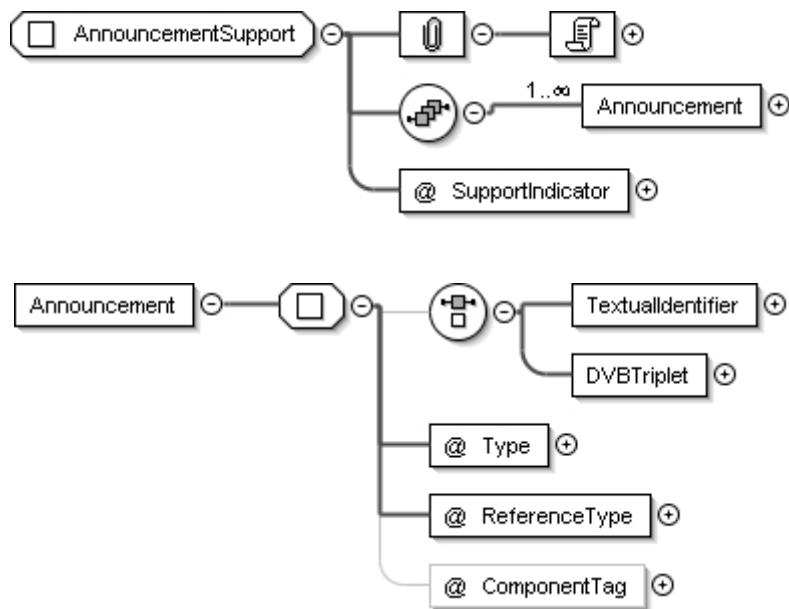


Figure 7af: AnnouncementSupport

Table 11ai: AnnouncementSupport Fields

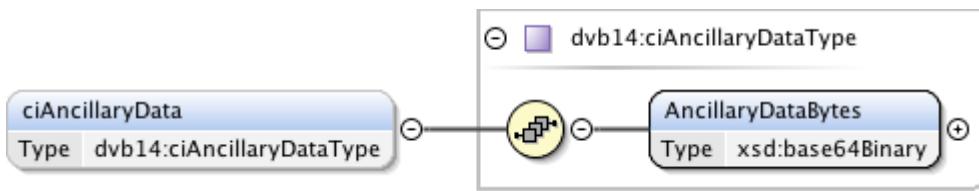
Name	Definition	Constraints
TextualIdentifier	The textual equivalent of the DVB triplet, as defined in clause 5.2.12.45. This field performs the same function as the DVB Triplet values original_network_id, transport_stream_id and service_id as defined in the announcement_support_descriptor defined in ETSI EN 300 468 [1].	Optional
DVBTriplet	This field, as defined in clause 5.2.12.8, carries the original_network_id, transport_stream_id and service_id as defined in the announcement_support_descriptor defined in ETSI EN 300 468 [1].	Optional
Type	This field carries the value announcement_type value, as defined in the announcement_support_descriptor defined in ETSI EN 300 468 [1].	Mandatory
ReferenceType	This field carries the value reference_type value, as defined in the announcement_support_descriptor defined in ETSI EN 300 468 [1].	Mandatory
ComponentTag	This field carries the component_tag value, as defined in the announcement_support_descriptor defined in ETSI EN 300 468 [1].	Optional
SupportIndicator	This field carries the announcement_support_indicator value, as defined in the announcement_support_descriptor defined in ETSI EN 300 468 [1].	Mandatory

5.2.12.1a ciAncillaryDataType

The ciAncillaryData type is used to carry the equivalent of the ci_ancillary_data descriptor defined in clause 6.4.1 (CI ancillary data descriptor) of ETSI EN 300 468 [1]. The purpose of this descriptor is to support companion screen functionality as described in ETSI TS 103 286-2 [125]. The fields in this type are direct matches to the fields in the descriptor, and the semantics of that descriptor apply here.

```

<xsd:complexType name="ciAncillaryDataType">
  <xsd:sequence>
    <xsd:element name="AncillaryDataBytes" type="xsd:base64Binary" />
  </xsd:sequence>
</xsd:complexType>
  
```

**Figure 7afa: ciAncillaryDataType****Table 11aia: ciAncillaryDataType Fields**

Name	Definition	Constraints
AncillaryDataBytes	The private data bytes from the ancillary_data_byte field of the ci_ancillary_data descriptor in ETSI EN 300 468 [1], concatenated in the order they occur in the descriptor. Each 8-bit value represented as a two hexadecimal digits.	Optional

5.2.12.2 CDSDownloadSessionDescriptionLocationType

This type is used to carry both the multicast address of the CDS Download Session, and to indicate if this is carried as SAP (in which case element SAP is used) or SD&S XML (in which case element DVBSTP is used).

```

<xsd:complexType name="CDSDownloadSessionDescriptionLocationType">
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="DVBSTP">
      <xsd:documentation>
        DVBSTP may include either IPv4 or IPv6 Service Provider ID, differentiated within
        the DVBSTP header structure by the value of the version
      </xsd:documentation>
      <xsd:complexType>
        <xsd:attributeGroup ref="dvb14:BasicMulticastAddressAttributesType" />
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="SAP">
      <xsd:complexType>
        <xsd:attributeGroup ref="dvb14:BasicMulticastAddressAttributesType" />
      </xsd:complexType>
    </xsd:element>
  </xsd:choice>
</xsd:complexType>
  
```

**Figure 7ag: CDSDownloadSessionDescriptionLocationType****Table 11aj: CDSDownloadSessionDescriptionLocationType Fields**

Name	Definition	Constraints
DVBSTP	This indicates that the service details are available as XML carried over DVBSTP at the indicated multicast address. This element carries the attributeGroup BasicMulticastAddressType defined in clause 5.2.11.1 to specify the multicast address of the DVBSTP service that is carrying the CDS service description.	Optional , but at least one of DVBSTP or SAP shall be present
SAP	This indicates that the service details are available via SAP at the indicated multicast address. This element carries the attributeGroup BasicMulticastAddressType defined in clause 5.2.11.1 to specify the multicast address of the SAP service that is carrying the CDS service description.	Optional, but at least one of DVBSTP or SAP shall be present

5.2.12.3 Cell

The Cell type is used to group civic addresses and provide the Regionalization ID that these addresses map into. For further discussion see clause 5.2.13.8.

```
<xsd:complexType name="Cell">
  <xsd:sequence>
    <xsd:element name="CountryCode" type="xsd:string"/>
    <xsd:element name="CA" type="dvh:CivicAddress" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:string" use="required"/>
</xsd:complexType>
```

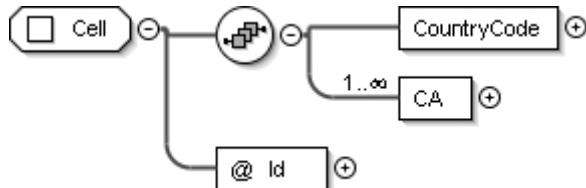


Figure 7ah: Cell

Table 11ak: Cell Fields

Name	Definition	Constraints
CountryCode	The Country Code to which this cell applies. This element shall be of the 2-letter format specified in ISO 3166 [50].	Mandatory
CA	The civic address, or nested addresses to which this ID applies, in the country specified by the CountryCode.	Mandatory
Id	The value of the ID is the value used within the SD&S information for the region. This flexibly formatted value is used to match with the Regionalization values Cells elements of the ServiceAvailabilityType defined in clause 5.2.12.32.	Mandatory

5.2.12.4 CivicAddress

The CivicAddress type is used to hold a potentially nested set of civic addresses that are used as part of the Regionalization process. See clause 5.2.13.8 for further discussions and details.

```
<xsd:complexType name="CivicAddress">
  <xsd:sequence>
    <xsd:element name="CA" type="dvh:CivicAddress" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="Type" type="xsd:string" use="required"/>
  <xsd:attribute name="Value" type="xsd:string" use="required"/>
</xsd:complexType>
```

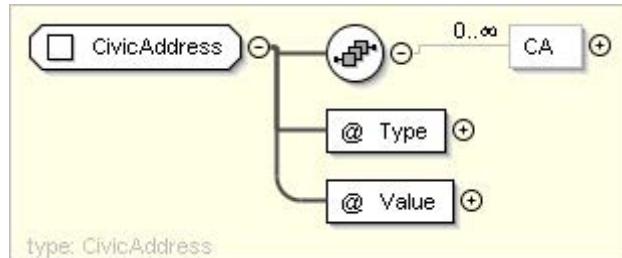


Figure 7ai: CivicAddress

Table 11al: CivicAddress Fields

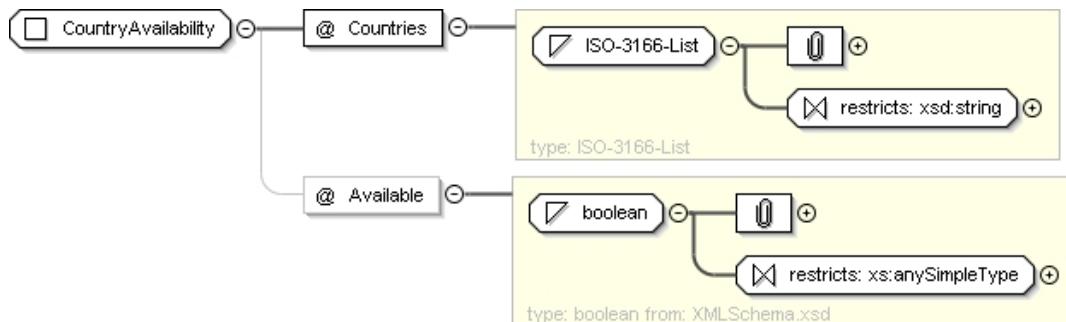
Name	Definition	Constraints
CA	An included subsidiary civic address. A CivicAddress of one type may contain other CivicAddresses of a different type, allowing a hierarchical description of addresses in a given Cell to allow for more efficient coding. See discussion in clause 5.2.13.8.2 for more details.	Optional
Type	Type of the Civic Address parameter, as specified in IETF RFC 4676 [97].	Mandatory
Value	Value for the Civic Address, of the type specified by the Type field. One of these shall match the value the HNED receives via the DHCP option 99, as per IETF RFC 4676 [97].	Mandatory

5.2.12.5 CountryAvailability

This is an XML representation of the Country availability descriptor in ETSI EN 300 468 [1]. The meanings and values of attributes and elements are defined in ETSI EN 300 468 [1].

NOTE: This type is deprecated.

```
<xsd:complexType name="CountryAvailability">
    <xsd:attribute name="Countries" type="dvb:ISO-3166-List" use="required"/>
    <xsd:attribute name="Available" type="xsd:boolean" default="true"/>
</xsd:complexType>
```

**Figure 7aj: CountryAvailability****Table 11am: CountryAvailability Fields**

Name	Definition	Constraints
Countries	A list of countries as defined by the type ISO-3166-List defined in clause 5.2.10. See the country_availability_descriptor defined in ETSI EN 300 468 [1] for more details.	Mandatory
Available	A Boolean indicating if the availability is true or false for the list of countries given. The default value is true. See the country_availability_descriptor defined in ETSI EN 300 468 [1] for more details.	Optional

5.2.12.6 DescriptionLocationBCG

This is an extension to the tva:TVAIDType type defined in clause 6.3.3 of ETSI TS 102 822-3-1 [60] that adds an optional attribute to signal if this is the preferred location for the description of a service. There shall be no more than one instance of preferred set to true in each relevant scope.

```
<xsd:complexType name="DescriptionLocationBCG" mixed="true">
  <xsd:simpleContent>
    <xsd:extension base="tva:TVAIDType">
      <xsd:attribute name="preferred" type="xsd:boolean" use="optional"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
```

NOTE: Base type changed from versions of the present document prior to release 1.5.1 from 'dvh:DescriptionLocation' to 'tva:TVAIDType' (based on 'xs:string') which reflects the actual type as defined in the Id attribute of the BCGOffering. This gives flexibility in terms of the format of the ID/URI which can be supported.

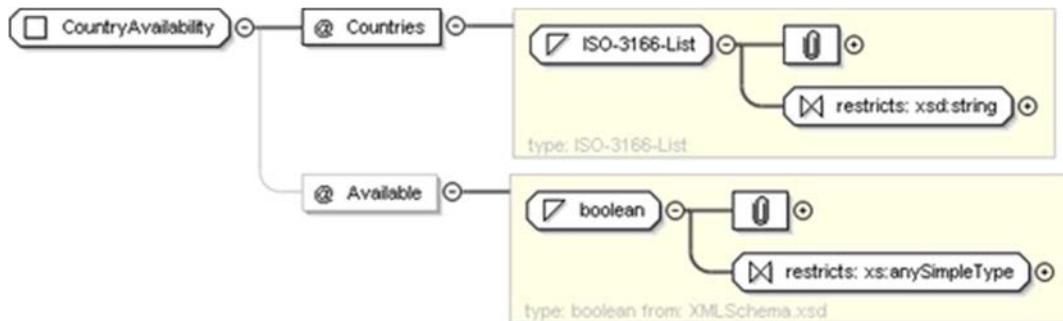


Figure 7ak: DescriptionLocationBCG

Table 11an: DescriptionLocation Fields

Name	Definition	Constraints
DescriptionLocationBCG (content of extended type)	This type extends the tva:TVAIDType type. This shall contain the identifier(s) of the BCG Record(s) for the BCG Discovery element that carries the information on this service.	Mandatory
preferred	If present and set to true, specifies that this location contains the preferred BCG. The default value for this attribute is false. There shall be only one preferred BCG.	Optional

5.2.12.6a DSMMType

This type conveys information about the DSM Manager and the methods available to connect to it.

```
<xsd:complexType name="DSMMType">
  <xsd:sequence>
    <xsd:element name="DSMMName" type="dvh:MultilingualType" maxOccurs="unbounded"/>
    <xsd:element name="DSMMID" type="xsd:decimal" minOccurs="0"/>
    <xsd:element name="Description" type="dvh:MultilingualType" minOccurs="0"
maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="LogoURI" type="xsd:anyURI" use="optional"/>
  <xsd:attribute name="DSMMlocation" type="xsd:anyURI" use="required"/>
</xsd:complexType>
```

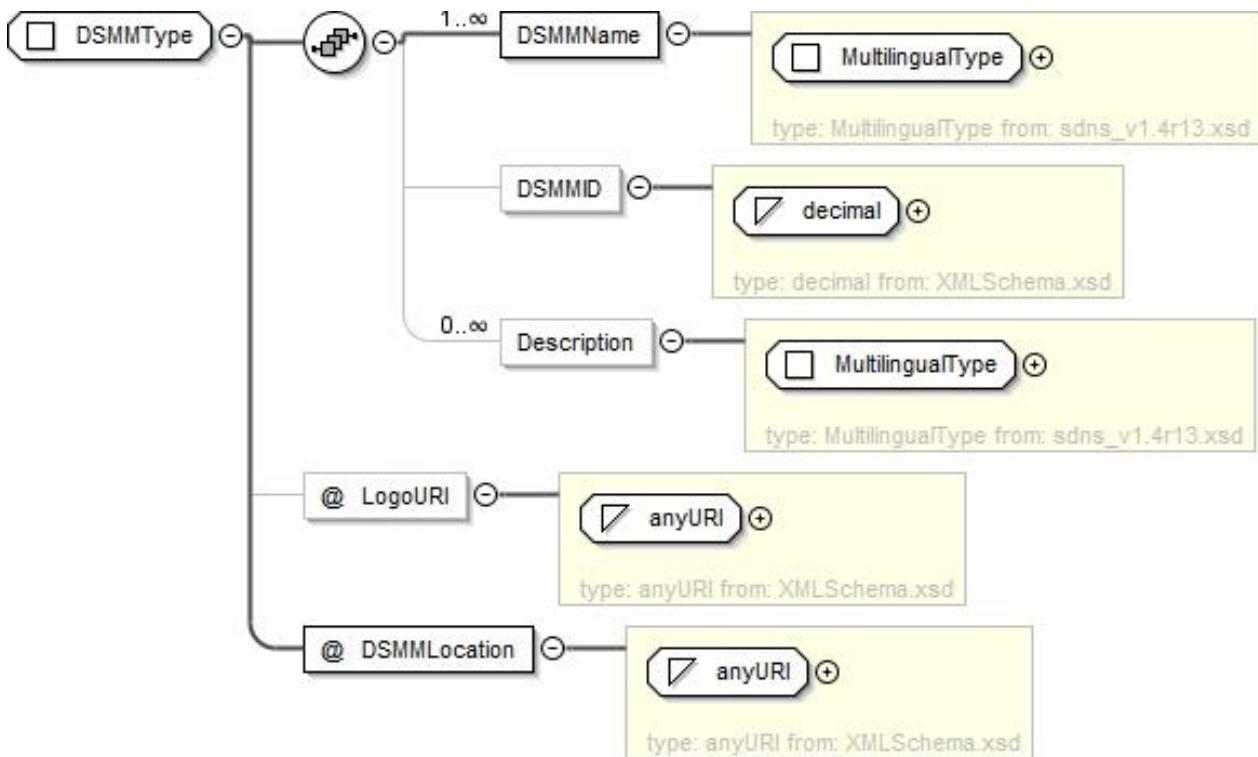


Figure 7aka: DSMMType

Table 11ana: DSMMType Fields

Name	Definition	Constraints
DSMMName	Multilingual name of DSMM, there may be multiple DSMMName for a single DSMM. Instantiated using MultilingualType as specified in clause 5.2.12.17.	Mandatory
DSMMID	Numeric identifier for the DSMM, in decimal form, if present there will be only one value per DSMM instance	Optional
Description	Multilingual description of DSMM, there may be multiple descriptions for a single DSMM. Instantiated using MultilingualType as specified in clause 5.2.12.17.	Optional
@LogoURI	URI from which logo of RMS may be obtained.	Optional
@DSMMLocation	URI to be used to connect to the DSMM.	Mandatory

5.2.12.7 DVBSTPTransportModeType

This type carries the details of the address and segments for information carried by the DVBSTP protocol.

```

<xsd:complexType name="DVBSTPTransportModeType">
    <xsd:complexContent>
        <xsd:extension base="dvb12:PayloadList">
            <xsd:attributeGroup ref="dvb14:MulticastAddressAttributes" />
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>

```

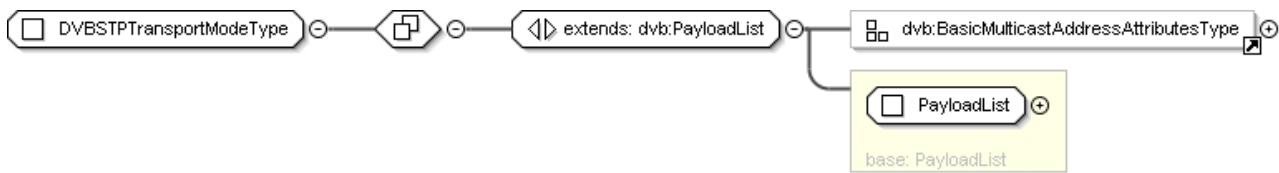


Figure 7al: DVBSTPTransportModeType

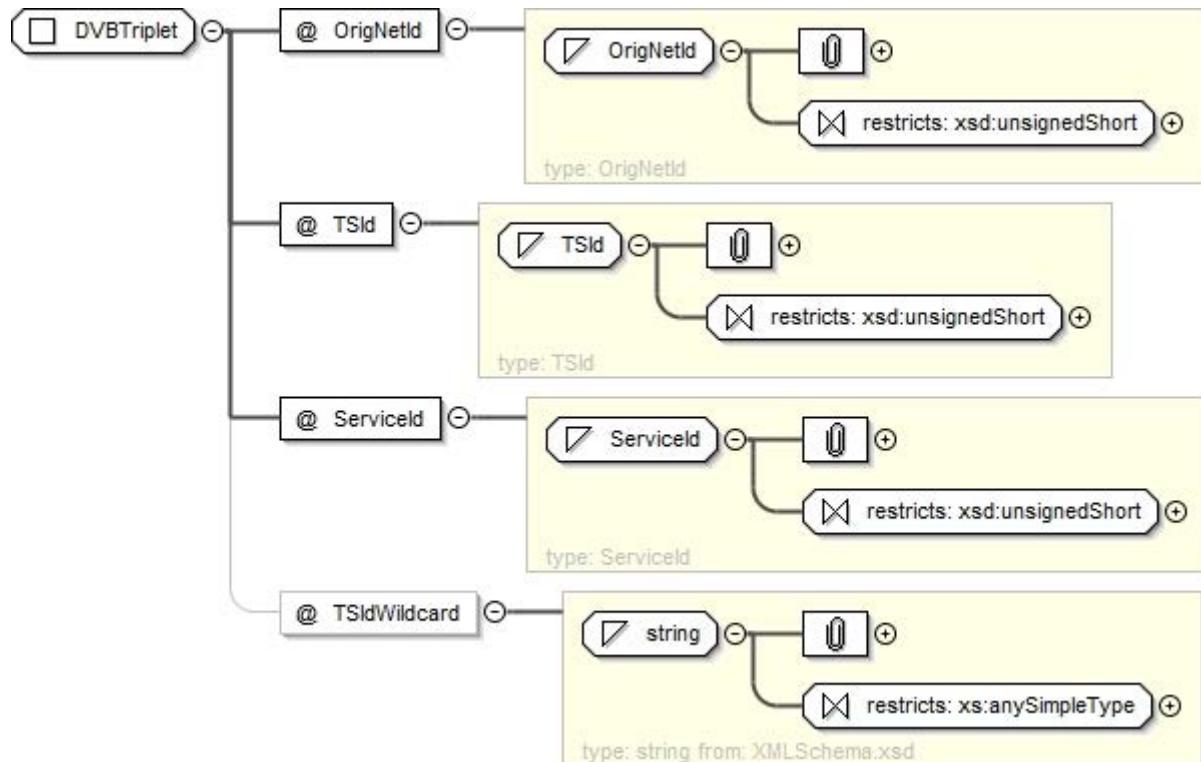
Table 11ao: DVBTPTTransportModeType Fields

Name	Definition	Constraints
DVBTPTTransportModeType (content of extended type)	This defines the segment and payloads that are carried at the specified address for the referenced information. The PayloadList type is defined in clause 5.2.12.22.	Mandatory
MulticastAddressAttributes (attributeGroup used to extend above type)	The Multicast address at which the information carried by the protocol is present. This attribute group is defined in clause 5.2.11.4.	Mandatory

5.2.12.8 DVBTriplet

This is a representation of the identifier for a service in a classic DVB system, as defined in ETSI TS 102 851 [115].

```
<xsd:complexType name="DVBTriplet">
  <xsd:attribute name="OrigNetId" type="dvb:OrigNetId" use="required"/>
  <xsd:attribute name="TSId" type="dvb:TSId" use="required"/>
  <xsd:attribute name="ServiceId" type="dvb:ServiceId" use="required"/>
  <xsd:attribute name="TSIdWildcard" type="xsd:string" fixed="*" use="optional"/>
</xsd:complexType>
```

**Figure 7am: DVBTriplet****Table 11ap: DVBTriplet Fields**

Name	Definition	Constraints
OrigNetId	Identifies the network Id of the originating delivery system. The format of this attribute is as defined in clause 5.2.10.	Mandatory
TSId	Identifies the Transport Stream. The format of this attribute is as defined in clause 5.2.10.	Mandatory
ServiceId	Identifies a service from any other service within the TS. The service Id is the same as the program number in the corresponding program map table. The format of this attribute is as defined in clause 5.2.10.	Mandatory
TSIdWildcard	If present, The TSId attribute can be ignored in favour of this wildcard, matching all value of TSId.	Optional

5.2.12.9 FECInfoType

This is the basic type that signals the presence and usage of FEC and conveys the necessary parameters to use the FEC with the service it is associated with.

```
<xsd:complexType name="FECInfoType">
  <xsd:sequence>
    <xsd:element name="FECBaseLayer" type="dvb14:FECLayerAddressType" />
    <xsd:element name="FECEnhancementLayer" type="dvb14:FECLayerAddressType" minOccurs="0" />
  </xsd:sequence>
  <xsd:attributeGroup ref="dvb:FECAttributeGroupType" />
</xsd:complexType>
```

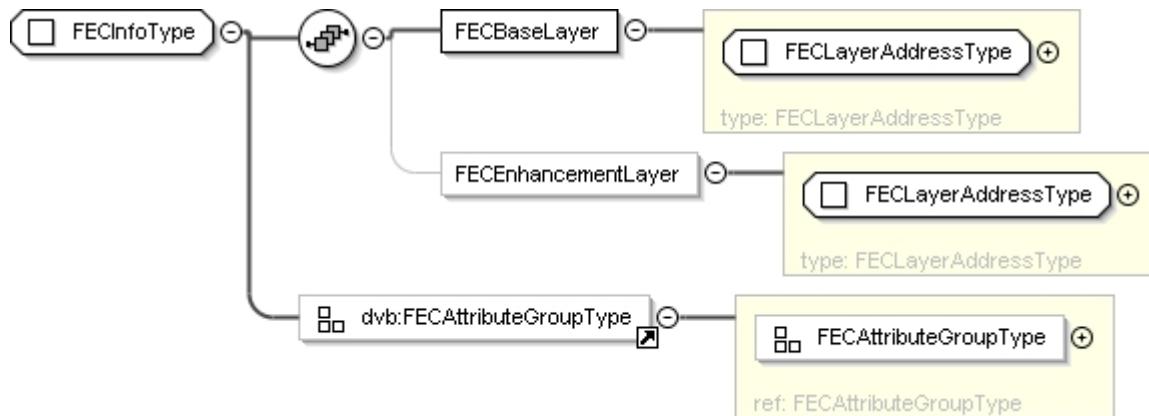


Figure 7an: FECInfoType Type

Table 11aq: FECInfoType Fields

Name	Definition	Constraints
FECBaseLayer	This carries the information of the FEC base layer, using the type defined in clause 5.2.12.10.	Mandatory
FECEnhancementLayer	This optional element carries details of the enhancement layer(s), using the type defined in clause 5.2.12.10.	Optional
FECAttributeGroup (included attributeGroup)	This attributeGroup defined in clause 5.2.11.3 is used to carry further details on the enhancement layer. All enhancement layers shall use the same parameter values, hence there is only one attribute group, even though there may be multiple enhancement layers.	Mandatory, if the EnhancementLayer is present

5.2.12.10 FECLayerAddressType

The Port attribute is optional as this type may be used in multiple places, however it shall be present in some cases. Specifically, the type is only optional when it is used in conjunction with CoDAnnounceDescribe and an RTSP based URL. In this case the relevant information port is obtained via the SETUP response message.

Where this type is used in the context of the BaseLayer, the PayloadTypeNumber shall have a default value of 96 (i.e. if there is no PayloadTypeNumber in a BaseLayer, the value 96 is inferred) and the TransportProtocol shall not be present.

Where this type is used in the context of the EnhancementLayer, the TransportProtocol shall have a default value of UDP/FEC (i.e. if there is no TransportProtocol in an EnhancementLayer, the value UDP/FEC is inferred).

```
<xsd:complexType name="FECLayerAddressType">
  <xsd:attribute name="Address" type="dvb14:IPOrDomainType" use="optional" />
  <xsd:attribute name="Source" type="dvb14:IPOrDomainType" use="optional" />
  <xsd:attribute name="Port" type="xsd:unsignedShort" use="optional" />
  <xsd:attribute name="MaxBitrate" type="xsd:positiveInteger" use="optional" />
  <xsd:attribute name="RTSPControlURL" type="xsd:anyURI" use="optional" />
  <xsd:attribute name="PayloadTypeNumber" type="xsd:unsignedInt" use="optional" />
  <xsd:attribute name="TransportProtocol" type="dvb:TransportProtocolType" use="optional" />
</xsd:complexType>
```

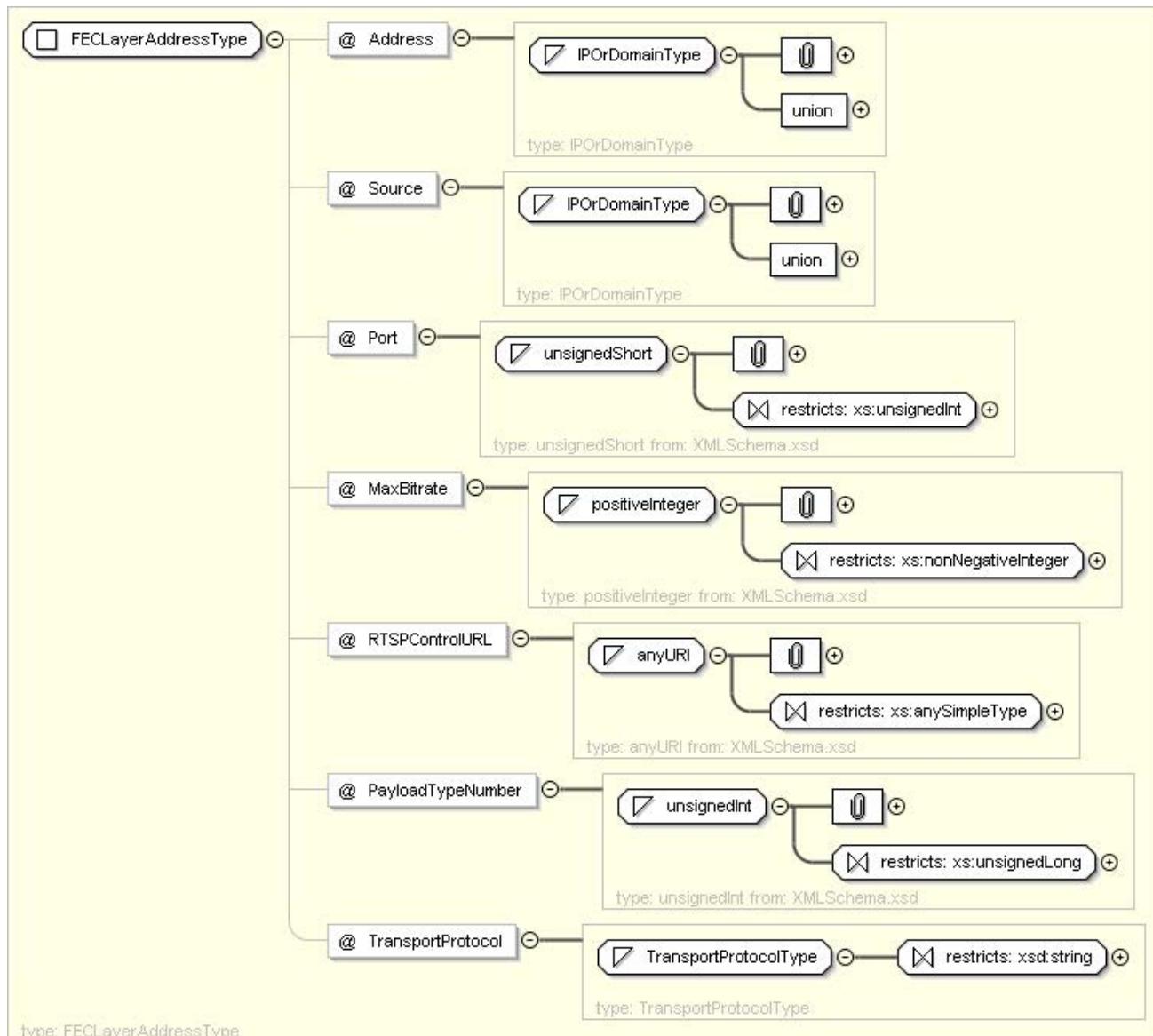


Figure 7ao: FECLayerAddressType

Table 11ar: FECLayerAddressType Fields

Name	Definition	Constraints
Address	IP Multicast Address for FEC Base Layer (SMPTE-2022-1 [66]). If the IP multicast address is omitted, then the FEC flow is assumed to be on the same multicast address as the original data.	Optional
Source	IP Multicast Source Address for FEC Base Layer (SMPTE-2022-1 [66]). If the IP multicast source address is omitted, then the FEC flow is assumed to be on the same multicast source address as the original data.	Optional
Port	UDP port for FEC Layer.	Mandatory, where FEC is used
MaxBitrate	Specifies the maximum bitrate (in kbits/s) of this Layer of the FEC flow, and calculated according to TIAS value in IETF RFC 3890 [80].	Optional
RTSPControlURL	The RTSP URL to be used for RTSP control messages (SETUP) for this FEC Layer.	Mandatory where FEC is used in conjunction with RTSP
PayloadTypeNumber	RTP payload type number for FEC Base layer. It shall be 96 (the 1st dynamic payload number) for SMPTE 2022 compatibility. If not present, the value 96 shall be inferred.	Optional
TransportProtocol	Transport Protocol of enhancement layer. In the current version the Identifier is restricted to UDP/FEC and RTP/AVP. If this element is omitted, the UDP/FEC shall be assumed for the protocol identifier.	Optional with FEC enhancement layers; prohibited with FEC Base layers

5.2.12.11 FUSAnnouncementType

This type contains information about the method used to carry one or more options for how an HNED should connect to receive update announcements.

```
<xsd:complexType name="FUSAnnouncementType">
  <xsd:sequence>
    <xsd:element name="FUSAnnouncementDescription" type="xsd:string" minOccurs="0" />
    <xsd:element name="MulticastAnnouncementAddress" type="dvb14:RMSFUSMulticastAddressType"
minOccurs="0" />
    <xsd:element name="FUSUnicastAnnouncement" type="xsd:anyURI" minOccurs="0" />
    <xsd:element name="QRCLocation" type="xsd:anyURI" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

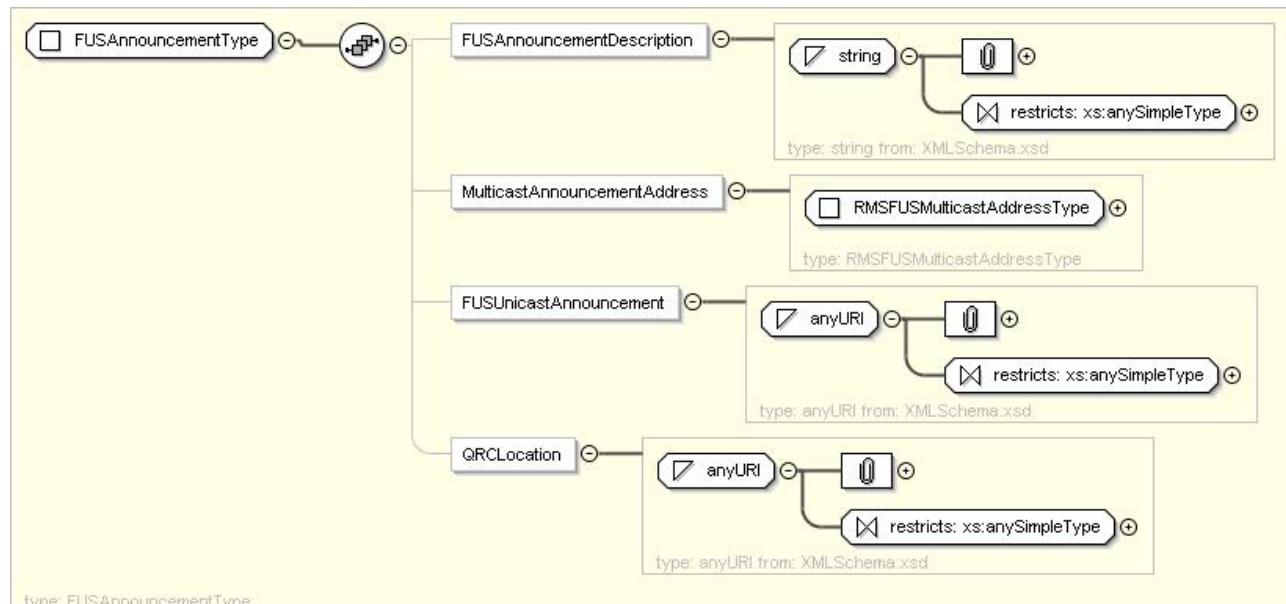


Figure 7ap: FUSAnnouncementType

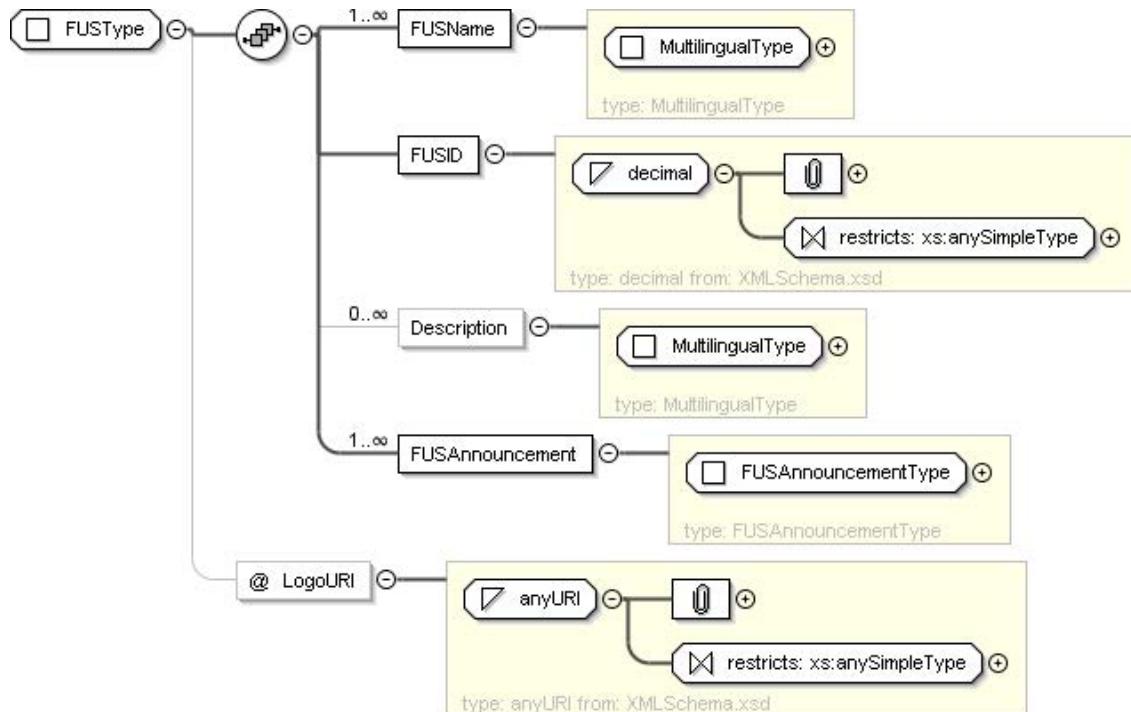
Table 11as: FUSAnnouncementType Fields

Name	Semantic Definition	Constraints
FUSAnnouncementDescription	Textual description of the announcement.	Optional
MulticastAnnouncementAddress	Instantiated using the RMSFUSMulticastAddressType defined in clause 5.2.12.27.	Optional
FUSUnicastAnnouncement	URI to which requests for unicast announcements should be made.	Optional
QRCLocation	URI to which connections to query/response channel should be made.	Optional

5.2.12.12 FUSType

This type conveys information about a firmware update server and the methods available to connect to it.

```
<xsd:complexType name="FUSType">
  <xsd:sequence>
    <xsd:element name="FUSName" type="dvb:MultilingualType" maxOccurs="unbounded" />
    <xsd:element name="FUSID" type="xsd:decimal"/>
    <xsd:element name="Description" type="dvb:MultilingualType" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="FUSAnnouncement" type="dvb14:FUSAnnouncementType" maxOccurs="unbounded" />
  </xsd:sequence>
  <xsd:attribute name="LogoURI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>
```

**Figure 7aq: FUSType****Table 11at: FUSType Fields**

Name	Semantic Definition	Constraints
FUSName	Multilingual name of FUS, there may be multiple FUSNames for a single FUS.	Mandatory
FUSID	Numeric identifier of FUS in decimal form, there will only be a single identifier for a FUS instance.	Mandatory
Description	Textual description of firmware update.	Optional
FUSAnnouncement	Multiple FUSAnnouncement instances may be provided. Instantiated using FUSAnnouncementType defined in clause 5.2.12.11.	Mandatory
@LogoURI	URI to download the URI of the FUS provider.	Optional

5.2.12.13 HTTPTransportModeType

This type carries the details of the address and segments for information that may be accessed by the HTTP protocol as described in clause 5.4.2 or optionally with SOAP in the case of the BCGOffering described in clause 5.2.13.1.

```
<xsd:complexType name="HTTPTransportModeType">
  <xsd:complexContent>
    <xsd:extension base="dvb:PayloadList">
      <xsd:attribute name="Location" type="dvb:PullURL" use="required"/>
      <xsd:attribute name="SOAP" type="xsd:boolean" default="false"/>
      <xsd:attribute name="PollingPeriodSecs" type="xsd:unsignedShort" use="optional"/>
      <xsd:attribute name="SpreadRequestSecs" type="xsd:unsignedShort" use="optional"/>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
```

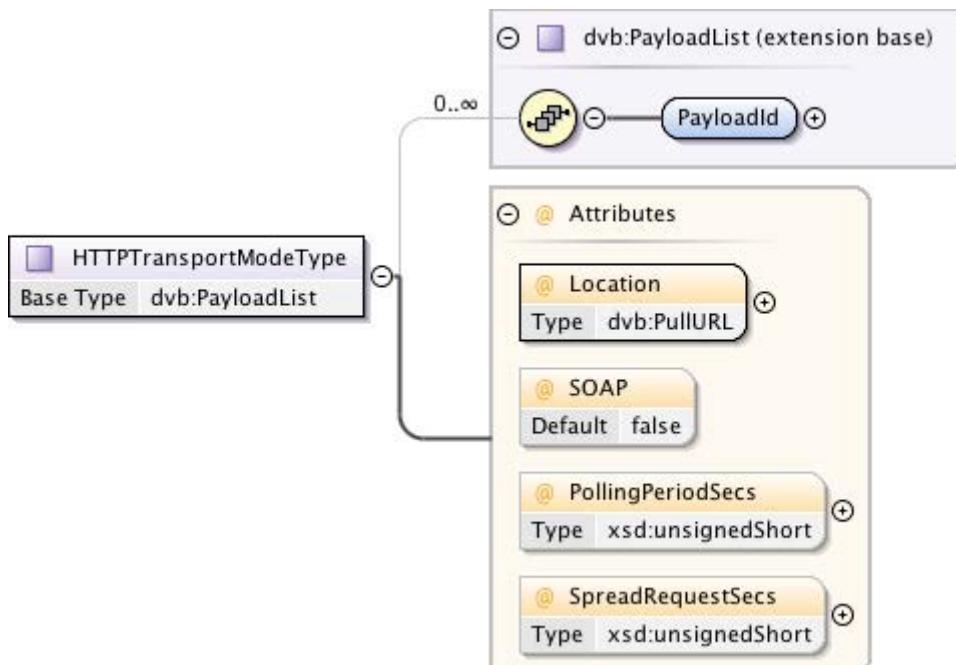


Figure 7ar: HTTPTransportModeType

Table 11au: HTTPTransportModeType Fields

Name	Definition	Constraints
HTTPTransportModeType (contents of extended type)	This defines the segment and payloads that are carried at the specified address for the referenced information. This base type is defined in clause 5.2.12.22.	Mandatory
Location	Specifies the location at which the guide may be found. The format of this type is defined in clause 5.2.10.	Mandatory
SOAP	This indicates if the guide may be queried using the SOAP protocol rather than the mechanism outlined in clause 5.4.2. The default value of this attribute is "false".	Optional
PollingPeriodSecs	This indicates the minimum interval in seconds between connection requests when polling is used to acquire the guide. Defined to align with UK DTG D-Book 7 Part A v4 [i.11].	Optional
SpreadRequestSecs	A wait period in seconds which is used to randomize requests by HNEDs when segment version changes are signalled via a push method, e.g. via broadcast signalling. The delay before issuing the request shall be determined by the following algorithm: $\text{wait period in seconds} \geq \text{rand(SpreadRequestSecs)}$. Defined to align with UK DTG D-Book 7 Part A v4 [i.11].	Optional

5.2.12.14 McastType

This is used to hold a multicast address and optionally signals the use of AL-FEC or RET/FCC and when such are present carries the information necessary for these optional components. The McastType, through the MulticastAddressAttributes, supports source specific multicast (SSM) addressing if the Source attribute is specified. Otherwise it supports any source multicast (ASM) addresses.

The CNAME and ssrc fields allow the carriage of values used by the service and may optionally be used to assist an HNED in identifying correct flows, and allocating unique numbers.

```
<xsd:complexType name="McastType">
    <xsd:sequence minOccurs="0">
        <xsd:element name="FECBaseLayer" type="dvb14:FECLayerAddressType" minOccurs="0" />
        <xsd:element name="FECEnhancementLayer" type="dvb14:FECLayerAddressType" minOccurs="0" maxOccurs="unbounded" />
        <xsd:element name="CNAME" type="xsd:string" minOccurs="0"/>
        <xsd:element name="ssrc" type="xsd:unsignedInt" minOccurs="0"/>
        <xsd:element name="RTPRetransmission" type="dvb:RETInfoType" minOccurs="0"/>
        <xsd:element name="ServerBasedEnhancementServiceInfo" type="dvb12:ServerBasedEnhancementServiceInfoType" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attributeGroup ref="dvb14:MulticastAddressAttributes"/>
</xsd:complexType>
```

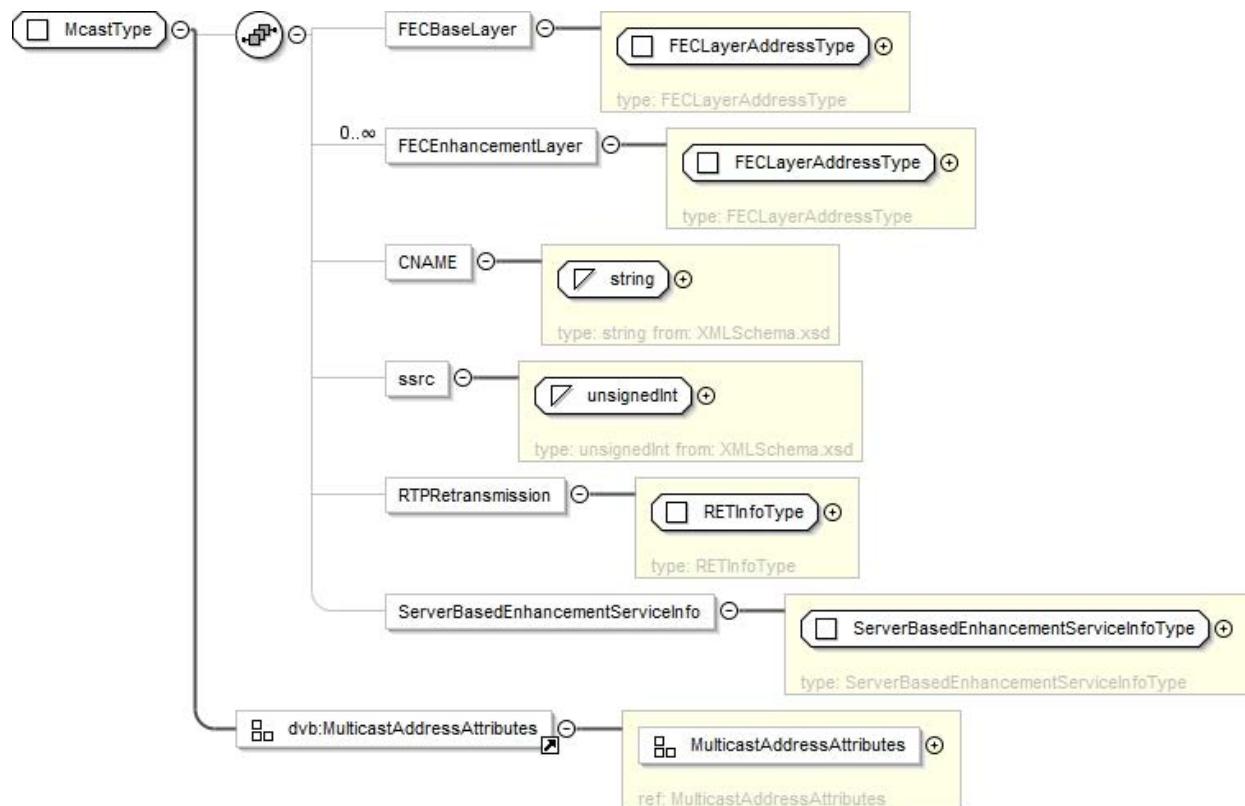


Figure 7as: McastType

Table 11av: McastType Fields

Name	Definition	Constraints
FECBaseLayer	The presence of this element signals the use of a FEC base layer on the referenced multicast. This field contains the multicast address and port of the AL-FEC stream (SMPTE-2022-1 [66]). The type is described in clause 5.2.12.10.	Optional, but mandatory if the FECEnhancementLayer element is present.
FECEnhancementLayer	The presence of this element signals the use of a FEC enhancement layer(s) on the referenced multicast. This field contains the multicast address and port of the AL-FEC enhancement stream(s). This element shall only be present if the FECBaseLayer element is present. This element may be repeated for multiple layers. The type is described in clause 5.2.12.10.	Optional
CNAME	This field, when present, carries the canonical name of the RTP stream.	Optional
Ssrc	This field, when present, carries the ssrc identifier value of the RTP stream.	Optional
RTPRetransmission	This field signals the use of RTP Retransmission (RET service) on the referenced multicast and carries the parameters associated with retransmission. The type is described in clause 5.2.12.26. See also clause I.2.14 for details on when to use it.	Optional
ServerBasedEnhancementServiceInfo	This field signals a server-based LMB enhancement service (server-based FCC and/or RET service) on the referenced LMB and carries the parameters associated with the enhancement service. This type is described in clause 5.2.12.31. See also clause I.2.14 for details on when to use it.	Optional
MulticastAddressAttributes (<i>included attributeGroup</i>)	These attributes are described and defined in clause 5.2.11.4 and specify the IP Multicast Address Parameters.	Mandatory

5.2.12.15 MosaicDescription

The mosaic description element identifies the elementary cells of a mosaic service, groups different elementary cells to form logical cells, and establishes a link between the content of all or part of the logical cell and the corresponding service or package information.

An implementation of the Mosaic descriptor from ETSI EN 300 468 [1]. All fields are defined in ETSI EN 300 468 [1].

The AudioLink field allows a tag and language to be associated with each logical cell of the mosaic. This enables a different audio stream to be associated with each logical cell.

```

<xsd:complexType name="MosaicDescription">
    <xsd:sequence maxOccurs="unbounded">
        <xsd:element name="LogicalCell">
            <xsd:complexType>
                <xsd:sequence>
                    <xsd:sequence maxOccurs="unbounded">
                        <xsd:element name="ElementaryCell">
                            <xsd:complexType>
                                <xsd:attribute name="CellId" type="dvb:Integer6bit" use="required"/>
                            </xsd:complexType>
                        </xsd:element>
                    </xsd:sequence>
                    <xsd:element name="AudioLink" minOccurs="0" maxOccurs="unbounded">
                        <xsd:complexType>
                            <xsd:attribute name="Language" type="dvb:ISO639-2" use="optional"/>
                            <xsd:attribute name="ComponentTag" type="dvb:Hexadecimal8bit"
use="required"/>
                        </xsd:complexType>
                    </xsd:element>
                </xsd:sequence>
                <xsd:choice minOccurs="0">
                    <xsd:element name="TextualId" type="dvb:TextualIdentifier"/>
                    <xsd:element name="DVBTriplet" type="dvb:DVBTriplet"/>
                    <xsd:element name="PackageId">
                        <xsd:complexType>
                            <xsd:simpleContent>

```

```

<xsd:extension base="dvb:Hexadecimal16bit">
    <xsd:attribute name="Domain" type="dvb:DomainType"
use="optional"/>
        </xsd:extension>
    </xsd:simpleContent>
</xsd:complexType>
</xsd:element>
</xsd:choice>
</xsd:sequence>
<xsd:attribute name="CellId" type="dvb:Integer6bit" use="required"/>
<xsd:attribute name="PresentationInfo" type="dvb:Hexadecimal3bit" use="required"/>
<xsd:attribute name="LinkageInfo" type="dvb:Hexadecimal8bit" use="required"/>
<xsd:attribute name="EventId" type="dvb:Hexadecimal16bit" use="optional"/>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
<xsd:attribute name="EntryPoint" type="xsd:boolean" default="true"/>
<xsd:attribute name="HorizontalCellsNumber" type="dvb:Hexadecimal3bit" use="required"/>
<xsd:attribute name="VerticalCellsNumber" type="dvb:Hexadecimal3bit" use="required"/>
</xsd:complexType>

```

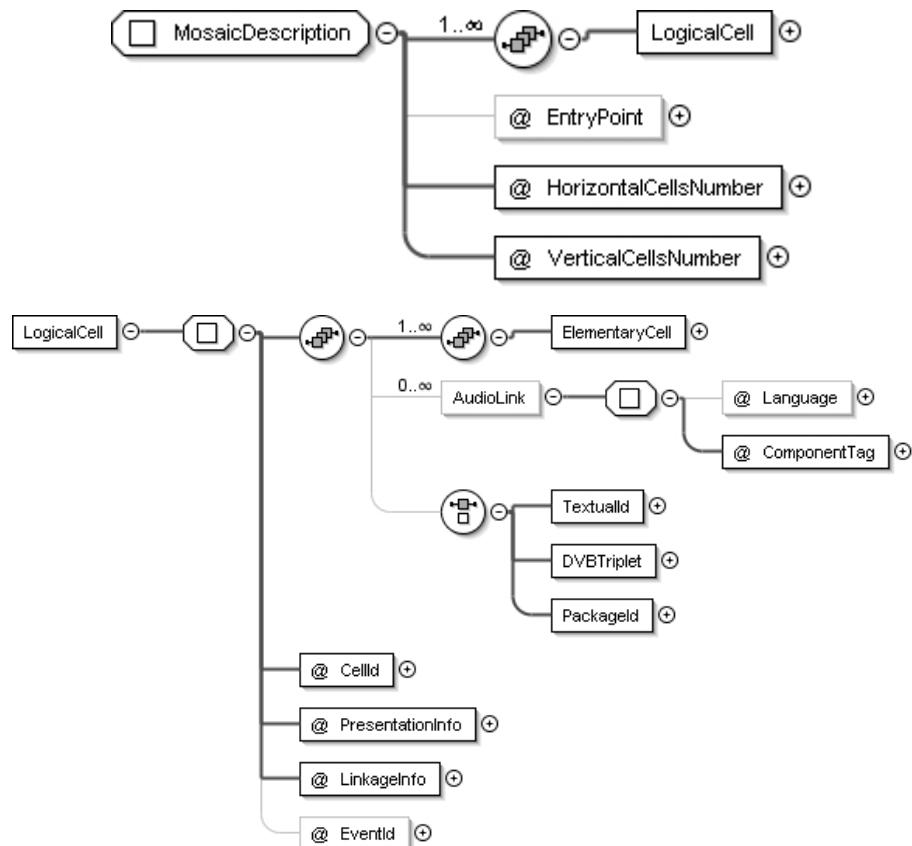


Figure 7at: MosaicDescription

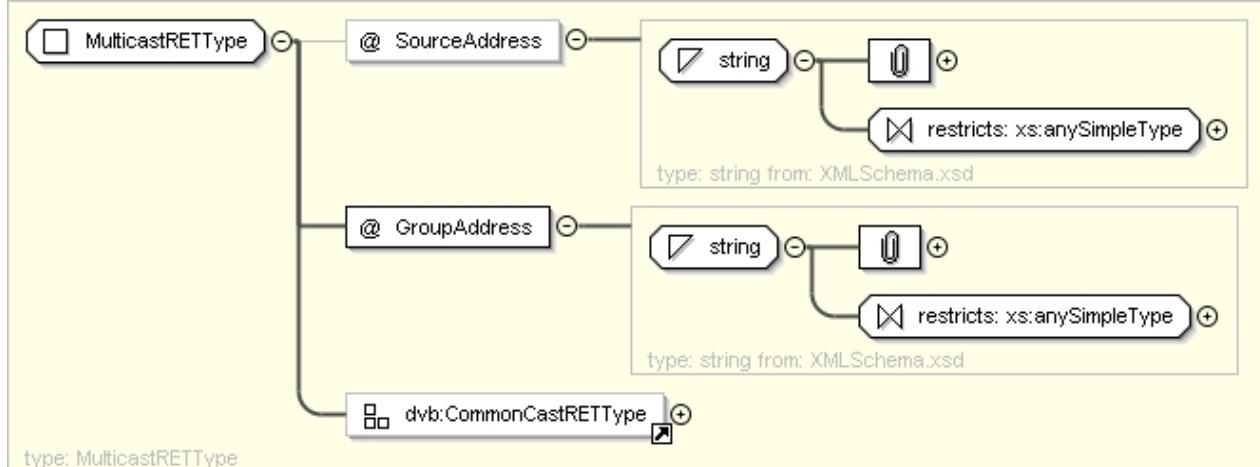
Table 11aw: MosaicDescription Fields

Name	Mosaic_descriptor equivalent name	Constraints
LogicalCell	Equivalent to loop in body of descriptor	Mandatory
ElementaryCell	Elementary_cell_id, repeated elementary_cell_field_length times	Mandatory
CellId	Logical_cell_id	Mandatory
AudioLink	Additional field to allow audio support	Optional
Language	Additional field to allow support for multiple language audios.	Optional
ComponentTag	Additional field to allow identification of audio component via component_tag in PMT.	Optional
TextualId	Textual, DNS form of Original_network_id, transport_stream_id, service_id	Optional
DVBTriplet	Original_network_id, transport_stream_id, service_id	Optional
PackageId	Bouquet_id	Optional
PresentationInfo	Logical_cell_presentation_info	Mandatory
LinkageInfo	Cell_linkage_info	Mandatory
EventId	Event_id	Optional
EntryPoint	Mosaic_entry_point	Mandatory
HorizontalCellsNumber	Number_of_horizontal_elementary_cells	Mandatory
VerticalCellsNumber	Number_of_vertical_elementary_cells	Mandatory

5.2.12.16 MulticastRETTType

This type provides the basic attributes needed for multicast RET, and includes the CommonCastRET type to provide a range of optional data, defined in clause 5.2.11.2. This is the multicast equivalent of the UnicastRETTType defined in clause 5.2.12.47.

```
<xsd:complexType name="MulticastRETTType">
  <xsd:attribute name="SourceAddress" type="xsd:string" use="optional"/>
  <xsd:attribute name="GroupAddress" type="xsd:string" use="required"/>
  <xsd:attributeGroup ref="dvb:CommonCastRETTType"/>
</xsd:complexType>
```

**Figure 7au: MulticastRETTType****Table 11ax: MulticastRETTType Attributes**

Name	Definition	Constraints
SourceAddress	A single IP address OR a single DNS SRV RR. This is the IP Source Address of the MC RTP RET packets. If not present, the IP Source Address of the MC RTP RET packets takes the same value as the IP Source Address of the unicast RTP RET packets (the information for unicast RTP RET shall be present even when multicast RTP RET is offered).	Optional
GroupAddress	Single IP address OR single DNS SRV RR representing the IP Group Address of MC RET.	Mandatory
CommonCastRETTType (included attributeGroup)	This carries additional MC RET parameters (see clause 5.2.11.2).	Mandatory

5.2.12.17 MultilingualType

The XML MultilingualType gives the capability to carry a string with an associated language.

```
<xsd:complexType name="MultilingualType">
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="Language" type="dub:ISO639-2" use="required" />
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
```

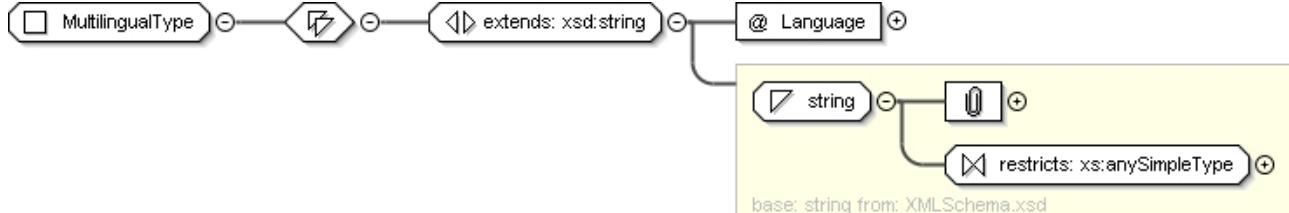


Figure 7av: MultilingualType

Table 11ay: MultilingualType Fields

Name	Description	Constraints
MultilingualType (contents of extended type)	The base XML type string contains a string value with the language as specified by the attribute Language. White space within strings is preserved in this usage.	Mandatory
Language	The 2 letter language code, defined as per ISO 639-2 [51].	Mandatory

5.2.12.18 OfferingBase

This is the base type from which all offerings should be derived. It provides the required Domain Type attribute, and the optional version field required when HTTP protocol is used.

```
<xsd:complexType name="OfferingBase">
  <xsd:attribute name="DomainName" type="dub:DomainType" use="required"/>
  <xsd:attribute name="Version" type="dub:Version" use="optional"/>
</xsd:complexType>
```

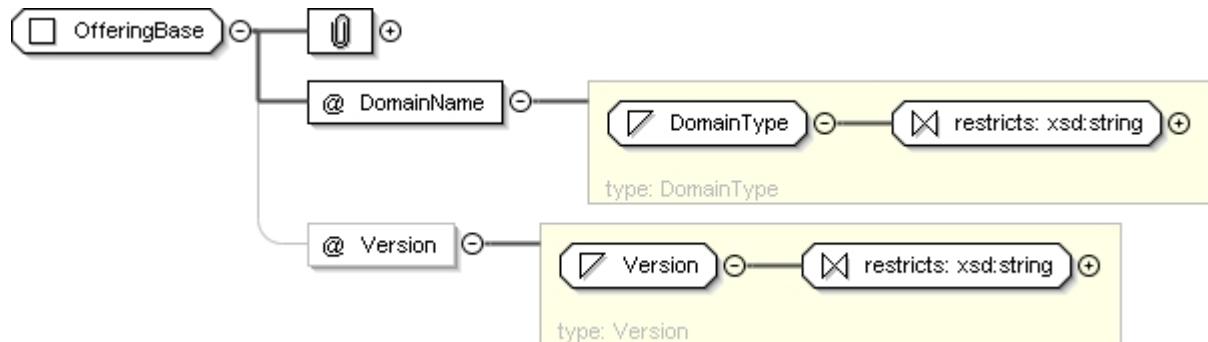


Figure 7aw: OfferingBase

Table 11az: OfferingBase Fields

Name	Description	Constraints
DomainName	An internet DNS domain name registered by the SP that uniquely identifies the SP. This field is used as a default value for certain fields within the record, as identified in their semantics.	Mandatory
Version	Version of the DVB-IPTV Offering record, the version number shall be incremented every time a change in the DVB-IPTV Offering record is made.	Mandatory where the record is provided on request (i.e. "pull mode") and is optional when the record is multicasted (i.e. "push mode").

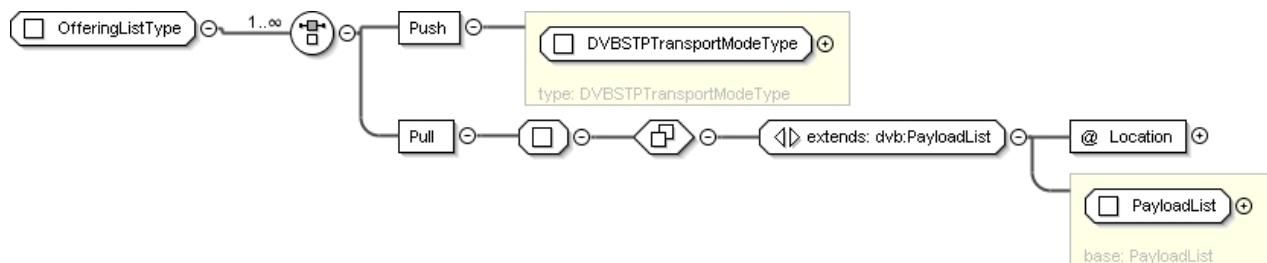
5.2.12.19 OfferingListType

The metadata to describe the Push and Pull methods available to the HNED are described in the following clauses.

This type is used to convey the locations at which an offering can be found. It allows an unlimited list of either push or pull locations at which the specified service or information can be found. Note that the Pull element shall contain Segment Ids and version numbers.

NOTE: The Pull element is deliberately not of type HTTPTransportModeType as there is no defined SOAP support for the SD&S information.

```
<xsd:complexType name="OfferingListType">
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="Push" type="dvb14:DVBSTPTransportModeType" />
    <xsd:element name="Pull">
      <xsd:complexType>
        <xsd:complexContent>
          <xsd:extension base="dvb12:PayloadList">
            <xsd:attribute name="Location" type="dvb:PullURL" use="required"/>
          </xsd:extension>
        </xsd:complexContent>
      </xsd:complexType>
    </xsd:element>
  </xsd:choice>
</xsd:complexType>
```

**Figure 7ax: OfferingListType****Table 11ba: OfferingListType Fields**

Name	Description	Constraints
Push	Signals the multicast address(es) at which the SD&S information may be found. The format is defined in clause 5.2.12.7.	Optional
Pull (Content of extended type)	The base type, <code>PayloadList</code> , is defined in clause 5.2.12.22, and the extensions use this to signal SD&S information which may be retrieved from the URL encoded in the <code>Location</code> attribute.	Optional
Location (attribute of Pull)	(see description of Pull above).	Mandatory, where Pull is used

5.2.12.20 PackageAvailabilityCountryCodeType

This type provides for a list of countries in which a service or package is either available or not available. This is used in conjunction with a string that lists the Cells which provide further subdivision of the country. For more details on the Regionalization supported by this mechanism, see clause 5.2.13.8.

```
<xsd:complexType name="PackageAvailabilityCountryCodeType">
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="Availability" type="xsd:boolean" default="true"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
```

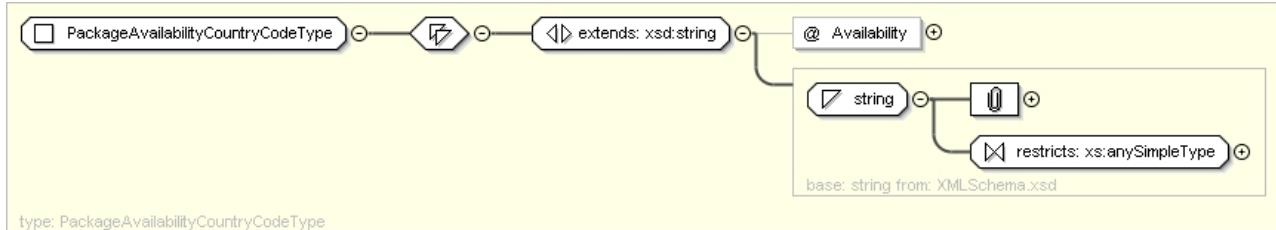


Figure 7ay: PackageAvailabilityCountryCodeType

Table 11bb: PackageAvailabilityCountryCodeType Fields

Name	Definition	Constraints
PackageAvailabilityCountryCodeType (contents of extended type)	This is an extension of the basic XML schema string type that carries the country for which the availability is being defined. This element shall be of the 2-letter format specified in ISO 3166 [50].	Mandatory
Availability	This flag indicates whether the service is available in the country specified by CountryCode. The default is TRUE. When TRUE, the service or package is available in the specified country with the exception of those regions identified by Cells. When FALSE, the service or package is not available in the specified country with the exception of those regions identified by Cells.	Optional

5.2.12.21 PackagedServiceType

This provides the type used for one service contained within a package, together with the logical channel number of the service and a location for a description of the service.

```
<xsd:complexType name="PackagedServiceType">
    <xsd:sequence>
        <xsd:element name="TextualID" type="dvb12:PackageTextualIdentifier" maxOccurs="unbounded" />
        <xsd:element name="DVBTriplet" type="dvb:DVBTriplet" minOccurs="0" />
        <xsd:element name="DescriptionLocation" type="dvb:DescriptionLocationBCG" minOccurs="0" />
        <xsd:element name="LogicalChannelNumber" type="xsd:positiveInteger" minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>
```

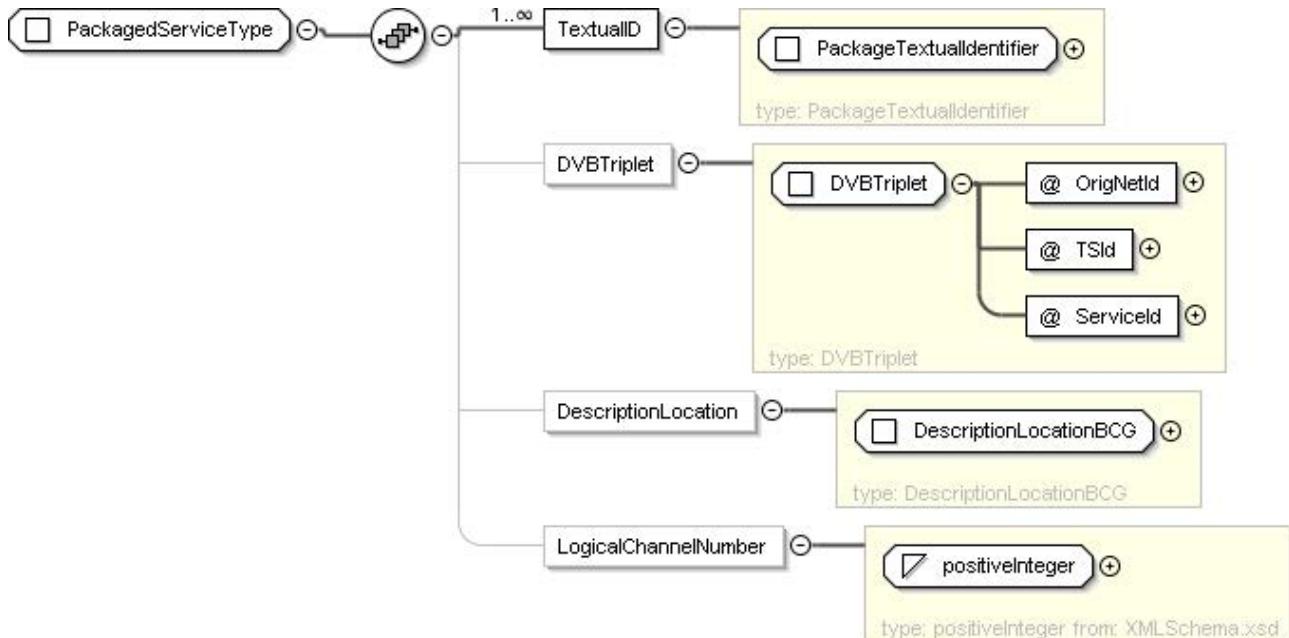


Figure 7az: PackagedServiceType

Table 11bc: PackagedServiceType Fields

Name	Definition	Constraints
TextualID	The textual reference of the service, as defined in clause 5.2.12.45.	Mandatory
DVBTriplet	The optional DVB Triplet equivalent to the TextualID service identification, as defined in clause 5.2.12.8.	Optional
DescriptionLocation	The location of the BCG description of the service, as defined in clause 5.2.12.6.	Optional
LogicalChannelNumber	The logical channel number of the service.	Optional

5.2.12.22 PayloadList

This type describes a list of payload IDs (as described in clause 5.4.4.1) and optional SegmentIDs (similarly described in clause 5.4.4.2). This is used by the DVBSTP and HTTP types to indicate which payload(s) and optionally segment(s) are available at the specified address for the information indicated by the usage of the type.

```
<xsd:complexType name="PayloadList">
    <xsd:sequence minOccurs="0" maxOccurs="unbounded" >
        <xsd:element name="PayloadId">
            <xsd:complexType>
                <xsd:sequence minOccurs="0" maxOccurs="unbounded" >
                    <xsd:element name="Segment" type="dvb12:PayloadListSegmentType" />
                </xsd:sequence>
                <xsd:attribute name="Id" type="dvb:Hexadecimal8bit" use="required" />
            </xsd:complexType>
        </xsd:element>
    </xsd:sequence>
</xsd:complexType>
```

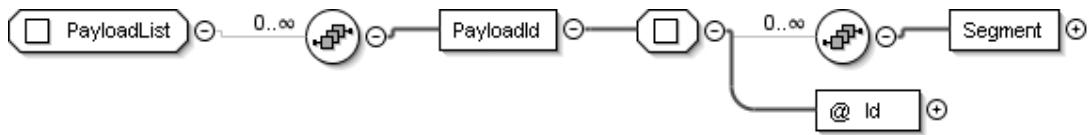


Figure 7ba: PayloadList

Table 11bd: PayloadList Fields

Name	Definition	Constraints
<code>PayloadId</code>	A <code>PayloadId</code> , specified by the <code>Id</code> attribute. This element optionally contains the list of segments and their IDs and versions that make up the referenced payload. Multiple occurrences of this element make up the full <code>payloadList</code> .	Optional
<code>Id</code>	The ID of the Payload. The ID values are defined in ETSI TS 101 162 [2], clause 9.1.2 and informatively in Table 12a in clause 5.4.4.1.	Mandatory
<code>Segment</code>	An optional list of segments that are carried, using the values defined by the type in clause 5.2.12.23.	Optional

5.2.12.23 PayloadListSegmentType

This type is used to carry the details of a segment that is available, together optionally with the target package to which the segment relates.

```

<xsd:complexType name="PayloadListSegmentType">
  <xsd:sequence>
    <xsd:element name="TargetPackage" type="dvb12:TargetPackageType" minOccurs="0"
maxOccurs="unbounded" />
  </xsd:sequence>
  <xsd:attribute name="Version" type="dvb:Version" use="optional"/>
  <xsd:attribute name="ID" type="dvb:Hexadecimal16bit" use="required"/>
</xsd:complexType>
  
```

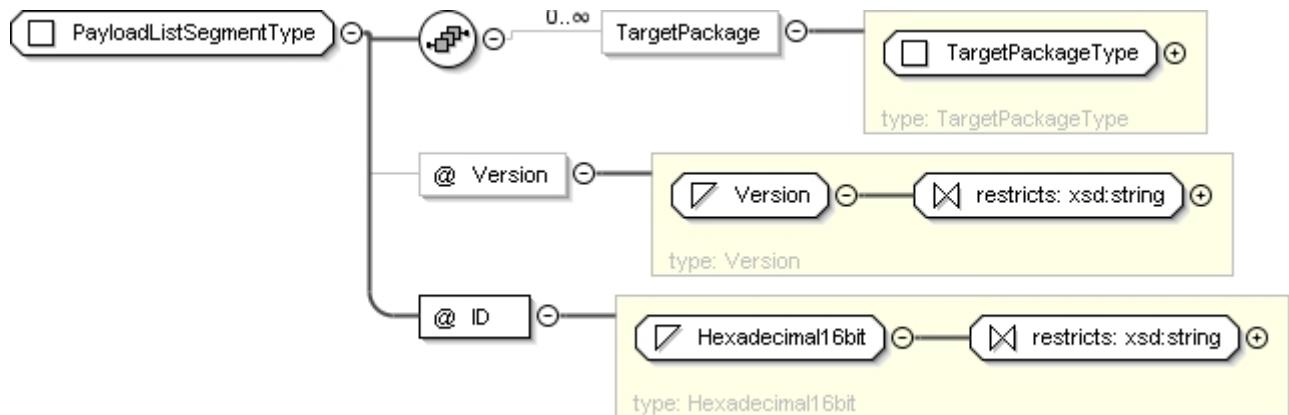


Figure 7bb: PayloadListSegmentType

Table 11be: PayloadListSegmentType Fields

Name	Definition	Constraints
<code>TargetPackage</code> (Child of <code>Segment</code>)	An optional list of <code>TargetPackage</code> s, as defined in clause 5.2.12.44.	Optional
<code>Version</code>	The <code>Version</code> number of the segment identified by the matching ID. The format of this is defined in clause 5.2.10.	Optional
<code>ID</code> (attribute of <code>Segment</code>)	The <code>segmentID</code> that is carried. The <code>segmentID</code> is defined by the operator and not within the scope of the present document.	Mandatory

5.2.12.24 ReferencedServiceProviderType

This type is used to list one or more services from a different provider that a current provider wishes to include in their context.

```
<xsd:complexType name="ReferencedServiceProviderType">
  <xsd:sequence>
    <xsd:element name="Service" minOccurs="0" maxOccurs="unbounded">
      <xsd:complexType>
        <xsd:attribute name="Name" type="dvb:Service" use="required"/>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
  <xsd:attribute name="Domain" type="dvb:DomainType" use="required"/>
</xsd:complexType>
```

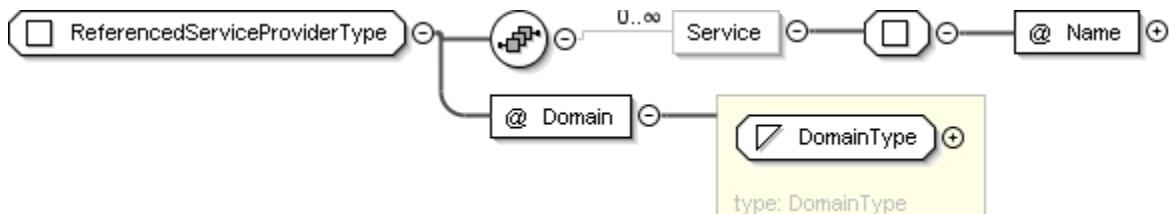


Figure 7bc: ReferencedServiceProviderType

Table 11bf: ReferencedServiceProviderType Fields

Name	Definition	Constraints
Service	A list of referenced services. This element may be omitted in which case the entire set of offerings from the SP is referenced.	Optional
@Domain	The domain component of the textual service identifier to which the SP is referring. An internet DNS domain name registered by the referenced SP that uniquely identifies the SP being referenced.	Mandatory

5.2.12.25 ReplacementService

This is an XML representation of the replacement service functionality of the linkage_descriptor in ETSI EN 300 468 [1]. The service indicated by either the DVB triplet or the textual identifier may be used when the specified service (as derived from the context) fails. It identifies a service replacement service which may be selected automatically by the HNED when the service being decoded fails.

NOTE: Linkage_type 0x08 (mobile hand-over) is not supported.

```
<xsd:complexType name="ReplacementService">
  <xsd:choice>
    <xsd:element name="TextualIdentifier" type="dvb:TextualIdentifier"/>
    <xsd:element name="DVBTriplet" type="dvb:DVBTriplet"/>
  </xsd:choice>
  <xsd:attribute name="ReplacementType" type="dvb:Hexadecimal8bit" use="optional" default="5"/>
</xsd:complexType>
```

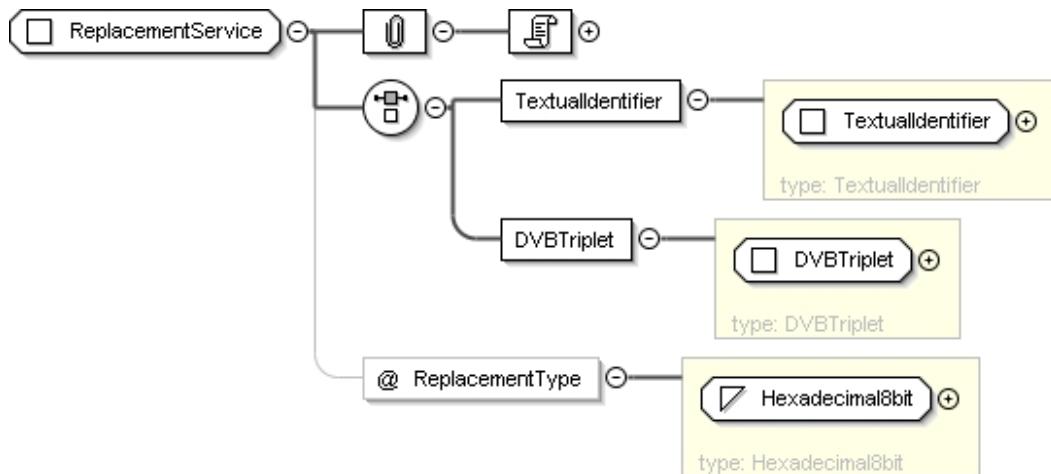


Figure 7bd: ReplacementService

Table 11bg: ReplacementService Fields

Name	Definition	Constraints
TextualIdentifier	The textual equivalent of the DVB triplet, as defined in clause 5.2.12.45. This field performs the same function as the DVB Triplet values <code>original_network_id</code> , <code>transport_stream_id</code> and <code>service_id</code> .	Optional
DVBTriplet	This field, as defined in clause 5.2.12.8, carries the <code>original_network_id</code> , <code>transport_stream_id</code> and <code>service_id</code> .	Optional
ReplacementType	This field carries the value of the <code>linkage_type</code> value, as defined in the <code>linkage_type</code> defined in ETSI EN 300 468 [1]. The default value equates to a service replacement service. Note that only those values of <code>linkage_type</code> that are valid to appear in a linkage descriptor in the SDT are allowed here.	Mandatory

5.2.12.26 RETInfoType

This type is used to signal the presence of unicast RTP retransmission (RET) service and multicast RTP Retransmission service mechanisms, and conveys the parameters needed to use the RET service.

```

<xsd:complexType name="RETInfoType">
  <xsd:sequence>
    <xsd:element name="RTCPReporting" type="dvb:RTCPReportingType" />
    <xsd:element name="UnicastRET" type="dvb:UnicastRETTType" minOccurs="0" />
    <xsd:element name="MulticastRET" type="dvb:MulticastRETTType" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
  
```

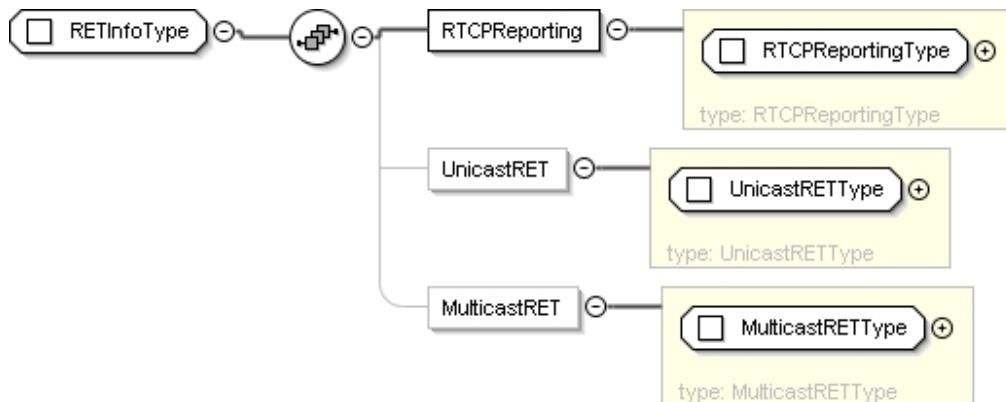


Figure 7be: RETInfoType

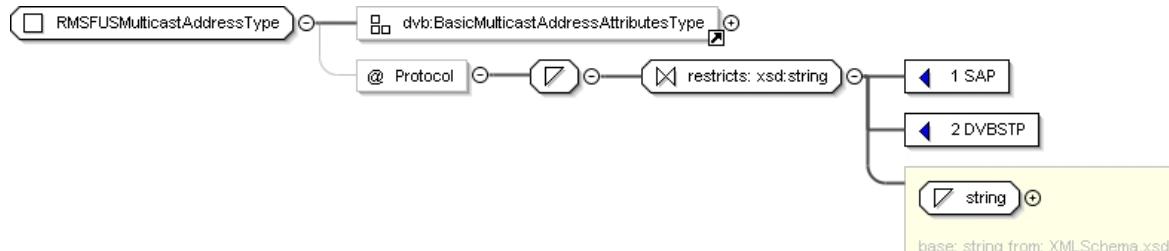
Table 11bh: RETInfoType Fields

Name	Definition	Constraints
RTCPReporting	This element signals the transport addresses and parameters associated with the RTCP reporting for the original multicast RTP session carrying the content associated with the RET service. This is defined in clause 5.2.12.29.	Mandatory
UnicastRET	This element signals presence of a unicast RTP Retransmission (RET) repair service, and the transport addresses and parameters associated with the unicast RET session. It is defined in clause 5.2.12.47	Mandatory
MulticastRET	This element signals the presence of Multicast RTP Retransmission (RET) repair service, and the transport addresses and parameters associated with the Multicast RET session. These parameters are only used if RTP retransmission is enabled and there is a multicast error repair service. It is defined in clause 5.2.12.16.	Only present when multicast RET is used

5.2.12.27 RMSFUSMulticastAddressType

This type defines the combination used to identify the multicast options for a FUS announcement service.

```
<xsd:complexType name="RMSFUSMulticastAddressType">
  <xsd:attributeGroup ref="dvb14:BasicMulticastAddressAttributesType" />
  <xsd:attribute name="Protocol" use="optional">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="1 SAP" />
        <xsd:enumeration value="2 DVBSTP" />
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>
</xsd:complexType>
```

**Figure 7bf: RMSFUSMulticastAddressType****Table 11bi: RMSFUSMulticastAddressType Fields**

Name	Semantic Definition	Constraints
RMSFUSMulticastAddressType	Instantiated using BasicMulticastAddressAttributesType, as specified in clause 5.2.11.1.	Optional
@protocol	Enumerated string, valid values are "1 SDP" and "2 DVBSTP"	Optional

5.2.12.28 RMSType

This is used to carry the description of the remote management server, including the connection location.

```
<xsd:complexType name="RMSType">
  <xsd:sequence>
    <xsd:element name="RMSName" type="dvb:MultilingualType" maxOccurs="unbounded" />
    <xsd:element name="RMSID" type="xsd:decimal" minOccurs="0" />
    <xsd:element name="Description" type="dvb:MultilingualType" minOccurs="0" maxOccurs="unbounded" />
  </xsd:sequence>
  <xsd:attribute name="LogoURI" type="xsd:anyURI" use="optional" />
  <xsd:attribute name="RMSLocation" type="xsd:anyURI" use="required" />
</xsd:complexType>
```

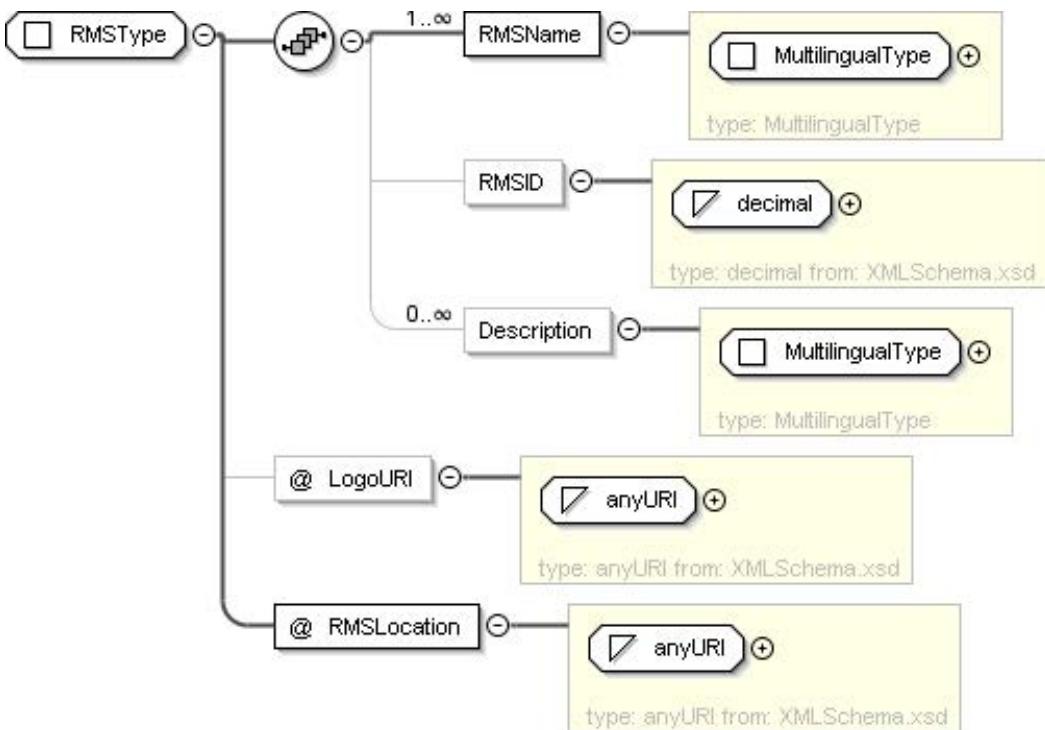


Figure 7bg: RMSType

Table 11bj: RMSType Fields

Name	Semantic Definition	Constraints
RMSName	Multilingual name of RMS, there may be multiple RMSNames for a single RMS. Instantiated using MultilingualType as specified in clause 5.2.12.17.	Mandatory
RMSID	Numeric identifier for the RMS, in decimal form, if present there will be only one value per RMS instance.	Optional
Description	Multilingual description of RMS, there may be multiple descriptions for a single RMS. Instantiated using MultilingualType as specified in clause 5.2.12.17.	Optional
@LogoURI	URI from which logo of RMS may be obtained.	Optional
@RMSLocation	URI to be used to connect to the RMS.	Mandatory

5.2.12.29 RTCPReportingType

This type is used in conjunction with the RET/server-based FCC mechanisms and represents the RTCP reporting parameters. They are common to both multicast RET and unicast RET/FCC implementations.

```

<xsd:complexType name="RTCPReportingType">
    <xsd:attribute name="DestinationAddress" type="xsd:string" use="optional"/>
    <xsd:attribute name="DestinationPort" type="xsd:unsignedShort" use="required"/>
    <xsd:attribute name="dvb-t-ret" type="xsd:positiveInteger" use="optional"/>
    <xsd:attribute name="rtcp-bandwidth" type="xsd:positiveInteger" use="optional"/>
    <xsd:attribute name="rtcp-rsize" type="xsd:positiveInteger" use="optional"/>
    <xsd:attribute name="trr-int" type="xsd:positiveInteger" use="optional"/>
    <xsd:attribute name="dvb-disable-rtcp-rr" type="xsd:boolean" use="optional" default="false"/>
    <xsd:attribute name="dvb-enable-bye" type="xsd:boolean" use="optional" default="false"/>
    <xsd:attribute name="dvb-t-wait-min" type="xsd:unsignedInt" use="optional" default="0"/>
    <xsd:attribute name="dvb-t-wait-max" type="xsd:unsignedInt" use="optional" default="0"/>
    <xsd:attribute name="dvb-ssrc-bitmask" type="dvb:Hexadecimal32bit" use="optional"
default="ffffffff"/>
    <xsd:attribute name="dvb-rsi-mc-ret" type="xsd:boolean" use="optional"/>
    <xsd:attribute name="dvb-ssrc-upstream-client" type="xsd:positiveInteger" use="optional"/>
</xsd:complexType>

```

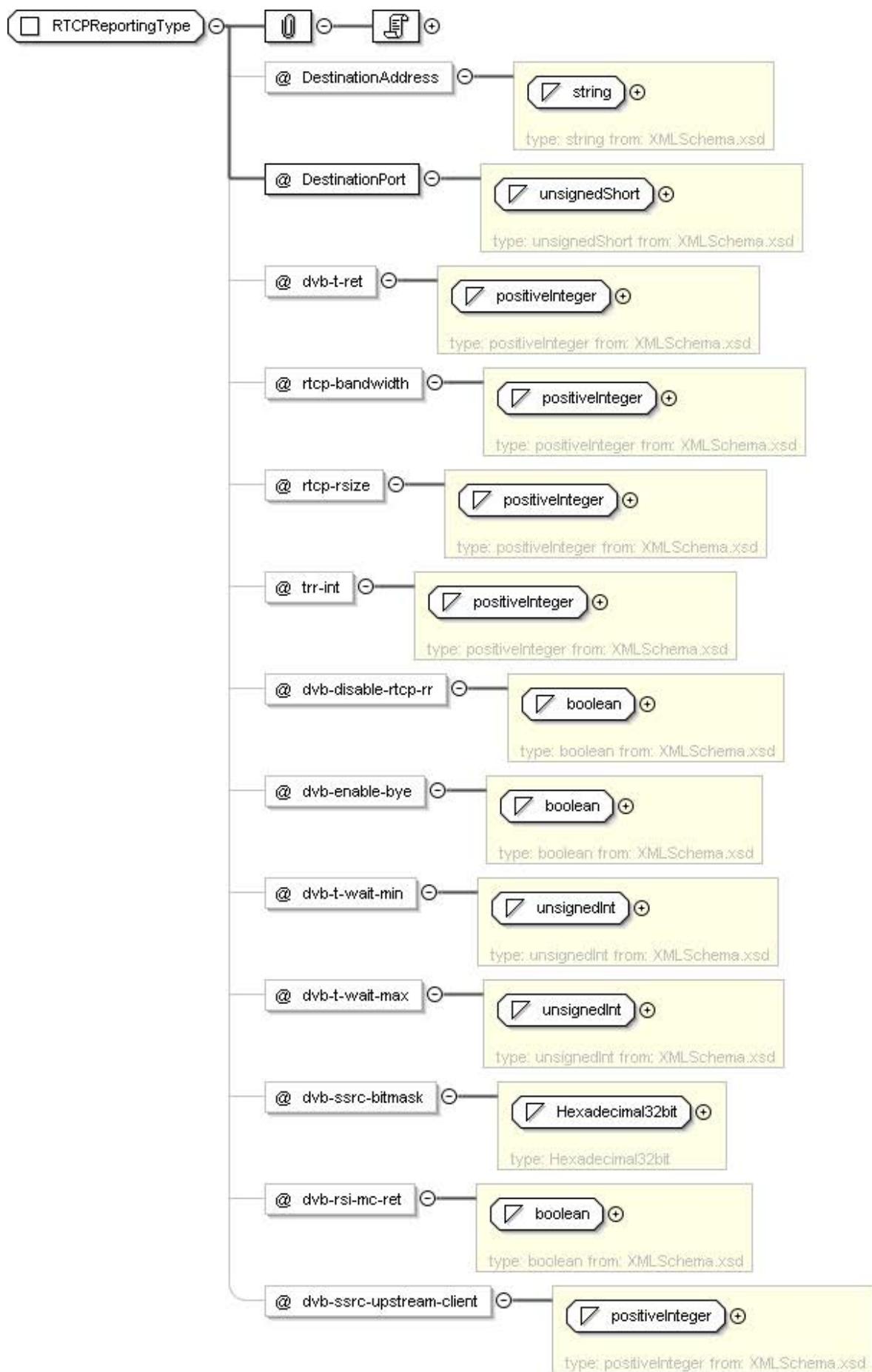


Figure 7bh: RTCPReportingType

Table 11bk: RTCPReportingType Fields

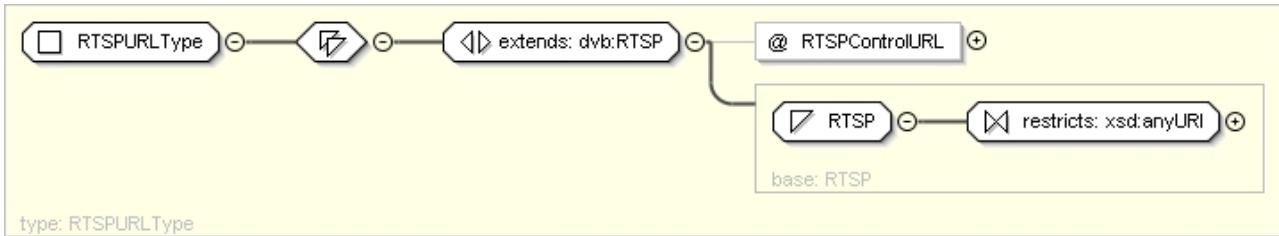
Name	Definition	Constraints
DestinationAddress	List of comma-separated IP addresses (minimum 1 IP address) OR single DNS SRV RR. The IP address selected from this list by the HNED or resolved by the HNED, is the IP address of the FCC/LMB RET server. If more than one IP address is provided, then the client will attempt to connect to each server in turn in the order presented until a successful connection results.	Optional
DestinationPort	UDP Destination Port of RTCP packets issued by the HNED in the primary/original multicast session.	Mandatory
dvb-t-ret	Minimum time a receiver should wait for a requested RET packet (per retransmission request/attempts) before issuing another retransmission request for the same packet(s). This time period has as starting point the sending of the RTCP FB NACK message, and is expressed in milliseconds. If not present, it is up to the HNED to choose an appropriate delay time with which failed retransmissions are re-attempted. This attribute is defined only for RET service.	Optional
rtcp-bandwidth	Amount of bandwidth an RTP receiver may use for its RTCP reporting (kb/s) in the primary/original multicast session. Default is 5 % of RTP stream bandwidth when this attribute is not present.	Optional
rtcp-rsize	Indicates that RTCP FB messages can be transmitted in reduced size format. Default behaviour is that RTCP FB messages are transmitted as compound RTCP reports.	Optional
trr-int	Minimum period for compound RTCP reporting, in milliseconds. Default value is zero when this attribute is not present.	Optional
dvb-disable-rtcp-rr	Is present when the HNED shall disable RTCP RR reporting. Default RTCP RR is enabled when this attribute is not present, i.e. the default value of this field is "false".	Optional
dvb-enable-bye	When present, the HNED shall issue BYE following rules as described in annex F. Default BYE usage is disabled when this attribute is not present.	Optional
dvb-t-wait-min	Upon packet loss detection, the HNED shall issue an RTCP FB NACK message in an interval randomly chosen between dvb-t-wait-min and dvb-t-wait-max (both expressed in ms). Default value for dvb-t-wait-min is 0 ms. This attribute is defined only for RET service.	Optional
dvb-t-wait-max	Upon packet loss detection, the HNED shall issue an RTCP FB NACK message in an interval randomly chosen between dvb-t-wait-min and dvb-t-wait-max (both expressed in ms). Default value for dvb-t-wait-max is 0 ms. This attribute is defined only for RET service.	Optional
dvb-ssrc-bitmask	Contains a 32-bit wide bitmask. Those HNEDs for which their SSRC match the SSRC inside the original MC streams on the bit positions that are set to 1 in the bitmask, shall set both dvb-t-wait-min and dvb-t-wait-max to zero, overruling the signalled values dvb-t-wait-min and dvb-t-wait-max. Default all bit positions in the bitmask are 1, meaning that the dvb-t-wait-min and dvb-t-wait-max are not overruled. This attribute is defined only for RET service.	Optional
dvb-rsi-mc-ret	Signals that the RSI packets of the original MC RTP session are distributed in the MC RET session.	Optional
dvb-ssrc-upstream-client	SSRC of upstream client for which LMB server translates RTCP FB message into RTCP FF message.	Optional

5.2.12.30 RTSPURLType

This type is used to allow an additional RTSP Control URL to be carried, as discussed in clauses 5 and 6, to assist with AL-FEC and/or RET services.

```

<xsd:complexType name="RTSPURLType">
  <xsd:simpleContent>
    <xsd:extension base="dvb:RTSP">
      <xsd:attribute name="RTSPControlURL" type="xsd:anyURI" use="optional"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
```

**Figure 7bi: RTSPURLType****Table 11bl: RTSPURLType Fields**

Name	Definition	Constraints
RTSPURLType (contents of extended type)	This carries the URL at which the service description may be accessed. When the service is composed of a single stream, this URL is used for all RTSP messages (SETUP, PLAY, TEARDOWN, etc) for controlling that stream. The format is as defined in clause 5.2.10.	Mandatory when the SP wants to use RTSP
RTSPControlURL	The URL that is used for SETUP, PLAY, PAUSE, and other control of the main audio-video stream, when AL-FEC and/or RET is used for that main audio-video stream. See clause 6.1.1.	Optional, but mandatory where RTSP used with RET or FEC

5.2.12.31 ServerBasedEnhancementServiceInfoType

This type is used to signal the presence of a server-based enhancement service, and conveys the parameters needed to use this service. The possible services are RET and Server-based FCC.

```

<xsd:complexType name="ServerBasedEnhancementServiceInfoType">
  <xsd:sequence>
    <xsd:element name="EnhancementService" type="dvb12:EnhancementServiceType" />
    <xsd:element name="RTCPReporting" type="dvb:RTCPReportingType" />
    <xsd:element name="Retransmission_session" type="dvb:UnicastRETTType" minOccurs="0" />
    <xsd:element name="MulticastRET" type="dvb:MulticastRETTType" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
  
```

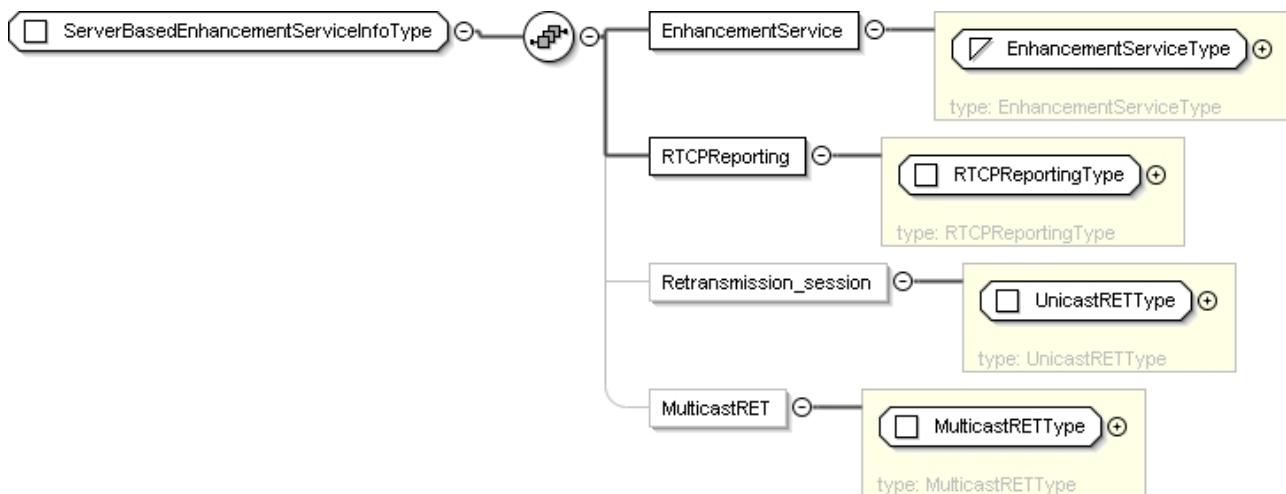
**Figure 7bj: ServerBasedEnhancementServiceInfoType**

Table 11bm: ServerBasedEnhancementServiceInfoType Fields

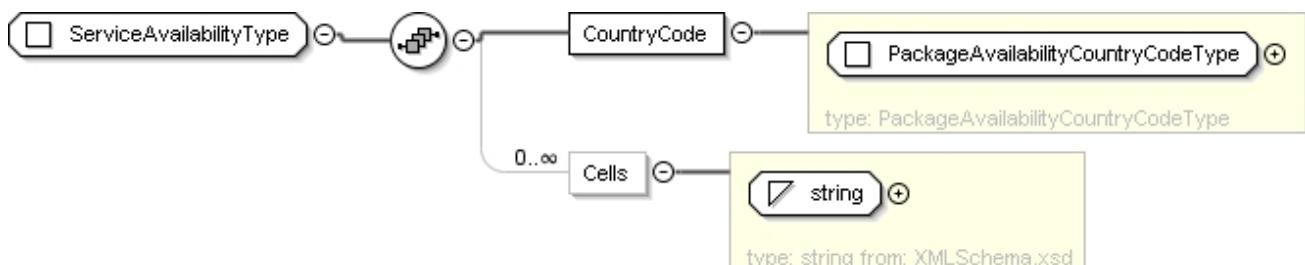
Name	Definition	Constraints
EnhancementService	Signals whether RET and/or FCC service is offered. This is defined in clause 5.2.10.	Mandatory
RTCPReporting	This element signals the transport addresses and parameters associated with the RTCP reporting for the original multicast RTP session. This is defined in clause 5.2.12.29.	Mandatory
Retransmission session	This element signals the transport addresses and parameters associated with the unicast retransmission session for the enhancement service. It is defined in clause 5.2.12.47.	Mandatory
MulticastRET	This element signals the presence of Multicast RTP Retransmission (RET) repair service, and the transport addresses and parameters associated with the Multicast RET session. These parameters are only used if RTP retransmission is enabled and there is a multicast error repair service. It is defined in clause 5.2.12.16.	Only present when multicast RET is used

5.2.12.32 ServiceAvailabilityType

This element provides support for Regionalization. It allows each service to have a list of 'cells' (regions) with which the service is associated. By default, all the single services are available everywhere. For more details on the use and initialization of the ServiceAvailability values, see clause 5.2.13.8.

There shall be at most one ServiceAvailability element for each CountryCode.

```
<xsd:complexType name="ServiceAvailabilityType">
    <xsd:sequence>
        <xsd:element name="CountryCode" type="dvb:PackageAvailabilityCountryCodeType" />
        <xsd:element name="Cells" type="xsd:string" minOccurs="0" maxOccurs="unbounded" />
    </xsd:sequence>
</xsd:complexType>
```

**Figure 7bk: ServiceAvailabilityType****Table 11bn: Service Availability Fields**

Name	Definition	Constraints
CountryCode	This element indicates the country for which the availability is being defined. The structure of this element is defined in clause 5.2.12.20.	Mandatory
Cells	A list of string identifiers representing geographical regions in the country identified by CountryCode. The Cells listed represent the exception to the value supplied by the flag, i.e. the negation of the Availability flag applies to any listed cells.	Optional

5.2.12.33 ServiceLocation

This describes the location(s) at which a service may be found, either a broadcast source or an IP source, but not both. In the case of an IP source, the location shall be either a multicast location or via an RTSP server, or both. At least one of the IPMulticastAddress, RTSPURL or Broadcast shall be present.

```
<xsd:complexType name="ServiceLocation">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">The location of a service. Currently this supports either a broadcast system identifier or a multicast address (ASM and SSM) or RTSP.</xsd:documentation>
  </xsd:annotation>
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="BroadcastSystem" type="dvb12:BroadcastSystemType" />
    <xsd:element name="IPMulticastAddress" type="dvb14:McastType" />
    <xsd:element name="RTSPURL" type="dvb:RTSPURLType" />
  </xsd:choice>
</xsd:complexType>
```

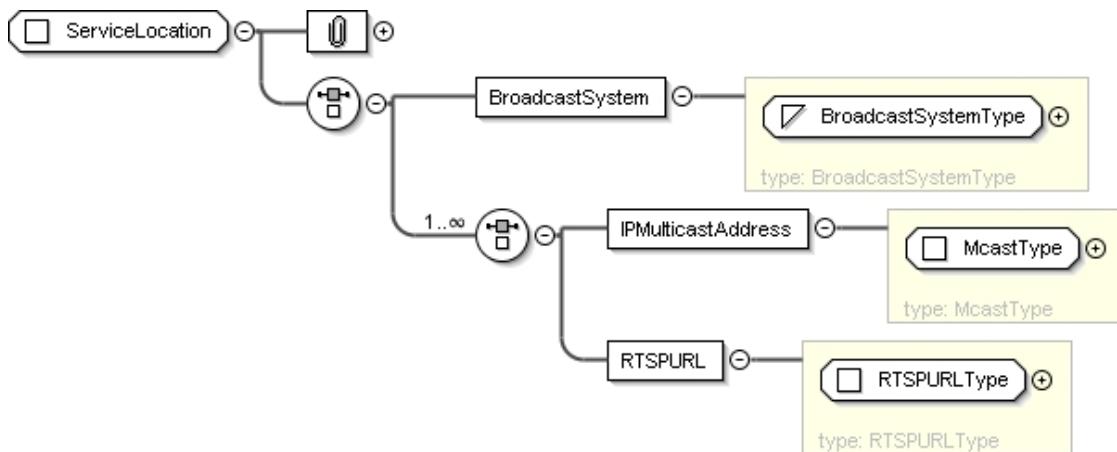


Figure 7bl: ServiceLocation

Table 11bo: Service Location Fields

Name	Definition	Constraints
BroadcastSystem	Identifies the broadcast delivery system where this service is being broadcast.	Optional
IPMulticastAddress	Provides the multicast transport address and other parameters at which the service may be accessed. This type is described in clause 5.2.12.14. As appropriate this type includes the details of FEC and RET, if available for the service.	Optional
RTSPURL	Signals the use of RTSP to access the service and provides the URL at which the service description may be accessed. This type is described in clause 5.2.12.30.	Optional

5.2.12.34 SI

This type describes the service information traditionally provided in a stream as DVB descriptors.

```
<xsd:complexType name="SI">
  <xsd:sequence>
    <xsd:element name="Name" type="dvb:MultilingualType" maxOccurs="unbounded" />
    <xsd:element name="Description" type="dvb:MultilingualType" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="ServiceDescriptionLocation" type="dvb:DescriptionLocationBCG" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="ContentGenre" type="dvb:Genre" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="CountryAvailability" type="dvb:CountryAvailability" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="ReplacementService" type="dvb:ReplacementService" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="MosaicDescription" type="dvb:MosaicDescription" minOccurs="0" />
    <xsd:element name="AnnouncementSupport" type="dvb:AnnouncementSupport" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

```

</xsd:sequence>
<xsd:attribute name="ServiceType" type="dvb:ServiceType" use="required"/>
<xsd:attribute name="PrimarySISource" type="dvb:PrimarySISource" use="optional" default="XML"/>
</xsd:complexType>

```

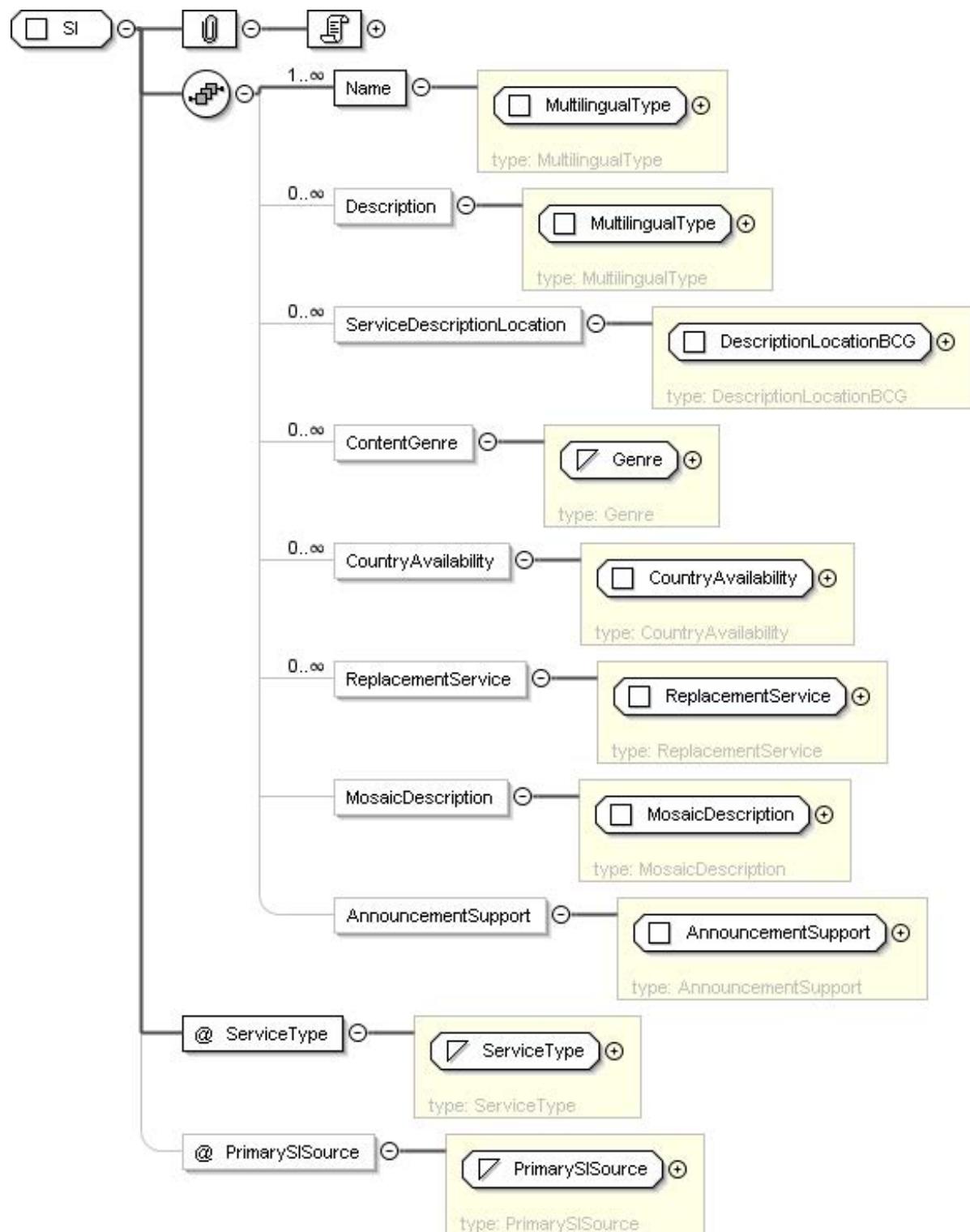


Figure 7bm: SI

Table 11bp: SI Fields

Name	Definition	Constraints
Name	The text form of the name by which the service is known to the user. This type is described in clause 5.2.12.17.	Mandatory
Description	A textual description of the service. This type is described in clause 5.2.12.17.	Optional
ContentGenre	The (primary) genre of the service. This type is described in clause 5.2.10	Optional
CountryAvailability	The list of countries in which the service is, or is not, available. This type is described in clause 5.2.12.5.	Optional
AnnouncementSupport	The announcements supported by the service, and linkage information as to their location. This type is described in clause 5.2.12.1.	Optional
ReplacementService	Details the linkage to a service that can be used in case of a failure of the service to which this SI record refers. This type is described in clause 5.2.12.25.	Optional
MosaicDescription	Details of the services, or service packages, which are displayed in a mosaic stream. This type is described in clause 5.2.12.15.	Optional
ServiceDescriptionLocation	The identifier(s) of the BCG Record(s) for the BCG Discovery element that carries the information on this offering. This type is described in clause 5.2.12.6.	Optional
@ServiceType	An attribute that is an eight-bit number encoding the type of the service, using traditional DVB values. This type is described in clause 5.2.10.	Mandatory
@PrimarySISource	An attribute indicating whether the XML record, or SI in the transport stream takes precedence. This type is described in clause 5.2.10.	Optional

5.2.12.35 SRMAnnouncementModeType

This type is used to convey details of either SAP or HTTP delivery of SRM Announcement Services. Further details on the use of this information are provided in clauses 5.2.13.9 and 12.

```
<xsd:complexType name="SRMAnnouncementModeType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">SAP or HTTP delivery of SRM Announcement Services</xsd:documentation>
  </xsd:annotation>
  <xsd:choice>
    <xsd:element name="SAP" type="dvb14:SRMAnnouncementModeSAPType" />
    <xsd:element name="HTTP" type="xsd:anyURI" />
  </xsd:choice>
</xsd:complexType>
```

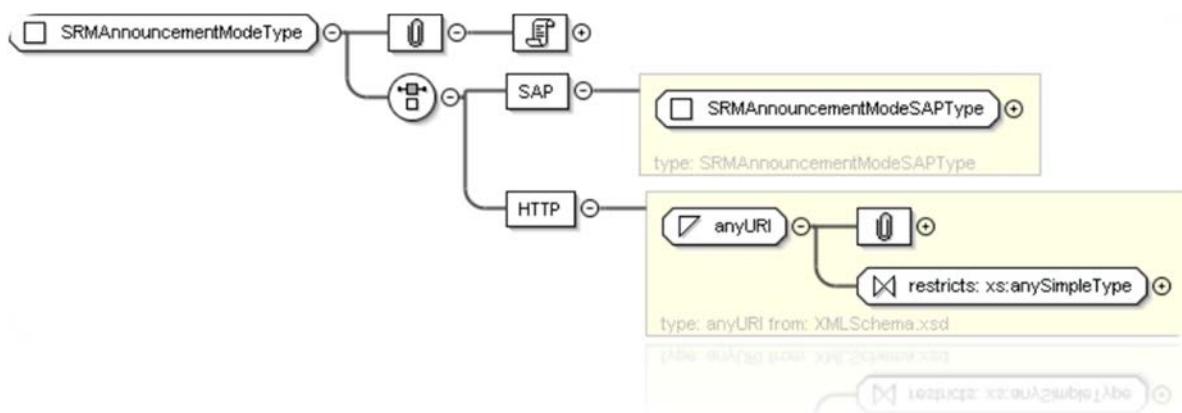
**Figure 7bn: SRMAnnouncementModeType**

Table 11bq: SRMAnnouncementModeType Fields

Name	Definition	Constraints
SAP	The details of the SAP address where the SRM announcement service can be found. This type is defined in clause 5.2.12.36.	Either SAP or HTTP shall be present
HTTP	File URI for unicast HTTP delivery.	Either SAP or HTTP shall be present

5.2.12.36 SRMAnnouncementModeSAPType

This type is used to carry and define the SAP address where details of the SRM announcement service can be found.

```
<xsd:complexType name="SRMAnnouncementModeSAPType">
  <xsd:attributeGroup ref="dvb14:BasicMulticastAddressAttributesType" />
</xsd:complexType>
```

**Figure 7bo: SRMAnnouncementModeSAPType****Table 11br: SRMAnnouncementModeSAPType Fields**

Name	Definition	Constraints
BasicMulticastAddressAttributesType (attribute group)	The details of the SAP address where the SRM announcement service is described.	Mandatory

5.2.12.37 SRMAnnouncementServiceType

This type provides the SRM Announcement Service information.

```
<xsd:complexType name="SRMAnnouncementServiceType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">SRM Announcement Service information</xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="SRMID" type="dvb12:SRMIDType" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="SRMAnnouncementMode" type="dvb14:SRMAnnouncementModeType" />
  </xsd:sequence>
  <xsd:attribute name="AnnouncementServiceVersion" type="dvb:Version" use="optional" />
</xsd:complexType>
```

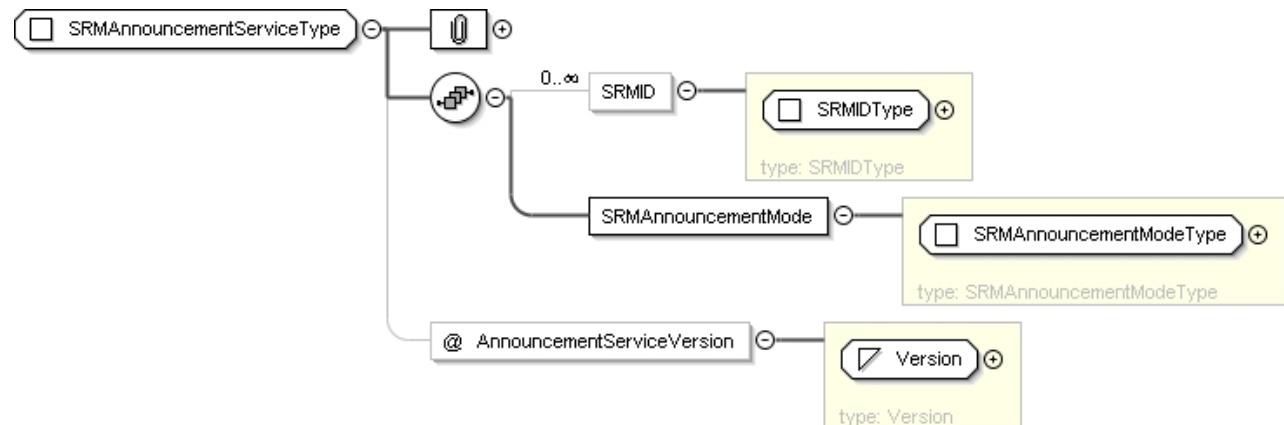
**Figure 7bp: SRMAnnouncementServiceType**

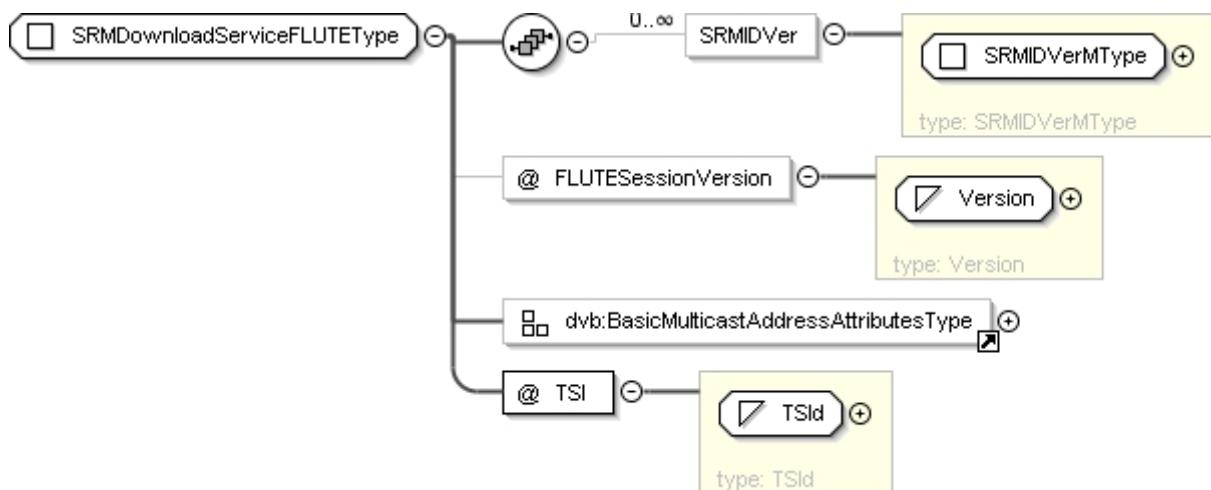
Table 11bs: SRMAnnouncementServiceType Fields

Name	Definition	Constraints
SRMID	The SRM IDs of the service this type announces. There is one SRMID element for each SRM supported by this announcement service. Thus this element builds a list of SRM IDs in this type.	Optional
SRMAnnouncementMode	Information on how to access the SRM Announcement Service.	Mandatory
AnnouncementServiceVersion	Version of the SRM Announcement Service (see clause 12.6.4).	Optional for SRM multicast announcement service and Mandatory for SRM unicast announcement service. See clause 12.6.4

5.2.12.38 SRMDownloadServiceFLUTEType

This type carries the details of the FLUTE download of the SRM files

```
<xsd:complexType name="SRMDownloadServiceFLUTEType">
  <xsd:sequence>
    <xsd:element name="SRMIDVer" type="dvb12:SRMIDVerMType" minOccurs="0"
maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="FLUTESessionVersion" type="dvb:Version"/>
  <xsd:attributeGroup ref="dvb14:BasicMulticastAddressAttributesType" />
  <xsd:attribute name="TSI" type="dvb:TSId" use="required"/>
</xsd:complexType>
```

**Figure 7bq: SRMDownloadServiceFLUTEType****Table 11bt: SRMDownloadServiceFLUTEType Fields**

Name	Definition	Constraints
SRMIDVer	A List of SRM IDs and SRM file version numbers of SRMs supported by this FLUTE Download Service, as defined in clause 5.2.12.42.	Optional
FLUTESessionVersion	FLUTE session version (see clause 12.6.2).	Optional
BasicMulticastAddressAttributes group	The address of the FLUTE Multicast channel, as specified in clause 5.2.11.1.	Mandatory
TSI	Transport Session Indicator of the FLUTE session.	Mandatory

5.2.12.39 SRMDownloadServiceHTTPType

This type carries the details of the HTTP download of SRM files.

```
<xsd:complexType name="SRMDownloadServiceHTTPType">
  <xsd:sequence>
    <xsd:element name="SRMIDVer" type="dvb12:SRMIDVerUType"/>
  </xsd:sequence>
  <xsd:attribute name="Location" type="xsd:anyURI" use="required"/>
</xsd:complexType>
```

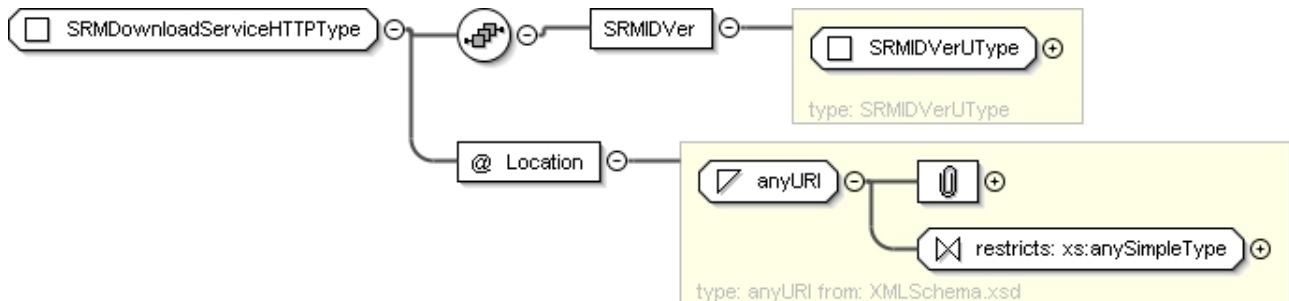


Figure 7br: SRMDownloadServiceHTTPType

Table 11bu: SRMDownloadServiceHTTPType Fields

Name	Definition	Constraints
SRMIDVer	SRM ID and SRM file version of SRM supported by the HTTP Download service, as defined in clause 5.2.12.43.	Mandatory
Location	File URI for unicast HTTP download.	Mandatory

5.2.12.40 SRMDownloadServiceType

This type carries the details of the SRM Download Service information, which shall be either FLUTE or HTTP, but not both.

```
<xsd:complexType name="SRMDownloadServiceType">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">FLUTE or HTTP download of SRM files</xsd:documentation>
  </xsd:annotation>
  <xsd:choice>
    <xsd:element name="FLUTE" type="dvb14:SRMDownloadServiceFLUTEType"/>
    <xsd:element name="HTTP" type="dvb12:SRMDownloadServiceHTTPType"/>
  </xsd:choice>
</xsd:complexType>
```

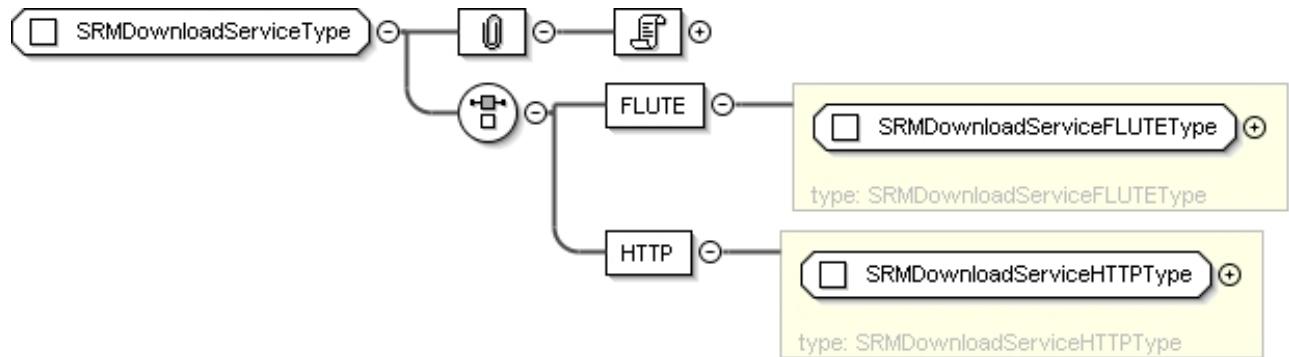


Figure 7bs: SRMDownloadServiceType

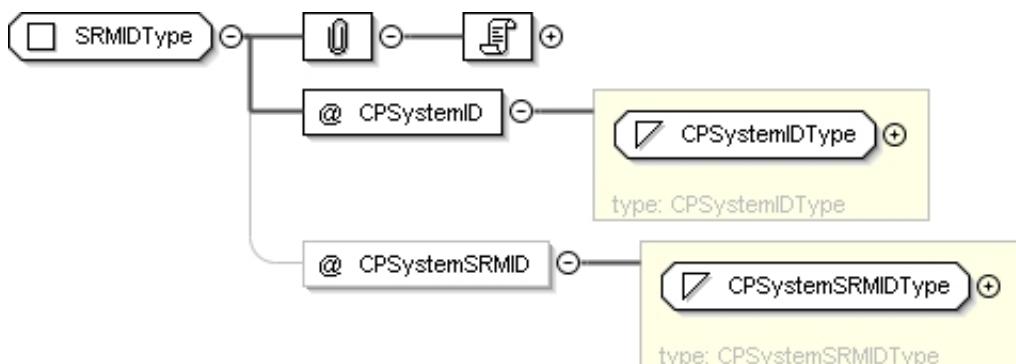
Table 11bv: SRMDownloadServiceType Fields

Name	Definition	Constraints
FLUTE	FLUTE download service information	Optional, but exactly one FLUTE or one HTTP shall be present
HTTP	HTTP download service information	Optional, but exactly one FLUTE or one HTTP shall be present

5.2.12.41 SRMIDType

This type carries the CP System and optional CP System SRM ID for a SRM.

```
<xsd:complexType name="SRMIDType">
  <xsd:annotation>
    <xsd:documentation>SRM specific ID (CP System ID, CP System SRM ID)</xsd:documentation>
  </xsd:annotation>
  <xsd:attribute name="CPSystemID" type="dvb12:CPSystemIDType" use="required"/>
  <xsd:attribute name="CPSystemSRMID" type="dvb12:CPSystemSRMIDType" use="optional" />
</xsd:complexType>
```

**Figure 7bt: SRMIDType****Table 11bw: SRMIDType Fields**

Name	Definition	Constraints
CPSystemID	This is the ID of the CP system (see definition of type in clause 5.2.10, and discussion in clause 5.2.13.9).	Mandatory
CPSystemSRMID	This is the ID for the SRM within the CP system (see definition in clause 5.2.10, and discussion in clause 5.2.13.9).	Optional

5.2.12.42 SRMIDVerMType

This type provides the CP System, optional CP System SRM ID and SRM file version number for a SRM, as used for FLUTE (or multicast) delivery. This extends the type SRMIDType defined in clause 5.2.12.41.

```
<xsd:complexType name="SRMIDVerMType">
  <xsd:annotation>
    <xsd:documentation>SRM ID and optional SRM file version</xsd:documentation>
  </xsd:annotation>
  <xsd:complexContent>
    <xsd:extension base="dvh12:SRMIDType">
      <xsd:attribute name="SRMFileVersion" type="dvh:Version" use="optional" />
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
```

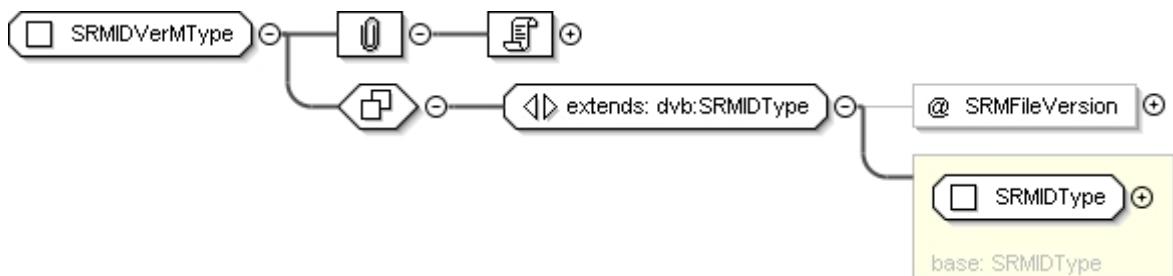


Figure 7bu: SRMIDVerMType

Table 11bx: SRMIDVerMType Fields

Name	Definition	Constraints
SRMFileVersion	SRM File version number. See discussion in clause 5.2.13.9.	Optional

5.2.12.43 SRMIDVerUType

This type provides the CP System, SRM File version number and optional CP System SRM ID for a SRM, as used for HTTP (or unicast) delivery.

```

<xsd:complexType name="SRMIDVerUType">
  <xsd:annotation>
    <xsd:documentation>SRM ID and SRM file version</xsd:documentation>
  </xsd:annotation>
  <xsd:complexContent>
    <xsd:extension base="dvb12:SRMIDType">
      <xsd:attribute name="SRMFileVersion" type="dvb:Version" use="required"/>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
  
```

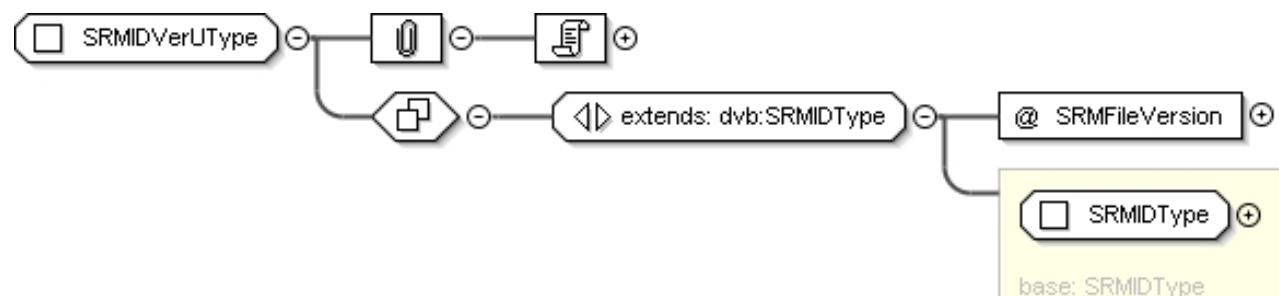


Figure 7bv: SRMIDVerUType

Table 11by: SRMIDVerUType Fields

Name	Definition	Constraints
SRMFileVersion	SRM File version number. See discussion in clause 5.2.13.9.	Mandatory

5.2.12.44 TargetPackageType

Segments may be used for delivery efficiency. However, this means that a receiver has to receive all the information to construct channel map regardless of package preference. By the use of the TargetPackage, a hierarchical architecture to build package and broadcast discovery record for delivery is enabled. This hierarchical architecture is achieved by adding a Package Attribute to each segment in the Service Provider Discovery Record. Receiver can use this Package information to filter segments contained in multicast stream or request only the desirable segments in unicast manner according to the preference of package. By doing so, receiver can generate channel map according to the preference of package without getting all the information. Receivers complying with earlier versions of the present document will ignore the newly added TargetPackage element, introduced in a backward-compatible manner.

The TargetPackage includes the PackageIDRef attribute and an optional PackageType element. The PackageIDRef contains the identifier of the Package Record referencing the Package Discovery element to which the information of the containing segments belongs to. The PackageType element contains a textual description of the package that may for example be used by an application to describe the package to the user or the HNED can use this information to filter segments according to their package preference.

```
<xsd:complexType name="TargetPackageType">
  <xsd:sequence>
    <xsd:element name="PackageType" type="dvb:MultilingualType" minOccurs="0"
maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="PackageIDRef" type="dvb:Hexadecimal16bit" use="required"/>
</xsd:complexType>
```

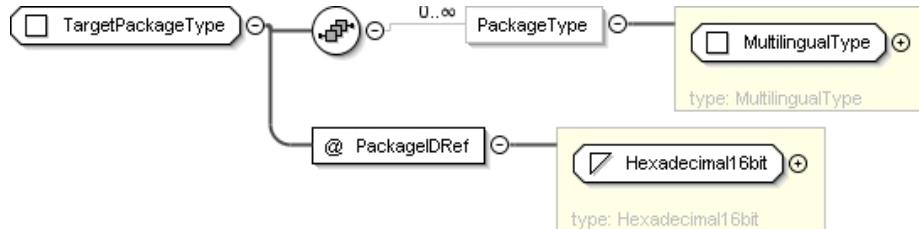


Figure 7bw: TargetPackageType

Table 11bz: TargetPackageType Fields

Name	Definition	Constraints
PackageIDRef (attribute of TargetPackage)	Contains the identifier of the Package Record referencing the Package Discovery element to which the information of this segment belongs.	Mandatory
PackageType	Description of the Target Package which can, for example, be used for filtering the segments or for description of the package.	Optional

5.2.12.45 TextualIdentifier

This type is used to identify a service in a textual fashion. This identifier is comprised of the domain name of the service provider and the textual service name. The domain name may be omitted where it can be inferred from the context. The Textual Identifier is the means of uniquely identifying an IP service.

This is an implementation of the textual service identifier, as specified in ETSI TS 101 812 [3], clause 14.9.1.

```
<xsd:complexType name="TextualIdentifier">
  <xsd:attribute name="DomainName" type="dvb:DomainType" use="optional"/>
  <xsd:attribute name="ServiceName" type="dvb:Service" use="required"/>
</xsd:complexType>
```

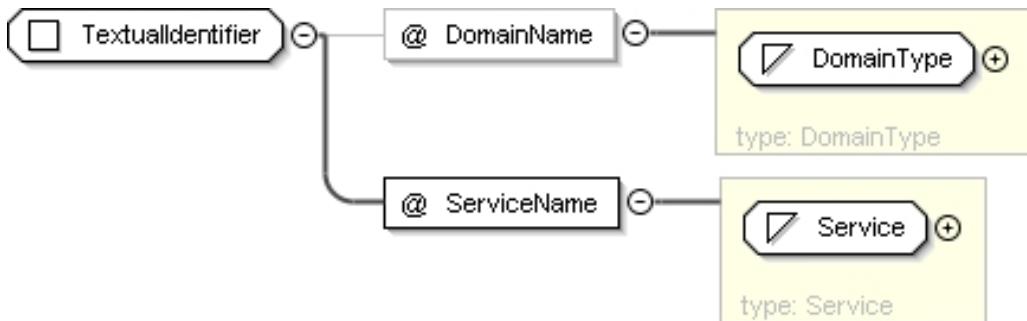


Figure 7bx: TextualIdentifier

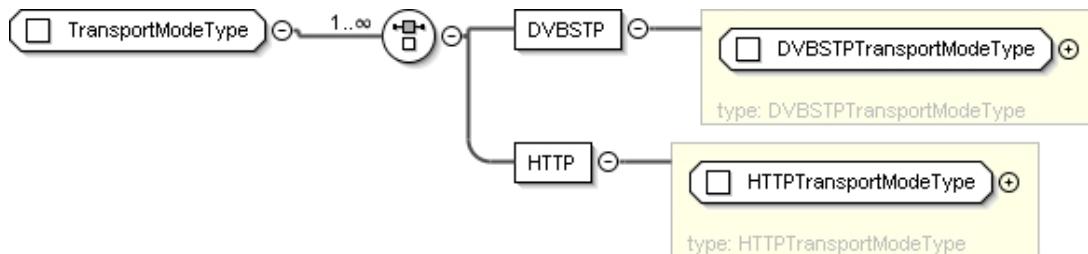
Table 11ca: TextualIdentifier Fields

Name	Definition	Constraints
DomainName	An internet DNS domain name registered by the SP that uniquely identifies the SP. If this is not present, then the DNS domain name from the DVB-IPTV Offering record is used. This type is described in clause 5.2.10.	Optional
ServiceName	A unique host name for the service within the SP's domain. This type is described in clause 5.2.10.	Mandatory

5.2.12.46 TransportModeType

This type is used to indicate the location and mechanism used to carry BCG information, and the payloadIds and segmentIds of the relevant information. At least one of the DVBSTP or HTTP fields shall be present, and both can be present in multiple times where the information is available through multiple locations.

```
<xsd:complexType name="TransportModeType">
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="DVBSTP" type="dvb14:DVBSTPTransportModeType" />
    <xsd:element name="HTTP" type="dvb14:HTTPTransportModeType" />
  </xsd:choice>
</xsd:complexType>
```

**Figure 7by: TransportModeType****Table 11cb: TransportModeType Fields**

Name	Definition	Constraints
DVBSTP	This indicates that the BCG information is available via multicast using the DVBSTP protocol defined in the present document, and carries the relevant multicast address(es) and the segments used for this information. This type is described in clause 5.2.12.7.	Optional
HTTP	This indicates that the BCG information is available via HTTP (either SOAP or segment download), and specifies the location(s) at which it is available. This type is described in clause 5.2.12.13.	Optional

5.2.12.47 UnicastRETTType

This types provides the basic attributes needed for unicast RET and server-based FCC, and includes the CommonCastRETT type to provide a range of optional data, defined in clause 5.2.11.2.

```
<xsd:complexType name="UnicastRETTType">
  <xsd:attribute name="trr-int" type="xsd:unsignedInt" use="optional" />
  <xsd:attribute name="DestinationPort-ForRTCPReporting" type="xsd:unsignedInt" use="optional" />
  <xsd:attribute name="SourceAddress" type="xsd:string" use="optional" />
  <xsd:attribute name="SourcePort" type="xsd:unsignedInt" use="optional" />
  <xsd:attribute name="RTSPControlURL" type="xsd:anyURI" use="optional" />
  <xsd:attributeGroup ref="dvb:CommonCastRETTType" />
</xsd:complexType>
```

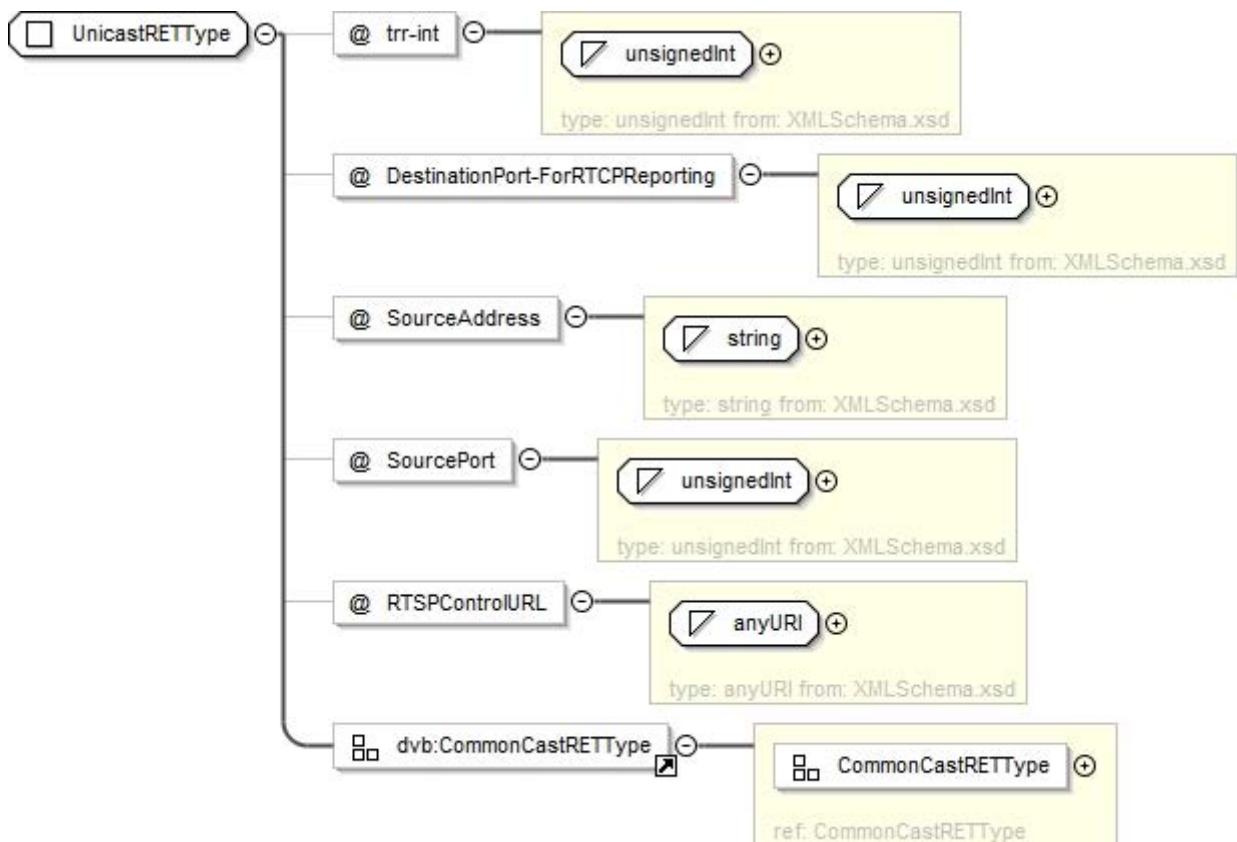


Figure 7bz: UnicastRETTType

Table 11cc: UnicastRETTType Attributes

Name	Definition	Constraints
<code>trr-int</code>	Minimum period for compound retransmission session RTCP reporting, in ms. Default value is zero when attribute is not present.	Optional
<code>DestinationPort-ForRTCPReporting</code>	The UDP destination port of RTCP packets issued by the HNED in the RTP retransmission session. If this attribute is not present, then RTCP RR on the RTP retransmission stream shall be disabled by the HNED.	Optional
<code>SourceAddress</code>	Source IP address of RET packets. If not present, the RET packets are SSRC multiplexed with the original RTP stream. This attribute is only defined for the unicast RET service for CoD service or LMB with trick mode service.	Optional
<code>SourcePort</code>	The UDP Source Port of unicast RTP retransmission session packets. If not present, the port number in these packets shall match the <code>DestinationPort</code> field in the RTCP Reporting element.	Optional
<code>RTSPControlURL</code>	The RTSP URL to be used for controlling the unicast RTP retransmission stream.	Optional
<code>CommonCastRETTType</code> (<i>included attributeGroup</i>)	This attribute group is defined in clause 5.2.11.2, and carries the common unicast RET/FCC and multicast RET attributes.	Mandatory

5.2.12.47a URILinkage

The `URILinkage` type is used to carry the equivalent of the `URI_linkage` descriptor defined in ETSI EN 300 468 [1]. The fields in this type are direct matches to the fields in the descriptor, and the semantics of that descriptor apply here.

```

<xsd:complexType name="URILinkageType">
    <xsd:sequence>
        <xsd:element name="UriLinkageType" type="dvb:Hexadecimal8bit"/>
        <xsd:element name="URI" type="xsd:anyURI"/>
        <xsd:element name="MinPollingInterval" type="xsd:unsignedShort" minOccurs="0"/>
        <xsd:element name="PrivateDataBytes" type="xsd:base64Binary"/>
    </xsd:sequence>
</xsd:complexType>
  
```

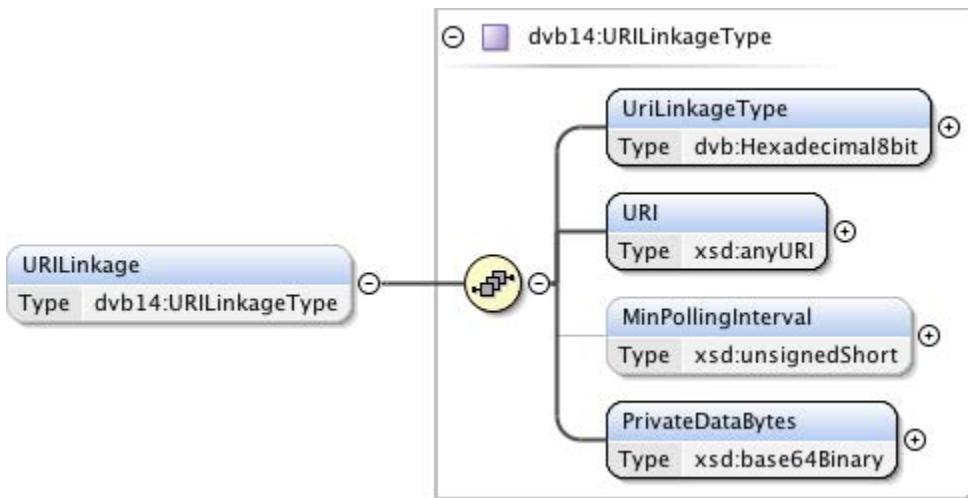


Figure 7bza: URILinkageType

Table 11cca: URILinkageType Fields

Name	Definition	Constraints
URILinkageType	The linkage type as defined for the field named uri_linkage_type in the URI_linkage_descriptor in ETSI EN 300 468 [1].	Mandatory
URI	The concatenated uri_char values as defined in the URI_linkage_descriptor.	Optional
MinPollingInterval	The min_polling_field from the URI_linkage_type in ETSI EN 300 468 [1].	Optional
PrivateDataBytes	The private data bytes from the URI_linkage_type concatenated in the order they occur in the descriptor in ETSI EN 300 468 [1]. Each 8-bit value represented as a two hexadecimal digits.	Optional

5.2.12.48 PackageTextualIdentifier

This type is used to identify a service in a textual fashion. This is an extension of the TextualIdentifier type. This type is only meant to be used in the PackageService context.

```

<xs:complexType name="PackageTextualIdentifier">
    <xs:complexContent>
        <xs:extension base="dvb:TextualIdentifier">
            <xsd:attribute name="Priority" type="xsd:positiveInteger" use="optional"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

```

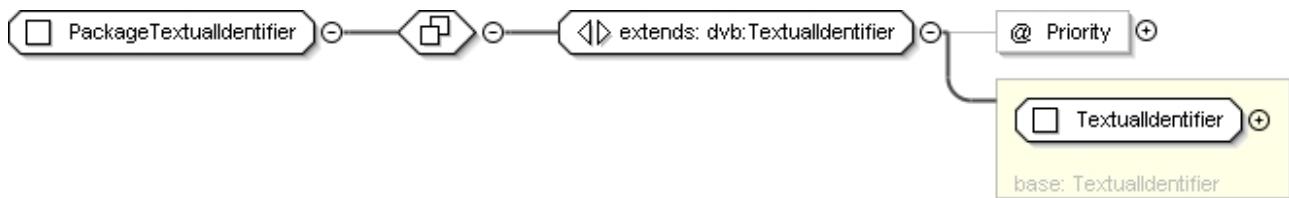


Figure 7ca: PackageTextualIdentifier

Table 11cd: PackageTextualIdentifier Fields

Name	Definition	Constraints
TextualIdentifier	Uses TextualIdentifier as a base, TextualIdentifier type is defined in clause 5.2.12.45.	Mandatory
Priority	This attribute defines a priority where multiple PackageTextualIdentifier are used in a single PackageService. The PackageTextualIdentifier with the lowest Priority value has the highest priority. This may be used by the HNED to select the service to use for this package service.	Optional

5.2.13 XML Main Types

5.2.13.0 Introduction

This clause defines the main XML types that are used for the records carried by the transport mechanisms described in clause 5.4.

All of the following types extend the OfferingBase type defined in clause 5.2.12.18. As such, the tables below do not define OfferingBase in the list of semantic meanings of the elements and attributes, but the definition is implied through the presence of the OfferingBase type in the XML type definitions below.

5.2.13.1 Broadband Content Guide Record: BCGOffering

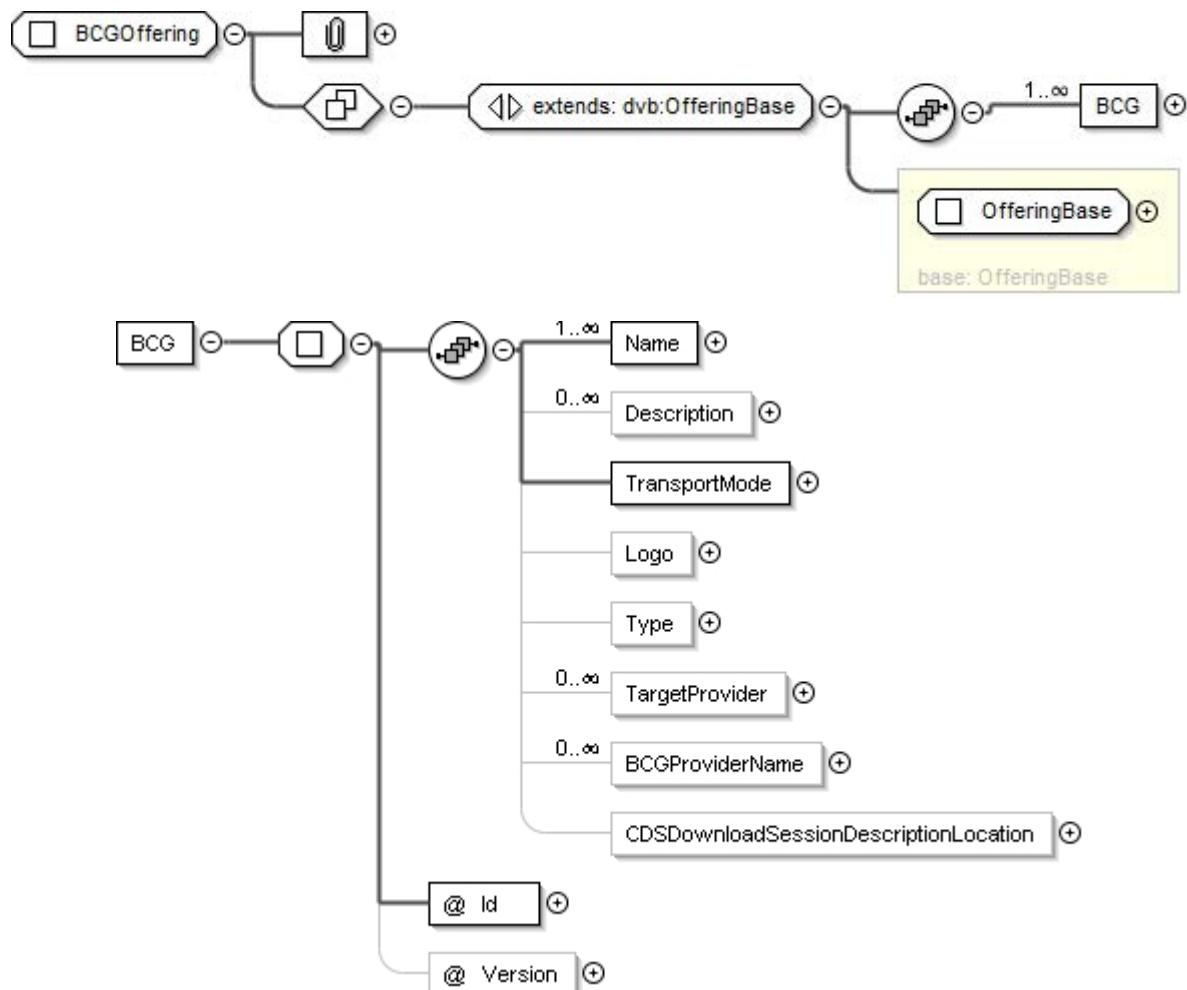
The Broadband Content Guide Record provides a means to discover the locations of guides listing the content that is available, either live (e.g. through a Broadcast Offering) or via CoD or via CDSs. A provider discovered through this shall offer a service as described in ETSI TS 102 539 [62].

For CDSs the location of download session descriptions distributed via multicast can be provided. This allows a HNED to cache the download session descriptions distributed via multicast (see clause 10.4.2).

This element is used to discover these Broadcast Content Guide (BCG) Offerings.

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 6.

```
<xsd:complexType name="BCGOffering">
  <xsd:complexContent>
    <xsd:extension base="dvb:OfferingBase">
      <xsd:sequence>
        <xsd:element name="BCG" maxOccurs="unbounded">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element name="Name" type="dvb:MultilingualType"
maxOccurs="unbounded"/>
              <xsd:element name="Description" type="dvb:MultilingualType"
minOccurs="0" maxOccurs="unbounded"/>
              <xsd:element name="TransportMode" type="dvb14:TransportModeType"/>
              <xsd:element name="Logo" type="xsd:anyURI" minOccurs="0"/>
              <xsd:element name="Type" type="tva:ControlledTermType" minOccurs="0"/>
              <xsd:element name="TargetProvider" type="dvb:DomainType" minOccurs="0"
maxOccurs="unbounded"/>
              <xsd:element name="BCGProviderName" type="dvb:MultilingualType"
minOccurs="0" maxOccurs="unbounded"/>
              <xsd:element name="CDSDownloadSessionDescriptionLocation"
type="dvb14:CDSDownloadSessionDescriptionLocationType" minOccurs="0"/>
            </xsd:sequence>
            <xsd:attribute name="Id" type="tva:TVAIDType" use="required"/>
            <xsd:attribute name="Version" type="dvb:Version" use="optional"/>
          </xsd:complexType>
        </xsd:sequence>
      </xsd:extension>
    </xsd:complexContent>
  </xsd:complexType>
```

**Figure 7cb: BCGOffering****Table 11ce: BCGOffering fields**

Name	Semantic Definition	Constraints
Name	The name of this broadband content guide that can be presented to the user. The format of this type is defined in clause 5.2.12.17.	Mandatory
Description	A Textual description of the broadband content guide that can be presented to the user. The format of this type is defined in clause 5.2.12.17.	Optional
TransportMode	The location where the broadband content guide may be found. The format of this type is defined in clause 5.2.12.46.	Mandatory
Logo	A URI for a logo for the BCG.	Optional
Type	The type of the BCG, defined as a tva:ControlledTermType. The different values of the BCG type are defined in the following extensible ClassificationScheme detailed below.	Optional
TargetProvider	The domain name of the provider whose content is described by this BCG (for example Canal+). The domain name shall be the same as a domain name present in the ServiceList. The format is defined in clause 5.2.10.	Optional
BCGProviderName	The name of the BCG provider (for example "Telerama"). This field shall be identical to the textual string of the Publisher attribute of the TVAMain element in the BCG metadata. The format of this type is defined in clause 5.2.12.17.	Optional
CDSDownloadSessionDescriptionLocation	The multicast location where details of the CDS download Session Description can be found. The format of this type is defined in clause 5.2.12.2.	Optional
@Id	Identifies a Broadband Content Guide Provider/Server; this Id is allocated by the SP.	Mandatory
@Version	Version of this record. A change in this value indicates a change in one of the BCG Records.	Optional

The classification scheme for the Type element is as follows:

```
<ClassificationScheme uri="urn:dvb:metadata:cs:BCGTypeCS:2007">
    <Term termID="1">
        <Name xml:lang="en">Live</Name>
        <Definition xml:lang="en">BCG for live TV programs</Definition>
    </Term>
    <Term termID="2">
        <Name xml:lang="en">CoD</Name>
        <Definition xml:lang="en">BCG for Content on Demand programs </Definition>
    </Term>
    <Term termID="3">
        <Name xml:lang="en">Downloadable Content</Name>
        <Definition xml:lang="en">BCG for downloadable content</Definition>
    </Term>
</ClassificationScheme>
```

This classification scheme is also attached as BCGTypeCS.xml in the file ts_102034v020101p0.zip which accompanies the present document.

5.2.13.2 Broadcast Discovery Record: BroadcastOffering

This element is used where the SP is offering a range of "broadcast" services, which are continuously streamed MPEG-2 transport streams. The services provided are grouped in ServiceLists (which may contain only a single service), which is represented by an instantiation of the complex type IPServiceList, that are in turn a list of IP services. This element is used in two forms: "TS Full SI" where the optional SI element may be omitted and therefore the full DVB service information as defined in ETSI EN 300 468 [1] is provided within the transport stream(s) at the location(s) given in the record. The second form, "TS Optional SI", shall have the SI element present in this record, and need not be present in the transport stream(s) found at the location(s) given.

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 2.

```
<xsd:complexType name="BroadcastOffering">
    <xsd:complexContent>
        <xsd:extension base="dvb:OfferingBase">
            <xsd:sequence>
                <xsd:element name="ServiceList" type="dvb14:IPServiceList" maxOccurs="unbounded" />
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>

<xsd:complexType name="IPServiceList">
    <xsd:sequence>
        <xsd:element name="ServicesDescriptionLocation" type="dvb:DescriptionLocationBCG"
minOccurs="0" maxOccurs="unbounded" />
        <xsd:sequence>
            <xsd:element name="SingleService" type="dvb14:IPService" maxOccurs="unbounded" />
        </xsd:sequence>
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="IPService">
    <xsd:sequence>
        <xsd:element name="ServiceLocation" type="dvb14:ServiceLocation"/>
        <xsd:element name="TextualIdentifier" type="dvb:TextualIdentifier"/>
        <xsd:element name="DVBTriplet" type="dvb:DVBTriplet"/>
        <xsd:element name="MaxBitrate" type="xsd:positiveInteger" minOccurs="0" />
        <xsd:element name="SI" type="dvb:SI" minOccurs="0" />
        <xsd:element name="AudioAttributes" type="tva:AudioAttributesType" minOccurs="0"
maxOccurs="unbounded" />
        <xsd:element name="VideoAttributes" type="tva:VideoAttributesType" minOccurs="0"
maxOccurs="unbounded" />
        <xsd:element name="ServiceAvailability" type="dvb:ServiceAvailabilityType" minOccurs="0"
maxOccurs="unbounded" />
        <xsd:element name="Usage" type="dvb14:Usage" minOccurs="0" maxOccurs="unbounded" />
        <xsd:element name="LinkedService" type="dvb14:IPService" minOccurs="0" maxOccurs="unbounded"
/>
        <xsd:element name="URILinkage" type="dvb14:URILinkageType" minOccurs="0" />
        <xsd:element name="ciAncillaryData" type="dvb14:ciAncillaryDataType" minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>
```

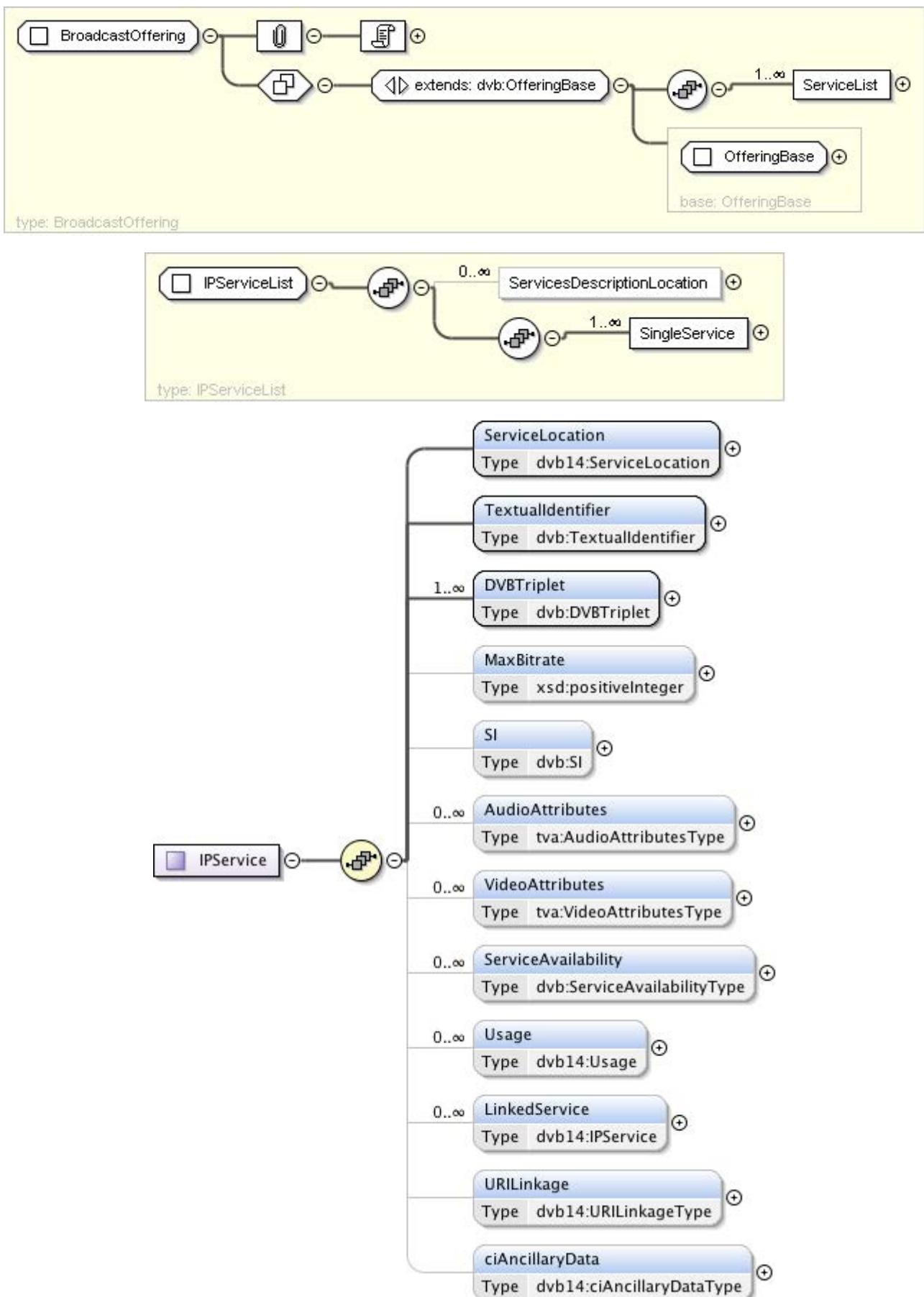


Figure 7cc: IPService (Informative)

Table 11cf: IP Service Fields

Name	Semantic Definition	Constraints
ServiceList	A list of the details and locations of IP services offered by the service provider. A service provider can divide their services into multiple service lists for administrative convenience.	Mandatory
SingleService	The details and location(s) of a single IP service offered by the service provider.	Mandatory
ServicesDescription Location	If present, this element shall contain the identifier(s) of the BCG Record(s) for the BCG Discovery element that carries the information (guide details) for the offerings grouped under the ServiceList with which this element is associated. This type is described in clause 5.2.12.6.	Optional
ServiceLocation	The location(s) at which the service can be found, and includes details of forward error correction or retransmission services if available. This location may be in a multicast or RTSP specified form. This type is described in clause 5.2.12.33.	Mandatory
TextualIdentifier	The Textual identifier by which the service is known. If the domain name is missing, it is taken from the context which in this case shall be the DomainName attribute of the BroadcastOffering (inherited from OfferingBase). This type is described in clause 5.2.12.45.	Mandatory
DVBTriplet	The DVB Triplet by which the service is known. This will match the service details inside the transport stream. This type is described in clause 5.2.12.8.	Mandatory
MaxBitrate	Specifies the maximum bitrate (in kbytes/s) of the overall stream carrying the service excluding any FEC or other layers and calculated according to TIAS value in IETF RFC 3890 [80] (see note).	Optional without DSM service, but mandatory when using a DSM service
SI	Service information about the service carried. This type is described in clause 5.2.12.34. There are two forms of an IP service ("TS Full SI" and "TS optional SI"), as described above, which differ in the presence of this element.	Optional for TS Full SI service; Mandatory for TS Optional SI service
AudioAttributes	Each instance of this value specifies a way of coding the audio that may be used at some point during the operation of the service. If this element is missing, then the default value of MPEG-1 or MPEG-2 layer 2 backwards compatible, mono or stereo shall be used; specifically this shall be the legacy value from ETSI TS 101 154 [58]. The format of this type is defined in clause 6.3.5 of ETSI TS 102 822-3-1 [60]. The values carried in the href attribute of the Coding element shall be defined by the classification specified in the file AudioCS.xml (and by reference MPEG7 AudioCS.xml) included in ts_102034v020101p0.zip, or, preferably, as defined by ETSI TS 102 323 [59].	Optional
VideoAttributes	Each instance of this value specifies a way of coding the video that may be used at some point during the operation of the service. If this element is missing, then the default value of MPEG-2 coded video, operating at MP@ML at a frame rate of 25 Hz shall be used; specifically this shall be the legacy value from ETSI TS 101 154 [58]. The format of this type is defined in clause 6.3.5 of ETSI TS 102 822-3-1 [60]. The values carried in the href attribute of the Coding element shall be defined by the classification specified in the file VideoCodecCS.xml (and by reference MPEG7 VisualCodingFormatCS.xml) included in ts_102034v020101p0.zip, or, preferably, as defined by ETSI TS 102 323 [59].	Optional
ServiceAvailability	Defines the geographical regions in which this service is available or not available. This element provides support for Regionalization. It allows each service to have a list of 'cells' (regions) with which the service is associated. By default, all the single services are available everywhere. There may be multiple ServiceAvailability elements, corresponding to multiple CountryCode. This element is described in clause 5.2.12.32.	Optional
Usage	This element is used to identify the usage for this service (e.g. main video, SD, HD, PiP, etc.). Several instances are possible to indicate all usages that can be found within this IPServices. This element is used to indicate that other IPServices exist for the same content, and that they will be exposed as sub-IPServices within this IPServices. This type is described in clause 5.2.10.	Optional without DSM service, but mandatory when using a DSM service
LinkedService	Holds the sub-IPServices.	Optional without DSM service, but mandatory when using a DSM service

Name	Semantic Definition	Constraints
URILinkage	This field supports the URILinkage functionality as defined in ETSI EN 300 468 [1], which includes support for companion screen functionality as described in [125]. This type is disclosed more in clause 5.2.12.47a.	Optional
ciAncillaryData	This field carries optional ancillary data used in the identifiers that support companion screen functionality as described in [125]. This type is disclosed more in clause 5.2.12.1a.	Optional
NOTE: Other layers may be carried on the same multicast address, and appropriate calculations should be made as necessary.		

5.2.13.3 Content on Demand Offering Record: CoDOffering

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 3.

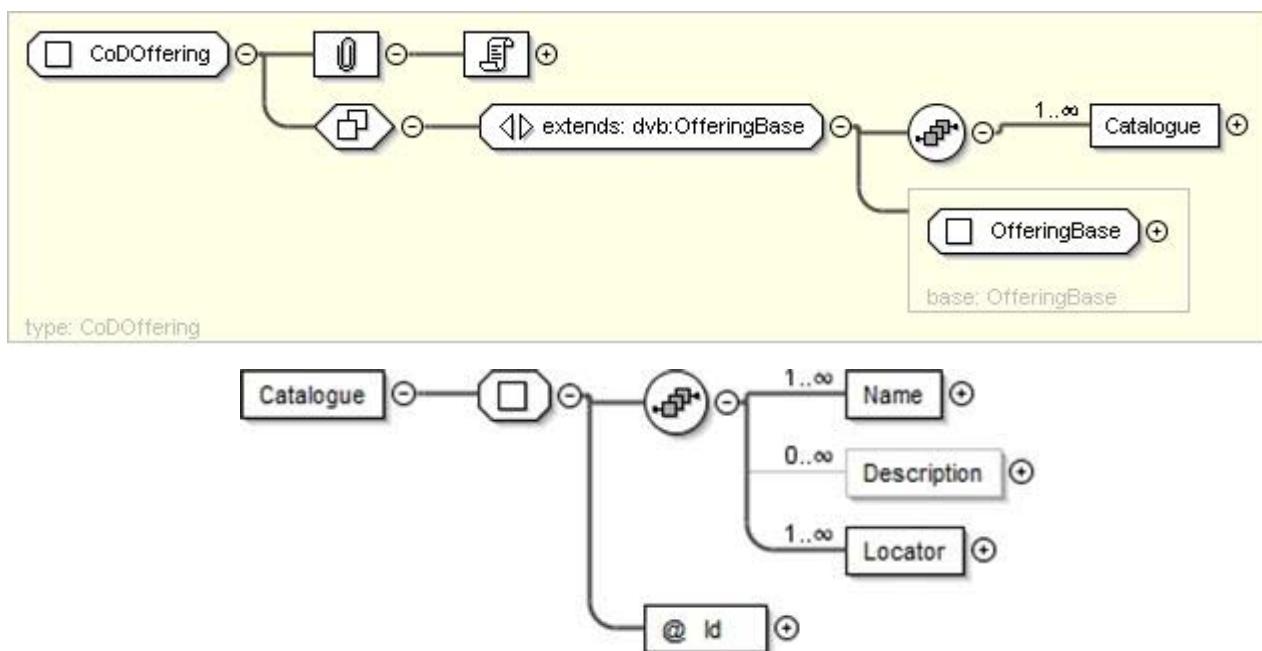
NOTE: The use of this is now deprecated and BCGOffering (clause 5.2.13.1) should be used instead. This record is retained solely for legacy reasons.

This provides information on Content on Demand Offerings.

The Content on Demand Discovery Record provides all the necessary information to discover the CoD servers available on the network and the location of their catalogue of contents. It does not provide any information on individual contents. The Content on Demand Discovery Record implements the CoD Discovery Information and Content Description Location, and by inheritance the DVB-IPTV Offering, components of the Data Model in clause 5.2.7. The component Content Location is deliberately not implemented; it is intended that this information is retrieved from the provider, possibly after negotiation.

```

<xsd:complexType name="CoDOffering">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">Provides information on Content on Demand Offerings. Note that use of this is now deprecated and BCGOffering should be used instead</xsd:documentation>
  </xsd:annotation>
  <xsd:complexContent>
    <xsd:extension base="dvb:OfferingBase">
      <xsd:sequence>
        <xsd:element name="Catalogue" maxOccurs="unbounded">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element name="Name" type="dvb:MultilingualType" maxOccurs="unbounded"/>
              <xsd:element name="Description" type="dvb:MultilingualType" minOccurs="0" maxOccurs="unbounded"/>
              <xsd:element name="Locator" type="xsd:anyURI" maxOccurs="unbounded"/>
            </xsd:sequence>
            <xsd:attribute name="Id" type="dvb:Hexadecimal16bit" use="required"/>
          </xsd:complexType>
        </xsd:element>
      </xsd:sequence>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
```

**Figure 7cd: CoDOffering services****Table 11cg: CoDOffering Fields**

Name	Description	Constraints
Catalogue	Description of where information on a group of content items may be found.	At least one instance shall be present per CoDOffering if the CoDDiscovery mechanism is supported
Name (<i>Child element of Catalogue</i>)	Name of the CoD offering catalogue for display in one or more languages; one name is allowed per language code, and at least one language shall be provided (though not necessarily more than one).	Mandatory
Description (<i>Child element of Catalogue</i>)	Description of the CoD general offering catalogue for potential display in one or more languages; one description per language code.	Optional
Locator (<i>Child element of Catalogue</i>)	One or more URI [20] where the aggregated content descriptions can be found (catalogue/metadata). An HTTP request on the "Locator" URI [20] shall return a record compliant to a schema that will be specified in a later revision of the present document.	Mandatory
Id (<i>attribute of Catalogue</i>)	Identifies a CoD Provider/Server; This Id is allocated by the SP.	Mandatory

5.2.13.4 Packaged Services: PackagedServices

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 5.

This provides a means to group services together into a "package" that the SP can offer or refer to as a unit, for marketing or other purposes, and that can be presented to the user as a grouping.

A service may belong to more than one package. A service does not have to be part of any package.

The package discovery information does not enable the discovery of new services. Discovery information relating to a service, or SP, such as the location of the service will need to be acquired directly from the SP providing the service, and is not "pointed to" from this record.

Additional information on services can optionally be provided in the context of a package, through the PackageDescription.

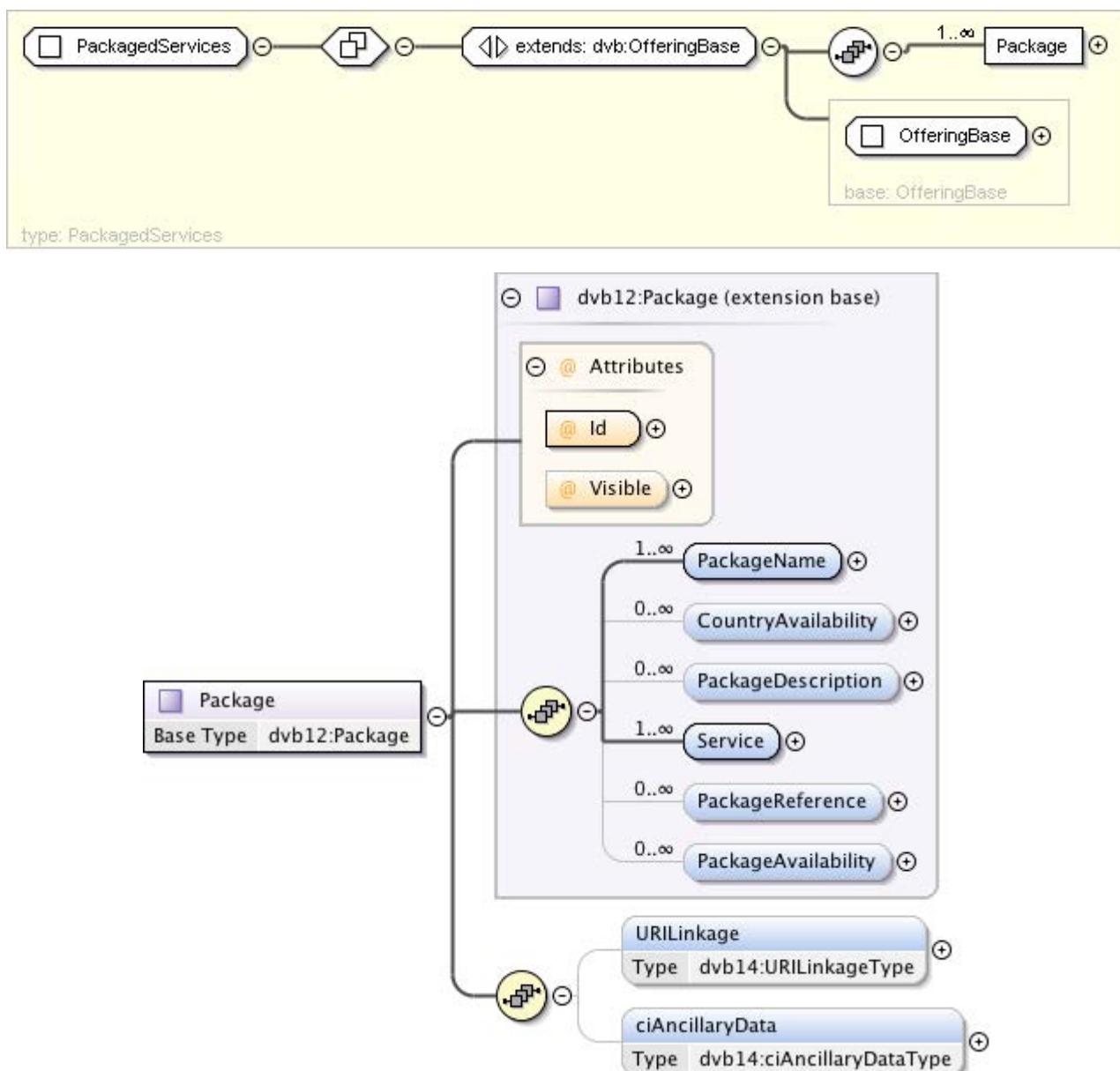
Where the PackageAvailability element is used, there may be multiple packages transmitted, each one corresponding to a specific set of regions. However, for any given HNED there shall only be a single package that both has the Visible attribute set to true and that has the PackageAvailability element that match the values held by the HNED.

NOTE: This means that once an HNED has found a visible package that matches the CountryCode, and if present, Cell values, the HNED has found the package it should use.

```

<xsd:complexType name="PackagedServices">
  <xsd:complexContent>
    <xsd:extension base="dvb:OfferingBase">
      <xsd:sequence>
        <xsd:element name="Package" type="dvb14:Package" maxOccurs="unbounded" />
      </xsd:sequence>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>

<xsd:complexType name="Package">
  <xsd:sequence>
    <xsd:element name="PackageName" type="dvb:MultilingualType" maxOccurs="unbounded" />
    <xsd:element name="CountryAvailability" type="dvb:CountryAvailability" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="PackageDescription" type="dvb:DescriptionLocationBCG" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="Service" type="dvb:PackagedServiceType" maxOccurs="unbounded" />
    <xsd:element name="PackageReference" minOccurs="0" maxOccurs="unbounded" >
      <xsd:complexType>
        <xsd:attribute name="Id" type="dvb:Hexadecimal16bit" />
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="PackageAvailability" type="dvb:ServiceAvailabilityType" minOccurs="0" maxOccurs="unbounded" />
    <xsd:element name="URILinkage" type="dvb14:URILinkageType" minOccurs="0" />
    <xsd:element name="ciAncillaryData" type="dvb14:ciAncillaryDataType" minOccurs="0" />
  </xsd:sequence>
  <xsd:attribute name="Id" type="dvb:Hexadecimal16bit" use="required" />
  <xsd:attribute name="Visible" type="xsd:boolean" use="optional" default="true" />
</xsd:complexType>
```

**Figure 7ce: Packaged services****Table 11ch: Package Fields**

Name	Definition	Constraints
PackageName	The textual name of the package for display in one or more languages. There shall be a maximum of one name per language code. The multilingual type is described in clause 5.2.12.17.	Mandatory
Service	One or more services which comprise the package. This type is described in clause 5.2.12.21.	Mandatory
CountryAvailability	A list of the countries and/or groups of countries within which the package is, or is not, available. This type is described in clause 5.2.12.5. This field is deprecated.	Deprecated
PackageDescription	A link to a BCG in the form of identifier(s) of BCG Record(s) that provides a description of the content available in the package. The type is described in clause 5.2.12.6.	Optional
PackageReference	This shall be the Id(s) of package(s) that are included in the current package. The Id is carried as the attribute of the element PackageReference.	Optional

Name	Definition	Constraints
PackageAvailability	This element provides support for Regionalization. It allows each package to have a list of 'cells' (regions) with which the package is associated. By default, the package is available everywhere. There shall be at most one PackageAvailability element for each CountryCode. The type is described in clause 5.2.12.32.	Optional
URILinkage	This field supports the URILinkage functionality as defined in ETSI EN 300 468 [1], which includes support for companion screen functionality as described in [125]. This type is disclosed more in clause 5.2.12.47a.	Optional
ciAncillaryData	This field carries optional ancillary data used in the identifiers that support companion screen functionality as described in [125]. This type is disclosed more in clause 5.2.12.1a.	Optional
Id (attribute)	This uniquely identifies the package, and is allocated by the Service Provider. The Service Provider shall ensure that it is unique within the scope of their services.	Mandatory
Visible (attribute)	A Boolean which indicates in combination with the PackageAvailability element, whether this package shall be presented to the user, when this package is directly used. When a package is referenced, the Visible attribute of the referenced package shall be ignored, and the Visible attribute of the referencing package shall be used. The default value is true. The attribute is present simply to provide efficient grouping of common packages without having the common packages displayed separately.	Optional

5.2.13.5 Referenced Services Offering: ReferencedServices

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 4.

This provides a means for a SP to list services provided by other SPs from within his own service discovery information via reference. These services are grouped by the service provider, and the reference takes the form of the Service type defined in clause 5.2.10 combined with the DomainType also defined in clause 5.2.10.

```

<xsd:complexType name="ReferencedServices">
    <xsd:complexContent>
        <xsd:extension base="dvb:OfferingBase">
            <xsd:sequence>
                <xsd:element name="ReferencedServiceProvider"
type="dvb12:ReferencedServiceProviderType" maxOccurs="unbounded" />
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>

```

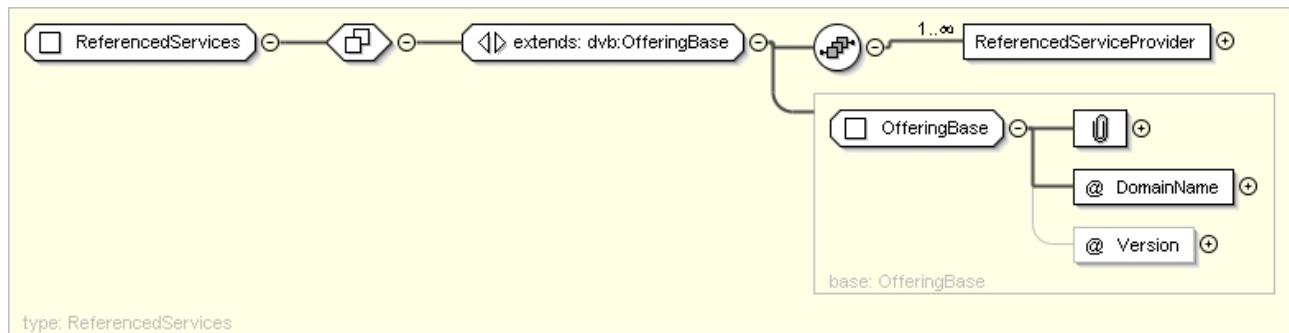


Figure 7cf: Referenced services

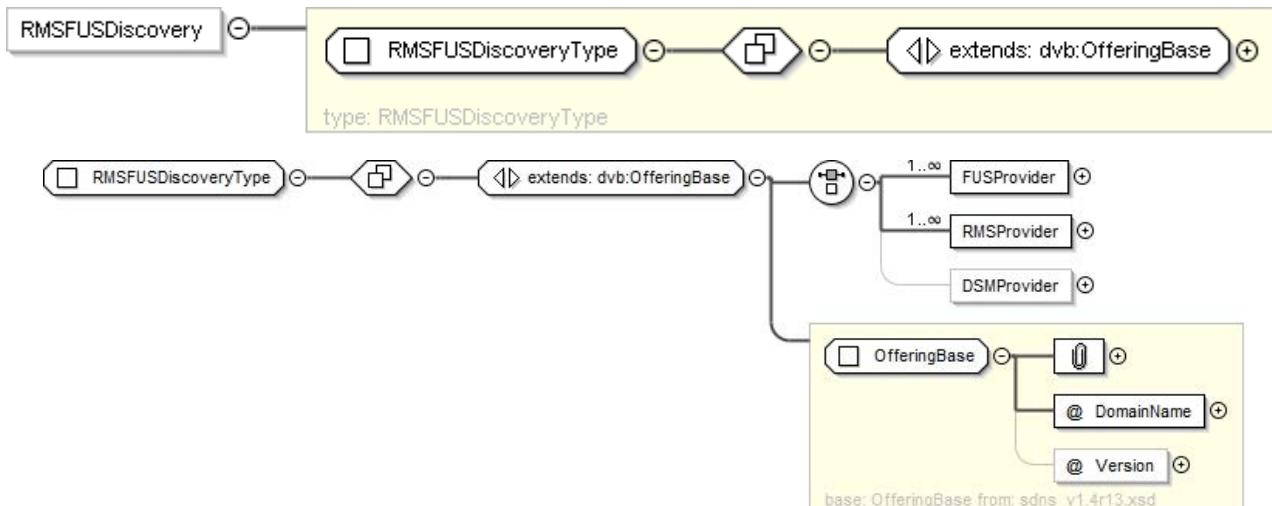
Table 11ci: Referenced services fields

Name	Definition	Constraints
ReferencedServiceProvider	A group of one or more service from a different SP to which the SP of the current context wishes to refer. ReferencedServiceProviderType is defined in clause 5.2.12.24.	At least one shall be present
@Name (attribute of Service which is element of ReferencedServiceProvider)	The name of the each referenced service. A unique host name for the service within the referenced SP's domain for each service from the referenced provider. Uses "Service" element as defined in clause 5.2.10.	Mandatory

5.2.13.6 RMS Offering: RMSFUSDDiscoveryType

When present this metadata provides information about available remote management and firmware update services, combinations of multiple services may be identified. When delivered by multicast, the PayloadID value for DVBSTP shall be 8, as detailed in Table 12a.

```
<xsd:complexType name="RMSFUSDDiscoveryType">
    <xsd:complexContent>
        <xsd:extension base="dvb:OfferingBase">
            <xsd:choice>
                <xsd:element name="FUSProvider" type="dvb14:FUSType" maxOccurs="unbounded"/>
                <xsd:element name="RMSProvider" type="dvb:RMSType" maxOccurs="unbounded"/>
                <xsd:element name="DSMProvider" type="dvb14:DSMMType" minOccurs="0" maxOccurs="1"/>
            </xsd:choice>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>
```

**Figure 7cg: RMSFUSDDiscoveryType****Table 11cj: RMSFUSDDiscoveryType Fields**

Name	Semantic Definition	Constraints
FUSProvider	The textual name of the provider of the FUS from which the updates may be sourced. More than one FUS may be referenced. This is instantiated using the "FUSType" and the format of this type is defined in clause 5.2.12.12.	Mandatory
RMSProvider	The textual name of the provider of the RMS managing the HNED. More than one FUS may be referenced. This is instantiated using the "RMSType" and the format of this type is defined in clause 5.2.12.28.	Mandatory
DSMProvider	The discovery information for the DSM service, a maximum of one DSM Provider is allowed, instantiated by the DSMMType defined in 5.2.12.6a.	Optional

5.2.13.7 Service Provider Discovery: ServiceProviderListType

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 1.

ServiceProviderDiscovery allows multiple service providers to be defined.

The first stage in the service discovery is the SP discovery phase. This enables the discovery of SPs offering DVB-IPTV services on the network and the acquisition of the location information of the various SPs' offering(s).

A SP Discovery Information record may aggregate discovery information on several SPs. This is intended to be useful when minimizing the number of records acquired, such as when the act of acquiring a record has an overhead associated with it. For example, a single HTTP request could retrieve the complete list of SPs providing DVB-IPTV services on the network.

```

<xsd:complexType name="ServiceProviderListType">
    <xsd:sequence>
        <xsd:element name="ServiceProvider" type="dvb14:ServiceProviderType" maxOccurs="unbounded" />
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ServiceProviderType">
    <xsd:sequence>
        <xsd:element name="Name" type="dvb:MultilingualType" maxOccurs="unbounded" />
        <xsd:element name="Description" type="dvb:MultilingualType" minOccurs="0" maxOccurs="unbounded" />
        <xsd:element name="Offering" type="dvb14:OfferingListType" minOccurs="0" />
    </xsd:sequence>
    <xsd:attribute name="DomainName" type="dvb:DomainType" use="required" />
    <xsd:attribute name="Version" type="dvb:Version" use="required" />
    <xsd:attribute name="LogoURI" type="xsd:anyURI" use="optional" />
</xsd:complexType>

```

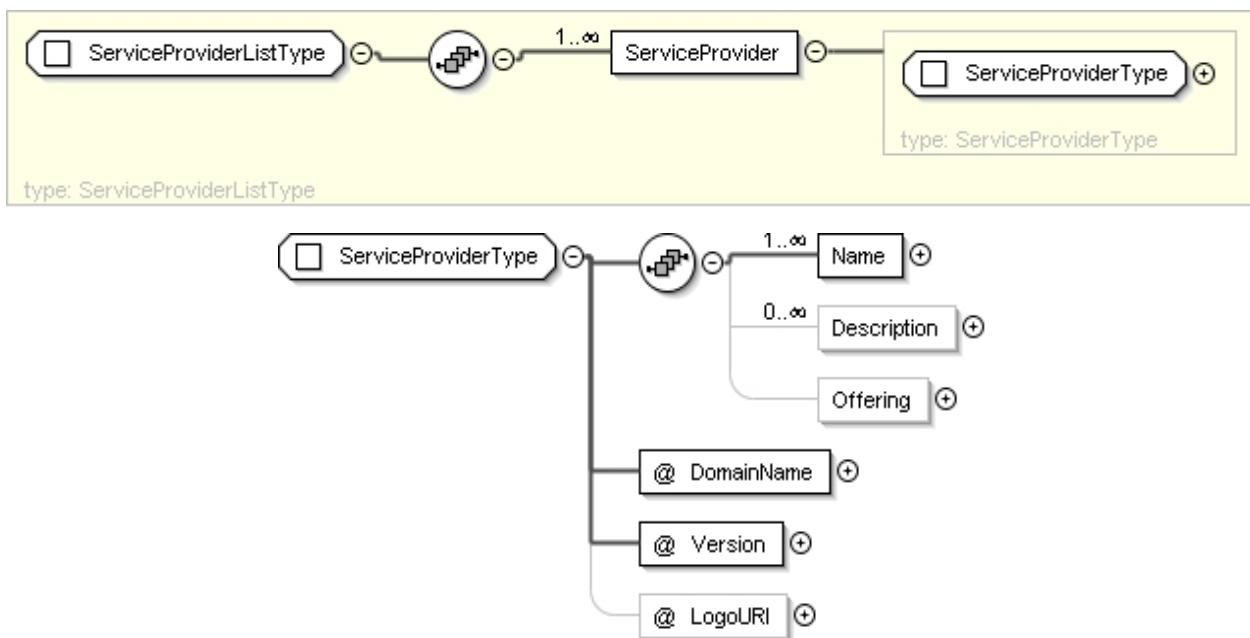


Figure 7ch: ServiceProviderDiscoveryType

Table 11ck: ServiceProviderDiscovery Fields

Name	Description	Constraints
ServiceProvider	Description of one or more service providers using ServiceProviderListType	At least one description shall be included per ServiceProvider
Name	Textual name of service provider, there may be more than one name which may be in different languages.	Optional
Description	Textual description of service, there may be more than one description which may be in different languages.	Optional
Offering	Defines available delivery methods and associated locations for Push and Pull delivery, as defined in clause 5.2.12.19. If the element Offering is missing, then the ServiceProvider is not currently providing any services, but simply announcing its presence.	Optional
DomainName attribute	Attribute carrying string defined to specific character constraints, as defined in clause 5.2.10	Mandatory
Version attribute	Attribute carrying string defined to specific alphanumeric character constraints, that details the version number of this ServiceProviderDiscoveryRecord. This is used with multicast delivery to identify update to the ServiceProviderDiscoveryRecord.	Mandatory
LogoURI attribute	Attribute containing URI of location of service provider logo.	Optional

5.2.13.8 Regionalization Discovery Information

5.2.13.8.1 Regionalization Offering

When delivered by multicast, the PayloadID value, as detailed in Table 12a, shall be 7.

An HNED is located geographically in a region which is defined by the SP and identified using a string identifier called a Cell ID which is unique within a country (i.e. the location of the HNED can be defined using the country code and Cell ID together). This identifier is used in the PackageAvailability element in Table 11ch and the ServiceAvailability element in Table 11cf to indicate which package and services can be received by the HNED.

The HNED obtains its location from the DHCP server via the DHCP option 99 defined in IETF RFC 4676 [97] as described in clause 8.1.1.11. The HNED can then retrieve its Cell ID by:

- either requesting it by sending its location information to a server - URI retrieved from the Regionalization Offering (Pull mode see clause 5.4.2.3);
- or matching the location information against the table pushed to it on an address retrieved from the Regionalization Offering (Push mode). The table is provided in the Regionalization Offering Record (as described in this clause).

The resulting identifier is the Cell ID which, in combination with the country code, can be matched against information in the PackageAvailability and ServiceAvailability elements to show which package and services can be received by the HNED in its region.

Unlike the rest of Service Discovery and Selection information, the format of the Regionalization information received by the HNED is different depending on the use of Push or Pull modes, (i.e. the data transmitted in the Push or Pull mode is not interchangeable). However, the way the Push and Pull locations are advertised in the Regionalization Offering is identical to other SD&S Offerings. The Regionalization Offering within the SP Discovery Record shall provide the IP address of either the Push or the Pull location, or both. If both a Push and Pull locations are provided then the HNED shall use the Pull location first and only on failure try the Push location. It is recommended to use the pull mode.

If Regionalization is used, i.e. PackageAvailability and ServiceAvailability elements are used in Package Discovery Records and Service Discovery Records, a Regionalization Offering should be defined within the SP Discovery information unless the relevant Regionalization information is already available to the HNED through some other proprietary means.

The Regionalization Discovery Record allows CellIDs to be sent to all HNEDs. An alternative pull mechanism is described in clause 5.4.2.3. The HNED checks the DHCP GEOCONF_CIVIC option 99 content and matches it against the table of values conveyed by the Regionalization Discovery Information to find the Cell ID for its location.

The Regionalization Discovery Record can be large so it is recommended to use compression (see Table 12). It is not necessary to carry all the CA types within the Regionalization Discovery record. The HNED shall minimize processing time by stopping when the CA type does not match the value supplied by the DHCP server.

All Civic Address parameters may not be used, and they may be used in any order within the Regionalization Discovery Record, compared to the DHCP message. Thus the HNED shall parse the XML structure and can stop parsing when a non-matching type/value pair is found. When all type/value pairs are matched, and the end of the CA elements tree has been reached, it means that a match has been found and that the Cell ID has been retrieved.

When the DHCP GEOCONF_CIVIC data have multiple languages set of parameters (CAtype="0"), it is sufficient to match one of these to retrieve the Cell ID.

```
<xsd:complexType name="RegionalisationOffering">
  <xsd:complexContent>
    <xsd:extension base="dvb:OfferingBase">
      <xsd:sequence>
        <xsd:element name="Cell" type="dvb:Cell" maxOccurs="unbounded" />
      </xsd:sequence>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
```

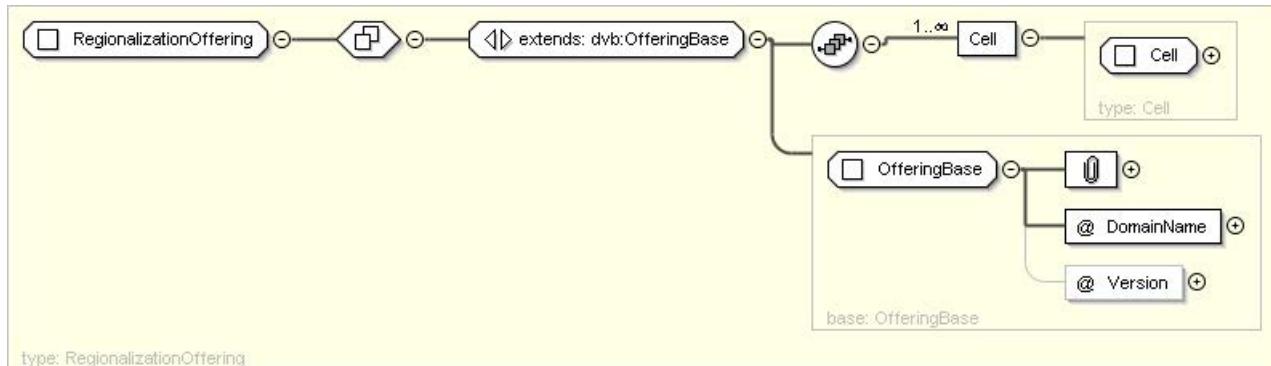


Figure 7ci: Regionalization Offering

Table 11cl: Regionalization Offering Fields

Name	Definition	Constraints
Cell	A Regionalization unit that contains a hierarchical list of civic addresses (the civic addresses are available via DHCP) to which the region applies.	Mandatory

5.2.13.8.2 Example Regionalization Information (Informative)

Following is an example where the DHCP GEOCONF_CIVIC option has supplied the location of the HNED as:

- Country code = "FR".
- CAtype = "0", CAvalue = "fr".
- CAtype = "128", CAvalue = "Latn".
- CAtype = "1", CAvalue = "IDF".
- CAtype = "3", CAvalue = "Paris".
- CAtype = "24", CAvalue = "75011".
- CAtype = "132", CAvalue = "private CA parameter".

Following is the relevant part of the long Regionalization Discovery Record that was pushed to the HNED which resulted in the Cell ID being "Paris East", "Ile de France", "Paris and Suburb".

```
<cell ID="Paris East">
  <CountryCode>FR</CountryCode>
  <CA type="0" value="fr">
    <CA type="128" value="Latn">
      <CA type="1" value="IDF">
        <CA type="3" value="Paris">
          <CA type="24" value="75003" />
          <CA type="24" value="75004" />
          <CA type="24" value="75005" />
          <CA type="24" value="75010" />
          <CA type="24" value="75011" />
          <CA type="24" value="75012" />
          <CA type="24" value="75019" />
          <CA type="24" value="75020" />
        </CA>
      </CA>
    </CA>
  </CA>
</cell>
```

5.2.13.9 SRM Offering Record

The SRM Offering Record provides information for the delivery of System Renewability Messages (SRMs) over IP networks to HNEDs.

The SRM Offering Record shall use the Payload ID value 0x09 as defined in Table 12a and inherit the base Offering Record defined in clause 5.2.12.18. The domain name is the domain name of the provider of the SRM delivery services.

For more information on SRM delivery over IP network see clause 12.

The SRM Offering Record provides a list of SRM announcement (see clause 12.4) and download services (see clause 12.5) for specific CP Systems. For each SRM announcement and download service the list of supported CP System IDs, optional CP System SRM IDs (see clause 12.3) and information on how to access the service is provided. The list of CP System IDs and CP System SRM IDs can have a single entry, multiple entries or no entry. In the latter case the HNED has to access the specific service in order to know which CP System IDs and CP System SRM IDs are supported by the service. In case a CP System uses CP System SRM IDs and only the CP System ID is provided in the announcement the HNED has to access the service in order to get information about which CP System SRM IDs are supported by the service.

NOTE 1: In case of a HTTP unicast SRM download service announcements one and only one CP System ID or combination of CP System ID and CP System SRM ID has to be provided to clearly identify the SRM provided by the service.

A SRM file version number shall be provided together with the CP System ID and optional CP System SRM ID for HTTP unicast SRM download services and may be provided for FLUTE unicast SRM download services. This SRM file version number shall be incremented each time an updated SRM file is available via the HTTP download. An announcement service version number may be provided for SRM announcement services. This announcement service version number shall be incremented each time new or updated announcements are available via the SRM announcement service. A FLUTE session version number may be provided for FLUTE multicast SRM download services. This FLUTE session version number shall be incremented each time new or updated SRM files are available via the FLUTE download session. For more information on the different version numbers and their usage see clause 12.6.

NOTE 2: Multiple announcement and download services can be offered for a specific CP System ID and CP System SRM ID. The behaviour of the HNED in selecting a particular service in this case is implementation specific.

```
<xsd:complexType name="SRMOffering">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">Provides a list of SRM Announcement and Download Services</xsd:documentation>
  </xsd:annotation>
  <xsd:complexContent>
    <xsd:extension base="dvb:OfferingBase">
      <xsd:sequence>
```

```

<xsd:element name="SRMAnnouncementService" type="dvb14:SRMAnnouncementServiceType"
minOccurs="0" maxOccurs="unbounded" />
  <xsd:element name="SRMDownloadService" type="dvb14:SRMDownloadServiceType"
minOccurs="0" maxOccurs="unbounded" />
</xsd:sequence>
</xsd:extension>
</xsd:complexContent>
</xsd:complexType>

```

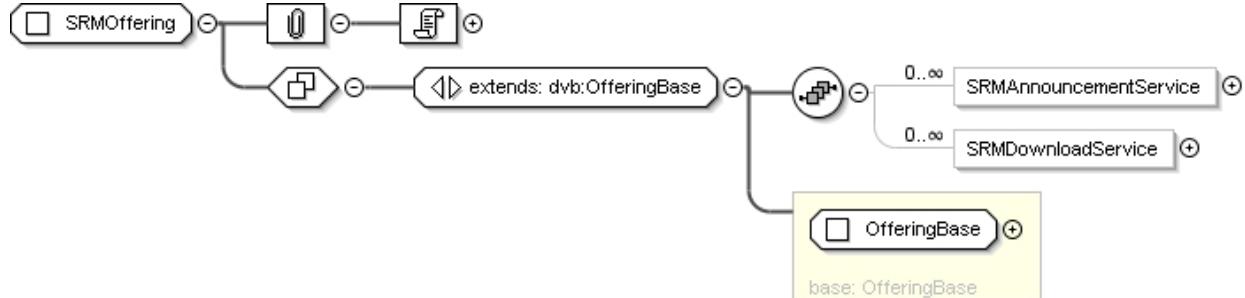


Figure 7cj: SRMOffering

This element is used where the SP is offering SRM delivery over IP networks. It provides a list of SRM Announcement and Download Services for specific CP System IDs.

Table 11cm: SRM Offering Fields

Name	Definition	Constraints
SRMAnnouncementService	Details of all of the SRM Announcement services, with one instance per service. The format of this is defined in clause 5.2.12.37.	Optional
SRMDownloadService	Details of the SRM Download service provided, with one instance per service. The format of this is defined in clause 5.2.12.40.	Optional

5.2.13.10 CoD Announce Describe Record

Figure 7ck shows the structure of the CoDAnnounceDescribe which shall only be present in documents used as part of the RTSP ANNOUNCE and DESCRIBE methods as outlined in clause 6.3.1.1 where full details of the elements are provided.

```

<xsd:element name="CoDAnnounceDescribe">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ContentDescription" type="tva:BasicContentDescriptionType" />
      <xsd:element name="FECInfo" type="dvb14?:FECInfoType" minOccurs="0" />
      <xsd:element name="RETInfo" type="dvb:RETInfoType" minOccurs="0" />
      <xsd:element name="ServerBasedEnhancementServiceInfo"
type="dvb:ServerBasedEnhancementServiceInfoType" minOccurs="0" />
    </xsd:sequence>
    <xsd:attribute name="RTSPControlURL" type="xsd:anyURI" use="optional" />
    <xsd:attribute name="Streaming" type="dvb:StreamingType" use="optional" />
  </xsd:complexType>
</xsd:element>

```

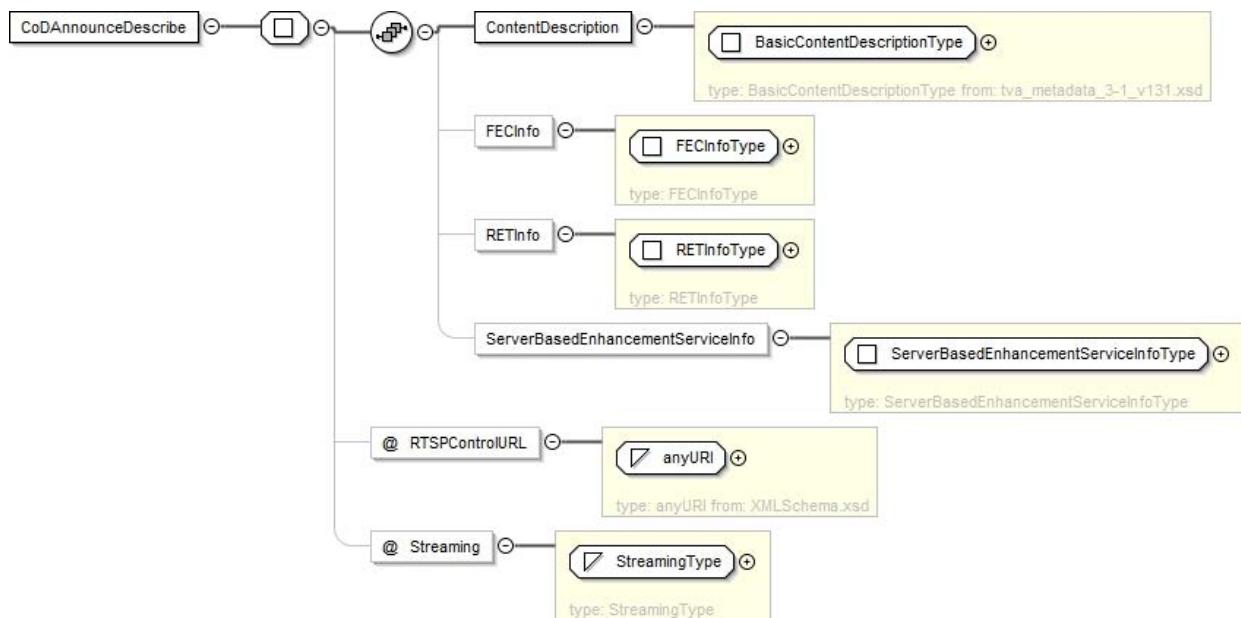


Figure 7ck: CoDAnnounceDescribe

Table 11cn: CoDAnnounceDescribe Fields

Name	Definition	Constraints
ContentDescription	A description of the item, using the TVAnytime format [60].	Mandatory
FECInfo	Details of the FEC available for this content item, if any. This is defined in clause 5.2.12.9.	Mandatory, if FEC is available for this item
RETInfo	Details of the RET available for this content item, if any. This is defined in clause 5.2.12.26.	Mandatory if RET is available for this item and no ServerBasedEnhancementServiceInfo is present
ServerBasedEnhancementServiceInfo	Details of the server-based enhancement service available for this content item, if any. This is defined in clause 5.2.12.31.	Mandatory if server-based FCC is available for this item
RTSPControlURL	The RTSP URL used to control this content item.	Mandatory, if a separate controlURL is used for RTSP
Streaming	When present, this attribute shall indicate the streaming format, as per the definition in clause 5.2.10.	Optional

5.2.13.11 SRM Download Record

For completeness, this record is listed here. Full information on the meaning and use of the SRM Download record is contained in clause 12.

```

<xsd:element name="SRMDownloadRecord">
  <xsd:annotation>
    <xsd:documentation xml:lang="en">Provides a list of SRM Download Services</xsd:documentation>
  </xsd:annotation>
  <xsd:complexType>
    <xsd:complexContent>
      <xsd:extension base="dvb:OfferingBase">
        <xsd:sequence>
          <xsd:element name="SRMDownloadService" type="dvb14:SRMDownloadServiceType" maxOccurs="unbounded"/>
        </xsd:sequence>
      </xsd:extension>
    </xsd:complexContent>
  </xsd:complexType>
</xsd:element>
  
```

```

</xsd:extension>
</xsd:complexContent>
</xsd:complexType>
</xsd:element>

```

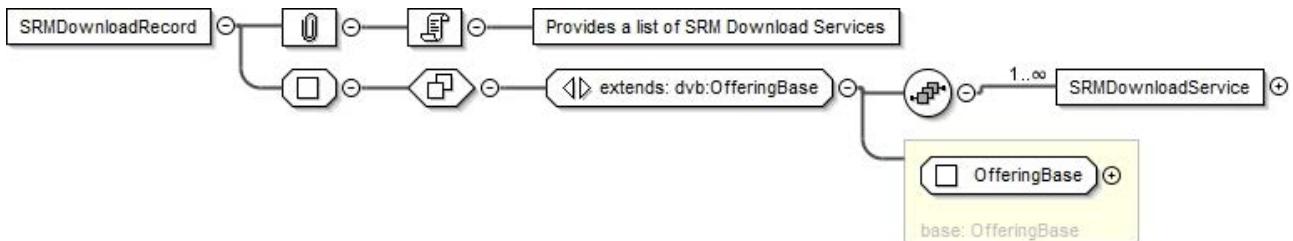


Figure 7cl: SRMDownloadRecord

Table 11co: SRMDownloadRecord Fields

Name	Definition	Constraints
SRMDownloadService	The SRMDownloadServiceType is defined in clause 5.2.12.40.	Mandatory, there may be multiple instances

5.2.13.12 Cell Request Record

For completeness, this record is listed here. Full information on the meaning and use of the Cell Request record is contained in clause 5.4.2.3.

```

<xsd:element name="CellRequestRecord">
<xsd:complexType>
  <xsd:sequence>
    <xsd:element name="CountryCode" type="xsd:string"/>
    <xsd:element name="CA" type="dvb:CivicAddress" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:element>

```

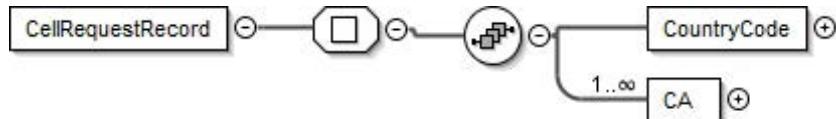


Figure 7cm: Cell Request Record

Table 11cp: Cell Request Record Fields

Name	Definition	Constraints
CountryCode	The Country Code to which this cell applies. This element shall be of the 2-letter format specified in ISO 3166 [50].	Mandatory
CA	The civic address, or nested addresses to which this ID applies, in the country specified by the CountryCode.	Mandatory

5.2.14 XML Schema

The full normative XML schema is available as the file sdns_v1.6r03.xsd in archive ts_102034v020101p0.zip which accompanies the present document. Sections of the schema are included here for informative purposes.

The namespace of this schema is defined in clause 5.2.8.

Clause 5.2.13 provides details on the elements that may be contained within the Service Discovery element, and additional elements that use the same delivery mechanism(s) and are contained within the same schema. This includes the SRMDownloadRecord described in clause 12, and for completeness listed in clause 5.2.13.11, the CoDAnnounceDescribe defined in clause 5.2.13.10 and the CellRequestRecord described in clause 5.2.13.12.

Note that the namespace used in the present document for "BroadcastOffering", "PackagedServices", "ServiceProviderListType", "BCGOffering", "RMSFUSDiscoveryType" and "SRMOffering" in the entry element ("ServiceDiscovery") is modified to associate with XML instances based on this version of the present document (DVB-IPTV phase 1.6). Legacy platforms with XML instances based on previous revisions of the specification will associate with "ServiceDiscovery" in the imported schema associated with that version, i.e. for ETSI TS 102 034 r1.4 (ts_102034v010401) "sdns_v1.4r13.xsd".

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="urn:dvb:metadata:iptv:sdns:2014-1"
  xmlns:tva="urn:tva:metadata:2011"
  xmlns:dvb12="urn:dvb:metadata:iptv:sdns:2012-1"
  xmlns:dvb14="urn:dvb:metadata:iptv:sdns:2014-1"
  xmlns:dvb="urn:dvb:metadata:iptv:sdns:2008-1"
  xmlns:mpeg7="urn:tva:mpeg7:2008"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xsd:annotation>
    <xsd:documentation>schema to validate the record of the description of the DVB-IPTV offering
of a service Provider
      This is the phase 1.6.1 version of the schema.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:import namespace="urn:tva:metadata:2011" schemaLocation=".tva_metadata_3-1_v171.xsd"/>
  <xsd:import namespace="urn:dvb:metadata:iptv:sdns:2008-1" schemaLocation=".sdns_v1.4r13.xsd"/>
  <xsd:import namespace="urn:dvb:metadata:iptv:sdns:2012-1" schemaLocation=".sdns_v1.5r25b.xsd"/>
  <xsd:import namespace="urn:tva:mpeg7:2008" schemaLocation=".tva_mpeg7_2008.xsd"/>

  <xsd:element name="ServiceDiscovery">
    <xsd:complexType>
      <xsd:choice>
        <xsd:element name="BroadcastDiscovery" type="dvb14:BroadcastOffering"
maxOccurs="unbounded"/>
          <xsd:element name="CoDDiscovery" type="dvb:CoDOffering" maxOccurs="unbounded"/>
          <xsd:element name="ServicesFromOtherSP" type="dvb12:ReferencedServices"
maxOccurs="unbounded"/>
            <xsd:element name="PackageDiscovery" type="dvb14:PackagedServices"
maxOccurs="unbounded"/>
              <xsd:element name="ServiceProviderDiscovery" type="dvb14:ServiceProviderListType"
maxOccurs="unbounded"/>
                <xsd:element name="BCGDiscovery" type="dvb14:BCGOffering" maxOccurs="unbounded"/>
                <xsd:element name="RegionalisationDiscovery" type="dvb:RegionalisationOffering"
maxOccurs="unbounded"/>
                  <xsd:element name="RMSFUSDiscovery" type="dvb14:RMSFUSDiscoveryType" minOccurs="0"
maxOccurs="unbounded"/>
                    <xsd:element name="SRMDiscovery" type="dvb14:SRMOffering" minOccurs="0"
maxOccurs="unbounded"/>
                      </xsd:choice>
                      <xsd:attribute name="Version" type="dvb:Version" use="optional"/>
        </xsd:complexType>
      </xsd:element>
    </xsd:schema>
```

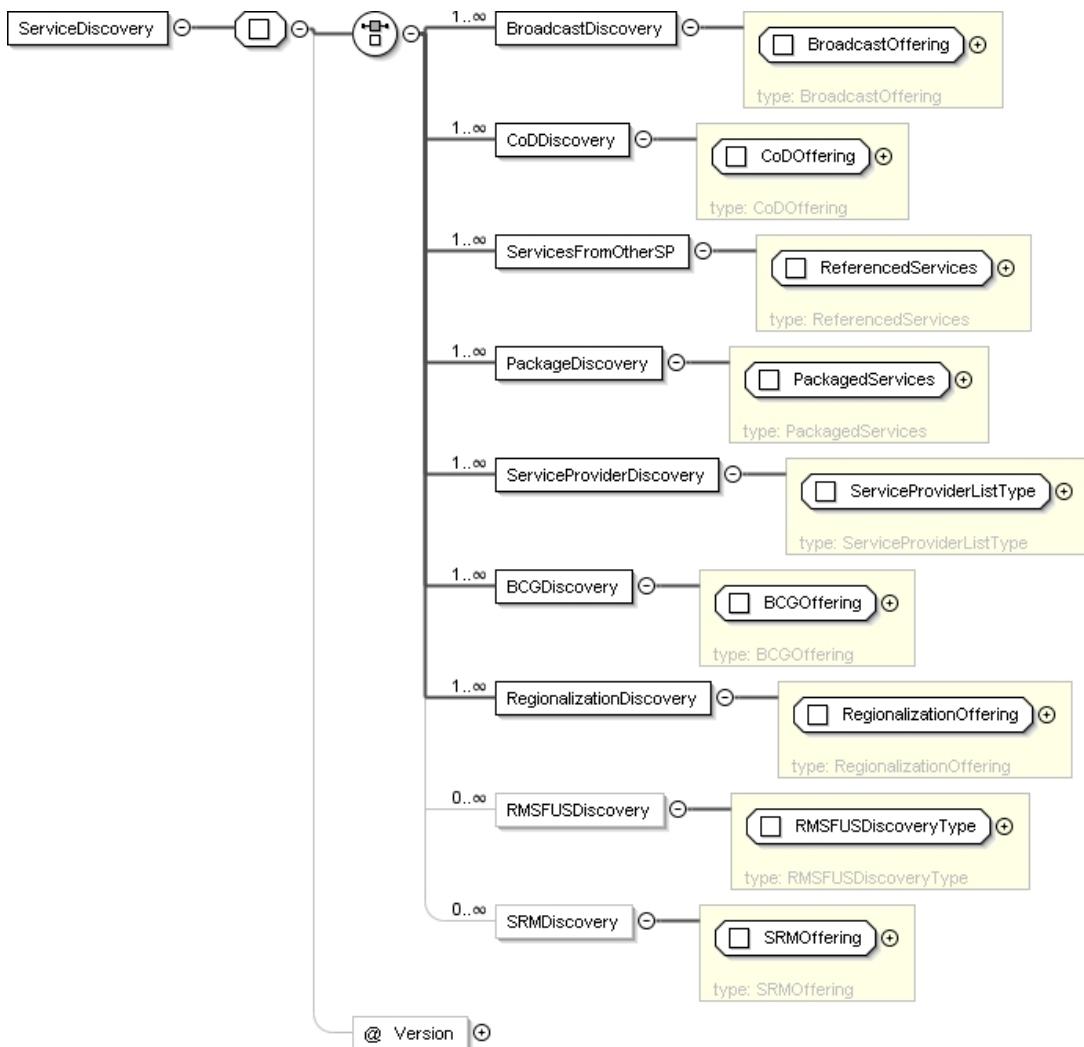


Figure 7cn: Service discovery

Figure 7cn shows the structure of a service offering. Each service offering shall contain only one of the "Element Types" as described in clause 5.2.13, but may have multiple instances of this type.

The version attribute of the offering is used as described in clauses 5.2.13 and 5.2.12.18. It is used to carry the version number of the XML document within the XML. Note that for records described in all sub-clauses of 5.2.13 other than in clause 5.2.13.7, the version number is provided through the OfferingBase type as defined in clause 5.2.12.18.

5.3 Service Selection

A streaming based service may be accessed by an individual HNED in the following ways:

- using RTSP;
- using the methods for joining a multicast group.

Live Media Broadcast services are delivered over IP multicast; they are streamed continuously and do not need to be initiated by each HNED. End devices can join and leave multicast services simply by issuing the appropriate messages, either for IPv4 or for IPv6. The element "Service Location" in the service discovery records gives all the information required to issue the appropriate message. No control of the stream, for example pause or fast-forward, is allowed.

Optionally for Live Media Broadcast services, SPs may choose to require the HNED to engage in explicit set up and tear down phases (possible reasons include accounting, conditional access, etc.). In such systems, the higher-layer session protocol, RTSP [30], shall be used. The element "Service Location" in the service discovery record signals the use of RTSP and gives all the information necessary to issue the appropriate RTSP method. Parameters required for the multicast message will be acquired via the SETUP method from RTSP. See clause 6 of RTSP [30] for the specification of the DVB-IPTV RTSP profile.

Media Broadcast with Trick Mode services are similar to Live Media Broadcast but delivered over IP unicast to enable control of the stream.

Content on Demand Services and Media Broadcast with Trick Mode Services are delivered using IP unicast and are intended for a specific user and need to be initiated explicitly by the end device. RTSP shall be used to access such services. Clause 6 on RTSP [30] specifies which methods to use.

Service selection for CDSs is covered in clause 10 of the present document.

5.4 Transport mechanisms

5.4.0 Overview

This clause specifies the protocols that are used to transport the SP Discovery Information and the Service Discovery Information. Two mechanisms are defined, one for multicast and one for unicast.

The SP Discovery Information, as with other information, may be multicast (push model) or retrieved on request (pull model). One or both models shall be supported by the server. Both models shall be supported by the client.

DVB defined a new protocol for the delivery of XML records over multicast. This protocol is called DVB SD&S Transport Protocol (DVBSTP) and is specified in clause 5.4.1. It shall be used to transport the SD&S information over multicast.

The protocol HTTP [39] shall be used to transport the SD&S information over unicast.

The two transport mechanisms shall be interchangeable in all steps and carry the same content encoded in the same way, with the exception of the format of the Regionalization information which is different depending on the use of Push or Pull modes, (i.e. the Regionalization information data transmitted in the Push or Pull mode is not interchangeable, see clause 5.2.13.8.1).

5.4.1 Protocol for multicast delivery of SD&S information

5.4.1.0 General rules

When the service discovery information is transmitted using multicast UDP packet, the protocol DVBSTP defined in this clause shall be used. All values defined below shall be transmitted in normal IP network byte order (most significant byte first).

The DVBSTP protocol is also used for the multicast delivery of Broadband Content Guide data [62], for the multicast delivery of firmware announcement messages [78] and for the multicast delivery of CDS XML download session descriptions as defined in clause 10.5.5.1.

A URI scheme for DVBSTP is introduced in clause G.3.

It is recommended that the version attribute of the root element (ServiceDiscovery) described in clause 5.2.14 is not present when the XML is delivered via push mode (multicast) and in this case the value of the missing Version attribute is equal to the Version field of the DVBSTP Segment header.

5.4.1.1 Datagram Syntax

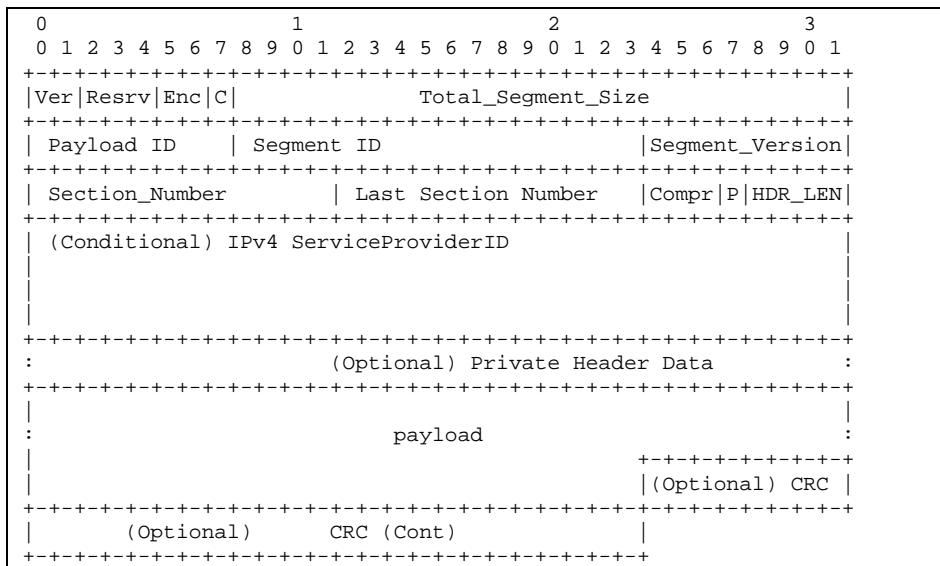


Figure 8: Datagram Syntax IPv4 SD&S multicast delivery protocol

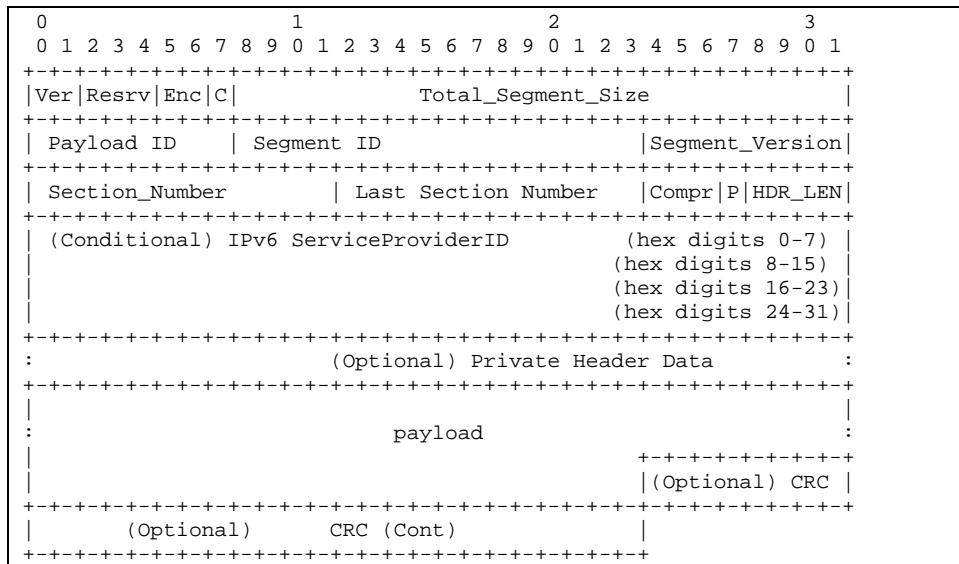


Figure 8a: Datagram Syntax IPv6 SD&S multicast delivery protocol

5.4.1.2 Semantics

Protocol Version (Ver): The protocol version. The value of this 2 bit field shall take a value as defined in Table 11cq which indicates whether the packet is structured for IPv4 or IPv6.

Table 11cq: IP Version values

Version value	Meaning
00	IPv4 packet structure
01	IPv6 packet structure
10 to 11	Not defined

Reserved (Resrv): These 3 bits are reserved and shall take the value "000".

Encryption (Enc): This 2 bit field shall be used to signal the presence of encryption. It shall take the value "00" to indicate that the payload is not encrypted. The syntax, semantics, behaviour and meaning of other values are not defined.

CRC flag (C): If the value is "1", this indicates the presence of a 32-bit CRC at the end of the packet. This flag may only be set on the final packet in a segment, i.e. when section_number is the same as last_section_number.

Total segment size: A 24 bit field that specifies a size in bytes. For uncompressed data (i.e. Compression is "000"), this is the cumulative size of all the payloads of all the sections comprising the segment (i.e. ignoring headers and CRC, if present).

For compressed data that is usable in the compressed form (e.g. BiM), this is the cumulative size of all the payloads of all the sections (see also clause 5.4.1.3.1) comprising the segment (i.e. ignoring headers and CRC, if present) - this is referred to as the "transmitted size". For compressed data that shall be decompressed before use (e.g. zlib), this is the size of the segment once decompressed by the specified algorithm (note that this may not be the same size as that of the original XML) - this is referred to as the "decompressed size". The definition of the compression field value shall also define which of these two interpretation of total segment size shall apply.

Payload ID: A 8 bit value used to identify the type of data being carried within the payload. The values this may take are set out in Table 12a.

Segment ID: A 16 bit value used to identify a segment of data for the declared PT (Payload ID) (see note).

NOTE: For example, you may have multiple Broadcast Discovery Information records, and each one will be assigned a unique Id.

Segment version: An 8 bit value used to define the current version of the segment being carried, i.e. the segment version is keyed on Payload ID together with Segment ID. Thus when the data within a segment changes, the segment version fields of all packets that comprise that segment ID and payload ID change. No other payload version fields are necessarily changed. The segment version is modulo 256, and wraps round.

The segment version should only change at the start of a segment. However, to handle packet loss, a receiver should cope with the segment version changing at any point in the segment.

Section number: A 12 bit field identifying the number of this section. The first section in a segment shall be 0.

Last Section number: A 12 bit field which specifies the last section number (the one with the highest section number) in a segment.

Compression (Compr): A 3 bit field used to indicate the compression scheme, if any, used on the payload. All segments of a given payload ID shall share the same compression value. The meanings of these values are given in Table 12. GZIP is only available with payload ID 0x08 for use with RMS/FUS or for payload ID 0x07 with the Regionalization Information Record.

Table 12: Compression values

Compression value	Meaning	Total Segment Size Meaning
000	No Compression	Transmitted Size
001	BiM (as defined in the present document)	Transmitted Size
010	GZIP	Transmitted Size
011 to 101	Reserved	
110	For ITU-T use	Transmitted Size
111	User Private	User Defined

ProviderID Flag (P): Flag signalling if the ServiceProviderID field is present. The value "1" defines the presence of the ServiceProviderID field in the header.

Private Header Length (HDR_LEN): A 4 bit field counting the number of 32 bit words in the header immediately following the header length field, or the Provider ID field if present. This is used to signal the presence of private header data. If no additional header data is sent, then this shall have the value "0000". The Provider ID field is not considered part of the private header, and so is not counted by the Private Header Length field.

ServiceProvider ID: The semantics of this field depend on whether the network is using IPv4 or IPv6 (see Figure 8 and Figure 8a respectively) as signalled in the version field. The usage of the Provider ID value shall be as defined in clause 5.4.1.3.3.

For IPv4: This is a 32-bit number representing an IPv4 address that is used to identify the SP. This number shall be an IPv4 address. The rest of the field shall be ignored.

For IPv6: This is a 128-bit number (carried as four 32 bit words) representing an IPv6 address that is used to identify the SP. All digits of the IPv6 address shall be provided, including leading zeroes.

It is the responsibility of the SP to ensure that this address is appropriately maintained with the appropriate authorities and maintains a unique value within the scope it is used in. Note that the ServiceProviderID is only for use by the HNED and not for any network filtering.

A ServiceProviderID field is mandatory unless the provider knows that no other SPs can use the same multicast address.

Private Header Data: This is private data. The meaning, syntax, semantics and use of this data is outside the scope of the present document. This field shall be a multiple of 4 bytes.

Payload: The payload of the packet, which is an integral number of bytes. The size of the payload can be calculated from the size of the received packet minus the size of the header (including the optional ProviderID field, if present and any optional private header data present) and the CRC (if present). Note that the payload may be zero bytes in length.

CRC: An optional 32-bit CRC. The standard CRC from ISO/IEC 13818-1 [52], annex A, shall be used. It shall be applied to the payload data of all sections comprising a segment. This field is not necessarily aligned with a 32 bit boundary.

5.4.1.3 Usage

5.4.1.3.0 Introduction

This profiling applies to services over both IPv4 and IPv6. However, different methods shall be followed if no suitable unique IP address is provided in the ServiceProviderID field, the mitigation methods are described in clause 5.4.1.3.3.

5.4.1.3.1 Use of sections

The size of segments may be substantially larger than that supported by the underlying network. To allow efficient delivery of data, it is necessary to be able to divide the segments into smaller units for delivery. The section mechanism provides this functionality.

Each section shall be sent in exactly one UDP datagram, and each UDP datagram shall carry exactly one section.

To assemble the entire segment, an HNED collects the payload from all the sections and orders them based on their section numbers. Only after an entire segment has been assembled can the CRC, if present, be checked.

Figure 9 illustrates the relationship between sections, segments and records.

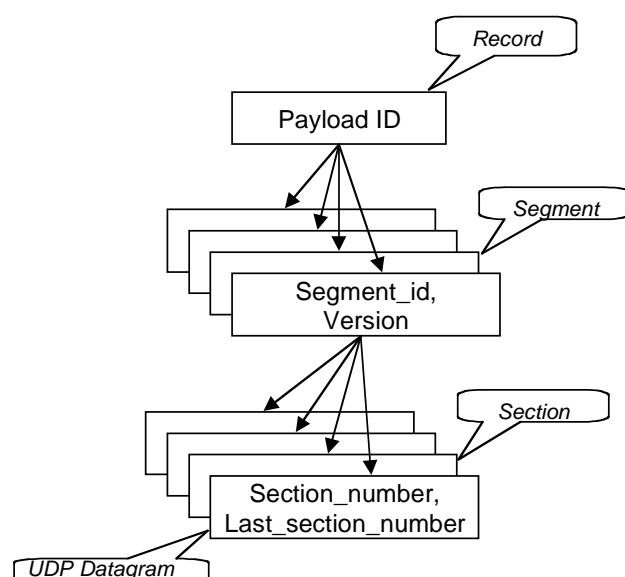


Figure 9: Relationship between records, segments and sections

5.4.1.3.2 Maximum section size

The amount of data that can be encapsulated in each UDP packet, and therefore the potential size of a section, is limited by the maximum size of the IP datagram (65 535 octets for both IPv4 and IPv6), minus the UDP and multicast protocol header sizes. To avoid network fragmentation, it is recommended to set the maximum size such that the underlying Maximum Transmission Unit (MTU) of the network is not exceeded.

Exceeding the network's MTU will lead to IP fragmentation, which significantly increases the effective loss rate of a network. This is because if one fragment is lost, the remaining fragments will need to be discarded by the receiver. It also puts additional load on the routers performing fragmentation and on the end-systems re-assembling the fragments.

For an IEEE Ethernet-based network, with an MTU of 1 492 bytes, the maximum section size should be limited to a maximum of 1 452 bytes. Where additional IP, UDP or multicast protocol options are used, then this value should be reduced by the appropriate amount.

If the section size is set such that fragmentation occurs, any end devices that do not support fragmentation will be unable to receive the SD&S payload. It is therefore recommended that SPs set the DF (Do not Fragment) bit in the IP header. With this bit set, routers will return an ICMP "fragmentation needed and DF set" message if the packet length exceeds the destination network's MTU. The SP can adjust the payload size, if such messages are received. IP (IETF RFC 791 [11]) requires that all hosts shall be prepared to accept datagrams of at least 576 octets.

5.4.1.3.3 Use of ServiceProviderID field

5.4.1.3.3.0 Introduction

Filtering packets on the basis of the source IP address of a packet limits the transmission of packets to sources whose IP addresses is constant and known to the HNED. The ServiceProviderID field overcomes this limitation. It allows an HNED to filter the packets without inspecting or decompressing them. It is expected that the ServiceProviderID field will only be used with SP Discovery records, i.e. when PayloadID is 0x01, since the discovery process will thereafter ensure that only multicast addresses of interest will be received.

5.4.1.3.3.1 Mitigation method if no unique IPv4 address is provided

If a provider does not have, and is not able to get, a suitable IPv4 address that is unique within the needed scope (that of the network carrying the UDP packets), then the "original_network_id" defined in ETSI TS 101 162 [2] may be used. This is mapped into the IPv4 address range using the bottom section of the special 0.0.0.0/8 address range (the "this" network), i.e. 0.0.0.0/16. As an example, an original_network_id of 0x1234 would be represented as 0.0.18.52.

5.4.1.3.3.2 Mitigation method if no unique IPv6 address is provided

A valid IPv6 is required in the ServiceProviderID field. If no address is provided or the address provided cannot be validated, the DVBSTP section shall be ignored.

5.4.1.3.4 Repetition rates

The population of receiving devices (HNEDs) will be dynamically changing. It is not assumed that any HNED stores the SD&S data permanently, so the data shall be continually retransmitted. This also provides a degree of reliability, as any corrupted or lost data can be received on the next repetition. To provide flexibility, different segments within a record (payload id) may be repeated more frequently if desired (e.g. to support faster access to some parts of the record). Similarly, different records may be repeated at different rates.

The full cycle to transmit all the segments of the SD&S records for a SP shall not exceed the Maximum Cycle Time defined in clause 5.4.4.3. A segment may be transmitted several times as required during the cycle and different segments may be transmitted at different rates.

This means that an HNED can assume that the complete SD&S information set of a SP has been transmitted after the Maximum Cycle Time.

5.4.2 Protocol for unicast delivery of SD&S Information

5.4.2.0 General rules

In the pull model of delivery of SD&S information, HTTP [39] Protocol shall be used for all communication between the HNED and the SD&S server(s). The pull model may be used for:

- requests for discovery information relating to SPs (see clause 5.4.2.1);
- requests for discovery information relating to the service offering of a SP (see clause 5.4.2.2);
- requests for obtaining the Cell ID, defined for the location, relating to the Regionalization offering of a SP. (see clause 5.4.2.3).

The HTTP request may contain header fields conforming to the IETF RFC 2616 [39].

The response to the HTTP requests above shall return the appropriate XML records defined in clause 5.2.6 unencrypted. The HNED should evaluate the message returned from the SD&S server simply to ensure that it contains a 200 series success status. If a 200 series success status is not returned then a retry should occur according to the congestion avoidance mechanism defined in clause 9.1.2.1.

After receiving a 200 series success status, the TCP connection is closed.

The HTTP client and server should negotiate a suitable compression using the Accept-Encoding header in the following way: both the client and server shall support the Accept-Encoding header (as defined in HTTP/clause 1.1 [39]).

In addition to this, clients and servers that choose to transfer SD&S data in a BiM encoded form shall signal BiM encoded content with a proper Content-Encoding header upon transmission, and shall not change the Content-Type corresponding to their content.

The content coding token corresponding to the BiM encoding shall be x-bim.

In case the transferred data is encoded in the BiM format, the client shall have acquired the DVB-TVA-init prior to acquiring the SD&S segments.

5.4.2.1 SP Discovery request

The SP discovery request shall return the SP discovery record as defined in clause 5.2.5 for one or all SPs operating on the network. The request has one parameter which can take the value ALL to request discovery information relating to all SPs (known to the queried server) or the domain name of a specific SP to request discovery information relating to the specified SP. When using the "pull mode", records containing SP discovery information (i.e. Payload ID 0x01) shall not be segmented. This SP discovery record shall exist in two forms, as a single XML record with the list of discovery information for the complete set of SPs operating on the network and as a collection of XML records, one per SP.

NOTE: A query with the parameter value set to ALL may not return every SP discovery record applicable to the HNED as the HNED may have to query multiple servers to get them all. The HNED may receive the same SP discovery record from different servers.

The SP discovery request shall comply with the following format:

```
'GET ' path request ' HTTP/1.1' CRLF
'Host: ' host CRLF
CRLF
```

Where:

```
request      = 'sp_discovery?id=' 'ALL'/ SPId.
path        = "/dvb/sdns/" .
host        = the domain name or IP address of the SD&S entry point(s) obtained as specified in
clause 5.2.4.
SPId       = SP domainName as defined in clause 3.3.1.1
```

For example, this leads to the following two possible requests, the first one with the value ALL to request discovery information relating to all SPs (known to the queried server) and the second one with the domain name of a specific SP with MyDomainName as identifier to request discovery information relating to the specified SP:

```
'GET /dvb/sdns/sp_discovery?id=ALL HTTP/1.1' CRLF
'Host: ' host CRLF
```

and

```
'GET /dvb/sdns/sp_discovery?id=MyDomainName HTTP/1.1' CRLF
'Host: ' host CRLF
```

The SP discovery request shall not be issued more than once per Maximum Cycle Time.

5.4.2.2 Service Discovery request

The service discovery request shall return the service discovery record as defined in clause 5.2.6 describing the service offering of a specific SP. The request has three mandatory parameters which take the domain name of the SP, the type of service offering (i.e. payload ID) and the segment ID. Optionally a segment version may be specified in the request, this will indicate to the server the current version of the segment that the HNED has.

When the segment version is specified, the response to the request shall return the service discovery record for the specified segment only if a new version is available. The version number of the returned segment can be found in the XML record. If the segment has not changed then the server shall return status code "204" as per the IETF RFC 2616 [39] to indicate that the request has been processed successfully but that there is no entity-body to return.

When the segment version is not specified, the response to the request shall return the service discovery record for the specified segment.

When a record is not found, the server shall return status code "404" as per the IETF RFC 2616 [39]; the HNED will then need to issue the appropriate SP discovery request to check whether the segment Id is still valid.

The HNED should only issue a service discovery request for the valid segment IDs as listed in the SP discovery record.

The service discovery request shall comply with the following format:

```
'GET ' path request ' HTTP/1.1' CRLF
'Host: ' host CRLF
CRLF
```

Where:

```
request      = 'service_discovery?id='SPId'&Payload='PayloadId'&Segment='SegmentItem
path        = the absolute path of the URI provided in the Location attribute of the Pull
element of the Offering element (of type OfferingListType, see clause 5.2.12.19), with an additional
'/' appended at the end if not already present.
Host        = the network location (authority) of the URL provided in the Location attribute of
the Pull element of the Offering element (of type OfferingListType, see clause 5.2.12.19).
SPId        = SP domainName as defined above in clause 3.3.1.1.
PayloadId   = 2 HEXDIG; any hex number from 00 to ff
SegmentId   = 4 HEXDIG; any hex number from 0000 to ffff
SegmentItem = SegmentId 0*1('&Version='VersionNumber)
```

SegmentItem is a SegmentId with an optional field for the version number.

```
VersionNumber = 2 HEXDIG; any hex number from 00 to ff
```

For example the following request can be constructed to request the service discovery information relating to the broadcast offering of a SP with MyDomainName as identifier:

```
'GET /dvb/sdns/service_discovery?id=MyDomainName&Payload=02&Segment=0001 HTTP/1.1' CRLF
'Host: ' host CRLF
```

The service discovery request should be used for the first acquisition of the SD&S information and then only when a change is detected in one of the segments.

5.4.2.3 Obtaining the Cell ID via HTTP (Pull mode)

Clause 5.2.13.8 provides description of the Regionalization mechanism and its operation which is relevant to this clause.

For obtaining the Cell ID using the pull mode, the HNED sends a POST message to the URI retrieved from the Regionalization Offering. The body of the POST method shall include the Country Code and all Civic Address information retrieved via DHCP option 99 (see clause 8.1.1.11). The server replies to the HTTP POST with the Cell ID defined for the location.

The Cell ID request shall use the following format:

```
'POST ' path request ' HTTP/1.1' CRLF
  'Host: ' host CRLF
  CRLF
message_body
```

where:

```
request      = 'CellID'.
path         = the absolute path of the URI provided in the Location attribute of the Pull element
               of the Regionalization Offering element (of type OfferingListType, see clause 5.2.12.19), with an
               additional '/' appended at the end if not already present.
host         = the network location (authority) of the URL provided in the Location attribute of
               the Pull element of the Regionalization Offering element (of type OfferingListType, see clause
               5.2.12.19).
message_body = a Cell Request Record element (see clause 5.2.13.12) including the Country Code and
               all Civic Address information retrieved via DHCP option 99 (see clause 8.1.1.11).
```

CountryCode is set to the value retrieved from the DHCP option 99, for example "FR" for France.

The CA elements can be listed in any order, but it is recommended to follow the same order as in the DHCP message.

When the DHCP GEOCONF_CIVIC data have multiple languages set of parameters (CAtype="0"), the HNED shall provide all of them to retrieve the Cell ID.

The body of the response from the HTTP server shall be a Regionalization Offering (see clause 5.2.13.8.1) containing a single Cell element with the resulting Cell ID that the SP has supplied for the location provided by the CAtype values in the request. The HNED should ignore the country code and CA elements possibly provided in the response.

Following is an example where the DHCP GEOCONF_CIVIC option has supplied the location of the HNED as:

- Country code = "FR"
- CAtype = "0", CAvalue = "fr"
- CAtype = "128", CAvalue = "Latn"
- CAtype = "1", CAvalue = "IDF"
- CAtype = "3", CAvalue = "Paris"
- CAtype = "24", CAvalue = "75011"
- CAtype = "132", CAvalue = "private CA parameter"

The resulting request from the HNED is:

```
POST /dvb/sdns/CellID HTTP/1.1
Host: cellid.tv5.fr
Content-type: text/xml
<?xml version="1.0" encoding="UTF-8"?>
<CellRequestRecord xmlns="urn:dvb:metadata:iptv:sdns:2011-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <CountryCode>FR</CountryCode>
  <CA type="0" value="fr">
    <CA type="128" value="Latn">
      <CA type="1" value="IDF">
        <CA type="3" value="Paris">
          <CA type="24" value="75011">
            <CA type="132" value="private CA parameter"/>
```

```

        </CA>
    </CA>
</CA>
</CA>
</CA>
</CellRequestRecord>
```

And the response is:

```

HTTP 200 OK
Content-type: text/xml
Date: "2009-01-26 18:35:39 UTC"
<?xml version="1.0" encoding="UTF-8"?>
<ServiceDiscovery xmlns="urn:dvb:metadata:iptv:sdns:2008-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <RegionalisationDiscovery DomainName="MyDomainName">
        <Cell ID="Paris East"/>
    </RegionalisationDiscovery>
</ServiceDiscovery>
```

5.4.3 Signalling of changes

Changes in the SP offering or the SP discovery information shall be signalled by incrementing the version number of the SP discovery information.

The Service Discovery Information describing the offering of a SP is divided up into segments per type of service discovery information. A change in the offering will translate to a change in the associated segment. Any change in the data carried in a segment shall be signalled by incrementing the segment version of a segment.

The HNED shall monitor the SP discovery record(s) on a regular basis to detect any change in version numbers. Upon detection of a new version of the SP discovery record, the HNED shall check if the SP description needs updating and then shall check if there is any change in the service offering. The HNED will determine which part of the service offering has changed by checking the segment version number of each segment the HNED wants to monitor. The HNED shall then only acquire the segments which have changed.

When using the pull mode, the SP discovery record shall not be checked more than once per Maximum Cycle Time.

In the case where the list of segments is provided in the SP discovery record (mandatory in the "pull" mode, optional in the "push" mode), the addition or removal of segments shall be detected by looking at the list of valid segment Ids for a SP.

When using the "push" mode, in the case where the list of segments is not provided in the SP discovery record and the SP discovery information changes without a change in the offering, it is accepted that the HNED will also check the version number of all the segment Ids it wants to monitor by joining the appropriate multicast address even though there has not been a change in the offering.

In the push mode, in the case where the list of segments is not provided in the SP discovery record, a segment shall be considered as deleted if no packet has been received for this segment for a minimum period of twice the Maximum Cycle Time.

As the DVB-IPTV offering record does not contain any information on the segment it forms (i.e. Segment Id), it is recommended that the HNED should keep a record of the Segment Id together with the relevant DVB-IPTV offering record.

5.4.4 Fragmentation of SD&S Records

5.4.4.1 SD&S Information data types

The following different information types have been specified above; additional information types may be added in the future, or by other standards:

- SD&S information relating to a SP.
- four types of SD&S information relating to the service offering of a SP.
- Broadband Content Guide Discovery record.

- Regionalization Discovery record to provide for local services.
- Firmware Announcement Information to allow for upgrade or changes to HNED firmware.

This is to cover the different types of service offering a SP may have. A SP offering can be made up of Live Media Broadcast services which may not include SI information in the SD&S (i.e. "TS Full SI") or which do include SI information in the SD&S (i.e. "TS Optional SI") records or CoD (via the BCG Discovery record). The SP can also reference services provided by another SP or define a package if it chooses to group several services and present them as a single entity.

These different types of SD&S information shall be identified by an 8-bit value called payload ID, and are defined in ETSI TS 101 162 [2], clause 9.1.2. For information, these values as of the time of publication are listed informatively in Table 12a. Table 12a includes payload IDs used outside of SD&S (e.g. CDS XML download session descriptions, BCG data) which use the same transport mechanisms for XML data (e.g. DVBSTP).

Table 12a: Payload ID values (informative)

Payload ID value	SD&S record carried
0x00	Reserved
0x01	SD&S Service Provider Discovery Information
0x02	SD&S Broadcast Discovery Information
0x03	SD&S COD Discovery Information
0x04	SD&S Services from other SPs
0x05	SD&S Package Discovery Information
0x06	SD&S BCG Discovery Information
0x07	SD&S Regionalization Discovery Information
0x08	FUS Stub file and SD&S RMS-FUS record
0x09	SRM announcement Information
0xA0 to 0xA0	Reserved
0xA1 to 0xAF	BCG Payload ID values defined in [62]
0xB0	Reserved
0xB1	CDS XML download session description
0xB2	RMS-FUS Firmware Update Announcements [78]
0xB3 to 0xBF	Reserved
0xC1	Application Discovery Information
0xC2 to 0xEF	Reserved
0xF0 to 0xFF	User Private

The payload ID values are used in either the DVBSTP protocol defined in clause 5.4.1. or the HTTP mechanisms defined in clause 5.4.2 to signal the type of information conveyed.

5.4.4.2 Fragmentation of SD&S records

The SD&S XML records may be of a substantial size, but only parts of them are needed by an HNED at any one time. Also, changes to the SD&S records may be localized to part of the records. For these reasons segments shall be supported to allow an SD&S record to be managed as a collection of smaller units. Segments are defined in the context of a single type of SD&S information, i.e. segments are defined for a declared payload ID.

Each segment shall be assigned a segment Id to identify a segment of data for the declared SD&S data type (payload ID). The segment Id shall be a 16-bit value. A segment shall be a well formed and valid XML record.

An 8-bit value shall be used to define the current version of a segment, this version shall be keyed on payload ID together with segment Id. Thus when the data within a segment changes, its version number called segment version shall be incremented. The segment versions of the unchanged segments do not need to change. The segment version is modulo 256, and wraps round.

Records containing SP discovery information (i.e. PayloadID 0x01) shall not be segmented when using the "pull mode". In all other cases, the XML records shall be segmented. Note that a record may be divided into a single segment.

Figure 9a illustrates the relationship between segments, payload ID and records.

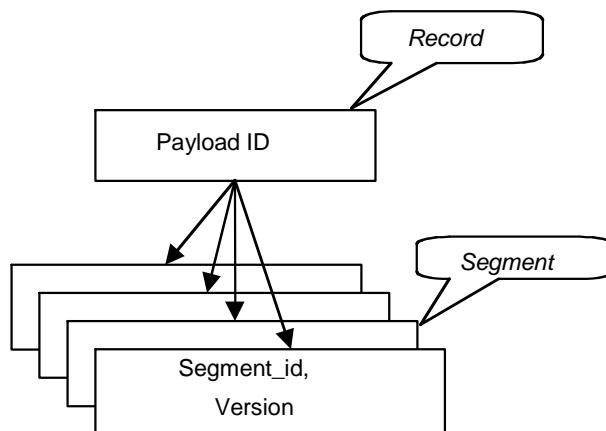


Figure 9a: Relationship between records, payload IDs and segments

5.4.4.3 Maximum cycle time of multicast delivery

The length of time required to transmit all the segments making up the full set of SD&S Information for a SP is called the Cycle Time. The Maximum Cycle Time shall be set to 30 s.

5.4.5 XML records and payload ID

XML records shall be constructed such that each record only contains elements of one of the types from clause 5.2.13. The payloadId field of the multicast protocol header shall be set to reflect the type of record contained within the transmitted multicast packets. Thus any XML record shall contain the root element (ServiceDiscovery) which contains an arbitrary number of only one type of element (e.g. BroadcastDiscovery). For the avoidance of doubt, any XML record shall contain the root element (ServiceDiscovery) which contains only an arbitrary number of BroadcastDiscovery elements, or only an arbitrary number of CoDDiscovery elements, or only an arbitrary number of ServicesFromOtherSP elements, or only an arbitrary number of PackageDiscovery elements, or only an arbitrary number of ServiceProviderDiscovery elements, or only an arbitrary number of BCGDiscovery elements, or only an arbitrary number of RegionalizationDiscovery elements, or only an arbitrary number of RMSFUSDDiscovery elements, or only an arbitrary number of SRMDiscovery elements.

5.4.6 Segmentation of XML records

Records containing SP discovery information (i.e. Payload ID 0x01) shall not be segmented when using the "pull mode".

In all other cases, the XML records shall be segmented, that is divided up into smaller units, to enable easier processing in the HNED, or variable access times. Note that a record may consist of a single segment.

Each segment shall contain a complete root element (ServiceDiscovery) which comprises of an integral number of child elements (e.g. BroadcastDiscovery), as defined in clause 5.2.13 (specifically, a segment shall not contain part of a child element). A segment shall not contain more than one type of child element (i.e. it shall be in accordance with clause 5.4.5).

Each segment shall be valid and well formed.

Each segment shall have a segment ID that is unique within the scope of the SP and the payload ID. For a shared multicast address the SP shall be signalled by the conditional ServiceProviderID field of the DVBSTP header (see clause 5.4.1). For a multicast address carrying only a single SP, this information is inferred from the multicast address. With HTTP, the SP is included in the request (see clause 5.4.2).

Segment Ids need not be contiguous.

Each segment may contain Broadcast Discovery elements or Package Discovery elements for only one package. If the segment is built for a particular package, the referenced package information shall be signalled by the PackageIDRef attribute of the TargetPackage element (see clause 5.2.12.44).

5.5 Encoding

5.5.1 Introduction

SD&S segments may be encoded with BiM [61]. However, the network provider shall also make accessible non-encoded SD&S segments either in the PULL or the PUSH mode, or both, so that HNEDs without a BiM implementation can still obtain non-encoded SD&S segments. In the case where one encoded and one non-encoded multicast stream are delivered, the HNED may discriminate between the streams according to the "compression" flag of the DVBSTP header.

NOTE: If the SP delivers a BCG, then the HNED is expected to support BiM encoding. In this case, it is recommended to use compression of SD&S.

5.5.2 Usage of BiM

5.5.2.1 Introduction

The format is compatible with the BiM format used in ETSI TS 102 323 [59] for the transport of TV-Anytime information.

5.5.2.2 DVB-TVA-Init and InitialDescription

In DVB, the DVB-TVA-init (see table 42 in [59]) is used to configure parameters required for the decoding of the binary Access Units and to transmit the initial state of the decoder (DecoderInit message).

The EncodingVersion parameter in the DVB-TVA-Init shall be set to "0xF0".

In the DecoderInit field, at least one schema URN shall be transmitted. Consequently, the field NumberOfSchemas of the DecoderInit shall be greater or equal to 1 and the field SchemaURI[0] of the DecoderInit shall be set to urn:dvb:metadata:iptv:sdns:2008-1. DVBContextPath of additional schemas are specified by the ContextPathCode in IEC 23001-1 [61].

As each SD&S segment is a valid stand-alone XML document tree, no initial description is required. Therefore, the InitialDescription() field of the DecoderInit message shall be empty.

5.5.2.3 BiM Access Unit

Each SD&S segment is transported in a DVBBiMAccessUnit as defined in ETSI TS 102 323 [59] (clause 9.4.2.3) with the following constraints:

- 1) As each segment is transported independently, NumberOfFUU should be equal to 1.
- 2) The table 55 in ETSI TS 102 323 [59] is updated with the following values.

Value	Description	EquivalentStartType
0x0030	serviceDiscovery	sdns:ServiceDiscovery type

where: sdns = urn:dvb:metadata:iptv:sdns:2008-1.

5.5.2.4 Codec

The BiM decoder used to decode SD&S segments shall use by default the Zlib codec, as defined in TV-Anytime (see clause 4.2.4.4 in ETSI TS 102 822-3-1 [60]), for decoding string data. This will be signalled in the DecoderInit using the ClassificationScheme "urn:tva:metadata:cs:CodecTypeCS:2004" defined in ETSI TS 102 822-3-2 [69].

6 RTSP Client

6.1 Usage of RTSP in DVB

6.1.0 Introduction

In this clause the use of the *Real Time Streaming Protocol* (RTSP) [30] for a playback capable HNED is specified.

NOTE: A recording capable HNED is not specified in the present document.

RTSP is an application-level protocol for control over the delivery of data with real-time properties. Here the use of RTSP for a classical broadcast like type of delivery of video (TV) and audio (radio) as well as for on-demand delivery of video and audio is specified.

6.1.1 Service selection

The Service Discovery and Selection process as described in clause 5 shall provide the HNED with the necessary RTSP information for accessing the RTSP based service in question. Depending on the number of streams composing the service, there can be multiple RTSP URLs in the SD&S record:

- If control URLs are present for FEC streams, then the /BroadcastDiscovery/ServiceList/SingleService/ServiceLocation/RTSPURL is the "aggregate" URL for the entire service except for the retransmission stream. When the service is composed of a single stream, this URL is used for all RTSP messages (SETUP, PLAY, TEARDOWN, etc.). In any case, this URL shall be used for the DESCRIBE message when description retrieval is needed.
- The "control" URLs are used when several streams compose the service. They are used to SETUP each stream separately. They can be used to control (PLAY, PAUSE) each stream separately when needed. They are used to TEARDOWN each stream separately. The control URLs are:
 - RTSPURL@RTSPControlURL: this URL is used to control the main audio-video stream;
 - FECBaseLayer@RTSPControlURL: this URL is used to control the FEC Base layer stream;
 - FECEnhancementLayer@RTSPControlURL: this URL is used to control the FEC Enhancement layer stream;
 - UnicastRET@RTSPControlURL: this URL is used for the RTSP control messages (SETUP) for unicast RET stream.

As an example the HNED listens to a multicast address and port number to get the SD&S description, which is presented to the user and from which subsequently the user can make a selection. When the service is selected, the HNED can use the associated RTSP URL(s) to access the service. The URL(s) indicate whether the session control is based on RTSP. When this is the case, the HNED shall use RTSP to access the service in question.

When the service uses retransmission or AL-FEC, it may be necessary to retrieve additional session description information to setup the session. See clause 6.3.1.

6.1.2 Session transport

DVB compliant HNEDs should use a persistent TCP connection for exchanging RTSP messages with the RTSP server. It is recommended to use a persistent TCP connection; otherwise there is no reliable way for the RTSP server to reach an HNED that is behind a firewall. Persistent TCP connections [39] are used in general to avoid using a separate transport connection for each request/response transaction; this is useful, for example, if the server intends to send asynchronous RTSP ANNOUNCE messages (see Table 13) to the HNED.

Multimedia streams, encapsulated as described in clause 7 and controlled by an RTSP server can be transmitted in either unicast or multicast mode. However, in multicast mode trick mode operation like *pause*, *fast forward* and similar cannot be done.

6.1.3 Service information

The HNED uses service information to inform the user about the kind - and availability of services, to locate and to access them. This information needs to be kept up-to-date.

Where possible, the RTSP server can send asynchronously service information to the HNED by using the ANNOUNCE method (see Table 13). Alternatively, the HNED can poll the server with the aid of a DESCRIBE method (see Table 13) to detect whether the service information is updated. This can be used e.g. in the case a transient connection is used between the HNED and the RTSP server.

When AL-FEC and/or RET is used according to annexes E and F, the session description parameters for LMB services shall be included in the SD&S IPMulticastAddress ServiceLocation type element or/and in the information available via the RTSP URL present in the SD&S RTSPURL ServiceLocation type element; both elements are in the Broadcast Discovery Record.

For LMB services, an RTSP URL may also be available through CRID resolution as described in BCG [62] or alternatively may also be available directly in the ProgramURL element of the tva:ScheduleEvent to confirm XML structure. If present, the CRID resolution is the recommended mechanism.

For CoD and MBwTM services, an RTSP URL shall be used to obtain the session description [62]. This RTSP URL may be available through CRID resolution as described in ETSI TS 102 539 [62] or alternatively may also be available directly in the ProgramURL element of the tva:onDemandProgram XML structure. If present, the CRID resolution is the recommended mechanism.

Whenever an RTSP URL is used by the HNED to retrieve the session description, either for LMB or COD/MBwTM services, the HNED shall issue an RTSP DESCRIBE message to obtain the session description.

The ANNOUNCE and DESCRIBE methods are used for conveying the service information to the HNED.

6.1.4 Security considerations

As the present document is based on RTSP and HTTP, the same security considerations apply as with these protocols (see related RFCs).

NOTE: It was decided not to specify security and authentication for DVB-IPTV Phase 1.

6.2 Profiles

6.2.1 Profile definitions

The present document defines the following three RTSP profiles:

- Live Media Broadcast (LMB).
- Media Broadcast with Trick Modes (MBwTM).
- Content on Demand (CoD).

Each RTSP profile contains a subset of the methods and headers defined in the RTSP protocol. The relationship between the RTSP profiles is such that the "Live Media Broadcast" profile is a subset of the "Media Broadcast with Trick Modes", which is in turn a subset of the "Content on Demand" one.

NOTE: The RTSP profile used depends on the application and on whether the service in question is delivered in unicast or multicast mode. Only the LMB is delivered in multicast mode.

6.2.2 Live media broadcast

The Live Media Broadcast RTSP Profile is characterized as the equivalent of the traditional broadcast like TV and radio. The actual media streams are delivered in multicast mode only. This means that the presentation is linear and that there is no support for trick mode operation like pause, fast forward and similar. The presentation is available as part of a continuous flow of events and not on demand.

6.2.3 Media broadcast with trick modes

The Media Broadcast with Trick Modes RTSP Profile is characterized as the equivalent of the Live Media Broadcast one with the addition of support for trick mode operation like pause, fast forward and similar. Therefore the actual media streams are delivered in unicast mode only. The presentation is available as part of a continuous flow of events. The difference with CoD Profile is that the user cannot initiate it.

6.2.4 Content on Demand (CoD)

The CoD RTSP Profile adds to the Media Broadcast with Trick Modes the ability to initiate the start (and stop) of a presentation as an isolated event. This means that this profile supports pause, fast forward and similar as well as the possibility to access media on a time of the user's choosing. Therefore the actual media streams are delivered in unicast mode only.

6.3 RTSP methods

6.3.0 List of supported RTSP methods

Table 13 specifies the RTSP methods to be supported by the IPI-1 interface for unicast mode of delivery. This applies to MBwTM and CoD profiles.

Table 13: RTSP methods for unicast mode

RTSP Method	Direction: H = HNED; S = Server;	IETF	DVB Requirement
ANNOUNCE	H→S	MAY	MAY
ANNOUNCE	S→H	MAY	SHOULD
DESCRIBE	H→S	SHOULD	SHOULD
GET_PARAMETER	H→S	MAY	SHOULD
GET_PARAMETER	S→H	MAY	MAY
OPTIONS	H→S	SHALL	SHALL
OPTIONS	S→H	MAY	MAY
PAUSE	H→S	SHOULD	SHALL
PLAY	H→S	SHALL	SHALL
REDIRECT	S→H	MAY	SHALL
SETUP	H→S	SHALL	SHALL
TEARDOWN	H→S	SHALL	SHALL

6.3.1 DVB specific usage of RTSP methods

6.3.1.1 ANNOUNCE

The ANNOUNCE method can be used to update asynchronously the service information at the HNED. This can be used for example in a LMB to update the service name.

The DVB RTSP client is required to support the reception of descriptions in XML format. For the broadcast profiles (LMB and MBwTM) the ANNOUNCE method shall contain the BroadcastOffering XML complex structure as described in clause 5.2.13.2. For other, on-demand content, the ANNOUNCE method shall contain the XML complex structure described in Table 11cn and clause 5.2.13.10).

The MIME Type in the Content-Type header (see Table 16) for such message shall be `text/xml` and the content of the Content-Encoding header and XML description shall be UTF-8. See IETF RFC 3023 [45] on XML Media Types.

```
<xsd:element name="CoDAnnounceDescribe">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ContentDescription" type="tva:BasicContentDescriptionType" />
      <xsd:element name="FECInfo" type="dvb14:FECInfoType" minOccurs="0"/>
      <xsd:element name="RETInfo" type="dvb:RETInfoType" minOccurs="0"/>
      <xsd:element name="ServerBasedEnhancementServiceInfo"
type="dvb12:ServerBasedEnhancementServiceInfoType" minOccurs="0"/>
    </xsd:sequence>
```

```

<xsd:attribute name="RTSPControlURL" type="xsd:anyURI" use="optional"/>
<xsd:attribute name="Streaming" type="dvb:StreamingType" use="optional"/>
</xsd:complexType>
</xsd:element>

```

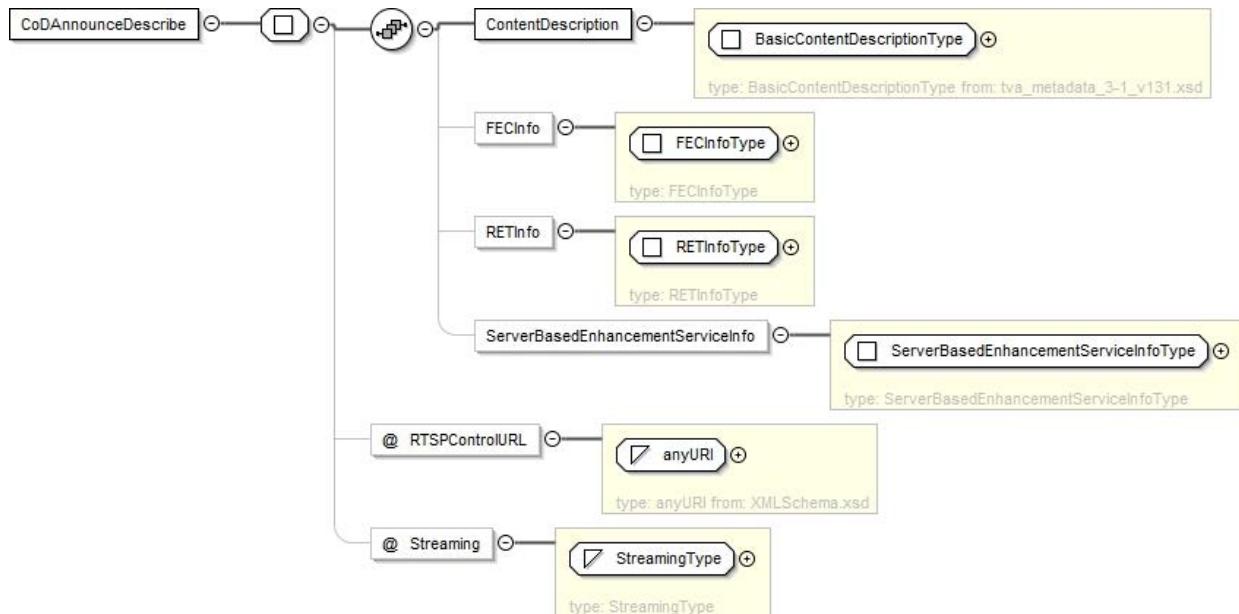


Figure 9b: RTSPAnnounceDescribe

Table 14: RTSPAnnounceDescribe Fields

Name	Semantic Definition	Constraints
<code>ContentDescription</code>	Uses <code>tva:BasicContentDescription</code> , defined in [60]	Mandatory
<code>FECInfo</code>	Uses <code>dvb14:FECInfoType</code> as defined in clause 5.2.12.9.	Mandatory if FEC Enhancement Layer used
<code>RETInfo</code>	Uses <code>dvb:RETInfoType</code> as defined in clause 5.2.12.26, with the following exceptions: <ul style="list-style-type: none"> the MulticastRET element and associated attributes are not defined for CoD RET and shall hence never be present as session information in RTSP Describe response/RTSP announce for CoD service; the following attributes of the RTCPReporting element are not defined for CoD RET and shall hence never be present for CoD service: <code>dvb-enable-bye</code>, <code>dvb-t-wait-min</code>, <code>dvb-t-wait-max</code>, <code>dvb-ssrcbitmask</code>, <code>dvb-rsi-mc-ret</code> and <code>dvb-ssrc-upstream-client</code>; the attribute <code>RTCPReporting</code> @ Destination Address in the context of CoD RET is redefined as: "the IP address to which the HNED shall send its RTCP reports. If provided, this value shall match the IP address of the CoD server (= the IP source address in the original RTP stream packets)"; whenever used in the definitions of the attributes defined-for LMB RET, the expression "LMB RET" shall be replaced with "RET" and the expression "original MC" shall be replaced with "original", when the service offering is a CoD item enhanced with RET. 	Mandatory if RET is available, and <code>ServerBasedEnhancementServiceInfo</code> not present
<code>ServerBasedEnhancedServiceInfo</code>	Based on <code>dvb:ServerBasedEnhancedServiceInfoType</code> as defined in clause 5.2.12.31.	Mandatory if server-based FCC is available
<code>@RTSPControlURL</code>	This element shall be identical to that described in Table 11cn with the addition that unicast sessions using RET aggregate URL is also allowed when session multiplexing is used.	Optional
<code>@Streaming</code>	This attribute shall indicate the streaming format, based on <code>dvb:StreamingType</code> defined in clause 5.2.10, as per the attribute of the same name in Table 11cn.	Optional

Additionally, DVB RTSP client supporting retransmission (RET) according to annex F or server-based FCC according to annex I, should understand session descriptions in SDP format [75]. The MIME Type of SDP descriptions is application/sdp and the SDP description itself also uses UTF-8. The HNED may include application/sdp in the Accept Header to explicitly indicate support for SDP.

6.3.1.2 DESCRIBE

The DVB RTSP client is required to support the reception of descriptions in XML format as supported for the ANNOUNCE method and described in clause 6.3.1.1.

The MIME Type for XML descriptions shall be text/xml and the XML descriptions shall be UTF-8. See IETF RFC 3023 [45] on XML Media Types. The HNED shall always include text/xml when the Accept header is used.

Additionally, DVB RTSP client supporting retransmission according to annex F, should understand session descriptions in SDP format [75]. The MIME Type of SDP descriptions is application/sdp and the SDP description itself also uses UTF-8. The HNED may include application/sdp in the Accept Header to explicitly indicate support for SDP.

6.3.1.3 GET_PARAMETER

The MIME Type in the Content-Type header of a GET_PARAMETER request or response shall be text/parameters and the content of the Content-Encoding header shall be UTF-8.

In the request, each parameter name is followed by a colon ":" and is separated by white space, and may be on separate lines or all on the same line. Parameters in the response are expected to be returned one per line in the form:

```
parameter = name ":" *(VCHAR) CR
```

See also clause 3.3 for correct notation.

Table 15 defines the minimal set of GET_PARAMETER parameters that shall be supported by the IPI-1 interface, in the case the GET_PARAMETER method is supported.

Table 15: GET_PARAMETER parameters

GET_PARAMETER parameter	Result	Description
Stream-state	<current stream state>	This parameter retrieves the current stream state. Possible returned values are: playing paused stopped
position	NPT	This parameter retrieves the current time position in a Cod multimedia session. The position is the number of seconds from the beginning of the multimedia session in NPT format. This can be used for indication by the HNED to the user how far the presentation of the current session has advanced in time. E.g. the result of a GET_PARAMETER request with the parameter "position" can be: position: npt=12:05:35.3- This parameters is undefined for LMB and MBwTM multimedia sessions.

6.3.1.4 SETUP

The HNED should not issue a SETUP request more than once for the same stream or multimedia session before issuing a TEARDOWN request.

6.3.2 Headers

6.3.2.1 RTSP request header fields

Table 16 presents the RTSP header fields that are generated by the HNED and are either mandatory or recommended for the IPI-1 interface.

Table 16: RTSP headers generated by the HNED

RTSP Request Header	IETF	DVB requirement	Remarks on usage for DVB
Accept	MAY	SHOULD	At least the media type: text/xml shall be supported. Other presentation description content types are optional.
Accept-Language	MAY	SHOULD	
Bandwidth	MAY	SHOULD	
Content-Encoding	SHALL	SHALL	
Content-Length	SHALL	SHALL	
Content-Type	SHALL	SHALL	The content types: text/xml and text/parameters shall be supported.
Cseq	SHALL	SHALL	The sequence number shall fit within an unsigned 32-bit number.
Timestamp	MAY	N.A. for LMB SHOULD for CoD	
If-Modified-Since	MAY	SHOULD	
Proxy-Required	SHALL	SHALL	
Range	MAY	SHOULD	
Require	SHALL	SHALL	
Scale	MAY	N.A. for LMB SHOULD for CoD.	At least the following scale factors should be supported: -4: fast rewind -2: rewind 0: pause 1: normal play 2: forward 4: fast forward
Session	SHALL	SHALL	
Transport	SHALL	SHALL	The HNED may supply multiple transport options from which the RTSP server may choose. The HNED shall support RTP/AVP/UDP transport for RTP streaming. It shall support MP2T/H2221/UDP and RAW/RAW/UDP for direct UDP streaming. The following transport configuration parameters should be provided by the HNED to help configuring intermediaries: unicast, multicast and client_port.
User-Agent	MAY	SHOULD	The following format for the User-Agent header is recommended: <code>User-Agent = "User-Agent" ":" deviceID " HNED V1.0"</code> See also clause 3.3. E.g.: User-Agent: <code>PHILIPS-CE/HN3200/A6743ABCD201 HNED V1.0</code>
NOTE 1: The column IETF presents the request headers required to be supported according to the IETF RTSP specification: RFC 2326 [30]. The DVB requirement columns present the request headers required to be supported for DVB.			
NOTE 2: The key words in bold indicate where the DVB specification differs from the IETF.			
NOTE 3: The HNED may generate RTSP request headers that are not listed in Table 16.			

Table 17 presents the RTSP header fields that are supported by the HNED (either mandatory or recommended) on the IPI-1 interface.

Table 17: RTSP headers parsed and understood by the HNED

RTSP Response Header	IETF	DVB requirement	Remarks on usage for DVB
Allow	MAY	SHOULD	
Connection	SHALL	SHALL	
Content-Encoding	SHALL	SHALL	
Content-Language	SHALL	SHALL	
Content-Length	SHALL	SHALL	
Content-Type	SHALL	SHALL	
Cseq	SHALL	SHALL	It is expected that the server generates sequence numbers that fit within an unsigned 32-bit number.
Expires	MAY	SHOULD	
Last-Modified	MAY	SHOULD	
Location	SHALL	SHALL	
Public	MAY	SHOULD	
Range	MAY	MAY	
RTP-Info	SHALL	SHALL for RTP streaming N.A. for UDP streaming	
Scale	MAY	N.A. for LMB SHOULD for MBwTM and CoD.	At least the following scale factors should be supported: -4: fast rewind -2: rewind 0: pause 1: normal play 2: forward 4: fast forward
Retry-After	MAY	SHOULD	
Server	MAY	SHOULD	The content of this header is left to the implementation of the RTSP server.
Session	SHALL	SHALL	It is expected that the RTSP server uses the timeout parameter with this header.
Transport	SHALL	SHALL	RTP/AVP/UDP transport shall be supported for RTP streaming. MP2T/H2221/UDP and RAW/RRAW/UDP shall be supported for direct UDP streaming. Furthermore, the HNED should support (and the server is expected to provide) at least the following transport configuration parameters: unicast, multicast, destination, port, client_port, source and server_port. These parameters can help intermediaries in forwarding the multimedia stream in question.
Timestamp	MAY	SHOULD	
Unsupported	SHALL	SHALL	
NOTE 1: The column IETF presents the response headers required to be supported according to the IETF RTSP specification: IETF RFC 2326 [30]. The DVB requirement columns present the response headers required to be supported for DVB.			
NOTE 2: The key words in bold indicate where the DVB specification differs from the IETF.			
NOTE 3: The HNED may ignore RTSP response headers that are not listed in Table 17.			

6.3.2.2 Transport Header parameters required for direct UDP encapsulation

The following additional "transport-protocol/profile/lower-transport" value sets for the RTSP "Transport:" header are defined for UDP streaming:

- MP2T/H2221/UDP; and
- RAW/RAW/UDP.

This indicates that an MPEG-2 transport stream is used and transported directly over UDP (without RTP).

6.4 Status codes in response to requests

Table 18 lists the RTSP and HTTP status codes that the RTSP enable HNED shall be able to interpret.

Table 18: RTSP response codes

Status Code	Description
200	"OK"
275	"OK - Request forwarded"
300	"Multiple Choices"
301	"Moved Permanently"
302	"Moved Temporarily"
304	"Not Modified"
400	"Bad Request"
401	"Unauthorized"
403	"Forbidden"
404	"Not Found"
405	"Method Not Allowed"
406	"Not Acceptable"
408	"Request Time-out"
410	"Gone"
411	"Length Required"
412	"Precondition Failed"
413	"Request Entity Too Large"
414	"Request-URI Too Large"
415	"Unsupported Media Type"
451	"Parameter Not Understood"
453	"Not Enough Bandwidth"
454	"Session Not Found"
455	"Method Not Valid in This State"
456	"Header Field Not Valid for Resource"
457	"Invalid Range"
459	"Aggregate operation not allowed"
460	"Only aggregate operation allowed"
461	"Unsupported transport"
462	"Destination unreachable"
463	"Destination required"
500	"Internal Server Error"
501	"Not Implemented"
503	"Service Unavailable"
505	"RTSP Version not supported"
551	"Option not supported"

NOTE 1: Particular response codes will be raised with a particular profile only.
 NOTE 2: The HNED shall use the most significant digit of the status code to identify its severity, in the case that the given status code is unknown to the HNED.

6.5 The use of RTSP with multicast

Optionally, it is possible to use RTSP for joining multicasts of Live Media Broadcasts.

NOTE 1: In principle a multicast does not support trick mode operation, therefore it cannot be used with the MBwTM and CoD RTSP profiles.

Using RTSP for joining multicast gives intermediaries the opportunity to inspect the nature of the multimedia session. Specifically, firewalls will be able to ascertain the incoming port being used i.e. this will allow them to open the ports and do any necessary port forwarding. Furthermore, it can be useful if the RTSP server wishes to count the number of receivers "tuned-in".

MLD or IGMP shall be used (next to RTSP) to signal to IP network to forward the multicast in question, when the media streams are delivered in multicast mode. During the set up of the multimedia session, an appropriate message shall be issued by the HNED for joining the given multicast. Furthermore, the HNED shall issue an IGMP LEAVE message (IPv4) or a Multicast Listener Done message (IPv6), when it leaves the multicast.

NOTE 2: It is mandatory that either IGMP version 3 [47] or MLDv2 [118] is used for all such messages on the IPI-1 interface.

The transport configuration parameters: destination and source (see Table 17) shall be used either by IGMP version 3 [47] or MLDv2 [118]. The former shall signal the multicast address, the latter can be used to signal the source address of the multicast for *Source-Specific Multicast* (SSM) (see IETF RFC 3376 [47]).

NOTE 3: IETF RFC 2326 [30] specifies that by default a multimedia stream is delivered in multicast mode, when no indication is given by RTSP whether the mode of delivery is unicast or multicast. See also the transport configuration parameters: unicast and multicast in Table 17.

For multicast mode of delivery, Table 19 presents the RTSP methods to be supported by the IPI-1 interface.

Table 19: RTSP methods for multicast mode

RTSP Method	Direction: H = HNED; S = Server;	DVB Requirement	Remark
ANNOUNCE	H→S	MAY	
ANNOUNCE	S→H	SHOULD	The multicast server can use this method to update asynchronously the service information.
DESCRIBE	H→S	SHOULD	
GET_PARAMETER	H→S	SHOULD	
GET_PARAMETER	S→H	MAY	
OPTIONS	H→S	SHALL	The HNED can use this method to request from the RTSP server which methods it supports.
PAUSE	H→S	N.A.	
PLAY	H→S	SHALL	This method can be used to signal to the intermediaries that the delivery of the multicast is about to start. The Range and Scale request headers should not be used (see Tables 16 and 17).
REDIRECT	S→H	SHALL	The multicast server can use this method for load balancing.
SETUP	H→S	SHALL	This method can be used by the intermediaries to allocate resources, open ports, etc. The SETUP method will have no effect on the multicast RTSP server's state. The server can use this method to count the number of HNEDs "listening".
TEARDOWN	H→S	SHALL	This method can be used by the intermediaries to reverse the effect of the SETUP method i.e. close ports, de-allocate resources, etc. The TEARDOWN method will have no effect on the multicast RTSP server's state. The server can use this method to count the number of HNEDs "listening".
NOTE 1: The keywords in bold indicate where the DVB specification differs from the IETF. NOTE 2: The RTSP methods RECORD and SET_PARAMETER are not supported.			

7 Transport of MPEG-2 TS for real-time services

7.0 Overview

The present document covers the delivery of DVB services over IP networks, as described in clause 4. The initial registration and configuration of the end-device (including IP address assignment), and the means of discovering and choosing a DVB service are covered in other clauses of the present document. This clause concentrates on the format of the service as it appears on the IP network and the requirements on that network for correct and timely delivery of real-time services (Live Media Broadcast and CoD). In accordance with clause 4, clause 7 pertains to the interface IPI-1 of the home network end device.

The present document has been designed to meet the requirements of direct-to-home (DTH) content delivery via IP, as specified in clause 4.

The transport of MPEG-2 TS for non real-time services (CDSs) is covered in clause 10.

7.1 Transport stream encapsulation

7.1.0 General rules

The present document can be used to encapsulate any ETSI TS 101 154 [58] compliant MPEG-2 Transport Stream (MTS), whether containing single or multiple programs. Those transport streams that contain multiple Program Clock References (PCRs) shall, by definition, be constant bitrate streams. Transport streams containing a single clock reference may be constant or variable bitrate.

NOTE: However, in the case of variable bitrate, the bitrate between PCRs is constant as defined by MPEG-2.

The Content Service Provider (CSP) may receive transport streams (e.g. from a satellite feed) that contain multiple programs. The CSP may choose to decompose these transport streams and generate separate single program transport streams (SPTSSs) for each program, or to transmit the Multiple Program Transport Stream (MPTS) in its entirety. This is an operational decision.

All transport streams shall be ETSI TS 101 154 [58] compliant, and shall be encapsulated either in RTP (Real-time Transport Protocol) according to IETF RFC 3550 [21] in conjunction with IETF RFC 2250 [29] or directly in UDP (User Datagram Protocol) according to Recommendation ITU-T H.610 [68].

7.1.1 Real-time Transport Protocol (RTP) encapsulation

7.1.1.0 Real-time Transport Protocol (RTP)

IETF RFC 3550 [21] indicates that RTP should use an even UDP port number, with the corresponding RTCP stream using the next higher (odd) port number.

Each IP packet [11] is made up of the standard IP header, a UDP header, an RTP header and an integer number of 188-byte MPEG-2 transport stream packets. See Figure 10. There is no requirement for every RTP packet in a stream to contain the same number of transport stream packets. The receiver should use the length field in the UDP header to determine the number of transport stream packets contained in each RTP packet.

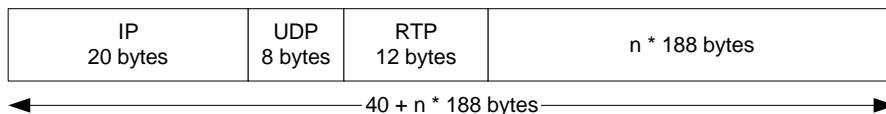


Figure 10: Minimal packet format (IPv4) for RTP encapsulation

The number of transport stream packets that can be encapsulated in each IP packet is limited by the maximum size of the IP datagram (65 535 octets both for IPv4 and IPv6). Care should be taken not to exceed the underlying maximum transmission unit of the network. Exceeding the network's MTU will lead to IP fragmentation, which significantly increases the effective loss rate of a network. This is because if one fragment is lost, the remaining fragments will need to be discarded by the receiver. It also puts additional load on the routers performing fragmentation and on the end-systems re-assembling the fragments.

For any Ethernet-based network, with an MTU of 1 492 bytes (IEEE 802.3 [7] frame with LLC) or 1 500 bytes (IEEE 802.3 [7] frame without LLC, see IEEE 802.3 [7] and IEEE 802.2 [6]), the number of MPEG packets per IP packet should be limited to seven (giving a maximum packet length of 1 356 bytes). Where IP or RTP header options are used the number of MTS packets per IP packet may need to be less than seven to stay within the MTU.

If the RTP payload is set such that fragmentation occurs, any end devices that do not support fragmentation will be unable to receive the stream. It is therefore recommended that CSPs set the DF (Do not Fragment) bit in the IP header. With this bit set, routers will return an ICMP "fragmentation needed and DF set" message if the packet length exceeds the destination network's MTU. The CSP can adjust the payload size if such messages are received. IP (IETF RFC 791 [11]) requires that all hosts shall be prepared to accept datagrams of at least 576 octets.

The CSP may choose not to calculate the UDP checksum and set this value to zero (as per IETF RFC 768 [10]).

The RTP header is shown in Figure 11.

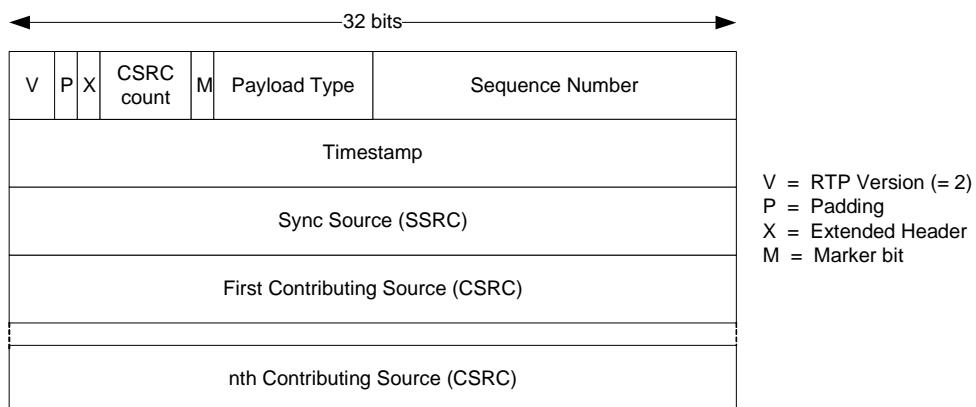


Figure 11: RTP header format

The PT shall be set to MP2T (33), as specified in IETF RFC 1890 [22].

The 16-bit sequence count in the RTP header should be used by the receiver to reorder out-of-order packets, delete duplicates, and detect packet loss.

The 32-bit timestamp in the RTP header is derived from a 90 kHz clock source that may be, but is not required to be, locked to the clock reference of one of the programs in the transport stream. This clock shall conform to the accuracy and slew constraints for MPEG-2 system clocks as defined in ISO/IEC 13818-1 [52].

Other fields are completed as per IETF RFC 3550 [21] and IETF RFC 2250 [29]. Optional CSRC fields should be ignored by the end device.

For most streams, the RTP/UDP/IP overhead of respectively 40 bytes for IPv4 and 60 bytes for IPv6 per RTP packet will be low (for example for IPv4, 3 % with a 1 316 byte payload). Although header compression could be beneficial in certain low bit rate applications, the additional complexity at the receiver is not justified. As such, header compression (such as IETF RFC 2508 [36]) shall not be used.

7.1.1.1 Real-time Transport Control Protocol (RTCP)

The RTP specification defines a second protocol - the Real-time Transport Control Protocol (RTCP). It is intended to provide feedback on the network reception quality from each participant and is also used to enable participants to determine the other participants in a session.

IETF RFC 3550 [21] defines two separate RTCP message sets. RTCP Compound Sender Reports are sent by the sender to each receiver and are used to inform receivers about transmission statistics (number of packets and bytes sent). RTCP Compound Receiver Reports are sent periodically from each receiver back to the sender to inform the sender about reception statistics (e.g. delay and jitter).

The IPI-1 interface shall not generate RTCP (Compound) Receiver Reports, unless the HNED is RET-enabled (see annex F). This decision is based on scalability as for large scale deployments Receiver Reports can generate a large volume of traffic at the sender.

The IPI-1 interface shall accept Sender Reports. CSPs are recommended to send Sender Reports to enable HNEDs to synchronize independent transport streams accurately (for picture in picture or other applications). If CSPs choose to send Sender Reports the time between repeat transmissions shall not exceed 10 s.

For two-way applications the RTCP specification allows senders to include Receiver Report fields within Sender Reports. These fields shall not be included in Sender Reports generated by CSPs.

An HNED may have the capability to receive and decode multiple transport streams simultaneously (picture in picture for example). The problem here is how to synchronize the two streams given that they are independently timed from independent clocks that have arbitrary values. For this application, sender reports should be used to convey the relationship between the RTP timestamp values and real time. Each sender report contains two timestamps taken at the same instance, one of the RTP clock source and the other of the wall clock time as determined by the Network Time Protocol (NTP) [18].

The sender reports allow the end device to calculate at what offset the two streams need to run to keep them in synchronization. The end device does not need to support NTP to synchronize multiple streams. The CSPs should use NTP in order to generate their sender reports. To enable correct synchronization at the receiver, CSPs should synchronize their NTP clocks to within 20 ms of each other (either by deriving them from a common clock or by some other means).

7.1.2 Direct User Datagram Protocol (UDP) encapsulation

In case of managed IP networks that can provide guarantees concerning packet loss, jitter and packet routing (e.g. no packet re-ordering), the transport stream may be directly encapsulated in UDP as defined in Recommendation ITU-T H.610 [68].

Each IP packet [11] is made up of the standard IP header, a UDP header, and an integer number of 188-byte MPEG-2 transport stream packets. See Figure 12. There is no requirement for every UDP packet in a stream to contain the same number of transport stream packets. The receiver should use the length field in the UDP header to determine the number of transport stream packets contained in each UDP packet.

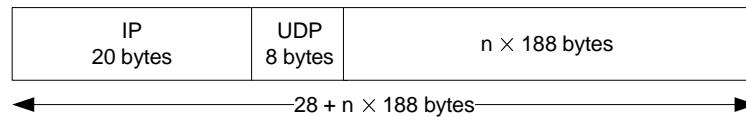


Figure 12: Minimal packet format (IPv4) for UDP encapsulation

The number of transport stream packets that can be encapsulated in each IP packet is limited by the maximum size of the IP datagram (65 535 octets both for IPv4 and IPv6). Care should be taken not to exceed the underlying maximum transmission unit of the network. Exceeding the network's MTU will lead to IP fragmentation, which significantly increases the effective loss rate of a network. This is because if one fragment is lost, the remaining fragments will need to be discarded by the receiver. It also puts additional load on the routers performing fragmentation and on the end-systems re-assembling the fragments.

For any Ethernet-based network, with an MTU of 1 492 bytes (IEEE 802.3 [7] frame with LLC) or 1 500 bytes (IEEE 802.3 [7] frame without LLC, see IEEE 802.3 [7] and IEEE 802.2 [6]), the number of MPEG packets per IP packet should be limited to seven (giving a maximum packet length of 1 356 bytes). Where IP header options are used the number of MTS packets per IP packet may need to be less than seven to stay within the MTU.

If the UDP payload is set such that fragmentation occurs, any end devices that do not support fragmentation will be unable to receive the stream. It is therefore recommended that CSPs set the DF (Do not Fragment) bit in the IP header. With this bit set, routers will return an ICMP "fragmentation needed and DF set" message if the packet length exceeds the destination network's MTU. The CSP can adjust the payload size if such messages are received. IP (IETF RFC 791 [11]) requires that all hosts shall be prepared to accept datagrams of at least 576 octets.

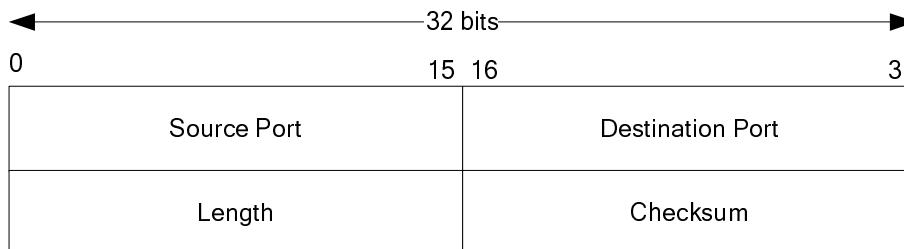


Figure 13: UDP header format

Setting of the source port is optional. If not used the CSP shall set it to zero. The CSP may choose not to calculate the UDP checksum and set this value to zero (as per IETF RFC 768 [10]).

7.1.3 Detection and Usage of RTP and direct UDP encapsulation (Informative)

The use of RTP or direct UDP encapsulation is signalled by SD&S (see clause 5.2.11.4, and definition of Streaming type in clause 5.2.10) for multicast and RTSP (see clause 6.3.2) for unicast streaming. In addition it is possible for a device to detect the use of RTP or direct UDP encapsulation. This shall be done by looking for the value 0x47 in the first byte after the UDP header. In case of direct UDP encapsulation this is the first byte of a 188 byte MPEG-2 TS packet which always has the value 0x47 (synchronization byte of transport stream header). In case of RTP encapsulation this is the first byte of the RTP header. Its value is always different from 0x47. So in case the byte has the value 0x47 then direct UDP encapsulation is used, whilst if it has any other value then RTP encapsulation is used.

7.1.4 Embedded Service Information (SI)

For transport streams with optional SI (TS - optional SI), all MPEG-2 [52] and DVB [1] tables other than those required by ETSI TS 101 154 [58] are optional.

TS - optional SI transport streams are intended for the more advanced situation where the SP wants to present its offering but where it cannot afford or does not want to use bandwidth for usual DVB service description information.

Where transport streams with SI (TS - Full SI) are transported over IP, they shall be compliant with ETSI EN 300 468 [1] and ETSI TR 101 211 [i.1] and contain all necessary DVB SI with the exception of the network information table (NIT). This table may be omitted as it has no meaning in the context of IP services.

7.2 Network requirements

7.2.0 General rules

The IP network shall comply with the mandatory network requirements to guarantee successful delivery and decoding by compliant HNEDs.

7.2.1 Mandatory constraints

7.2.1.1 Packet Jitter

MAXIMUM 40 ms peak-to-peak.

Packet jitter is defined as the variation in delay between the source of the stream and the end device. The peak-to-peak jitter, J , implies that the deviation in network delay, d , is bounded by $-J/2 \leq d \leq +J/2$. To be more precise, the HNED shall comply with the MPEG-2 Real Time Interface Specification (ISO/IEC 13818-9 [53]) with $t_{\text{jitter}} = 20$ ms.

7.2.1.2 Direct User Datagram Protocol (UDP) Packet Reordering

If the HNED is using direct User Datagram Protocol (UDP) then the network shall not allow packet reordering.

7.2.2 Recommended constraints

7.2.2.0 Introduction

The recommended constraints are given for information only. They are provided as typical values that users might consider acceptable. Failure to meet these recommendations will not prevent the system operating successfully, but may significantly degrade the user's experience.

7.2.2.1 Packet loss

MAXIMUM one noticeable artefact per hour.

The IP packet error rate that results in this quality level depends on the transport stream bit rate. For a 4 Mb/s transport stream with seven transport stream packets per IP packet, one error per hour is equivalent to an IP packet error rate of less than 1×10^{-6} .

When AL-FEC and/or RET is used according to annexes E and F then the acceptable IP packet loss rate may be higher.

7.2.2.2 Multicast timing

Leave time: MAXIMUM 500 ms
 Join time: MAXIMUM 500 ms

These constraints are intended to bound the time taken to join and leave multicast groups. The "Leave time" is the maximum time that should elapse between an end device emitting an IGMP multicast LEAVE (IPv4) or a Multicast Listener Done (IPv6) and it receiving any further packets of the associated flow. The "Join time" is the maximum time that should elapse between an end device emitting a multicast Join and the first packet of that flow arriving at the end device.

7.3 Service initiation and control

7.3.0 Introduction

The present document supports the delivery of DVB services either to a single user (using IP unicast), or to many users simultaneously (using IP multicast). These two delivery mechanisms are intended to support different types of service - multicast will be used to deliver "traditional" broadcast DVB services, whereas unicast can be used for personalized DVB services such as video on demand.

7.3.1 Multicast services

Multicast-capable networks will typically restrict the distribution of multicast streams until such time that an end device signals that it is interested in receiving the stream. For such a signalling, the IPI-1 interface shall respectively support IGMP version 3 as defined in IETF RFC 3376 [47] for IPv4 and MLD version 2 as defined in IETF RFC 3810 [118] for IPv6.

IGMP version 3 as well as MLD version 2 add support for "source filtering"; that is, the ability for a system to report interest in receiving packets only from specific source addresses (or from all but specific source addresses) sent to a particular multicast address. This facility eases the allocation of multicast addresses.

To receive a service, the HNED shall perform a group JOIN according to IGMPv3 for IPv4 or a Listener Report according to MLD version 2 for IPv6. The appropriate join message shall include the list of valid source addresses returned by the Service Discovery mechanism if provided.

To terminate reception of a service, the HNED shall perform a group LEAVE according to IGMPv3 for IPv4 or a Listener Done according to MLD version 2 for IPv6.

Services delivered over IP multicast are streamed continuously and do not need to be initiated by each end device. HNEDs can join and leave multicast services simply by issuing the appropriate messages. However, SPs may choose to require the end device to engage in explicit set up and tear down phases (possible reasons include accounting, conditional access, etc.). In such systems, a higher-layer session protocol, such as RTSP, would be used. When a session protocol is used, the messages for joining and leaving a multicast group shall be issued when appropriate (for example when the set up and tear down phases are completed).

7.3.2 Unicast services

Services delivered using IP unicast are intended for a specific user and need to be initiated explicitly by the end device. Once the flow is established, many applications will require stream control from the end device (typically VCR-like controls for a VOD service).

Unicast services will be initiated and controlled using the DVB profile of the Real Time Streaming Protocol (RTSP) as defined in clause 6.

7.4 Quality of Service

In order to provide the required Quality of Service (QoS) MPEG-2 TS real-time streams shall be assigned to the "real-time video bearer" traffic types as defined in clause 11.

8 IP Address allocation and network time services

8.1 IP Addressing and routing

8.1.1 IP Address assignment using IPv4 methods

8.1.1.0 Introduction

The HNED requires one IP address per interface, which will be obtained from a DHCP server. The DHCP server can provide other information as detailed in clause 8.1.1.4.

8.1.1.1 Dynamic Addressing only

The IP address, subnet mask, DNS Server address(es), default gateway, gateway and, if necessary, WINS/NetBIOS servers shall only be allocated dynamically via DHCP.

Static addressing using whatever method is not recommended.

8.1.1.2 Dynamic Host Configuration Protocol (DHCP)

DHCP is defined in a number of RFCs of which the main ones are IETF RFC 2131 [24] and IETF RFC 2132 [25]. The protocol consists of a number of messages that have the same fixed format as shown in Figure 14.

0	7 8	15 16	23 24	31
op	htype	hlen	hops	
xid				
secs		flags		
ciaddr				
yiaddr				
siaddr				
giaddr				
chaddr (16 bytes)				
sname (64 bytes)				
file (128 bytes)				
options (variable)				

Figure 14: DHCP Format

The messages contain a variable size options part that allows the message to carry additional information other than the IP address. The present document divides the specification of the DHCP client in the HNED into the messages and options.

8.1.1.3 DHCP messages

The DHCP client shall support all the messages of IETF RFC 2131 [24] and IETF RFC 2132 [25].

DHCP requires a client identifier which is the MAC address in Ethernet or Ethernet like products (IETF RFC 2131 [24] and IETF RFC 2132 [25]). This identifier shall be unique.

8.1.1.4 DHCP options

8.1.1.4.0 List of (public) DHCP options

The DHCP option number space (1 to 254) is split into two parts. The site-specific option codes (128 to 254) are defined as "Private Use", and are implementation dependent.

The public option codes (0 to 127, 255) are defined by a range of RFCs in addition to IETF RFC 2132 [25] and are detailed in Table 20.

Table 20: DHCP options table

Option description	Reference (IETF RFC 2132 [25] unless otherwise stated)	Option number	Support on IPI-1
Pad Option	3.1	0	Mandatory
Subnet Mask	3.3	1	Mandatory
Time Offset	3.4	2	Optional
Router Option	3.5	3	Mandatory
Time Server Option	3.6	4	Optional
Name Server Option	3.7	5	Optional
Domain Name Server Option	3.8	6	Mandatory
Log Server Option	3.9	7	Optional
Cookie Server Option	3.10	8	Optional
LPR Server Option	3.11	9	Optional
Impress Server Option	3.12	10	Optional
Resource Location Server Option	3.13	11	Optional
Host Name Option	3.14	12	Optional
Boot File Size Option	3.15	13	Optional
Merit Dump File	3.16	14	Optional
Domain Name	3.17	15	Mandatory
Swap Server	3.18	16	Optional
Root Path	3.19	17	Optional
Extensions Path	3.20	18	Optional
IP Forwarding Enable/Dizble Option	4.1	19	Optional
Non-Local Source Routing Option	4.2	20	Optional
Policy Filter Option	4.3	21	Optional
Max. Datagram Reassembly Size	4.4	22	Optional
Default IP TTL	4.5	23	Optional
Path MTU Aging Timeout	4.6	24	Optional
Path MTU Plateau Option	4.7	25	Optional
Interface MTU Option	5.1	26	Optional
All Subnets are Local Option	5.2	27	Optional
Broadcast Address Option	5.3	28	Optional
Perform Mask Discovery Option	5.4	29	Optional
Mask Supplier Option	5.5	30	Optional
Perform Router Discovery Option	5.6	31	Optional
Router Solicitation Address Option	5.7	32	Optional
Static Route Option	5.8	33	Optional
Trailer Encapsulation Option	6.1	34	Optional
ARP Cache Timeout	6.2	35	Optional
Ethernet Encapsulation Option	6.3	36	Optional
TCP Default TTL Option	7.1	37	Optional
TCP Keepalive Interval Option	7.2	38	Optional
TCP Keepalive Garbage Option	7.3	39	Optional
Network Information Service Domain Option	8.1	40	Optional
Network Information Servers Option	8.2	41	Optional
Network Time Protocol Servers Options	8.3	42	Mandatory
Vendor Specific Info	8.4	43	May be used with DSL Forum TR-069 [99] as the RMS.
NetBIOS over TCP/IP Name Server Option	8.5	44	Optional
NetBIOS over TCP/IP Datagram distribution server option	8.6	45	Optional
NetBIOS over TCP/IP Node Type Option	8.7	46	Optional (see clause 8.1.1.4.2)
NetBIOS over TCP/IP Scope Option	8.8	47	Optional (see clause 8.1.1.4.2)
X Window System Font Server Option	8.9	48	Optional
X Window System Display Manager Option	8.10	49	Optional
Requested IP Address	9.1	50	Mandatory
IP Address Lease Time	9.2	51	Mandatory
Option Overload	9.3	52	Mandatory
DHCP Message Type	9.6	53	Mandatory
Server Identifier	9.7	54	Mandatory
Parameter Request List	9.8	55	Mandatory

Option description	Reference (IETF RFC 2132 [25] unless otherwise stated)	Option number	Support on IPI-1
Message	9.9	56	Mandatory
Max DHCP Message Size	9.10	57	Mandatory if DHCP message size exceeds 378 bytes, otherwise Optional
Renewal (T1) Time Value	9.11	58	Mandatory
Rebinding (T2) Time Value	9.12	59	Mandatory
Vendor class identifier	9.13	60	May be used with DSL Forum TR-069 [99] as the RMS.
Client-identifier	9.14	61	Mandatory
Network Information Service+ Domain Option	8.11	64	Optional
Network Information Service+ Servers Option	8.12	65	Optional
TFTP Server Name	9.4	66	Optional
Bootfile Name	9.5	67	Mandatory see clause 9
Mobile IP Home Agent Option	8.13	68	Optional
SMTP Server Option	8.14	69	Optional
POP3 Server Option	8.15	70	Optional
NNTP (News) Server Option	8.16	71	Optional
Default WWW Server Option	8.17	72	Optional
Default Finger Server Option	8.18	73	Optional
Default IRC Server Option	8.19	74	Optional
StreetTalk Server Option	8.20	75	Optional
StreetTalk Directory Assistance Server Option	8.21	76	Optional
User Class	IETF RFC 3004 [43]	77	Mandatory
SLP (Service Location Protocol) Directory Agent	IETF RFC 2610 [38]	78	Optional
SLP Service Scope Option	IETF RFC 2610 [38]	79	Optional
Rapid Commit	IETF RFC 4039 [101]	80	Optional
Client FQDN (Fully Qualified Domain Name)	IETF RFC 4702 [102]	81	Optional
Relay Agent Information	IETF RFC 3046 [46]	82	Optional
iSNS (Internet Storage Name Service)	IETF RFC 4039 [101]	83	Optional
NDS Servers	IETF RFC 2241 [28]	85	Optional
NDS Tree Name	IETF RFC 2241 [28]	86	Optional
NDS Context	IETF RFC 2241 [28]	87	Optional
BCMCS Controller Domain Name list	IETF RFC 4280 [94]	88	Optional
BCMCS Controller IPv4 address option	IETF RFC 4280 [94]	89	Optional
Authentication	IETF RFC 3118 [89]	90	Optional
client-last-transaction-time option	IETF RFC 4388 [95]	91	Optional
associated-ip option	IETF RFC 4388 [95]	92	Optional
Client System Architecture	IETF RFC 4578 [96]	93	Optional
Client Network Device Interface	IETF RFC 4578 [96]	94	Optional
LDAP (Lightweight Directory Access Protocol)	IETF RFC 3679 [100]	95	Optional
UUID/GUID-based Client Identifier	IETF RFC 4578 [96]	97	Optional
User Authentication Protocol List	IETF RFC 2485 [34]	98	Optional
GEOCONF_CIVIC (used for CellID Localization)	IETF RFC 4676 [97]	99	Mandatory
PCode (IEEE 1003.1 [117] TZ String)	IETF RFC 4833 [98]	100	Optional
TCode (Reference to the TZ Database)	IETF RFC 4833 [98]	101	Optional
NetInfo Parent Server Address	IETF RFC 3679 [100]	112	Optional
NetInfo Parent Server Tag	IETF RFC 3679 [100]	113	Optional
URL	IETF RFC 3679 [100]	114	Optional
Autoconfigure	IETF RFC 2563/2.0 [37]	116	Mandatory that this option is not implemented
Name Service Search (Search order)	IETF RFC 2937 [41]	117	Optional
Subnet Selection	IETF RFC 3011 [44]	118	Mandatory
DNS domain search list	IETF RFC 3397 [88]	119	Optional

Option description	Reference (IETF RFC 2132 [25] unless otherwise stated)	Option number	Support on IPI-1
SIP Servers DHCP Option	IETF RFC 3361 [87]	120	Optional
Classless Static Route Option	IETF RFC 3442 [90]	121	Optional
CableLabs Client Configuration	IETF RFC 3495 [91]	122	Optional
GeoConf Option	IETF RFC 3825 [92]	123	Optional
Vendor-Identifying Vendor Class	IETF RFC 3925 [93]	124	Optional
Vendor-Identifying Vendor-Specific	IETF RFC 3925 [93]	125	Optional
PXE Options	IETF RFC 4578 [96]	128,129,1 30, 131,132,1 33, 134 and 135	Optional
End Option	3.2	255	Mandatory

8.1.1.4.1 Max DHCP message size

The maximum DHCP message size option is mandatory when the DHCP message size exceeds 378 bytes, however under 378 bytes it is not required.

8.1.1.4.2 NetBIOS over TCP/IP options

The NetBIOS over TCP/IP options shall be implemented if the HNED requires connectivity to servers that use NetBIOS over TCP/IP. If there is no requirement to connect to a NetBIOS/WINS server then these options shall not be implemented.

8.1.1.4.3 DHCP user class option (RFC 3004 [43])

This shall be implemented in the DHCP client and provision shall be made for multiple user classes. It is not possible for the user to change these class names, however the Remote Management System may add additional class names. Following are the class IDs currently defined.

The class designator should be:

Table 21: Class Designators

Class Name	Description
dvb-ip-stb-video	HNED that is using the IP address for decoding standard DVB video streams
dvb-ip-stb-voice	HNED that is using the IP address for voice over IP
dvb-ip-stb-data	HNED that is using the IP address for non-specific data such as web pages
Vendor defined class names	Subject to registration with DVB

8.1.1.4.4 DHCP relay agent information

There should be no need to implement the DHCP Relay Agent Option (IETF RFC 3046 [46]) in the HNED.

8.1.1.5 DHCP server unavailable

If the remote DHCP server is unavailable for some reason, then products on the home network should still be able to communicate. The method shall use IETF RFC 3927 [49].

8.1.1.6 Multiple DHCP servers

The scenarios currently do not allow multiple DHCP servers on the same home network whether internal or external to the DNG.

8.1.1.7 DNS Server allocation and default gateway

DNS server allocation shall happen via DHCP. A default gateway shall be specified by DHCP.

8.1.1.8 Universal plug and play

Currently there is no need to implement any aspect of Universal Plug and Play in the HNED but it can be added as an option.

8.1.1.9 Server Implementation

If a DHCP server is implemented in an HNED then it shall be possible to enable and disable the server to allow only a single active DHCP server on the network.

8.1.1.10 RTP Retransmission Server Address and future DVB DHCP Extensions

The RTP retransmission server address can be delivered by a DHCP option, however, the available options have been used up, so all future DVB options will be structured as "Vendor-Identifying Vendor Specific Information Options" according to IETF RFC 3925 [93] The Enterprise number assignment for DVB is 2696 (Reference [108]):

<http://www.iana.org/assignments/enterprise-numbers>. The HNED should send the Vendor Identifying Class Option (124) first with the DVB enterprise number assignment (2696) and a vendor-class-data N of 14 resulting in a data-Len of 1.

The HNED, if using the RTP retransmission option and receiving the server address via DHCP, shall receive the Vendor-Identifying Vendor Specific Information Option (125) containing the DVB enterprise number assignment (2696) with a suboption code of 10 and a suboption containing the a comma-delimited list of the IP addresses or URLs of the RTP retransmission servers. The servers shall be in the order of priority from first to last server to connect to. The method for connecting to the server and assuring its operation is vendor specific.

8.1.1.11 Location Parameter for CellID

The location parameter for CellID is obtained using DHCP option 99 as defined in the IETF RFC 4676 [97] GEOCONF_CIVIC. This option allows the DHCP server to supply country and postal address information of the HNED based on the client address (chaddr) of the HNED sent to the DHCP server. The HNED shall use this option and the DHCP server shall supply the appropriate civic address elements for CellID to work.

Figure 15 shows the format of the GEOCONF_CIVIC option. The "what" field shall have a value of "2" and the country code shall represent the country of location of the HNED.

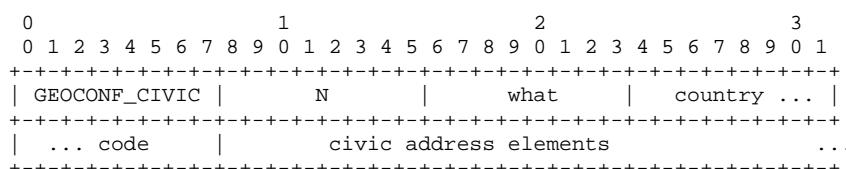


Figure 15: GEOCONF_CIVIC Format

A postal address consists of several parts which vary by country hence the option divides them up into different fields with an index known as the CAtype (see Table 22). The HNED shall be able to accept any of the CAtypes including the private information fields. It is recommended that where a postal/zip code provides sufficient location information that this should be used. All fields shall be encoded in UTF-8. The CAtype list should in numerical order.

If a Network SP would like to use some other civic address element to indicate location, for example the name of the DSLAM, then it shall use a CAtype outside of the range 0 to 128 for proprietary purpose with the appropriate value.

The contents of the civic address elements, once received by the HNED from the DHCP server, are then used to obtain the CellID by either sending them to the SD&S server (see clause 5.4.2.3) or by matching against the SD&S provided table (see clause 5.2.13.8).

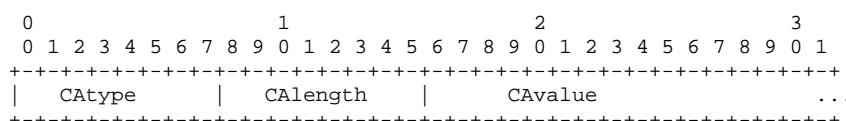


Figure 16: Civic Address Elements

Table 22: Example of Some Civic Address Types (CAtype)

CAtype	NENA	PIDF	Description	Examples
0			Language	i-default
16	PRD	PRD	leading street direction	N
17	POD	POD	trailing street suffix	SW
18	STS	STS	street suffix or type	Ave, Platz
19	HNO	HNO	house number	123
20	HNS	HNS	house number suffix	A, 1/2
21	LM	LMK	landmark or vanity address	Columbia University
22	LOC	LOC	additional location information	South Wing
23	NAM	NAM	name (residence and office occupant)	Joe's Barbershop
24	ZIP	PC	postal/zip code	10027-1234
25			building (structure)	Low Library

8.1.2 IP address assignment using IPv6 methods

8.1.2.0 Introduction

The HNED requires one IP address per interface which can either be obtained by using the SLAAC method of IPv6 for autonomously generating global IPv6 addresses or from a DHCPv6 server in a way that is functionally comparable to the address assigning described in clause 8.1.1. The DHCPv6 server can also provide other information as detailed in clause 8.1.2.4.

8.1.2.1 Dynamic addressing only

The IP address, the subnet mask, DNS server addresses, gateway addresses etc. shall be allocated dynamically.

8.1.2.2 Unicast IP address assignment using SLAAC

SLAAC (Stateless Address Autoconfiguration) is an IPv6 method in which the HNED is assigned a 64-bit prefix of the IPv6 address (also called the subnet prefix) by the DNG, and then the last 64 bits of the HNED's IPv6 address (also called the interface ID) are derived with help of Extended Unique Identifier (EUI-64) process which ensures that the autoconfigured IPv6 address is unique on a global level. The steps the HNED shall follow to achieve a stateless autoconfiguration are described in IETF RFC 4862 [120].

The assignment of the 64-bit prefix by the DNG shall be done using the message format as described in clause 4.6.2 of IETF RFC 4861 [121]. By implementing the 64-bit EUI-64 format, the HNED can automatically assign itself a unique 64-bit IPv6 interface identifier without the need for manual configuration or DHCP. This is accomplished on Ethernet interfaces by referencing the already unique 48-bit MAC address, and reformatting that value to match the EUI-64 specification. The creation of the EUI-64 based interface ID shall follow one of the approaches specified in IETF RFC 3513 [129].

8.1.2.3 IP address assignment using Dynamic Host Configuration Protocol Version 6 (DHCPv6)

The assignment of IP addresses to the HNED can also be achieved by using DHCPv6. It enables the DNG to act as a DHCP router and to pass configuration parameters such as IPv6 network addresses to the HNED. This method offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol which is specified in IETF RFC 3315 [122] is the stateful counterpart to the SLAAC method of IETF RFC 4862 [120].

The protocol consists of a number of messages. These messages contain a variable size options part that allows the message to exchange specific information between the HNED and the DHCP server. All DHCP messages possess a fixed format header and a variable format area for options as shown in Figure 16a.

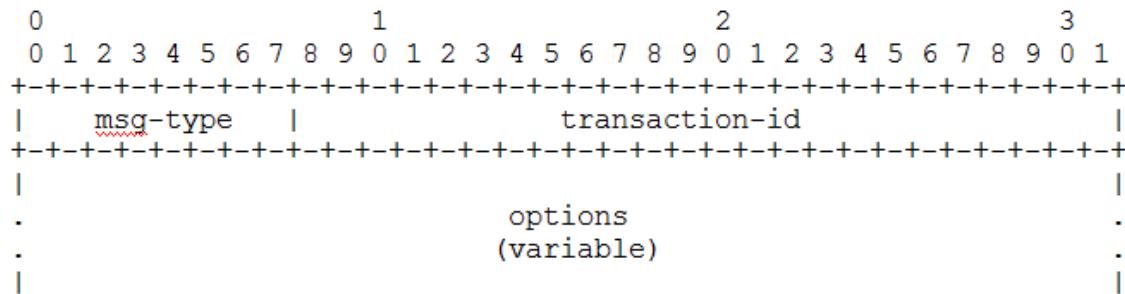


Figure 16a: Format of a DHCPv6 message

- msg-type: Identifier for the DHCP message type as specified in clause 5.3 of IETF RFC 3315 [122].
- transaction-id: Transaction-ID for the message exchange.
- options: Options carried in this message.

In order to guarantee an unambiguous message exchange between the HNED and the DHCP server, each device identifies itself by the help of a DHCP Unique Identifier (DUID). Several possibilities to create such DUIDs are described in clause 9 of IETF RFC 3315 [122]. The HNED shall support all the messages specified in IETF RFC 3315 [122].

The way the HNED locates the DHCP server and the set-up of the message exchange between these two devices in order to assign IP addresses and other types of information to the HNED shall follow the steps as described in clause 17 of IETF RFC 3315 [122].

The DHCPv6 options are spread over several RFC documents. For those IPv4 options the support of which is marked as "Mandatory" in Table 20, the following Table 22a contains information about their functional IPv6 counterpart. Some options can contain other options, in which case the options contained in that option have meaning only for the option they are contained in. As a result of the IPv6 protocol architecture not all of the DHCPv4 options were mapped into appropriate DHCPv6 options as mentioned in the last column of Table 22a. For the reader's convenience the rows of this table are listed in increasing order of DHCPv4 option numbers.

Table 22a: List of mandatory DHCPv4 options and their synonyms using IPv6 methods

Option No. DHCPv4	Name	DHCPv6 Description (unless otherwise stated)	DHCPv6 / ICMPv6
0	Pad Option	DHCPv4: Causes the subsequent fields to align on word boundaries.	Not necessary because options are serially stored with no padding in between (see section 6 of IETF RFC 3315 [122]).
1	Subnet Mask	DHCPv4: Client's subnet mask, as per IETF RFC 950 [126]. If both the Subnet Mask and the Router option are specified in a DHCP reply, the Subnet Mask option shall be first.	IETF RFC 3633 [127] in combination with IETF RFC 3315 [122] (Option 6)
3	Router Option	DHCPv4: List of IP addresses for routers on the client's subnet. Routers should be in order of preference.	Not necessary because the client contacts routers via multicast address.
6	Domain Name Server Option	List of Domain Name System servers available to the client. Servers should be in order of preference.	IETF RFC 3646 [124] (Option 23)
15	Domain Name	Domain name that the client should use when resolving host names through the Domain Name System.	IETF RFC 3646 [124] (Option 24)
42	Network Time Protocol Servers Option	List of IP addresses indicating NTP servers that are available to the client.	IETF RFC 5908 [130] (Option 56)

Option No. DHCPv4	Name	DHCPv6 Description (unless otherwise stated)	DHCPv6 / ICMPv6
43	Vendor Specific Info	This option is used by clients and servers to exchange vendor-specific information. The information is interpreted as vendor-specific code on the clients and servers. DVB: May be used with DSL Forum TR-069 [99] as the RMS.	IETF RFC 3315 [122] (Option 17)
50	Requested IP Address	Used in a client request to allow the client to request that a particular IP address be assigned.	IETF RFC 3315 [122] (Option 5)
51	IP Address Lease Time	Used in a client request to allow the client to request a lease time for the IP address. In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.	IETF RFC 3315 [122] (Option 5)
52	Option Overload	DHCPv4: Indicates that the DHCP name or file fields are being overloaded by using them to carry DHCP options. A DHCP server inserts this option if the returned parameters will exceed the usual space allotted for options.	No synonym in IPv6
53	DHCP Message Type	DHCPv4: Used to convey the type of DHCP message.	Replaced by DHCP Message Types as listed in section 24.2 of IETF RFC 3315 [122]
54	Server Identifier	Used for identifying a server in a message exchange between a client and a server.	IETF RFC 3315 [122] (Option 2)
55	Parameter Request List	Used by a DHCP client to request values for specified configuration parameters.	IETF RFC 3315 [122] (Option 3)
56	Message	DHCPv4: Used by a DHCP server to provide an error message to a DHCPclient in a DHCPNAK message in the event of a failure.	Replaced by status codes in DHCPv6, see section 24.4 in IETF RFC 3315 [122] in combination with Option 13
57	Max DHCP Message Size	DHCPv4: Maximum length DHCP message that a server is willing to accept. The length is specified as an unsigned 16-bit integer. A client can use the maximum DHCP message size option in DHCPDISCOVER or DHCPREQUEST messages, but should not use the option in DHCPDECLINE messages.	No synonym, there is no message size limitation for IPv6.
58	Renewal (T1) Time Value	Time interval at which the client contacts the server from which the IP addresses were obtained to extend the lifetimes of the addresses.	IETF RFC 3315 [122] (Option 3)
59	Renewal (T2) Time Value	Time interval at which the client contacts any available server to extend the lifetimes of the IP addresses	IETF RFC 3315 [122] (Option 3)
60	Vendor Class Identifier	Used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. Vendors can choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.	IETF RFC 3315 [122] (Option 16)
61	Client identifier	Used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings.	IETF RFC 3315 [122] (Option 1)

Option No. DHCPv4	Name	DHCPv6 Description (unless otherwise stated)	DHCPv6 / ICMPv6
67	Bootfile URL	Identifies a bootfile location for network booting of the DHCP client.	IETF RFC 5970 [128] (Option 59)
77	User Class	This option is used by a DHCP client to optionally identify the type or category of user or applications it represents. A DHCP server uses the User Class option to choose the address pool it allocates an address from and/or to select any other configuration option.	IETF RFC 3315 [122] (Option 15)
99	GEOCONF_CIVIC	Used for CellID location DVB: See section 8.1.1.11.	IETF RFC 4776 [123] (Option 36)
116	Autoconfigure	Mandatory that this option is not implemented.	No one-to-one counterpart. The possibilities are signaled by the M and O flags in the ICMPv6 Router Advertisement (section 4.2 of IETF RFC 4861 [121])
118	Subnet Selection	DHCPv4: The option contains a single IPv4 address that is the address of a subnet. The value for the subnet address is determined by taking any IPv4 address on the subnet and ANDing that address with the subnet mask. This value is sent to the DHCP server asking for an IP address on this subnet.	No one-to-one counterpart. ICMPv6 Router Advertisements carry prefixes for a link, no need for a subset mask
255	End Option	DHCPv4: This option is a single octet of decimal 255 ("FF") used to indicate the end of a DHCP options area in DHCP message packets.	Not necessary because the length of the option data field is signaled

8.1.2.4 Implementation details for IPv6 functionalities

8.1.2.4.0 Introduction

The descriptions collected in this clause relate to the IPv6 methods introduced in clause 8.1.2.2 and in clause 8.1.2.3 and give more detailed information about the implementation of methods and DHCPv6 options. In this clause the term "DHCP" refers to the Dynamic Host Configuration Protocol for IPv6.

DHCPv6 messages are exchanged over UDP port 546 and 547. Clients listen for DHCP messages on UDP port 546 while servers listen for DHCP messages on UDP port 547.

8.1.2.4.1 Maximum DHCP message size

For DHCPv6 messages there is no limitation of the message size.

8.1.2.4.2 NetBIOS over TCP/IP options

These options are no longer supported.

8.1.2.4.3 DHCP user class option (IETF RFC 3315 [122])

This option shall be implemented in the HNED and provision shall be made for multiple user classes. It shall not be possible for the user to change these class names, however the service provider's management system may add additional class names. The class names currently defined are listed in Table 21.

8.1.2.4.4 DHCP relay agent information

There should be no necessity to implement DHCP Relay Agent Messages (see IETF RFC 3315 [122]) in the HNED.

8.1.2.4.5 DHCP server unavailable

If the remote DHCP server is unavailable for some reason, the devices on the home network should still be able to communicate to each other in case they are connected to the same link. The devices shall use the method as described in IETF RFC 4862 [120].

8.1.2.4.6 Multiple DHCP servers

In an IPv6 environment the HNED can communicate to all link-scoped DHCP servers using the well known multicast address FF02::1:2. The procedure shall follow the steps as described in clause 17 of IETF RFC 3315 [122]. The HNED sends out a Solicit message and waits for the reception of any Advertise message. Upon receipt of one or more Advertise messages, the HNED starts a selection process for one DHCP server for further communication.

An HNED may also send messages directly to a dedicated server using unicast. This method is described as option 12 of IETF RFC 3315 [122].

8.1.2.4.7 DNS Server allocation and default gateway

DNS server allocation shall happen via DHCPv6 option 23 as described in IETF RFC 3646 [124]. In a list of DNS IPv6 addresses the first entry shall specify the default gateway for the HNED to use.

8.1.2.4.8 Universal plug and play

Currently there is no need to implement any aspect of Universal Plug and Play in the HNED but it can be added as an option.

8.1.2.4.9 Server implementation

If a DHCP server is implemented in an HNED then it shall be possible to enable and disable the server to allow only one single active DHCP server on the network.

8.1.2.4.10 RTP Retransmission Server address and future DVB DHCP extensions

The RTP retransmission server address as well as other future DVB options can be delivered by the use of two DHCPv6 options, option 16, the Vendor Class Option and option 17, the Vendor-specific Information Option. Both options make use of an enterprise number in order to assign a vendor to the data transported in these options. The enterprise number assignment for DVB is 2696 (Reference [108]): <http://www.iana.org/assignments/enterprise-numbers>.

As a first step the HNED should send the Vendor Class Option (option 16) with the DVB enterprise number assignment (2696) and a vendor-class-data N of 14 resulting in a vendor-class-len value of 2.

The HNED, if using the RTP retransmission option and receiving the server address via DHCPv6, shall receive the Vendor-specific Information Option (option 17) containing the DVB enterprise number assignment (2696) with an opt-code value code of 10 and an option-data area containing the comma-delimited list of the IP addresses or URLs of the RTP retransmission servers. The servers shall be listed in the order of priority from first to last server to connect to. The method for connecting to the server and assuring its operation is vendor specific.

8.1.2.4.11 Location parameter for CellID

The location parameter for CellID is obtained by using DHCPv6 option 36, GEOCONF_CIVIC, as defined in IETF RFC 4776 [123]. This option allows the DHCP server to supply country and postal address of the HNED based on the client address of the HNED. The HNED shall use this option and the DHCP server shall supply the appropriate civic address elements for CellID to work.

Figure 16b shows the format of the GEOCONF_CIVIC option for DHCPv6. The "what" field shall have a value of "2" and the country code shall represent the country of location of the HNED.

```
0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      OPTION_GEOCONF_CIVIC      |      option-len      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      what      |      country code      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
.                           civic address elements
.
.
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Figure 16b: GEOCONF CIVIC format for DHCPv6

A postal address consists of several parts which vary by country hence this option divides them up into different fields with an index known as the CAtype (see Table 22). The HNED shall be able to accept any of the CAtypes including the private information fields. It is recommended to use the a postal/zip code where this provides sufficient information for location. All fields shall be encoded in UTF-8. The CAtype list should be in numerical order.

If a network or service provider would like to use some other civic address elements to indicate location, for example the name of the DSLAM, then it shall use a CAtype outside of the range 0 to 128 for proprietary purpose with the appropriate value.

The contents of the civic address elements, once received by the HNED from the DHCP server, are then used to obtain the CellID either by sending them to the SD&S server (see clause 5.4.2.3) or by matching the location information against the table as provided by SD&S (see clause 5.2.13.8).

8.2 Network time services

8.2.0 Network time services types

The HNED will require network time services for a real-time clock, logging and optionally for the transport stream. These services divide into two:

- 1) Network time services for applications such as a real-time clock with accuracy of 100 ms.
 - 2) Network time services for the transport stream with accuracy better than 50 ms.

It should be noted that both services can be implemented using the same time server.

It may be desirable to implement a secure real-time clock mechanism for security reasons, in which case section 15 of IETF RFC 5905 [23] should be applied.

8.2.1 Real-Time Clock or other applications with an accuracy of 100 ms

The real time clock in the HNED should be implemented using the Simple Network Time Protocol (SNTP) defined in section 14 of IETF RFC 5905 [23], Network Time Protocol Version 4.

8.2.2 Accurate time services

Network Time Protocol (Version 4) as detailed in IETF RFC 5905 [23] should be implemented when time services with an accuracy of 1 ms to 50 ms are needed.

For example, a clock with such accuracy may be required when decoding content encapsulated in a transport stream.

8.2.3 Time server address discovery

The HNED shall look for the time server addresses in the priority order defined below:

- 1) Provided via the Network Time Server DHCP option (42).
- 2) Optionally, pre-defined by the manufacturer.

NOTE: It should be noted that using public NTP time servers will result in huge overhead on these servers; instead it is recommended to use dedicated NTP time servers.

9 File Upload System Stub (FUSS) to Enable Optional Updates of the System Software of an HNED

9.0 Introduction

This clause replaces the clause "Identification Agent for the transport of DVB Services over IP based networks" in the versions of the present document prior to release 1.4.1. It is intended to work with the updated and separate "Remote Management and Firmware Update System for DVB-IPTV Services" [78] to allow the system software of an HNED to be updated on a power-cycle or reboot. The updating of the system software after power-cycle or reboot will be handled by the mechanisms in the optional "Remote Management and Firmware Update System for DVB-IPTV Services" specification [78].

The FUSS shall be supported in every HNED and its use is mandatory, however, downloading and replacement of the system software pointed to by the stub, whilst strongly recommended, should only be done once vendor specific security measures have been passed.

The procedure to upgrade the firmware of the HNED consists of 4 steps:

- 1) Obtaining the Stub File either via unicast or multicast. The filename in the unicast case is always "dvb-ipi-fus-stub.dvb".
- 2) Examination of the Stub File to find possible upgrade candidates.
- 3) (optional) Downloading the upgrade.
- 4) (optional) Execution of vendor supplied security measures and replacement of current firmware.

9.1 Obtaining the Stub File

9.1.0 Acquiring Stub File location

On start-up of the device, the device shall find out a URL or IP address for the stub file in the following priority with the following methods:

- 1) Check the DHCP next server "*siaddr*" field. If "*siaddr*" contains a valid unicast IP address then the device shall obtain the stub file using HTTP(S) with the URL: http(s)://*siaddr*/dvb-ipi-fus-stub.dvb. If "*siaddr*" contains a valid multicast address then the device shall obtain the file using DVBSTP as described below.
- 2) If the "*siaddr*" field is set to 0 or is an invalid IP address then the device shall check the bootfile DHCP option (67). The bootfile option shall contain the fully qualified URI for the file which should use HTTP(S) for unicast as in method 1 above, or can contain a single multicast IP address for downloading using DVBSTP as described below. If there are filenames or URIs without the dvb extension then they shall be skipped. If there are multiple URIs with the extension dvb then they shall all be tried in no particular order.
- 3) If there is no bootfile name or IP address in the bootfile option then the device shall listen to a globally reachable and public IGMPv3/SSM address of 232.255.255.254 as defined for IPv4 in IETF RFC 3171 [i.3]. For IPv6, the device shall listen to a globally reachable and public SSM address of FF3F::FFFF:FFFE as defined in IETF RFC 3306 [i.10]. The HNED shall listen for DVBSTP for a maximum of 10 s on this address.
- 4) The device manufacturer has the option of hard coding a URL or IP address into the box for use with HTTP or DVBSTP.

9.1.1 Using DVBSTP to Obtain the Stub File via Multicast

Once the multicast address has been obtained, the HNED shall listen on the multicast address on the port number 3937 (dvbservdsc) as assigned by IANA. The HNED listens for payload ID 0x08 and Segment ID 0x00 to find the payload containing the Stub File. It uses the ServiceProviderID, if present, to select whether the Stub File is meant for this HNED.

Clause 5.4.1 describes the use of DVBSTP for obtaining SD&S data. The use of the semantics in clause 5.4.1.2 shall be followed with the exceptions below:

Compression (Compr): The FUS Stub file should be fairly small so it should have no need to be compressed, thus this value shall be 000.

ProviderID Flag (P): This flag signals if the ServiceProviderID field is present in SD&S but in FUSS indicates whether multiple FUS Stub providers are being used. The value "1" defines the presence of the ServiceProviderID field in the header and that the SP is multicasting multiple FUS Stub Files to the HNEDs. The setting of the ProviderID Flag and use of the SP ID is optional.

ServiceProvider ID: A 32-bit number that is used to identify the FUS Stub provider without examining the payload. The 32-bit number shall be formed from the 24-bit ManufacturerOUI with the remaining 8-bits set to 0 to be reserved for later usage. The HNED shall check the ServiceProviderID if the ProviderID flag is set to 1, and shall then compare the lower 24-bits of the content of the ServiceProviderID to its ManufacturerOUI. If the ServiceProviderID is the same as its ManufacturerOUI then the DVBSTP payload should be taken, otherwise the whole DVBSTP message should be ignored as it is for a different type of HNED and the HNED should return to examining the multicast traffic.

CRC: The optional 32-bit CRC should be used if there is no Manifest header within the payload. The standard CRC from ISO 13818-1 [52], annex A, shall be used. It shall be applied to the payload data of all sections comprising a segment. This field is not necessarily aligned with a 32 bit boundary.

9.1.2 Using HTTP(S) to Obtain the Stub File via Unicast

9.1.2.0 HTTP(S) mechanism

The unicast address for the FUS Stub file may be provided in the "siaddr" field of the DHCP message:

- If the siaddr carries a valid unicast IP address and the HNED carries a certificate to support the SSL/TLS operation, the FUS Stub File may be obtained using the URL: <https://siaddr/dvb-ipi-fus-stub.dvb> based on the "siaddr" supplied. TLS is specified in IETF RFC 2246 [106] and its association with HTTP in IETF RFC 2818 [107].
- If the siaddr carries a valid unicast IP address and no certificate is present or the HTTPS is unsuccessful the operation should be repeated using the URL: <http://siaddr/dvb-ipi-fus-stub.dvb>.

Alternatively the fully qualified HTTP or HTTPS URI of the FUS Stub file may be carried in DHCP option 67 in the "bootfile name", e.g. https://10.1.5.51/stub_repository/dvb-ipi-fus-stub.dvb".

9.1.2.1 HTTP Congestion avoidance mechanism

A congestion avoidance mechanism is required in case of a power cut or other failure that causes a large number of HNEDs to send data at startup so overloading the FUS servers.

Each time the HNED attempts to contact the HTTP(S) server, a Backoff timer shall be initialized to a value of 2 seconds. Immediately before each attempt to establish a connection, a random delay of between Backoff and $2 \times$ Backoff seconds shall be imposed. Upon failure to establish this connection, the Backoff timer shall be doubled and the connection will be retried. When doubling of the Backoff timer results in an arithmetic overflow (just before the 16th attempt when Backoff is a 16 bit unsigned integer), retry attempts should be abandoned.

9.2 Stub File Format

The Stub File format is a simple text like format that is simple to parse and compact. The contents are a subset of the metadata defined in annex B of "RMS Remote Management and Firmware Update System for DVB-IPTV Services" [78]. It may either be sent in compact or long form. The compact form uses the "Coding" representation while the long form uses the full names enclosed in "[" for easier human reading. All files have a header "[_DVB-STUB-HEADER-v1.0].

The compact form represents the elements by a coding number shown in Table 23 which have an "=" appended and then the value. The elements shall be separated by a ";" character, and if any ";" characters occur in the strings they shall be expressed as escape values.

Example of long form:

[_DVB-STUB-HEADER - v1.0]

[DeviceClassInfo]
 ManufacturerOUI = 4567
 ProductClass = "Fred"
 HardwareVersion = "1.01"
 SoftwareVersion = "2.003"
 SignedPackage = 0

[SoftwarePackageInfo]
 Packagename = "Fred"
 Packagesize = 12345
 FootprintSizeVolatile = 5000000
 FootprintSizeNonVolatile = 25000000
 SignedPackaged = 0

[ResourceAccessInfo]
 URL=http://download.cisco.com/STB-Software/fred1001.bin

Example of same long form information in the compact form:

[_DVB-STUB-HEADER - v1.0]

1a=4567;1b="Fred";1c="1.01";1d="2.003";2a="Fred";2b=12345;2c=5000000;2d=25000000;
 2e=0;3a=http://download.cisco.com/STB-Software/fred1001.bin.

The URI can be used two ways:

- 1) **Unicast only:** This may point directly to a file image for downloading from the FUS directly.
- 2) **Multicast and Unicast:** This can point to a pointer message in the multicast announcement service or to the description announcement message sourced from the FUS which identifies the download.

If the final image file is to be made up of several component files, the URL shall point to the description announcement message sourced from the FUS, either directly or through a pointer.

Table 23: Stub File Format Elements

Element description		Coding	Type	Mandated/ Optional/ Conditional	Description
DeviceClassInfo	ManufacturerOUI	"1a="	24 bit number	M	Organizationally unique identifier of the device manufacturer. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros. The value shall be a valid OUI as defined in IETF.

Element description		Coding	Type	Mandated/ Optional/ Conditional	Description
	ProductClass	"1b="	String	O	Identifier of the class of product for which the serial number applies. That is, for a given manufacturer, this parameter is used to identify the product or class of product over which the SerialNumber parameter is unique.
	HardwareVersion	"1c="	String	O	A string identifying the particular CPE hardware model and version.
	SoftwareVersion	"1d="	String	O	A string identifying the software version. To allow version comparisons, this element should be in the form of dot-delimited integers, where each successive integer represents a more minor category of variation. For example, 3.0.21 where the components mean: Major.Minor.Build.
SoftwarePackageInfo	PackageName	"2a="	String	O	Opaque string with no specific requirements for its format. The value is to be interpreted based on the HNED's vendor-specific package naming conventions.
	PackageSize	"2b="	Long integer (bytes)	O	The size of the package in bytes.
	FootprintSizeVolatile	"2c="	Long integer (bytes)	O	Required available size of installed image in memory e.g. RAM that is erased at power-off or reboot.
	FootprintSizeNonVolatile	"2d="	Long integer (bytes)	O	Required available size of installed image in memory e.g. Flash that is kept after power-off or reboot.
	SignedPackaged	"2e="	Boolean (0 or 1)	O	Switch indicating that a manifest is used - 0 = false, 1 = true, for the file reached by the URL below.

Element description		Coding	Type	Mandated/ Optional/ Conditional	Description
ResourceAccessInfo	URL	"3a="	IPv4 URI	M	This URI may identify: <ul style="list-style-type: none">• The location of a unicast download• The "dvb-mcast" URI (defined in clause G.3) for the multicast pointer or announcement message,• Multicast address for the multicast pointer or announcement message; in this case the "Protocol" field below shall be used.
	Protocol	"3b="	Integer	M for multicast except when "dvb-mcast" URI used	The multicast protocol used for the IP address given by the URL. See Table 24. It is not required if the "ResourceAccessInfo" field above provides "dvb-mcast" URI defined in clause G.3 but it shall be present if the "ResourceAccessInfo" field above provides the multicast address only.

Where a multicast service is identified, the use of the "dvb-mcast" URI form of the URL is recommended over the use of the multicast address/protocol fields. The "dvb-mcast" URI is defined in clause G.3.

Table 24: ResourceAccess Info Protocol

Description	Value
SAP	1
DVBSTP	2
Flute	3
DSMCC	4

10 Content Download Service (CDS)

10.1 Overview

CDSs allow for the download of content items to a local storage of the HNED via a broadband IP connection. A CDS can be used to provide IPTV services in areas where a broadband connection suitable for streaming services is not available or prone to errors, for simultaneous delivery of multiple content items to HNEDs or for reduced cost offers as the bandwidth consumption may be limited compared to streaming services.

DVB-IPTV CDSs shall support two different service modes:

- The **push download service** mode that is defined as a distribution of content items where the distribution decision is taken by the SP, without explicit request from the user.
- The **pull download service** mode provides for download of content items at the explicit request of a user.

In support of these two service modes, the CDS delivery system supports two "download modes": multicast download and unicast download. The protocol used for the multicast download mode is the File Delivery over Unicast Transport (FLUTE) protocol [70] and may be combined with a file repair mechanisms. The unicast download mode is based on the HTTP 1.1 protocol [39]. Download of a file from a single server and download of the file in chunks from multiple servers are supported. A reception reporting procedure allows the HNED to report the successful download of content.

NOTE: While the push download service mode might most often be realized using the multicast download mode and the pull service mode might most often be realized by the unicast download mode, other combinations are possible according to SP requirements. For example, a push download service to a small population of HNEDs can make use of unicast download and a pull download service for popular content items that is expected to be downloaded by a large number of users can make use of carousel multicast download.

The CDS functions enable to download content items. Content items consist of one or more files (e.g. A/V file and related metadata). The available content items, the related files for download and the download mechanisms are announced to the HNED using the BCG and dedicated *download session descriptions*. The HNED either automatically initiates the download (push download service mode) or acts on a user request (pull download service mode).

While the content download mechanisms as such are agnostic to the file formats that are transferred, the present document exclusively specifies the download of content encapsulated into an MPEG-2 transport stream and related BCG metadata. The usage of the specification for other content formats is not in the scope of the present document.

CDSs are transparent to any content protection systems and therefore do not prevent the implementation of content protection systems that build on the DVB CPCM specifications [103]. If authentication is required to set up unicast connections between the CDS HNED and the CDS Network function for either session descriptions or file download, it is recommended to use the methods described in RMS/FUS specification [78], clause 5.4.

10.2 Functional Architecture

10.2.0 CDS Functional Architecture Diagram

To support CDSs, the CDS functional architecture according to Figure 17 may serve as a reference architecture. The architecture includes logical interfaces between HNED and other CDS network functional components. The present document aims at specifying these functional components and interfaces. All CDS interfaces are part of the IPI-1 interface.

NOTE: All functions identified in the figure are logical rather than physical. No physical device is implied. The arrow direction indicates the main message flow.

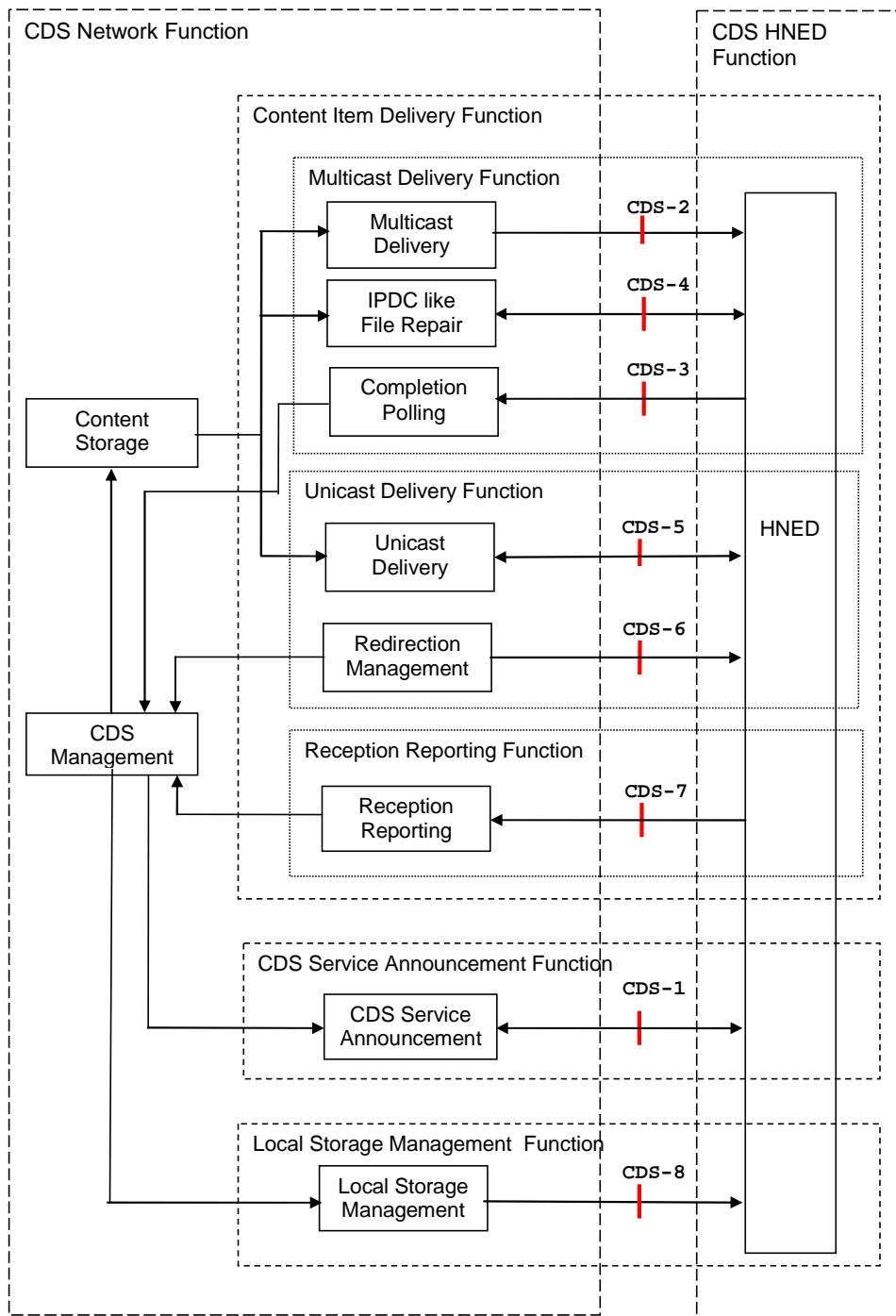


Figure 17: Content Download System Functional Architecture

Interfaces without any numbering are not in the scope of the present document.

10.2.1 CDS Functional Components

An overview of the functional components is provided:

CDS HNED: The user device aims at providing an easy, fast and secure access to the IPTV services. HNEDs that support CDS services shall implement the CDS HNED functions of the present document and shall provide storage dedicated to CDSs. A prescriptive description of the overall behaviour of the HNEDs is out of scope of the present document.

CDS Announcement: The CDS Announcement function advertises the availability of content items for pull service or push service download mode as well as the corresponding download session parameters. The details of the service announcement within CDS are introduced in clause 10.3.

Multicast download functions: The multicast download mode reliably distributes content items to a group of receivers simultaneously. The details of the multicast download functions are introduced in clause 10.6.2. The multicast download functions include:

- **Multicast download:** The multicast download component downloads content items to HNEDs. The multicast download component is based on the FLUTE protocol. The details of the FLUTE protocol are introduced in clause 10.6.2.2.
- **Completion polling:** This component is used by the CDS network function to determine when all HNEDs of the multicast group have completed the reception of the contents to be able to stop a multicast download. The details of the completion polling are introduced in clause 10.6.2.5.
- **File repair:** The file repair enables the repair of incomplete files after the multicast download session has been completed. Two types of file repair are defined. For CDS specific file repair the HNED uses the unicast download component of the unicast download function (see below) to download the missing parts of the file over the CDS-5 interface. For IPDC like file repair dedicated repair data is requested by the HNED and provided by the CDS network function. The details of the file repair are introduced in clause 10.6.2.6.

Unicast download function: The unicast download mode aims at reliably distributing content items to individual receivers. The details of the unicast download functions are introduced in clause 10.6.3.

Unicast download: The unicast download component aims at distributing the content items to individual HNED's upon their request. This download mode is based on the HTTP protocol [39]. The details of the unicast download component are introduced in clause 10.6.3.

Redirection management: This component aims at redirecting the unicast download requests to alternative download sources such as a single alternative server, a multicast session on which the requested content is available or a list of multiple servers each of which providing a different portion of the requested content. Moreover this component indicates to the HNED when to carry out the redirection requests e.g. immediately or at some later time. Details on redirection management are provided in clause 10.6.3.4.

Reception Reporting: After a successful download of file chunks, files or content items the HNED may inform the reception reporting function on the successful download. This function offers the possibility for the CDS network to collect statistics about the content download activity and can be used for monitoring or for adapting the download strategy dynamically. The reception reporting function is introduced in clause 10.6.5.

Local storage management: This function allows the CDS network to manage CDS storage and content on the HNED. The details of the storage management are introduced in clause 10.7.

CDS management: This component controls all other CDS functions. This function is not within the scope of the present document.

CDS network content storage: The CDS network content storage function prepares and stores the content items and associated metadata before they get delivered to the HNEDs. This function is not within the scope of the present document. Only the content item and file formats are addressed and are described in clause 10.4.

10.2.2 CDS Interfaces

CDS defines eight interfaces between the CDS network functions and the CDS HNED function. All interfaces are part of the IPI-1 interface. Table 25 provides the interfaces between the CDS HNED functions and the CDS Network functions. The reference to the clause of the present document specifying each one of the interfaces is given in Table 25.

Table 25: CDS interfaces on IPI-1

Interface	Description	Protocols	Clause
CDS-1	Carries CDS service announcement information to the HNEDs	BCG XML/DVBSTP XML/HTTP XML/SOAP SDP/SAP SDP/HTTP	10.3 and 10.5
CDS-2	Multicast download of content items from the network to the HNEDs	FLUTE	10.6.2.2
CDS-3	Multicast completion polling interface notifies the multicast content download status to the CDS Network	LCT ext. UDP	10.6.2.5
CDS-4	IPDC like file repair	HTTP	10.6.2.6
CDS-5	Unicast download of the content items from the network to the HNEDs	HTTP	10.6.3
CDS-6	Carries the redirection information of a unicast download request to the HNEDs	XML/HTTP SDP/HTTP	10.6.3.4
CDS-7	Notifies the successful completion of the content download to the CDS Network	XML/HTTP	10.6.5
CDS-8	Carries information to manage the HNED local storage	BCG	10.7

10.2.3 CDS Protocol Stack

Figure 18 shows the protocols used over the IPI-1 interface for the support of CDSs. The top layer of the stack signifies the application (content item and service announcement). At the bottom the IP layer serves as the common network transport layer and physical and data link layers.

NOTE: The protocol stack is provided for information only as it cannot express all functions in CDS in sufficient detail.

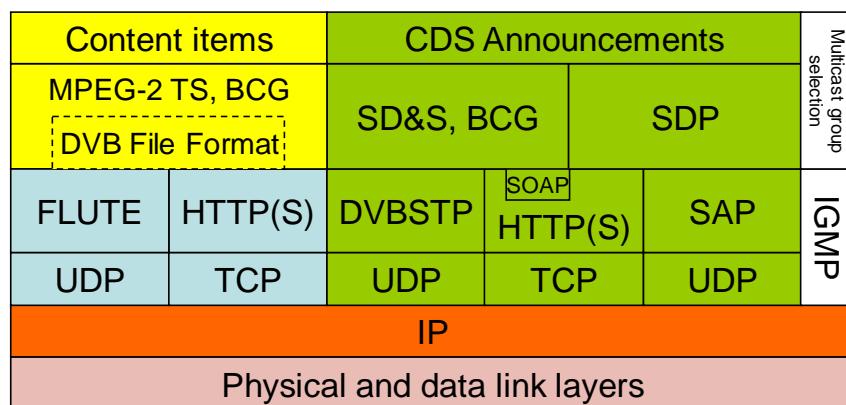


Figure 18: CDS protocol stack

10.3 CDS Announcement through BCG

10.3.0 Introduction

The CDS Announcement functions provide the CDS HNED functions with information about content items that are offered by the CDS network function for push and pull download service modes to the CDS HNED. This includes metadata for the content items, the availability for download and download session description information. The CDS Announcement information is exclusively delivered over the CDS-1 interface.

10.3.1 Usage of SD&S, BCG and TVA for CDS

The TV Anytime (TVA) based Broadband Content Guide (BCG) as defined in ETSI TS 102 539 [62] shall be used for CDS announcement and the announcement of individual content items. Specifically, the metadata fragments as defined in ETSI TS 102 539 [62], clause 6 with extensions shall be used for the announcement of content items for download. An extended version of the OnDemandProgramType is defined in clause G.1.1 and is introduced for the announcement of the content items available in the pull download service mode. A new PushDownloadType is defined in clause G.1.2 and is introduced for the announcement of the content items available in the push download service mode. The PushDownloadType is introduced as part of the ProgramLocationType. For this purpose the ProgramLocationType is extended as defined in clause G.1.3. CRID resolution shall be performed as defined in ETSI TS 102 539 [62], clause 5. The locator for CDS can be a URI locator or an extended on-demand decomposed binary locator as defined in clause G.1.4. The URIs specifically used for CDS in the locators and ProgramURL are defined in clause 10.3.2.

NOTE: CDS Announcement requires extension of the BCG as well as extension of TVA. The BCG OnDemandProgram Type and the on-demand decomposed binary locator are extended in order to differentiate between streaming and download modes and with content download specific information (see clause G.1.1). A new BCG type *PushDownloadType* is introduced. Relevant specifications are expected to be updated in their next releases. To provide a consistent CDS specification in the present document, these extensions are collected in clause G.1.

Content items that are available for pull download are announced via the BCG in the same way as it is done for streaming CoD content items. Information about the content item itself is provided by the Content Description Metadata (see ETSI TS 102 822-3-1 [60], clause 6.3) and information about the actual download session is provided by the extended OnDemandProgram Type Instance Description Metadata and/or by the URI locator or extended on-demand decomposed binary locator provided by the CRID resolution.

Content items that are available within a pull download service can be selected by the user for download. The CDS HNED shall initiate the download accordingly.

Content items that are available for push download service are announced via the BCG PushDownloadType Instance Description Metadata (see clause G.1.2). CDS HNEDs that have subscribed to the push download service shall autonomously download these content items. PushDownloadType content item instances shall not be announced to the user. After the successful download the content item can be announced via OnDemandProgramType Instance Description Metadata and/or by the URI locator or extended on-demand decomposed binary locator provided by the content resolution as available for consumption to the user with the URI pointing to the content item on the CDS HNED storage (see clause 10.3.2). The OnDemandProgramType metadata can be provided via the normal BCG mechanisms or as part of the content download.

The description of a content download session requires several parameters. These parameters are provided by a dedicated *download session description* mechanism outside of the BCG. The download session description contains all relevant information to reliable download a content item. Download session descriptions may be described in XML or SDP syntax. CDS HNEDs shall support download session descriptions in XML format and may support download session descriptions in SDP format. The BCG instance description metadata and the locators provide the link to the download session description. This link is referred to as *CDS URI* and is specified in clause 10.3.2. The transport of download session descriptions may be unicast or multicast. The transport methods for CDS download session description are specified in clause 10.5.5.

The SD&S BCG record (see clause 5.2.13.1) may provide information about download session description being delivered via multicast. This allows the HNED to listen to the announced multicast delivery and to cache the download session descriptions. In case a specific download session description is requested from a multicast delivery the HNED can access it from the cache and does not have to wait until this download session description is sent out on the multicast delivery.

10.3.2 URIs for Download Session Description

10.3.2.0 Overview

The link to the CDS download session description may be provided by:

- the ProgramURL of the PushDownloadType or the OnDemandProgramType; as well as
- the URI of the URI locator or the Extended-On-demand decomposed binary locator.

The syntax of the URIs used for the different CDS download session description protocols and transport methods are specified in this clause. Four different URIs schemas are specified taking into account different download session description methods (XML and SDP) and transport mechanisms (unicast and multicast). CDS HNEDs shall support CDS URIs that locate XML-based download session descriptions, i.e. the locators specified in clauses 10.3.2.1 and 10.3.2.2 and may support CDS URIs that locate SDP-based download session descriptions, i.e. the locators specified in clauses 10.3.2.3 and 10.3.2.4.

10.3.2.1 CDS XML Multicast Locator

CDS content may be located by a reference to an XML-based download session description delivered over multicast. The actual multicast delivery of XML-based session descriptions is defined in clause 10.5.5.1 based on DVBSTP. In this case, the XML segments with download session descriptions are constantly sent on a multicast group. The multicast group information (multicast address, port and optional source address), the SegmentID and the optional ServiceProviderID have to be provided in order to access the specific XML segment containing the referenced download session description.

As the segment may contain several download session description records the Download-Session-ID has to be provided in addition in the download session description URI.

The CDS HNED function shall extract the specific download session description referenced by the Download-Session-ID from the delivered segment. The Download-Session-ID is part of each session description record as defined in clause 10.5.3.

The DVB-MCAST URI for DVBSTP as defined in clause G.3.2 is used for referencing the multicast delivery of an XML session description. The payload is always provided and shall be set to 'dvbstp'. The dvbstpPayloadID is always provided and shall be set to the value "b1".

For CDSs and content items located by a CDS XML Multicast Locator, the following format shall be used:

```
'dvb-mcast:// [ src-host '@' ] mcast-addr [': port] ?payload=dvbstp [&service-provider=' ServiceProviderID ] '&dvbstp-
```

payload=' b1 [&segment=' SegmentID] [#? dvb-cds-session-id=' Download-Session-ID]
For instance, the following sample shows an URI referencing an XML-based download session description to be delivered over dvbstp:

```
dvb-mcast://132.45.1.1@230.100.1.1:1000?payload=dvbstp&dvbstp-payload=b1&segment=23#?dvb-cds-  
session-id=20
```

10.3.2.2 CDS XML Unicast Locator

CDS content may be located by a reference to a XML-based download session description delivered over unicast. The actual unicast delivery of XML-based session descriptions is defined in clause 10.5.5.2 using http. The download session description is provided in an XML segment from the host application. The session description URI needs to provide the host, optional port, application (/dvb/cds/session_description), and the Segment ID have to be provided in order to access the specific XML segment.

A HTTP URI is used to reference the XML-based download session description. In case the segment contains several session description records the SessionID has to be provided in addition. The CDS HNED function shall extract the specific download session description defined by the Download-Session-ID from the delivered segment. The Download-Session-ID is part of each session description record as defined in clause 10.5.3.

NOTE 1: A DVBSTP service provider ID is not provided. It is assumed that the host application supports a single SP.

NOTE 2: A DVBSTP payload ID is not provided. The application /dvb/cds/session_description already indicates that a session description type of payload is requested.

NOTE 3: The segment version is not provided in the URI as always the latest version of the segment will be used. It might be included automatically in the request by the HNED in case the segment is already in the local cache.

For CDSs and content items located by a CDS XML Unicast Locator, the following format shall be used:

```
'http:// host [': port ] '/dvb/cds/session_description?Segment=' SegmentID [ '#?dvb-cds-session-
id=' Download-Session-ID]

SegmentID      = 4*4 HEXDIG; any hex number from 0x0000 to 0xffff
Download-Session-ID = String
```

For instance, the following sample shows a URI referencing an XML-based download session description to be delivered over http:

```
http://announcements.provider1.org:80/dvb/cds/session_description?Segment=a0ff#?dvb-cds-session-
id=102
```

10.3.2.3 CDS SDP Multicast Locator

CDS content may be located by a reference to a SDP-based download session description delivered over multicast. The actual multicast delivery of SDP-based download session descriptions is defined in clause 10.5.5.3. The session descriptions are constantly send on a multicast group. The multicast group information (multicast address, port and optional source address) and the Download-Session-ID have to be provided in the download session description URI in order to access the specific SDP session description. The Download-Session-ID is part of each session description record.

For CDSs and content items located by a CDS SDP Multicast Locator, the DVB-MCAST URI for SAP as defined in clause G.3.3 shall be used. The payload is always provided and shall be set to 'sap'.

```
'dvb-mcast:// [ src-host '@' ] mcast-addr [': port] '?payload=sap' '#?sdp-session-id=' Download-
Session-ID
```

For instance, the following sample shows an URI referencing an SDP-based download session description to be delivered over multicast:

```
dvb-mcast://132.45.1.1@230.100.1.1:1000?payload=sap#?sdp-session-id=12
```

10.3.2.4 CDS SDP Unicast Locator

CDS content may be located by a reference to a SDP-based download session description delivered over unicast. The actual unicast delivery of the SDP-based download session descriptions is defined in clause 10.5.5.4. The session description is provided as file. The host and the path to the file and the filename have to be defined in order to access the file. The default file extension is ".sdp", however other extensions can be used.

A HTTP URI is used to reference the SDP file. An SDP file contains a single session description. The Download-Session-ID therefore does not need to be defined in the reference. However, if it is defined the HNED shall only accept the download session description in the delivered file if the Download-Session-ID in the reference and of the session description record match. In case they do not match, the download session description shall be ignored.

For CDSs and content items located by a CDS SDP Unicast Locator, the following format shall be used:

```
'http:// host [': port ] '/' path '/' filename [ '#?sdp-session-id=' Download-Session-ID]

Download-Session-ID = String
```

For instance, the following sample shows an URI referencing an SDP-based download session description to be delivered over unicast:

```
http://announcements.provider1.org:80/session_announcements/session14.sdp
```

10.3.3 URI for files on the CDS HNED storage

After the successful download of a content item, the HNED can access the files of the content item from the CDS HNED storage. In order to reference a file located on the CDS HNED storage from the BCG metadata (e.g. ProgramURL of OnDemandProgramType) and locators (e.g. URI locator, URI of Extended On-demand decomposed binary locator) the DVB CDS Local URI scheme shall be used.

```
'dvb-cds-local://File-Reference
File-Reference = absolute path
<absolute-path> as defined in clause 10.5.2
```

The *File-Reference* which identifies a specific file on the CDS HNED storage shall be the same as provided in the download session description or FLUTE FDT for that specific file. The CDS network, i.e. the SP, shall ensure that the *File-Reference* is unambiguous.

The content type of the file is available from the download procedure, either from the download session description (*File-Content-Type*), the FLUTE FDT or the HTTP session.

In case of a push download the metadata which announces the downloaded content item to the user after the download shall use this DVB CDS Local URI.

In case of a pull download the metadata will indicate that the content item is available for pull download. After the download however the CDS HNED knows that the content item is available for local play out and it shall replace that pull download information with a link to the file on the CDS HNED storage for immediate play out.

10.4 CDS Content Item and File Formats

10.4.1 General

The content item download procedures defined in clause 10.6 are in general transparent to the formats of the files that are delivered. CDS however is focused on the download of content items that consist of one or more audio/video files and optional related metadata. Specifically, the present document primarily specifies the download of content items based on the MPEG-2 TS file format [109].

CDS differentiates between content item formats and file formats. Content item formats provide a high-level description of the content item, i.e. the collection of files in one session description, and also provide hints to the CDS HNED function, how to handle the consumption and play-out of the content item. The content item format is part of the download session description as *Content-Item-Format* parameter. Supported content item formats are defined in clause 10.4.3.

Content items generally consist of one or several files whereby each file has a specific file format or content type. The content type may be signalled in the download session description in the *File-Content-Type* attribute, in entity header field *Content-Type* of the http request or reply or in the *Content-Type* field of the FDT. Content types should be registered MIME media types. Supported file formats and the associated MIME media types are defined in clause 10.4.2.

10.4.2 File Formats and Media types

10.4.2.1 MPEG-2 Transport Stream file format

The CDS HNED shall support the reception and consumption of content files in MPEG-2 transport stream format. An MPEG-2 transport stream file consists of the concatenated 188 bytes transport stream packets stored in the order they are delivered. The transport stream shall be compliant to ETSI TS 101 154 [58].

MIME media type:

- video/mp2t (for video and combined video and audio content), see IETF RFC 3555 [82].
- audio/mp2t (for audio only content).

NOTE 1: Despite IETF RFC 3555 [82] defines the MIME media type video/mp2t only for transfer over RTP, it is re-used here for the purpose of CDS.

NOTE 2: Audio/mp2t is not a registered MIME media type.

10.4.2.2 BCG Metadata file format

The CDS HNED shall support BCG metadata files as defined in ETSI TS 102 539 [62]. The XML file shall contain at least an element of the type `tva:ProgramInformationType` describing the associated content. The XML file may be delivered as uncompressed or BiM compressed textual schema-valid XML file. In case BiM compression is used the `Content-Encoding` parameter in the FLUTE FDT and HTTP header shall be set to "x-bim".

After the successful download of a content item the CDS HNED shall interpret the downloaded BCG metadata files as part of it BCG processing as defined in ETSI TS 102 539 [62].

MIME media type:

- application/xml.

10.4.2.3 DVB File Format

The CDS may support files in the DVB File Format as specified in ETSI TS 102 833 [109].

MIME media type:

- video/vnd.dvb.file (for video and combined video and audio content).
- audio/vnd.dvb.file (for audio content).

Files complying to the DVB File Format specification shall contain descriptive metadata as specified in ETSI TS 102 833 [109].

NOTE: The DVB File Format can support content formats other than the MPEG-2 Transport Stream. At present it is expected that the DVB file format would only contain the MPEG-2 Transport Stream representations of content, but in the future other representations may be supported.

10.4.3 Content Item Formats

A single content item may include a single file or may consist of several files. All files of a content item shall be announced in a single download session description and are downloaded in a single download session. The HNED shall keep track of this association between content item and files. The download session description may announce the content item format in the `Content-Item-Format` attribute.

The following content item formats shall be supported:

- *Content-Item-Format=0:*
In this case, the download session description describes the download of any collection of files. The CDS HNED should interpret the Content-Type of the first file in the download session description for the consumption of the content item.
- *Content-Item-Format=1:*
In this case, the download session description describes the download of a single MPEG-2 Transport Stream with the content type according to clause 10.4.2.1.
- *Content-Item-Format=2:*
In this case, the download session description describes the download of an MPEG-2 Transport Stream with the format according to clause 10.4.2.1 and associated BCG metadata according to clause 10.4.2.2. The CDS HNED shall always interpret the BCG metadata before accessing the MPEG-2 Transport Stream.

The following content item formats may be supported:

- *Content-Item-Format=3:*
In this case, the download session description describes the download of a file in DVB File format to clause 10.4.2.3 where the file encapsulates an MPEG-2 TS.

If the content item format is not present, then `Content-Item-Format=0` shall be assumed.

NOTE 1: By the use for `Content-Item-Format=0`, it is not prevented that other formats are carried within CDS services, especially if the appropriate MIME media type is defined.

NOTE 2: Details of which codec(s) are used by the file may be signalled within the AVAttributes field within the descriptive metadata associated with the file. An HNED is able to inspect this field and to decide if it wishes to download the file.

10.5 CDS Download Session Description

10.5.1 Overview

Each content item is acquired in a download session that is described by a download session description. A download session description is composed of several download session parameters and provides information to initiate or join download sessions and to reliably download content items. The download of content items requires the download of one or several individual files.

The acquisition of the individual files of a content item requires the construction of a unique reference link for each file. The referencing methods of file locations in CDS download session descriptions are introduced in clause 10.5.2. The download session parameters and their semantics are introduced in clause 10.5.3. Different types of download sessions are described in clause 10.5.4 along with the assigned download session parameters. The following download session types are distinguished:

- Scheduled Multicast Download (SMD) Session.
- Carousel Multicast Download (CMD) Session.
- Unicast Download (UD) Session.

The CDS HNED function shall support all mandatory features of all three types of download sessions.

Download session descriptions can be provided in XML or in SDP syntax. The CDS HNED shall support XML syntax. The CDS HNED may support SDP syntax. Both download session descriptions support the same parameter set. The XML syntax for the download session parameters is defined in clause C.2.3. The SDP syntax for the download session parameters is defined in clause G.2.

The transport of download session descriptions is defined in clause 10.5.5.

10.5.2 Referencing file locations for download

The downloading of content items includes the download of one or more files within a download session. The download session description provides the information about all files that have to be downloaded for a specific content item. In addition, each file within a content item may be downloaded from different locations. Therefore, the download session descriptions for unicast download may define alternative sources in the initial session description or in the description of a redirection of the actual file download (see clause 10.6.3). In case of multicast download the files have to be identified within the File Delivery Table (FDT) and the file repair procedures have to know the location of the repair data (see clause 10.6.2).

In CDS file locations are uniquely referenced using the URI scheme defined in IETF RFC 3986 [79] with some restrictions. The following definitions as defined in IETF RFC 3986 [79] are re-used in the present document:

- *Generic URI* <URI> as defined in IETF RFC 3986 [79], clause 3.
- *Scheme syntax component* <scheme> as defined in IETF RFC 3986 [79], clause 3.1.
- *Authority syntax component* <authority> as defined in IETF RFC 3986 [79], clause 3.2.
- *Query syntax component* <query> as defined in IETF RFC 3986 [79], clause 3.4.
- *Fragment syntax component* <fragment> as defined in IETF RFC 3986 [79], clause 3.5.
- *Absolute URI* <absolute-URI> as defined in IETF RFC 3986 [79], clause 4.3.
- *Relative reference* <relative-ref> as defined in IETF RFC 3986 [79], clause 4.2.
- *Absolute path* <path-absolute> as defined in IETF RFC 3986 [79], clause 3.3.

NOTE: The *absolute path* syntax <path-absolute> is a special case of the *relative reference* syntax <relative-ref>.

The following definition is used in the context of the present document:

- *HTTP-Server Base URI* <http-server-base-URI> is an <absolute-URI> with a fixed scheme of "http://" and an <authority> component (host, port) only. The URI shall not contain any absolute path, query or fragment syntax component.

The following principles apply for referencing files:

- A file location is referenced by a *target URI* that has the syntax of an absolute URI <absolute-URI>. By the definition of the absolute URI syntax, a fragment syntax component shall not be used. Furthermore, the target URI referencing the file location shall not use any *query* syntax component.
- A CDS HNED may construct a target URI by *reference resolution* as defined in IETF RFC 3986 [79], section 5. To create a target URI by the application of reference resolution, the CDS HNED requires
 - a *base URI* of syntax <http-server-base-URI>;
 - a *relative reference* of syntax <path-absolute>.
- In the CDS context the base URI identifies the server part and the files that have to be downloaded are referenced by an absolute path syntax component <path-absolute>.

10.5.3 Download Session Description Parameters

10.5.3.0 Introduction

Download session descriptions contain several parameters that describe the content item format as well as the methods on how to acquire the content item. The semantics of the parameters is described.

10.5.3.1 General Parameters

The following download session parameters are applicable to any download session.

Service-Provider-Domain: The SP domain is an Internet DNS domain name registered by the SP that uniquely identifies the SP. There shall be exactly one occurrence of a *Service-Provider-Domain* parameter in a download session description.

Download-Session-ID: The download session ID is a numeric string and identifies a specific session description. There shall be exactly one occurrence of a *Download-Session-ID* parameter in a download session description.

Download-Session-Version: The download session version identifies the version of a specific session description. It is an integer value between 0 and 255 which is increased by 1 for each new version of a session description. It overflows from 255 to 0. There shall be exactly one occurrence of a *Download-Session-Version* parameter in a download session description.

Content-Item-Format: The content item format describes the format of the content item. If the content item format is not present, then *Content-Item-Format=0* shall be assumed. For details on content-item formats refer to clause 10.4.3.

Download-Session-Mode: The download session type specifies one of the three download session modes: "SMD", "CMD" or "UD" according to clause 10.5.4. There shall be exactly one occurrence of a *Download-Session-Mode* parameter in a download session description.

NOTE 1: The differentiation between single server and multiple servers unicast download is based on the unicast download parameters and not the *Download-Session-Mode*.

Download-Session-Time-Information: The *Download-Session-Time-Information* provides the information when a CDS download session is active and the HNED can join it to perform the download. In case of a Unicast and Carousel Multicast Download the start and end time of the active time window shall be defined. In case of a Scheduled Multicast Download only the start time of the session shall be defined. The information is provided at the session level.

NOTE 2: This information is identical to the availability for download information in BCG the extended OnDemandProgramType and Extended On-demand decomposed binary locator defined above.

Successful reception of the advertised content items shall be reported to the CDS network function. To enable this, the HNED requires reception reporting parameters.

For each reception reporting server:

- Reception-Reporting-Server-URI: HTTP URI of the reception reporting server.
- In case more than one server is provided the CDS HNED function shall randomly select one of the provided servers. In the absence of the parameter, reception reporting is not supported for this download session.

If at least one reception reporting server is provided then the following parameters may be provided:

- Reception-Reporting-Mode: Defines the level of details provided by the reception reporting:
 - Reception-Reporting-Mode=0: Content item reporting.
 - Reception-Reporting-Mode=1: Content item and file reporting.
 - Reception-Reporting-Mode=2: Content item, file and chunk reporting.

In the absence of the parameter, the CDS HNED function shall assume *Reception-Reporting-Mode=0*. In case of multicast download, *Reception-Reporting-Mode=2* shall not be used.

Reception-Reporting-Offset-Time: This parameter defines the offset time for the reception reporting back-off time (see clause 10.6.5). It is an integer value expressed in seconds. In the absence of the parameter, the CDS HNED function shall assume *Reception-Reporting-Offset-Time =0*.

Reception-Reporting-Random-Time-Period: This parameter defines the random time period for the reception reporting back-off time (see clause 10.6.5). It is an integer value expressed in seconds. In the absence of the parameter, the CDS HNED function shall assume *Reception-Reporting-Random-Time-Period=0*.

10.5.3.2 Unicast Download Related Parameters

The following download session parameters are applicable to unicast download session.

For each file that has to be downloaded:

- File-Reference*: This is a reference to the file to be downloaded. The syntax of this reference shall conform to the *absolute path* syntax <path-absolute>.
- File-Content-Type*: Content-Type of file as defined in clause 10.4.2 referring to a registered MIME-type.
- File-Length*: Length of file (as defined in IETF RFC 2616 [39] for the Content-Length entity header field).
- File-Digest*: Base64 of 128 bit MD5 digest of the file as defined in IETF RFC 2616 [39] for the Content-MD5 entity header field.

In case download of a file in individual chunks is provided:

- Chunk-Length*: Length of a chunk of the file. The file is divided into chunks of constant length as defined by this parameter (except for the last chunk which could be shorter depending on the file length) that can be downloaded separately.

For each chunk (chunks are numbered from 1 to n in the order they make up the file):

- Chunk-Digest*: Base64 of 128 bit MD5 digest of chunk as defined in IETF RFC 2616 [39] for the Content-MD5 entity header field.

For each server where the file is available for download:

- Server-Base-URI*: The base URI of the file location represents the server from which the file can be downloaded. The *Server-Base-URI* syntax of this reference shall conform to the <http-server-base-URI> syntax (see clause 10.5.2).

In case download of a file in individual chunks is provided:

- Available-Chunk-List*: List of all chunks of a file that are available on that server (*chunks are numbered from 1 to n in the order they make up the file*). If the parameter is not provided the whole file (all chunks) is available on the server.

"Available-Chunks-List" grammar using conventions of [39], clause 2:

```

chunks-list      = 1#( single-chunk-num | chunk-range-spec )
single-chunk-num = 1*DIGIT
chunk-range-spec = first-chunk-num "-" last-chunk-num
first-chunk-num  = 1*DIGIT
last-chunk-num   = 1*DIGIT

```

Examples of valid "Available-Chunks-List":

- 6.
- 8-11.
- 3, 14, 29.
- 5-12, 22, 36.

In case multiple servers and chunk information (at least *File-Length* and *Chunk-Length*) is provided, the download of the file can be distributed over these servers (see clause 10.6.3.3), otherwise the file is downloaded from a single server (see clause 10.6.3.2).

10.5.3.3 Multicast Download Related Parameters

The following download session parameters are applicable to multicast download sessions.

For each file that has to be downloaded:

File-Reference:

This is a reference to the file to be downloaded. The syntax of this reference shall conform to the *absolute path* syntax <path-absolute>. In the absence of the parameter, the CDS HNED function shall download all files transported by the FLUTE session. In case *Content-Item-Format=0* is used and the content item contains more than one file, this field is mandatory.

To join a FLUTE multicast download session the following parameters based on the definitions in ETSI TS 102 472 [65], clause 6.1.13 are used.

IP-Source-Address:

Source IP address of the multicast group of the FLUTE session. There shall be exactly one IP source address per multicast file download session.

Transport-Session-Identifier:

Transport Session Identifier (TSI) of the session. The TSI together with the *IP-Source-Address* uniquely identifies a FLUTE session for a given IP source address during the time that the session is active, and also for a large time before and after the session is active. There shall be exactly one occurrence of this parameter in a FLUTE session description. The TSI shall be an integer value.

FEC-Encoding-ID:

Describes the FEC scheme. Two schemes are supported:

- *FEC-Encoding-ID=0*: Compact No-Code FEC scheme.
- *FEC-Encoding-ID=1*: Raptor FEC scheme.

If the *FEC-Encoding-ID* is not provided, the CDS HNED function shall assume *FEC-Encoding-ID=0*.

Note that FEC Object Transmission Information (OTI) shall be delivered using the ALC/LCT extension header EXT_FTI or the FDT (see clause 10.6.2.2).

Number-Of-Channels:

Number of FLUTE/LCT channels of the FLUTE session. The multiple channel attribute parameter indicates to the receiver that the sender is using multiple channels in the FLUTE session to transmit data. The attribute also indicates the number of channels used by the sender. In absence of this parameter, a CDS HNED function shall understand that exactly one FLUTE channel is used for the multicast download session.

For each channel:

<i>IP-Multicast-Address:</i>	IP multicast address for each FLUTE channel. There shall be exactly one occurrence of this parameter for each channel in a FLUTE session description.
<i>IP-Multicast-Port-Number:</i>	Port number for each FLUTE channel. There shall be exactly one occurrence of this parameter for each channel in a FLUTE session description.
<i>Max-Bandwidth:</i>	Maximum bandwidth to be used by each FLUTE channel. The TIAS bandwidth modifier as defined in IETF RFC 3890 [80] shall be used. In the absence of the parameter, no maximum bandwidth limit shall be assumed.

Furthermore, the order of FLUTE channels in the download session description provides the order in which the HNED shall join and leave the channels.

To participate in completion polling in a scheduled multicast download session, the CDS HNED function needs to know the following parameters associated with the completion polling. In the absence of the parameters, completion polling is not applied for this download session.

<i>Completion-Poll-Response-Server-Address:</i>	IP address to which CDS HNED function will send completion poll responses.
---	--

<i>Completion-Poll-Response-Server-Port-Number:</i>	Port number for completion poll responses.
---	--

If the file repair mechanism for multicast download is supported (see clause 10.6.2.6), the CDS HNED function needs to know the following parameters associated with file repair mechanism.

For each recovery server:

<i>Recovery-Server-Base-URI:</i>	The base URI of a unicast recovery server. The <i>Recovery-Server-Base-URI</i> syntax of this reference shall conform to the <http-server-base-URI> syntax (see clause 10.5.2).
----------------------------------	---

If a *Recovery-Server-Base-URI* is provided then the following parameters may be provided:

<i>Recovery-Mode:</i>	Describes which file repair procedure to be applied, an IPDC-like file repair procedure or a specific CDS file repair procedure. <ul style="list-style-type: none"> ▪ <i>Recovery-Mode=0:</i> CDS file repair procedure. ▪ <i>Recovery-Mode=1:</i> IPDC-like file repair procedure.
-----------------------	---

In the absence of the parameter, the CDS HNED function shall assume *Recovery-Mode=0*.

<i>Recovery-Offset-Time:</i>	This parameter defines the offset time for the file repair back-off time (see clause 10.6.2.6). It is an integer value expressed in seconds. In the absence of the parameter, the CDS HNED function shall assume <i>Recovery-Offset-Time=0</i> .
------------------------------	--

<i>Recovery-Random-Time-Period:</i>	This parameter defines the random time period for the file repair back-off time (see clause 10.6.2.6). It is an integer value expressed in seconds. In the absence of the parameter, the CDS HNED function shall assume <i>Recovery-Random-Time-Period =0</i> .
-------------------------------------	---

10.5.4 Download session Modes

CDS download sessions may be operated in one of four modes:

- Scheduled Multicast Download (SMD) Session.
- Carousel Multicast Download (CMD) Session.
- Unicast Download (UD) session with Single Server (SS) downloads.
- Unicast Download (UD) session with Multiple Server (MS) downloads.

The download session descriptions of each of the download sessions requires and permits certain parameters from the list of download session parameters in clause 10.5.3. Table 26 provides the mapping of download session parameters to download session types: "M" refers to a mandatory parameter and shall be included by the CDS network function in a download session description. "O" refers to an optional parameter and may be included by the CDS network function in an announcement of the respective download session. "N" refers to the case that this parameter shall not be included for this download session mode. The table also provides the type for each parameter.

Table 26: Mapping of Download session Parameters to Download sessions Modes

Parameter	Type	SMD	CMD	UD	
				SS	MS
General parameters					
Service-Provider-Domain	domain name	M	M		
Download-Session-ID	unsigned integer	M	M		
Download-Session-Version	unsigned integer	M	M		
Content-Item-FormatType	unsigned integer(2)	O	O		
Download-Session-Mode	syntax specific	M	M		
Download-Session-Time-Information	syntax-specific	M	M		
Reception-Reporting-Server-URI (one per sever)	<http-server-base-URI>	O	O		
Reception-Reporting -Offset-Mode (one per sever)	unsigned integer (2)	O	O		
Reception-Reporting -Offset-Time (one per server)	unsigned integer(64)	O	N		
Reception-Reporting-Random-Time-Period (one per server)	unsigned integer(64)	O			N
Unicast Download Related Parameters					
File-Reference (one per file)	<path-absolute>	N	N	M	M
File-Content-Type (one per file)	MIME type	N	N	O	O
File-Length (one per file)	unsigned integer	N	N	O	M
File-Digest (one per file)	base64	N	N	O	O
Chunk-Length (one per file)	unsigned integer	N	N	N	M
Chunk-Digest (one per file and chunk)	base64	N	N	N	O
Server-Base-URI (one per file and server)	<http-server-base-URI>	N	N	M	M
Available-Chunk-List (one per file and server)	list of unsigned integer	N	N	N	O
Multicast Download Related Parameters					
File-Reference (1...n)	<path-absolute>	O	O		N
IP-Source-Address	IP address or fully qualified domain name	M	M		N
Transport-Session-Identifier	unsigned integer (48)	M	M		N
FEC-Encoding-ID	unsigned integer (8)	O	O		N
Number-Of-Channels	unsigned integer (4)	O	O		N
IP-Multicast-Address (one per channel)	IP address	M	M		N
IP-Multicast-Port-Number (one per channel)	unsigned integer (16)	M	M		N
Max-Bandwidth (one per channel)	unsigned integer	O	O		N
Completion-Poll-Response-Server-Address	IP address or fully qualified domain name	O	N		N
Completion-Poll-Response-Server-Port-Number	unsigned integer (16)	M	N		N
Recovery-Server-Base-URI (one per server)	<http-server-base-URI>	O	O		N
Recovery-Mode	unsigned integer(1)	O	O		N
Recovery-OffsetTime	unsigned integer(64)	O	O		N
Recovery- Random-Time-Period	unsigned integer(64)	O	O		N
NOTE:	M=Mandatory. O=Optional. N=Not applicable.				

10.5.5 Transport of download session descriptions

10.5.5.0 Introduction

The XML-based and SDP-based download session descriptions are provided to the HNED by use of unicast or multicast transport via the CDS-1 interface.

10.5.5.1 Multicast transport of XML-based download session descriptions

For the multicast transport of XML session descriptions, the DVBSTP protocol as defined in clause 5.4.1 is used with the following CDS specific profile:

- The Payload ID field shall be set to 0xB1 as specified in Table 12a.
- XML-based session descriptions can be delivered un-compressed or BiM compressed as defined in clause 5.5.2.

The CDS XML fragments are constantly sent out on the multicast group in a carousel manner. In order for the HNED to access a specific segment it may have to wait until the segment is sent out on the multicast group. In case the multicast download session is announced to the HNED beforehand via the SD&S BCG record (see clause 5.2.13.1) the HNED can constantly listen to the multicast group and cache the latest versions of the XML segments. The HNED can in this case access the relevant segment immediately from the cache without the need to wait until the segment is send out on the multicast group.

In case the segment contains more than one session description record the optional *Download-Session-ID* fragment identifier in the referencing URI (see clause 10.3.2.1) identifies the specific session description record.

Where multicast is used to distribute the download session description information, XML records may be segmented, that is divided up into smaller units, to enable easier processing in the HNED, or variable access times. Note that a record may be divided into a single segment. Each segment shall contain an integral number of download session elements as defined above (specifically, a segment shall not contain part of a download session element). Each segment shall be valid and well formed. Segment IDs need not be contiguous.

The multicast group may be shared between several SPs. The optional ServiceProviderID field of the DVBSTP header is in this case used to identify the SP.

10.5.5.2 Unicast transport of XML-based download session descriptions

The unicast transport of XML session descriptions is aligned with the SD&S unicast transport as defined in clause 5.4.2. The HTTP Protocol shall be used for the communication between the HNED and the CDS session description server(s). A session description request is defined for the delivery of a specific session description record. The request shall return a XML segment with one or more download session description records.

NOTE: In case the returned segment contains more than one session description record the optional *Download-Session-ID* fragment identifier in the locator identifies the specific session description record. The specific session description record is always extracted by the HNED. The request always delivers the whole segment to the HNED.

The request has one mandatory parameter that takes the SegmentID. Optionally a segment version may be specified in the request, this will indicate to the server the current version of the segment at the HNED.

The HNED may cache segments. In case a download session description from the same segment is requested later the HNED can provide the version of the cached segment, which can be found in the XML record, in the request. The response to the request shall return the service discovery record for the specified segment only if a newer version is available. If the segment has not changed then the server shall return status code "204" as per the IETF RFC 2616 [39] to indicate that the request has been processed successfully but that there is no entity-body to return.

When the segment version is not specified, the response to the request shall return the actual version of the specified segment. When a record is not found, the server shall return status code "404" as per the IETF RFC 2616 [39].

The download session description request shall comply with the following format:

```
'GET /dvb/cds/session_description' '?Segment=' SegmentItem 'HTTP/1.1' CRLF
'Host: ' host [':' port] CRLF
```

The SegmentItem parameter is a SegmentId with an optional field for the version number.

SegmentItem	= SegmentId 0*1('&Version='VersionNumber)
SegmentId	= 4*4 HEXDIG; any hex number from 0x0000 to 0xffff
VersionNumber	= OCTET; any hex number from 0x00 to 0xff

Note that a payload ID as defined for the service discovery request in clause 5.4.2.2 is not provided as the request type of "/dvb/cds/session_description" already indicates that session description information is requested.

For example the following request can be constructed to request the session description records of segment 1 from the server sdes.dvb.org:

```
'GET /dvb/cds/session_description?Segment=0001 HTTP/1.1' CRLF
'Host: xyz.company.com:1022' CRLF
```

10.5.5.3 Multicast transport of SDP-based download session descriptions

The multicast transport of SDP session descriptions uses the SAP Protocol as defined in IETF RFC 2974 [76] with the following CDS specific profile:

- The PT is "application/sdp".
- The payload can be compressed using zlib.
- Authentication is not supported.

SDP session descriptions are constantly sent out on the multicast channel in a carousel manner. In order for the HNED to access a specific session description it may have to wait until it is send out on the multicast channel. In case the multicast delivery channel is announced to the HNED in advance in the BCG record (see clause 5.2.13.1), the HNED may constantly listen to the multicast channel and cache the latest versions of the session descriptions. The HNED can in this case access the relevant session description immediately from the cache without the need to wait until the segment is sent out on the multicast channel.

10.5.5.4 Unicast transport of SDP-based download session descriptions

The unicast transport of SDP session descriptions uses the HTTP Protocol for all communication between the HNED and the CDS session description server(s). The HNED requests a SDP file from the CDS session description server. The file shall contain a single SDP session description as defined in clause G.2. The Content-Type for the SDP file shall be "application/sdp". The file is delivered uncompressed.

10.6 CDS Content Item Download

10.6.1 Overview

CDS content item download is concerned with the reliable distribution of content items to a single HNED or a population of HNEDs in non real-time manner.

A content item may consist of one or more files. These can be video, audio, combined video and audio and related metadata files as defined in clause 10.4. CDS supports the download of all files associated with a content item as part of a single download session. Within a CDS session the files are delivered either via unicast or multicast download. A CDS session is announced either being unicast or multicast, but not a mixture of both. However by the use of unicast file repair for a multicast session or multicast redirection of a unicast download session, the download mode may change during a session.

CDS is only concerned with the download of the content item, but not with the play out and presentation of the content item. Appropriate consumption and presentation of a content item that consist of several files has to be ensured by the use of the *Content-Item-Format*.

A CDS HNED function shall support:

- all mandatory features of multicast content download as specified in clause 10.6.2;
- all mandatory features of unicast content download as specified in clause 10.6.3; and
- all mandatory features of the reception reporting procedures as specified in clause 10.6.5.

Before initiating the download of a content item, it is assumed that the CDS HNED function has access to a download session description that describes the procedures on how to download the referenced content item (see clause 10.5).

The CDS HNED function has completed the download of the content item only if all files of the accessed content item have been completely downloaded.

If the *Download-Session-Mode* is "SMD" or "CMD", the CDS network and CDS HNED functions shall apply the multicast content download procedures specified in clause 10.6.2.

If the *Download-Session-Mode* is "UD", the CDS network and CDS HNED functions shall apply the unicast content download procedures specified in clause 10.6.3.

Clause 10.6.4 provides guidelines for the parallel download of content items from one or multiple servers.

If the download session description contains at least one Reception-Reporting-Server-URI, the CDS network and CDS HNED functions shall apply the reception reporting procedures as specified in clause 10.6.5.

10.6.2 Multicast Content Download

10.6.2.1 Overview

Multicast download modes provide download of content items to multiple HNEDs using IP multicast. It is therefore suitable for efficiently downloading the same content items to many receivers. The availability of content items via Multicast download mode is advertised in the download session description.

Multicast Content Download is organized in download sessions. A download session is characterized as an instance of the CDSs with a start time and optionally an end time as well as addresses of the IP flows used for the download of the files between the start and end time. The start and end times are signalled in the *Download-Session-Time-Information* parameter.

A download session description refers to the download of exactly one content item. However, a multicast session may include the files for more than one content item. In this case the download session description of specific content item identifies which files belong to that content item and only these files will be downloaded. Otherwise all files shall be downloaded.

The *Download-Session-Mode* parameter indicates if Scheduled Multicast Download (SMD) or Carousel Multicast Download (CMD) is applied.

In SMD mode, a multicast session is explicitly scheduled by the network to begin at a start time. HNEDs may choose to join the session at the appointed time. The CDS network function should use completion polling in SMD mode.

In the CMD mode, a session is scheduled to be available over a long period of time and CDS HNEDs may join and leave at any time. The CDS network function shall not use completion polling in CMD mode.

For the actual multicast file distribution, at the appointed session start time, the CDS Network Multicast Server Function begins distribution of the files using the FLUTE protocol [70]. Details on the use of FLUTE in CDS are specified in clause 10.6.2.2. The CDS HNEDs join the session by joining one or more of the IP Multicast groups. For multicast channel selection the IGMPv3 protocol IETF RFC 3376 [47] is used for IPv4 or the MLD protocol Version 2 [118] for IPv6. Procedures on which and how many IP Multicast groups are joined are specified in clause 10.6.2.3.

For SMD mode sessions the SP should continue the session until all receivers still joined to the group have received the content items being downloaded. The length of the session can be determined using the completion polling function as specified in clause 10.6.2.5.

Furthermore, for SMD sessions, the CDS HNED function should join the multicast session latest at the appointed start time. In case a CDS HNED joins the scheduled session after the appointed start time and CDS system applies the completion mechanism, the HNED shall not respond to the completion poll request messages of the CDS network functions.

In case the CDS HNED cannot complete the download of the content item during the time the multicast session is active, CDS provides file repair mechanisms. These file repair mechanisms are described in clause 10.6.2.6.

10.6.2.2 FLUTE Transport Protocol in CDS

10.6.2.2.0 General rules

The File deLivery over Unidirectional Transport (FLUTE) protocol [70] shall be used for CDS multicast download. The usage of the FLUTE protocol is closely aligned with the Delivery Protocol for File Delivery Services in ETSI TS 102 472 [65]. In addition to the basic protocol as specified in IETF RFC 3926 [70], the CDS multicast download is comprised of parts that further specify how FLUTE is used. The purpose of file delivery is to deliver content items in files. A file may contain any type of data (e.g. Audio/Video file, Binary data, Still images, Text, BCG metadata). In the present document the term "file" is used for all objects carried by FLUTE (with the exception of the FDT Instances).

FLUTE is built on top of the Asynchronous Layered Coding (ALC) protocol instantiation [72]. ALC combines the Layered Coding Transport (LCT) building block [71] a congestion control building block and the Forward Error Correction (FEC) building block [48] to provide congestion controlled reliable asynchronous delivery of content to an unlimited number of concurrent receivers from a single sender. See Figure 19 for an illustration of FLUTE building block structure.

FLUTE is carried over UDP/IP, and is independent of the IP version and the underlying link layers used.

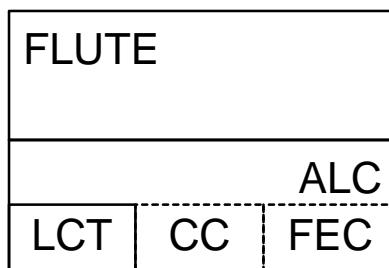


Figure 19: Building block structure of FLUTE

ALC uses the LCT building block to provide in-band session management functionality. The LCT building block has several specified and under-specified fields that are inherited and further specified by ALC. ALC uses the FEC building block to provide reliability. The FEC building block allows the choice of an appropriate FEC code to be used within ALC, including using the no-code FEC code that simply sends the original data using no FEC coding.

ALC is under-specified and generally transports binary objects of finite or indeterminate length. FLUTE is a fully-specified protocol to transport files (any kind of discrete binary object), and uses special purpose objects - the File Delivery Table (FDT) Instances - to provide a running index of files and their essential reception parameters in-band of a FLUTE session.

The CDS HNED and the CDS network shall implement all the mandatory parts of the FLUTE specification IETF RFC 3926 [70], as well as ALC IETF RFC 5775 [72] and LCT IETF RFC 5651 [71] features that FLUTE inherits.

In addition, several optional and extended aspects of FLUTE, as described in the following clauses, shall be supported by the CDS HNED and network functions.

10.6.2.2.1 Segmentation of files

Segmentation of files shall be provided by:

- a blocking algorithm which calculates source blocks from source files; and
- a symbol encoding algorithm which calculates encoding symbols from source blocks.

10.6.2.2.2 Symbol Encoding Algorithm

The applied Symbol Encoding Algorithm is signalled in the download session parameter *FEC-Encoding-ID*.

The "Compact No-Code FEC scheme" [73] (*FEC-Encoding-ID=0*, also known as "Null-FEC") shall be supported.

The "Raptor FEC Scheme" (*FEC-Encoding-ID=1*) as defined in [65], clause 8 and IETF RFC 5053 [77] consists of two distinct components:

- Source block and source packet construction and reception.
- Repair packet construction and reception and Raptor FEC encoding and decoding.

The CDS HNED function shall support the source block and source packet construction and reception for the "Raptor FEC Scheme". Support of the Source Block and Source Packet construction component requires support of the FEC Payload ID and FEC Object Transmission Information defined in [65], clauses 8.1.2 and 8.1.3 as well as the source packets constructed according to [65], clauses C.3.1 and C.3.2.1.

The CDS HNED function that supports repair packet construction and reception and Raptor FEC encoding and decoding requires support of annex C of [65].

10.6.2.2.3 Use of multiple FLUTE channels

A file (or some encoding symbols of a file) may be sent simultaneously or at different times over multiple channels.

The number of FLUTE channels is signalled in the delivery parameter *Number-of-Channels*.

The use of multiple FLUTE channels for a FLUTE session shall be supported by CDS HNEDs and may be supported by CDS network functions.

The HNED shall support the reception of at least 16 FLUTE channels within one FLUTE session.

Multiple channels may be used to provide multicast rate adaptation according to clause 10.6.2.3.

10.6.2.2.4 Blocking Algorithm

In the case of the Compact no-Code FEC Scheme (*FEC-Encoding-ID=0*) [73], the "Algorithm for Computing Source Block Structure" described within the FLUTE specification shall be used.

In the case of the Raptor FEC Scheme (*FEC-Encoding-ID=1*), the source block construction algorithm described in ETSI TS 102 472 [65], clause C.3.1, shall be used.

10.6.2.2.5 Congestion Control

No mechanisms for multicast congestion control are provided in the present specification. Multicast rate adaptation as introduced in clause 10.6.2.3 may be used for the purpose of congestion control.

10.6.2.2.6 Content encoding of files for transport

Files may be content encoded for transport in the file delivery method using the GZip algorithm IETF RFC 1952 [74]. Terminals shall support GZip content decoding of FLUTE files. For GZip-encoded files, the FDT File element attribute "Content-Encoding" shall be given the value "gzip".

10.6.2.2.7 Further Considerations

For informative ALC packet size considerations, refer to ETSI TS 102 472 [65], clause 6.1.8.

For normative procedures on signaling the end of file delivery and end of file download session, refer to ETSI TS 102 472 [65], clause 6.1.9.

Spanning files over several download sessions shall not be used.

File grouping as specified in ETSI TS 102 472 [65], clause 6.1.11 shall not be used. The grouping of files for a content item is signalled by the download session description.

File versioning as specified in ETSI TS 102 472 [65], clause 6.1.12 shall not be used. Instead content item versioning as defined in clause 10.6.6 is used.

10.6.2.2.8 Signalling of Parameters with FLUTE

10.6.2.2.8.1 Signalling of Parameters with basic ALC/FLUTE Headers

FLUTE and ALC mandatory header fields shall be as specified in the FLUTE specification IETF RFC 3926 [70] and the ALC specification IETF RFC 5775 [72], with the following additional specializations:

- In FLUTE the following applies: The length of the CCI (Congestion Control Identifier) field shall be 32 bits and it is assigned a value of zero (C=0).
- The Transmission Session Identifier (TSI) field shall be of length 16 bits (S=0, H=1, 16 bits) or 32 bits (S=1, H=0) when TOI is an identifier of 32 bits.
- The Transport Object Identifier (TOI) field should be of length 16 bits (O=0, H=1) or 32 bits (O=1, H=0).
- Only Transport Object Identifier (TOI) 0 (zero) shall be used for FDT Instances.
- The following features shall be used for signalling the end of session; the following features should be used for signalling an end of object transmission to the receiver prior to the FDT expiry date:
 - The Close Session flag (A) for indicating the end of a session as described in ETSI TS 102 472 [65], clause 6.1.9.
 - The Close Object flag (B) for indicating the end of an object as described in ETSI TS 102 472 [65], clause 6.1.9.

In FLUTE the following applies:

- The LCT header length (HDR_LEN) shall be set to the total length of the LCT header in units of 32-bit words.
- For "Compact No-Code FEC scheme" (*FEC-Encoding-ID*=0), the payload ID shall be set according to IETF RFC 3695 [73] such that a 16 bit Source Block Number (SBN) and then the 16 bit ESI are given.

10.6.2.2.8.2 Signalling of Parameters with FLUTE Extension Headers

FLUTE extension header fields EXT_FDT, EXT_FTI, EXT_CENC according to IETF RFC 3926 [70] shall be used as follows:

- EXT_FTI shall be included in every FLUTE packet carrying symbols belonging to any FDT Instance.
- FDT Instances shall not be content encoded and therefore EXT_CENC shall not be used.

In FLUTE the following applies:

- EXT_FDT is in every FLUTE packet carrying symbols belonging to any FDT Instance.
- FLUTE packets carrying symbols of files (not FDT instances) shall not include the EXT_FDT.

The optional use of EXT_FTI for packets carrying symbols of files (not FDT instances) shall comply to FLUTE for the signalling of FEC Object Transmission Information associated to FEC Encoding 0.

When Raptor forward error correction code (*FEC-Encoding-ID*=1) is used, the EXT_FTI format as defined in ETSI TS 102 472 [65], clause 8.1.3, shall be used.

10.6.2.2.8.3 Signalling of parameters with FDT instances

The FLUTE FDT Instance schema defined in clause 10.6.2.2.8 shall be used. Some of the data elements can be included at the FDT-Instance or at the file level. In this case, the data element values in the file element override the same in the FDT Instance element. In addition, the following applies to both the FDT-Instance level information and all files of a FLUTE session.

The inclusion of these FDT Instance data elements is mandatory according to the FLUTE specification:

- Content-Location (URI of a file); this shall be an *absolute path* syntax <path-absolute> as defined in clause 10.5.2. No server information shall be included;

- TOI (Transport Object Identifier of a file instance);
- Expires (expiry data for the FDT Instance).

Additionally, the inclusion of the following FDT Instance data elements is mandatory:

- Content-Length (source file length in bytes);
- Content-Type (content Mime type). This attribute shall be either in the FDT-Instance or File element or in both.

The inclusion of the following FDT Instance data elements is optional and depends on the FEC Scheme:

- FEC-OTI-Maximum-Source-Block-Length;
- FEC-OTI-Encoding-Symbol-Length;
- FEC-OTI-Max-Number-of-Encoding-Symbols;
- FEC-OTI-Scheme-Specific-Info.

These optional FDT Instance data elements may or may not be included for FLUTE in CDS:

- Complete (the signalling that an FDT Instance provides a complete, and subsequently not modifiable, set of file parameters for a FLUTE session may or may not be performed according to this method);
- FEC-OTI-FEC-Encoding-ID (the default value is FEC Encoding ID 0);
- FEC-OTI-FEC-Instance-ID;
- Content_Encoding;
- Transfer_length;
- Content-MD5 (Checksum of the file as defined in IETF RFC 3926 [70]).

10.6.2.2.9 FDT Structure

Table 27 provides an overview of the FDT structure. The corresponding XML schema is given in ETSI TS 102 472 [65], clause 6.1.15. For details on syntax and semantics refer to IETF RFC 3926 [70].

**Table 27: Overview - FLUTE File Delivery Table (FDT) structure
(for details, refer to RFC 3926 [70])**

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
FDT-Instance-Attributes	Common Attributes for all the files described by the FDT instance	
Expires	expiry time of the FDT Instance.	M
Complete	when present and TRUE, signals that no new data will be provided in future FDT Instances within this session.	O
Content-Type	content type.	O
Content-Encoding	Content encoding.	O
FDT-Instance-Delivery-Attributes	Attributes related to the delivery of all files described by the FDT instance	
FEC-OTI-FEC-Encoding-ID	Identification of FEC algorithm.	O
FEC-OTI-FEC-Instance-ID	FEC instance depending on the FEC algorithm identification.	O
FEC-OTI-Maximum-Source-Block-Length	The maximum number of source symbols per source block.	O
FEC-OTI-Encoding-Symbol-Length	Length of encoding symbols in bytes.	O
FEC-OTI-MaxNumber-Of-Encoding-Symbols	Maximum Number of Encoding Symbols that can be generated for a source block.	O
FEC-OTI-Scheme-Specific-Info		O
File Attributes (one per file)		
Content-Type	MIME media type of content.	O
Content-Encoding	Compression.	O
Content-Location	<path-absolute>.	M
Content-Length	Size of the content.	M
Content-Digest	Hash of the content (MD5).	O
Content-Delivery-Attributes	Attributes related to the delivery of the file	
TOI	Transport Object Identifier.	M
Transfer-Length	Size of the transport object carrying the content.	O
Bandwidth-Requirement	Aggregate rate of sending packets to all channels.	O
FEC-OTI-FEC-Encoding-ID	Identification of FEC algorithm.	O
FEC-OTI-FEC-Instance-ID	FEC instance depending on the FEC algorithm identification.	O
FEC-OTI-Maximum-Source-Block-Length	The maximum number of source symbols per source block.	O
FEC-OTI-Encoding-Symbol-Length	Length of encoding symbols in bytes.	O
FEC-OTI-MaxNumber-Of-Encoding-Symbols	Maximum Number of Encoding Symbols that can be generated for a source block.	O
FEC-OTI-Scheme-Specific-Info		O

NOTE 1: Mandatory (M) here means that if the Optional parent element is transmitted, then this field shall be present.

NOTE 2: Mandatory means that the CDS network function shall signal the corresponding element.

10.6.2.3 Multicast Rate Adaptation

10.6.2.3.0 General rules

Multicast rate adaptation is supported by the use of multiple FLUTE channels for a single FLUTE session. All channels are transported via different multicast groups.

10.6.2.3.1 CDS network procedures

To support multicast rate adaptation, the CDS network multicast download function should use multiple FLUTE channels in combination with "Raptor FEC Scheme". The number of FLUTE channels is advertised in the download session description in the parameter *Number-Of-Channels*.

Each FLUTE channel is transported via a dedicated multicast group identified by a unique *IP-Multicast-Address*. In addition to support multicast rate adaptation the CDS network function should also signal the *Max-Bandwidth parameter*, for each channel. By the order of the channels listed in the download session description, the CDS network function defines in which order the HNED shall join the channels.

The CDS network function shall not exceed the maximum bandwidth advertised by the *Max-Bandwidth* parameter, for each multicast group.

The distribution of source packets as well as FEC packets, if applicable, to different multicast groups may be done in various fashions by the CDS network function and is beyond the scope of the present document.

In case Raptor FEC is supported by all CDS HNED functions, the CDS network function should evenly distribute FLUTE/UDP packets across multicast groups according to the data rate for each group.

The allocation of bandwidth to multicast groups may be done in various fashions by the CDS network function and is beyond the scope of the present document.

10.6.2.3.2 CDS HNED procedures

By the reception of the download session description the CDS HNED has access to the number of multicast groups in this session (*Number-of-Channels*) as well as for each multicast group access to:

- multicast group identifier, IP-Source-Address, IP-Multicast-Address and IP-Multicast-Port-Number;
- the maximum bandwidth, Max-Bandwidth;
- the multicast group order, defined by the order in which the channels are listed in the download session description.

CDS HNEDs may join the session by joining one or more of the multicast groups. HNEDs should join a number of multicast groups such that the total bandwidth approximates the HNEDs available bandwidth. The HNED can detect the current available bandwidth by measuring the incoming data rate from the subscribed multicast groups. If this is less than the sum of the advertised rates of the subscribed multicast groups, then this measured rate equals the available bandwidth (at that time).

During reception of a CDS multicast session or sessions, the HNED shall calculate the following two figures:

Subscribed CDS bandwidth This is the total bandwidth of the subscribed multicast groups being the sum of the rates of the subscribed multicast groups as advertised in the download parameter *Max-Bandwidth*.

Observed CDS bandwidth: This is the total observed data rate of incoming CDS data at any given time. The timescale on which observed bandwidth is measured and the exact bandwidth measurement algorithm are implementation specific. The timescale should be less than the frequency with which multicast group membership is adjusted and should be greater than one tenth of this time.

The HNED should adjust multicast group membership on a continuous basis such that the *Subscribed CDS bandwidth* is the least possible value which is not less than the *Observed CDS bandwidth*. The possible values of Subscribed CDS bandwidth are constrained by the advertised multicast groups and their data rates. The HNED shall not adjust its CDS multicast group membership more than once every 30 s.

The CDS HNEDs shall join and leave multicast groups in the order as they are listed in the download session description. Multicast groups that are listed first shall be joined first and left last.

10.6.2.4 File download from the FLUTE session

The files that have to be downloaded by the HNED from the FLUTE session are provided in the download session description (by the *File-Reference* parameters). If the *File-Reference* parameter is not present all files of the FLUTE session shall be downloaded.

In case *File-Reference* parameters are provided the HNED compares them against the *Content-Location* URIs in the Flute FDT in order to identify the files in the FLUTE session.

In case that from a previous download session for the same content item (identified by the same CRID) a file with the same <path-absolute> already exists on the local storage and a MD5 digest and content length is provided for the file in the FLUTE FDT the HNED compares that against the content length and MD5 digest of the file on the local storage. If they are the same the file should not be downloaded. Otherwise the file on the CDS HNED storage shall be deleted and the new version of the file shall be downloaded.

If requested by the download session description, the HNED shall perform a reception reporting as defined in clause 10.6.5 after the successful download of all files of the content item.

10.6.2.5 CDS Network-based Session Completeness

10.6.2.5.1 Basic Principle

If the download session is a scheduled multicast session, i.e. *Download-Session-Mode* = "SMD", the CDS network function should use a completion polling mechanism to determine when to stop the multicast download session at the Multicast File Server.

CDS HNEDs, which have completely received the file or files being distributed, shall leave the subscribed multicast groups and terminate their participation in this download session.

As a result, the multicast tree will shrink as time passes and receivers complete the reception. However, it is likely that not all receivers will complete at the same time due to:

- different receivers have different incoming available bandwidth;
- different receivers experience different packet loss levels.

For this purpose the CDS Multicast Download Function periodically sends a "Completion Poll" message within the FLUTE session. The Completion Poll contains a single, 32-bit field, "POLL_MASK" which HNEDs use to determine whether or not to send a reply to the server. For this purpose, each CDS HNED function is configured with a fixed "pseudo-random" 32-bit number, referred to as POLL_MASK_X. If not specified otherwise the HNED shall use the 4 least significant bytes of its MAC address.

To prevent the possibility of message implosion at the server when there are many HNEDs, the HNEDs use the POLL_MASK field from the Completion Poll message to determine whether to reply. The poll request is received only by those HNEDs that have not completed the reception of the file. With the reception of the poll request the CDS HNED calculates the logical AND of its internal POLL_MASK_X and the POLL_MASK value provided by the server. If the result is zero, the HNED replies to the Completion Poll message by sending a completion poll response message using the completion poll response server connection information.

The Completion Poll response message uses a simple UDP-based protocol. The message is specified in clause 10.6.2.5.2 and contains:

- The sequence number of the request message to which the message refers to.
- The source address and TSI of the FLUTE session.
- The HNED's local poll mask.
- The CDS HNED's estimation of the remaining time it requires to receive the file or files.

NOTE: No special reliability mechanisms are required for the Completion Poll message or the reply. Since the Completion Poll with POLL_MASK=0 will be repeated several times before ending the session the chance that the session ends too early (whilst receivers are still listening) can be made exceedingly low.

The completion poll message formats, the CDS network procedures, and the HNED procedures are described.

10.6.2.5.2 Message formats

10.6.2.5.2.1 Completion Poll Request

The Completion Poll Request is a LCT Header Extension as defined in [71]. The Congestion Poll LCT Header Extension shall be included in a normal FLUTE packet associated with a transport object and the normal rules for LCT header settings apply.

The format of the Completion Poll Request LCT Header Extension is shown in Figure 20.

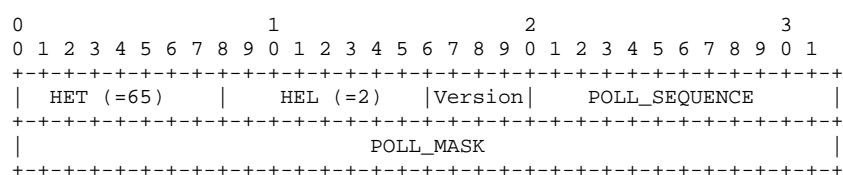


Figure 20: Completion Poll Request LCT Header Extension

Header Extension Type (8 bits) (HET): This field identifies the header extension as a Completion Poll Request. The value shall be set to 65 as assigned by IANA.

Header Extension Length (8 bits) (HEL): This field gives the length of the header extension in units of 32-bit words.

Version (4 bits): The protocol version. In this version of the protocol this field shall be set to zero.

POLL_SEQUENCE (12 bits): A sequence number for the Completion Poll Request.

POLL_MASK (32 bits): A value chosen by the CDS network function to support filtering of poll responses.

10.6.2.5.2.2 Completion Poll Response

The completion poll response message shown in Figure 21 is sent over UDP transport to the address specified in the *Completion-Poll-Response-Server-Address* and the port *Completion-Poll-Response-Server-Port-Number*.

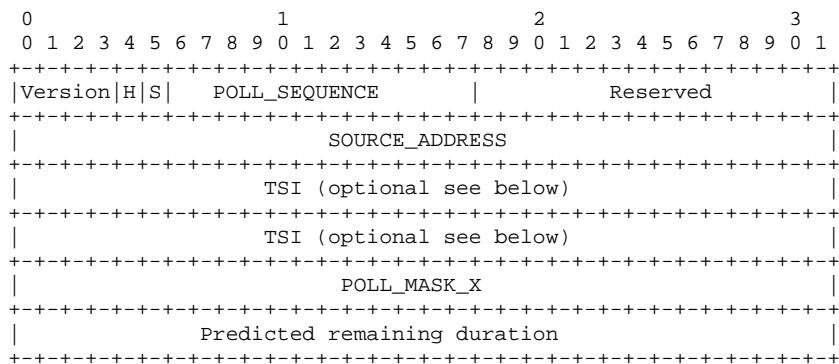


Figure 21: Completion Poll Response

Version (4 bits): This shall be set to zero in this version of the protocol.

Transport Session Identifier flag (S, 1 bit): This is the number of full 32-bit words in the TSI field. The TSI field is $32*S + 16*H$ bits in length, i.e. the length is either 0 bits, 16 bits, 32 bits, or 48 bits. It shall be identical to the S-flag of the FLUTE session to which this completion poll response corresponds.

Half-word flag (H, 1 bit): The TSI field is a multiple of 32-bits plus 16*H bits in length. Shall be identical to the H-flag of the FLUTE session to which this completion poll response corresponds.

Reserved (10 bits): This shall be set to zero in this version of the protocol. The receiver shall ignore this field.

POLL_SEQUENCE (12 bits): This shall be set to the POLL_SEQUENCE value of the Completion Poll Request message which triggered this response.

SOURCE_ADDRESS (32 bits): This shall be set to the IPv4 Source Address of the FLUTE session as provided in the download session description.

TSI (0, 32, 64 bits): Depending on the S and H flag, the length of the field is:

- 0 bit for S=H=0;
- 32 bit if S=1 and H=0 or S=0 and H=1;
- 64 bit for S=H=1.

The first $32*S + 16*H$ bit of this field shall be identical to the TSI-value of the FLUTE session to which this completion poll response corresponds. The last $16*H$ bit shall be set to "0".

POLL_MASK_X (32 bits): This shall be set to the POLL_MASK_X value used by the client when processing the Completion Poll Request.

Predicted Remaining Duration (32 bits): This shall be set to an estimate of the remaining time in seconds that will be required for this receiver to complete reception of the file, or zero if no estimate can be made. The estimation of the remaining time is implementation specific.

10.6.2.5.3 CDS network procedures

In the scheduled download session mode (*Download-Session-Mode*="SMD") the CDS network function should use completion poll mechanism.

The CDS network function shall indicate the use of completion polling by the provisioning of completion poll response server information (*Completion-Poll-Response-Server-Address* and *Completion-Poll-Response-Server-Port-Number*) in the download session description.

The Completion Poll procedure is initiated by the CDS network function by including a Completion Poll Request message in one or more packets of the multicast transmission of the base FLUTE channel. If there are multiple multicast groups, the Completion Poll Request shall only be included in the base FLUTE channel.

The CDS network function sets the POLL_SEQUENCE value according to the number of executions of the Completion Poll procedure for the session so far: for the first Completion Poll Request procedure, the POLL_SEQUENCE value shall be zero and it shall be incremented by one for each new Completion Poll Request procedure.

The CDS network function should set the POLL_MASK value preferably based on an estimate of the number of active receivers and a target number of responses. Note that before execution of the Completion Poll procedure, there is no way to estimate this number and so the server should use a default, maximal value. The target number of response is implementation-specific.

Initially, the CDS network function should choose a POLL_MASK value with a large number of non-zero bits. The probability that a HNED sends a reply to the Completion Poll is then very low (in fact it is 2^{-b} , where b is the number of non-zero bits in POLL_MASK.) Even if there are many receivers still listening to the session, the response to the Completion Poll will be small.

If there are no replies to a Completion Poll message after a short time, the CDS network function should repeat the message with fewer non-zero bits. This process is repeated until either a reply is received, or a number of Completion Poll message have been sent with POLL_MASK = 0 (in which case all HNEDs should reply) and there are no replies. In this last case the session ends.

The Completion Poll Request should be included in *Nrepeat* packets in each multicast group, in which case the POLL_SEQUENCE and POLL_MASK values shall be the same in every message. The recommended value of *Nrepeat* is 20.

On receipt of a Completion Poll Response message, the server shall check the POLL_SEQUENCE field of the received response against the POLL_SEQUENCE value included in the last sent Completion Poll Request message. If they are different, the received message shall be discarded.

Otherwise, the CDS network function shall calculate the logical AND of the received POLL_MASK_X value and the POLL_MASK of the last sent Completion Poll Request message. If the result is non-zero the server shall discard the received message.

Otherwise, the CDS network function may use the Predicted Remaining Duration field to determine the remaining duration of the session. The exact use of the Predicted Remaining Duration field is outside the scope of the present document.

The CDS network function should count the number of received responses within a timeout of *Tresponse*. The recommended value of *Tresponse* is 10 seconds. This number, multiplied by 2^w , where w is the poll weight used to calculate the POLL_MASK field of the Completion Poll Request may be used as the estimated number of active receivers for the next Completion Poll Request.

Finally, if no responses are received to the Completion Poll Request within *Tresponse*, and if the poll weight, w, used was non-zero, the CDS network function should repeat the Completion Poll procedure using poll weight w-1.

10.6.2.5.4 CDS HNED procedures

The CDS HNED shall determine the end of file delivery according to the procedures provided in clause 10.6.2.2.

If a CDS HNED has completely received all the files being defined by the download session description, the download session is completed for this HNED and it shall leave the subscribed multicast groups terminating its participation in the download session. It will therefore also no longer receive completion poll request messages.

If completion poll response server information (*Completion-Poll-Response-Server-Address* and *Completion-Poll-Response-Server-Port-Number*) is provided in the scheduled download session mode (*Download-Session-Mode="SMD"*) and the HNED is participating in this download session the CDS HNED shall expect the reception of Completion Poll Request messages on the first joined multicast group.

On receipt of a Completion Poll Request message, the HNED first checks the POLL_SEQUENCE value. If the HNED has previously processed a Completion Poll Request with a POLL_SEQUENCE value greater than or equal to this one, then the message shall be discarded.

Otherwise, the HNED checks the received POLL_MASK value. Each HNED is provided, by implementation-specific means, with a fixed pseudo-random 32-bit number POLL_MASK_X. The HNED calculates the logical AND of the received POLL_MASK and the provided POLL_MASK_X. If this calculated value is non-zero, the Completion Poll Request shall be discarded.

Otherwise, the HNED shall construct and send a Completion Poll Response message according to the procedures of clause 10.6.2.5.2 and send it to the address indicated in the *Completion-Poll-Response-Server-Address* parameter of the download session description and the UDP destination port indicated in the *Completion-Poll-Response-Server-Port-Number* parameter of the download session description.

A single message is sent from HNED to the server over UDP containing identification of the session the message refers to, the POLL_SEQUENCE, as well as the CDS HNEDs estimate of the remaining time it requires to receive all the files of this download session.

An HNED compliant to this version of the protocol shall ignore the Version field of the Completion Poll Request and shall ignore any additional data after the POLL_MASK field.

An HNED compliant to this version of the protocol shall set the Version field of the Completion Poll Response to zero.

10.6.2.6 File Repair Procedure

10.6.2.6.1 General Procedure

The purpose of the File Repair Procedure is to repair and complete files for which the multicast download session was not completed successfully.

Incomplete reception of a multicast download session may occur for different reasons. Examples are that the HNED is forcibly disconnected from a session, or that an HNED joins a scheduled session after the appointed start time and the download cannot be completed, etc.

The CDS network function indicates the availability of a file repair procedure for this download session by providing the base URI (see clause 10.5.2) of one or more recovery servers in the download session description (*Recovery-Server-Base-URI* parameter).

Moreover a *Recovery-mode* flag in the download session description indicates to the CDS HNED which kind of file repair procedures to apply: an IPDC-like file repair procedure or a specific CDS file repair procedure.

The CDS HNED shall only initiate the file repair procedure in case the content version of the content item has not changed. For the detailed behaviour see clause 10.6.6.

In case of an IPDC-like file repair procedure the CDS HNED follows exactly the File Repair Strategy described in ETSI TS 102 472 [65], clause 7.3. The general procedure is then:

- The HNED identifies the missing data from a file delivery according to ETSI TS 102 472 [65], clause 7.3.3.
- It waits for the Back-off Time as defined in clause 10.6.2.6.3 of the present document.
- It sends requests for the missing parts of the file according to ETSI TS 102 472 [65], clause 7.3.6.
- The CDS network function responds to the message with repair data according to ETSI TS 102 472 [65], clause 7.3.7.

- Optionally a redirection of the file repair to another repair server or a multicast session that delivers the same files as defined in ETSI TS 102 472 [65], clauses 7.3.7 and 7.3.8 can be used.
 - In case of a redirection to a unicast repair server the returned URI shall contain the server base URI in <http-server-base-URI> syntax.
 - In case of a redirection to a multicast repair service the returned URI shall point to the download session description of the multicast download session as defined in clause 10.5, i.e. the returned URI shall be any URI as defined in clause 10.3.2. Both unicast and multicast transport of the session description are supported. The CDS HNED shall then follow the multicast content download procedures defined in this clause to join the session and download the missing data.

In case of a specific CDS file repair the procedure basically follows the IPDC-like file repair procedures except that the unicast download procedures as specified in clause 10.6.3 are used for the file repair procedure. In this case the general procedure is the following:

- The HNED identifies the missing data from a file delivery according to clause 10.6.2.6.2.
- By applying *reference resolution*, it generates a request-URI in *absolute URI* syntax <absolute-URI> constructed from the *Recovery-Server-Base-URI* in <http-server-base-URI> syntax of a randomly selected recovery server and the *File-Reference* in <path-absolute> syntax of the file with the missing data.
- It waits for the Back-off Time as defined in clause 10.6.2.6.3.
- It sends a HTTP requests for the missing parts of the file using the request-URI. The HTTP range header of the request identifies the missing and requested data.
- The CDS network function responds to the request and returns the data or initiates a redirection as defined in clause 10.6.3.4.
- The response could be a redirection as defined in clause 10.6.3.4.

Note that in this case HNEDs which entirely miss a file in the multicast session should simply use the Unicast download mode in straightforward fashion.

10.6.2.6.2 Identification of file repair needs

At the end of a file delivery (see clause 10.6.2.2) the HNED identifies its file repair needs associated to the delivered content item. The FLUTE stack provides the receiver with sufficient information to determine the source block and encoding symbol structure of each file and corresponding FDT instance.

In case of IPDC-like file repair (*Recovery-mode=1*), the procedures in ETSI TS 102 472 [65], clause 7.3.3 shall be applied. In case of CDS-based file repair (*Recovery-mode=0*) the CDS HNED function should invert the Source Blocking as specified in clause 10.6.2.2 to map the received encoding symbols to a partially received file. From this information, the receiver is able to determine the ranges of missing bytes sufficient to complete the reception and recovery of the file and request those bytes range over the recovery procedure.

In the case that the Raptor FEC scheme is used, the receiver should take into account any Raptor parity symbols that have already been received when determining the ranges of missing bytes sufficient to complete the reception of the specific file. Specifically, the acquired data through the repair procedure should be mapped to encoding symbols by the use of the Source Blocking as specified in clause 10.6.2.2 and if appropriate, FEC decoding should be applied to recover source blocks and the entire file.

Every time the end of a multicast download session is detected, every CDS HNED shall check whether there is missing content in the session in comparing the files received in the FLUTE session against the files announced in the service advertisement (e.g. download session description or FLUTE FDT). If some parts of the delivered content are missing the CDS HNED shall request sufficient data to recover the entire content item.

10.6.2.6.3 Distribution of Recovery requests over time

To resolve the problem of feedback implosion at each end of file delivery and at the end of the download session every request messages to a unicast download mode server is delayed in adopting the same strategy than in ETSI TS 102 472 [65], clause 7.3.4. The offset time and random time period parameters are provided by the session announcement (*Recovery-Offset-Time* and *Recovery-Random-Time*).

10.6.3 Unicast Content Download

10.6.3.1 General

The Unicast content download mode provides download of content items to single HNEDs using IP unicast based on HTTP as defined in RFC 2616 [39]. The availability of content items via Unicast download mode is advertised in the download session descriptions according to clause 10.5.

Unicast Content Download is also organized in download sessions. A download session is characterized as an instance of the CDS with a start time and optionally an end time as well as download URIs for the files corresponding to the content item between the start and end time. The start and end times are signalled in the *Download-Session-Time-Information* parameter.

The download session parameter *Download-Session-Mode*="UD" shall be used by the CDS network function to indicate unicast download.

Individual files of different content items may be either downloaded from a single server (single server unicast download) as defined in clause 10.6.3.2 or from multiple servers (single server unicast download) as defined in clause 10.6.3.3.

In case of a single server unicast download, redirection to an alternative single server download, to a multiple server download or to a multicast download session as defined in clause 10.6.3.4 may be performed.

In case that from a previous download session for the same content item (identified by the same CRID) a file with the same *File-Reference* already exists on the local storage and a MD5 digest and content length is provided for the file in the download session description the HNED compares that against the content length and MD5 digest of the file on the local storage. If they are the same the file should not be downloaded. Otherwise the file on the CDS HNED storage shall be deleted and the new version of the file shall be downloaded.

10.6.3.2 Single server unicast download

Single server file download shall be performed if no file chunk information (missing *File-Length* and *Chunk-Length* parameters) or only a single server location (*Server-Base-URI* parameter) is provided for the file.

The HNED shall generate the request-URI by *reference resolution* with the base URI *Server-Base-URI* of a randomly selected server out of the list of announced servers for the file and the relative reference *File-Reference* and initiates a HTTP transfer of the file using the request URI. In case the File-Content-Type is present in the download session description an Accept header shall be included in the request with the specified Content-Type.

The CDS network function (HTTP server) may respond with:

- the requested file;
- a redirection request as defined in clause 10.6.3.4;
- a "503" (Service Unavailable) status code and a "Retry-After" response header which indicates to the HNED to retry the initial file request after the delta time or after the date and time provided by the "Retry-After" header;
- a "410" (Gone) status code which indicates that the download session is terminated (see clause 10.6.6).

If the server does not respond as above, e.g. a "500" (Internal Server Error) status code or a "503" (Service Unavailable) without a "Retry-After" response, the CDS HNED shall select another server out of the list of servers announced for that file and start a new file download. The CDS HNED shall continue this procedure until the request was successful or all announced servers have been tried.

In case reception reporting servers are defined in the download session description, the HNED shall perform reception reporting as defined in clause 10.6.5 after the successful download of a file and/or all files of the content item.

10.6.3.3 Multiple server unicast download

Multiple server file download shall be performed if file chunk information (at least *File-Length* and *Chunk-Length* parameters) and multiple server locations (*Server-Base-URI* parameters) are provided for a certain file. In this case the following procedures shall apply.

In this case the HNED shall randomly distribute the download of individual chunks of the file over the server locations provided for the file, taking into account the availability of the chunks on the individual servers (*Available-Chunk-List* parameter). The HNED shall ensure that all chunks of the file are downloaded.

NOTE 1: The method for distributing the requests over the server locations is outside the scope of the present document.

For each selected server the HNED shall generate the request-URI by *reference resolution* with the base URI *Server-Base-URI* and the relative reference *File-Reference*.

For each chunk that shall be downloaded from the server the HNED calculates the byte range based on the constant chunk length (*File-Chunk-Length* parameter) and the chunks position. The byte range shall be calculated as defined for the HTTP range header in IETF RFC 2616 [39]. It should be noted that the length of the last chunk could be shorter than the constant chunk length.

The HNED initiates a HTTP request for the chunk using the request-URI and including the byte range of the chunk that is requested from this server into the HTTP range header. In case the Content-Type of the file is specified (*File-Content-Type* parameter) an Accept header shall be included in the request with the specified MIME media type.

The CDS network function (requested HTTP server) shall return the requested chunk with a status code of 206 (Partial content) and indicate the delivered content range in the Content-Range header.

A HNED may combine the requests for several chunks from the same server location (same request-URI) into a single HTTP request by including the byte ranges of all the chunks into the range header. The server shall respond to a request for multiple none consecutive byte ranges (chunks) with a multipart message (multipart media type "multipart/byteranges") as defined in IETF RFC 2616 [39]. Each byte range is delivered in a separate part of the multipart message.

NOTE 2: The use of a single combined request or several individual requests of chunks from the same server location is outside the scope of the present document.

If the MD5 digest is provided for the chunks in the download session description (*Chunk-Digest* parameter) the HNED shall verify the correct reception of the chunk by comparing that digest with the digest of the received chunk. If they are different the received chunk shall be discarded.

In case the server returns a 410 (Gone) status code the download session is terminated (see clause 10.6.6).

If a chunk cannot be downloaded successfully the HNED shall try to download the chunk from another server if available.

The HNED constructs the file from the received chunks. If the MD5 digest is provided for the file in the download session description (*File-Digest* parameter) the HNED shall verify the correct reception of the file by comparing that digest with the digest of the file constructed from the received chunks. If they are different the received file shall be discarded.

The HNED may try to download the file again from other servers if available.

In case reception reporting servers are defined the HNED shall perform reception reporting as defined in clause 10.6.5 after the successful download of a chunk and/or file and/or the content item.

NOTE 3: It is worth to note that nothing in the multiple server unicast download procedures makes any assumptions about the location or topology of the various servers. For example, servers may be network-based or may reside on HNEDs to support advanced distributed media delivery. However, server locations and management is not in the scope of the present document.

10.6.3.4 Redirection

10.6.3.4.0 Types of redirection

A single server unicast download request might be redirected to:

- an alternative single server file download (see clause 10.6.3.4.1);
- a multiple server file download (see clause 10.6.3.4.2);
- a multicast download session (see clause 10.6.3.4.3).

Redirection is indicated by the CDS network function by providing a HTTP response with a redirection status code (3xx) to the initial HTTP request of the HNED.

10.6.3.4.1 Alternative single server redirection

For a redirection to an alternative single server file download the CDS network function shall respond to the file download request with a status code of "302" (Found). A new *base URI* with syntax of <http-server-base-URI> for the alternative server is provided by the location field of the response. A "Retry-After" response header may be provided which indicates to the HNED to perform the redirection after the delta time or after the date and time provided by the "Retry-After" header.

The HNED shall initiate a single server file download after the delta time or data and time defined by the "Retry-After" header or immediately if this header is not provided. The single server file download procedures as defined in clause 10.6.3.2 shall be performed. The new *base URI* provided by the redirection shall be used as the new *Server-Base-URI*.

10.6.3.4.2 Multiple server redirection

For a redirection to a multiple server file download the CDS network function shall respond to the file download request with a status code of "300" (Multiple Choices). The entity of the response contains the description for the multiple server file download. A "Retry-After" response header may be provided which indicates to the HNED to perform the redirection after the delta time or after the date and time provided by the "Retry-After" header assuming that this time falls into the download session time announced in the download session description (see clause 10.5).

The description for the multiple server file download uses the semantics and syntax defined in clause 10.6.3.3 for a unicast download session. The CDS HNED shall support XML syntax and may support SDP syntax. The syntax is indicated by the appropriate Content-Type in the response. For the interpretation of the redirection information see clause 10.6.3.4.4.

NOTE 1: The same redirection method is also used for the multicast download redirection. The HNED will know from the Download-Session-Mode parameter which kind of redirection is used. A value of "UD" indicates a unicast redirection. A value of "SMD" or "CMD" indicates a multicast download redirection.

The HNED uses the original *File-Reference* of the file to identify the relevant information in the download session description.

NOTE 2: The download session description may contain information for more than one file, for example if the download session description for the whole content item is reused. Each file is uniquely identified by its *File- Reference* parameter.

The HNED shall initiate the multiple server download after the delta time or data and time defined by the "Retry-After" header or immediately if this header is not provided.

The multiple server file download procedure defined in clause 10.6.3.3 shall be used.

It should be noted that the download session description may define a single server file download instead of a multiple server file download for the file. In this case the single server file download procedure as defined in clause 10.6.3.2 shall be used.

10.6.3.4.3 Multicast download redirection

For a redirection to a multicast download the CDS network function responses to the file download request with a status code of "300" (Multiple Choices). The entity of the response contains the description for the multicast download. A "Retry-After" response header shall not be used. Information about the time of the multicast download session is provided in the session description.

The description for the multicast download uses the semantics and syntax defined in clause 10.5 for multicast download session. The CDS HNED shall support XML syntax and may support SDP syntax. The syntax is indicated by the appropriate MIME type in the response. For the interpretation of the redirection information see clause 10.6.3.4.4.

NOTE 1: The same redirection method is also used for the multiple server download redirection. The HNED will know from the Download-Session-Mode parameter which kind of redirection is used. A value of "SMD" or "CMD" indicates a multicast download redirection. A value of "UD" indicates a unicast redirection.

The HNED shall initiate the multicast download after the delta time or data and time defined by the "Retry-After" header or immediately if this header is not provided.

The multicast download procedure defined in clause 10.6.2 shall be used. The HNED shall use the *File-Reference* parameter of the file to identify it in the FDT of the FLUTE session.

NOTE 2: The FLUTE session and download session description may contain more than one file, for example if the redirection points to a FLUTE session for the whole content item. Each file is uniquely identified by its path-absolute relative reference (File-Path-Absolute parameter).

The present document does not define the procedures used by the CDS network function to determine whether redirection to a multicast session should be used. However, by way of example, one possibility for deciding when to establish a multicast session vs. serving the request via unicast download mode servers, and for coordinating the establishment of the session across multiple servers is described here:

- Unicast download mode requests may be received by many different unicast download mode servers. These servers inform the CDS management function whenever they begin serving a content item.
- The CDS management function is responsible for detecting when a substantial number of users request the same content item and, based on this, establishing a Multicast download session for that content item.
- When a Multicast Download session is established, the CDS management function sends a Session Advertisement over a local multicast group (for example using the Session Announcement Protocol (SAP)). This Session Advertisement is received by the various unicast download mode servers. The unicast download mode server will then redirect subsequent requests for the same content item to the multicast download session.
- Unicast download mode file servers which receive a session announcement for a multicast distribution session may choose to terminate unicast download mode sessions that are in progress for the content item. This should cause HNEDs to re-request the item, receiving the multicast session advertisement in response.

Redirection to both carousel and scheduled multicast download sessions is supported. However carousel multicast download is more likely to be used as it does not require the HNED to join the session at a specific time.

10.6.3.4.4 Interpretation of redirection information

The redirection information provided in the entity body by a "300" (Multiple Choices) response uses the download session description information as defined in clause 10.5 either in XML or SDP format. This information shall be interpreted as follows:

- *Service-Provider-Domain* and *Download-Session-ID* shall be the same as in the original request. If this is not the case the redirection information shall be ignored.
- *Download-Session-Version* might be different.
- *Content-Item-Format* information shall be the same as in the original request in case it is provided.
- *Download-Session-Mode* shall be provided and the indicated download mode shall be used for the redirection.

- *Download-Session-Time-Information* shall be provided. In case of unicast download ("UD") the HTTP redirection Retry-After information shall be taken into account. In case the time calculated based on the Retry-After information is outside the announced download session time window the HNED shall perform the redirection at the earliest time that fits into the announced download session time window. In case of a multicast download ("CMD" or "SMD") the HNED shall perform the redirection at the earliest time that fits to the announced download session time information.
- In case Reception Reporting information (*Reception-Reporting-Server-URI*, *Reception-Reporting -Mode*, *Reception-Reporting -Offset-Time*, *Reception-Reporting-Random-Time-Period*) is provided, it shall be the same as in the original request.
- Unicast or multicast specific information has to be provided for the redirected file download. The *File-Reference* parameter for the redirected file has to be the same as in the original download session description. The HNED shall use the original *File-Reference* parameter to identify the file specific parameters in the redirection information. In case of a redirection to a multicast download the HNED shall use the original *File-Reference* parameter to identify the file in the FDT of the FLUTE session (compare against the FDT Content-Location).

The CDS HNED shall update initial download session description with the information received in the redirection information.

10.6.4 Parallel downloads

A CDS HNED may perform parallel download of multiple content items in parallel download sessions. This depends on time of availability of the content items, the requested content items by the user in the pull download mode and the announced content items by the SP in the push download mode. The parallel content item download sessions can have different download session modes.

In case of parallel multicast downloads of multiple content items, the CDS HNED should adapt the multicast rate adaptation as introduced in clause 10.6.2.3 and share the observed bandwidth among the multicast downloads.

In case of any unicast download the HNED may perform parallel download of the files of a single content item. The details of parallel file downloads is outside the scope of the present document.

In case of a multiple server file download the HNED may perform parallel download of file chunks. The details of parallel file chunk downloads is outside the scope of the present document.

10.6.5 Reception Reporting

10.6.5.1 General

The CDS network function shall indicate the use of reception reporting by provisioning one or more *Reception-Reporting-Server-URIs* in the download session description.

The *Reception-Reporting-Mode* parameter defines the details of the reporting. This can be:

- content item reporting (*Reception-Reporting-Mode=0*);
- content item and file reporting (*Reception-Reporting-Mode=1*); and
- content item, file and chunk reporting (*Reception-Reporting-Mode=2*).

If the *Reception-Reporting-Mode* parameter is not provided, content item reporting (*Reception-Reporting-Mode=0*) shall be used. If chunk reporting is requested for the content item, it shall only be used for multiple servers file downloads. For files that are downloaded from a single server, *Reception-Reporting-Mode=1* (file reporting) shall be used.

The CDS HNED shall determine if the item(s) for which reporting is requested (e.g. content item, file, chunk) are successfully downloaded as defined in the download specifications above and send the reception reporting reports to a reception reporting server. The reception reporting server shall be chosen randomly from the list of reception reporting servers provided in the download session description (*Reception-Reporting-Server-URI* parameter). In case of a multicast download session the request shall be delayed by the back-off time as defined in clause 10.6.5.2. The reception reporting server shall respond as defined in clause 10.6.5.4.

10.6.5.2 Distribution of Reception reporting request over time

To resolve the problem of feedback implosion in case of multicast download, every request messages to a reception reporting server is delayed in adopting the same strategy used in ETSI TS 102 472 [65], clause 7.3.4. The offset time and random time period parameter are provided by the download session description (*Reception-Reporting-Offset-Time* and *Reception-Reporting-Random-Time-Period* parameter).

NOTE: The "Offset-Time" and "Random-Time-Period" used for delivery confirmation in multicast download mode may have different values from those used for file repair.

This back-off timing mechanism for the reception reporting is not used in unicast download mode. In this case the CDS HNED function shall initiate the reception reporting process immediately after the verification of download completion.

10.6.5.3 Reception reporting message

The HNED shall send a Reception Report request using the HTTP 1.1 POST request IETF RFC 2616 [39] carrying XML formatted reception reporting message.

Table 28 describes the parameters of the Reception Reporting message. The corresponding XML schema is provided in clause C.2.4.

For the successful download of a content item a content item reception report message shall be sent which includes information about the content item and all files of the content item as provided by the download session description. For each file it is indicated whether the download was performed or not performed in case the latest version of the file as identified by the file length and digest was already available at the HNED.

For the successful download of a file, a file reception report message shall be sent. In case the file download was not performed as the latest version of the file as identified by the file length and digest was already available at the HNED no reception reporting message shall be sent.

For the successful download of a file chunk a chunk reception report message shall be sent.

Table 28: Reception Reporting message

Parameter	Description	Type	Usage
Reporting type	Content item, file or chunk report.	inherent	all messages
Client-ID	Identification of the client.	string	all messages
Push-Action	Indicates that the download was initiated by a PushDownloadType (see clauses 10.3.1 and G.1.2).	boolean	all messages
CRID	Content Reference Identifier as provided by the BCG.	URI	all messages
Content-Version	Content Version number (see clause 10.6.6).	unsigned integer (8)	all messages
Download-Session-Parameters			
Service-Provider-Domain	Service provider domain (see clause 10.5.3).	domain name	all messages
Download-Session-ID	Identification of the download session (see clause 10.5.3).	unsigned integer	all messages
Download-Session-Version	Version of the download session (see clause 10.5.3).	unsigned integer	all messages

Parameter	Description	Type	Usage
Files (one per file)			
File-Reference	Relative reference of the file (see clause 10.5.2).	<path-absolute>	all messages
Chunks (one per chunk)			
Byte-Range	Byte range of the chunk of the file (as defined for HTTP range header IETF RFC 2616 [39]).	first byte position (unsigned integer); last byte position (unsigned integer)	Chunk message only

The Mime type of XML reception reporting message shall be set to application/xml.

The reporting for several items of the same type (e.g. several chunks in a chunk reception report message, several files in a file reception reporting message) can be aggregated into a single message.

Multiple messages of different types can be aggregated into a single HTTP request using Multipart MIME (multipart/mixed).

The "Client-ID" provides a unique identification of the CDS HNED that sends the reception reporting message. The specific value of the client ID and its provisioning at the HNED is outside the scope of the present document. If not specified otherwise the HNED shall use its MAC address as Client-ID.

NOTE: The HNED IP address cannot be assumed a unique identification as the HNED may use a private IP address in case it is located in a home network with network address translation.

10.6.5.4 Reception report response message

The reception reporting server shall respond with a HTTP response with status code "200" (OK) to signal successful reception and processing of a reception report. Other status codes may be used in error cases as defined in IETF RFC 2616 [39]. The HNED shall in case of a response with an error status code or in case no response is received resend the reception reporting message to an alternative server if provided.

10.6.6 Content Version Numbering

A content item announced for download might have errors that prevent the correct play out of the content item. In order to provide an updated version of such a content item a Content Version number is provided in the BCG instance description metadata (OnDemandProgramType and PushDownloadType Content Version attribute, see clauses G.1.1 and G.1.2) and decomposed binary locator (Extended On-demand decomposed binary locator content_version attribute, see clause G.1.4).

In case of a change to any file of a content item, the CDS network function shall setup a new download session for the content item and announce the new download session in the BCG with a new content version number (using the same CRID). A new multicast download session shall use a different TSI.

In case the change occurs while the download session for the old content version is active the CDS network function shall stop this download session. For unicast download sessions the servers shall response with a HTTP status code of 410 "Gone" to any download request. For multicast download sessions the CDS network function shall terminate the FLUTE delivery the session. CDS HNEDs that actively participate in a download session shall terminated their participation in this outdated download session (including file repair, redirection and reception reporting actions) and delete the already downloaded data as soon as they receive an updated BCG announcement with a new content version number. For unicast download the HNED shall in addition check for an updated content version number in case it receives a HTTP status code of 410 "Gone" to a file download request. For multicast download the HNED shall in addition check for an updated content version number before it starts a file repair in case the file download is incomplete.

The HNED shall join the new download session as announced in order to download the updated content item.

In case the HNED has already successfully downloaded the content item and terminated its participation in the download session, the HNED shall download the updated content item if it receives a BCG PushDownloadType announcement with a new content version. For pull download announcements (via the OnDemandProgramType or Extended On-demand decomposed binary locator), the HNED shall check for a new content version before the play out of the content item. In case a new content version is available it shall be downloaded before the play out is started.

The files of the outdated content version shall be deleted and replaced by the updated content version. Files that have not changed (indicated by the same <path-absolute>, file length and MD5 digest) should be kept from the old version and not be downloaded again.

10.6.7 Priority settings

CDS unicast and multicast download sessions shall use the "Best effort data" traffic type with the associated IP DSCP and Ethernet priority marking as defined in clause 11. Thus CDS download traffic is unable to cause congestion except for other CDS download traffic itself or any other traffic using this traffic type.

10.7 CDS HNED Storage Management

The current version of the present document provides a limited set of content and storage management functionality.

If the HNED supports CDS, it shall dedicate a sufficient amount of storage to the CDS. This dedicated storage is referred to CDS HNED Storage.

NOTE 1: A 4 MBit/s MPEG-2 TS stream would for example requires roughly 1,8 GByte of storage per hour.

Before acquiring a new content item the HNED shall verify that sufficient space on the CDS HNED storage is available. If storage is not sufficient the HNED shall not initiate the download session for the content item.

The CDS network function may monitor the CDS HNED Storage by tracking reception reporting of content items of individual HNEDs. However, the detailed usage of reception reporting for Storage Management is outside the scope of the present document.

A downloaded content item may have an associated "*ExpiryTime*" provided in the BCG OnDemandProgramType, PushDownloadType or on-demand decomposed binary locator (see clauses G.1.1, G.1.2 and G.1.4). When this "*ExpiryTime*" is due, the CDS HNED function shall automatically delete all the files that are associated with the content item from the CDS HNED storage.

Specifically, the download of new content items shall not be prevented by content items on the CDS HNED Storage with expired "*ExpiryTime*" (e.g. due to insufficient storage space).

NOTE 2: Content item deletion only refers to the removal of the content item from the CDS HNED storage. Any content item that has been moved outside or is moved outside the CDS HNED storage - even if it was acquired through CDS - is not affected by this deletion process. The permission to move the content item from the CDS HNED storage to a private storage on the HNED or even to a different device is outside the scope of the present document. Hence, the content item deletion process is no secure way of preventing access to the content item after the deletion. Content protection mechanisms are required if restricted access to the content needs to be provided.

11 Quality of Service

11.0 Classification

For the network to provide the required Quality of Service (QoS) to the end user there shall be a method for determining the type of data contained in each datagram and a mechanism for prioritizing the traffic based on this classification.

The method of classification will follow the Differentiated Services model described in IETF RFC 2475 [33]. IP packets passing over the IPI-1 interface shall be appropriately marked at the originating source, as described in clause 11.1.

NOTE: It is assumed that other guideline documents will be needed to recommend good practice within both the home and the Service Provider(s) domain.

11.1 DSCP packet marking

The Differentiated Services marking uses the 8-bit Type of Service field in the IP header and is described in IETF RFC 2474 [32]. Networks compliant with IETF RFC 2474 [32] use 6 bits of this ToS field to contain the differentiated services codepoint - a numeric value used within the network to manage queuing policies. Networks not compliant with IETF RFC 2474 [32] use a 3-bit field within the ToS to determine precedence.

Within IP networks designed to carry DVB services, the markings detailed in Table 29 shall be used. It is recommended that the full DSCP value be used.

Table 29: DSCP markings

Traffic Type	IP DSCP Value	Corresponding IP Precedence
Voice Bearer (see note 1)	0b110000	0b110
Real-time Video Bearer (high priority) (see note 2)	0b100010	0b100
Real-time Video Bearer (lower priority) (see note 3)	0b100100	0b100
Voice and Video Signalling	0b011010	0b011
Best effort data	0b000000	0b000
NOTE 1: The voice bearer is listed here to ensure that there is no interference with DVB-IPTV services.		
NOTE 2: Normal marking for real-time video.		
NOTE 3: Use of this marking is application dependent. It is intended to allow a CSP to suggest that some video packets are less important than others.		

11.2 Ethernet Priority

The interface IPI-1 on an Ethernet MAC based HNS shall support IEEE 802.1Q [5], with defined user priority classes. The IEEE 802.1D [9] field shall be supported in an IEEE 802.1Q [5] compliant Ethernet frame. The marking shall be based on the DiffServ CodePoint (DSCP) marking method [42] as described in clause 11.1.

Table 30: DSCP Values and corresponding Ethernet IEEE 802.1D [9] marking

Traffic type	IP DSCP value	Corresponding IEEE 802.1D [9] User Priority value
Voice bearer (see note)	0b110000	0b110
Video bearer (high priority)	0b100010	0b100
Video bearer (lower priority)	0b100100	0b100
Video signalling	0b011010	0b011
Best effort data	0b000000	0b000
NOTE: The voice bearer is listed here to ensure that there is no interference with DVB-IPTV services.		

For a HNS based on Ethernet MAC these DSCP values are used to map a traffic type onto the corresponding IEEE 802.1D [9] priority codes. Packets shall be marked using the Layer 2 Class of Service (CoS) settings in the User Priority bits of the IEEE 802.1D [9] portion of the 802.1Q header. These can be mapped to the IP Precedence/DSCP bits in the Type of Service (ToS) byte of the IPv4 header. Note that the 802.1Q header adds an additional 4 bytes of data into an Ethernet frame header. The IEEE 802.1D [9] priority field is one of the fields in the 802.1Q header, and is a 3 bit field. Any switching device that implements the IEEE 802.1Q [5] specification can use the user-priority field to determine the scheduling class a packet belongs to.

Note that mapping the IP precedence field is easy, as it can be copied to the user-priority field directly, as both the fields are 3 bits long. To map the DSCP field to the user-priority field, the DSCP shall be shifted right by 3 bits, i.e. the user-priority field is the first 3 bits of the DSCP field. To map the user-priority field to the DSCP field, the user-priority field shall be tested for values that match the user-priority value in Column 3. If the user-priority value does not match any of the values shown in column 3, the packet shall be marked with a DSCP value which is the user-priority shifted left by 3 bits.

12 SRM delivery over IP networks

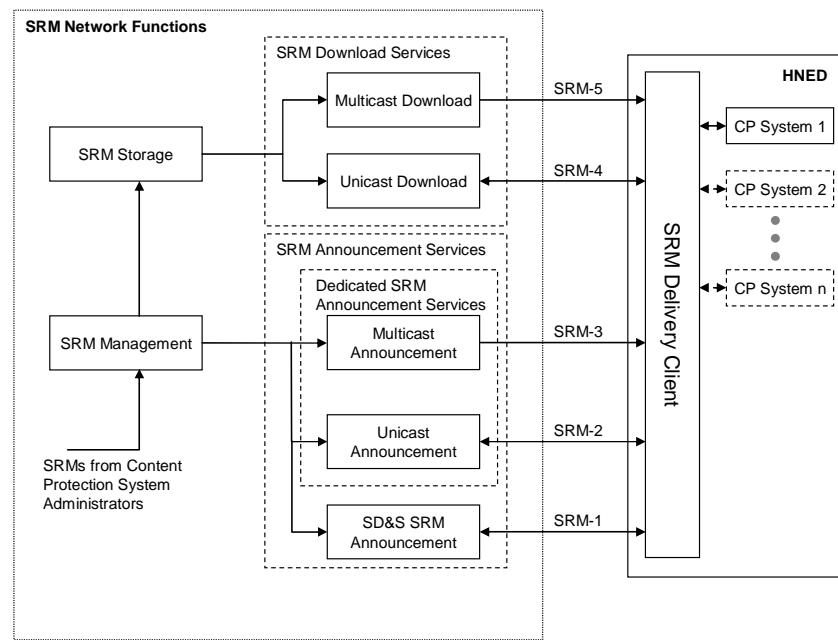
12.1 Overview

An important function of Content Protection (CP) Systems is the field renewability of important parts of the system implementation in order to replace or revoke such parts which have been compromised and fail in further preventing undesired use of content. That renewability information is conveyed to consumer equipment in the form of System Renewability Messages (SRMs). SRMs are for example delivered as part of the content on packaged media like DVDs. For delivery over broadcast networks DVB has defined SRM transport in a MPEG-2 transport stream in ETSI TS 102 770 [110]. While MPEG-2 transport streams with SRMs can also be delivered over IP networks, the following clauses define the delivery of SRMs to HNEDs directly over IP out-of-band of the media delivery.

NOTE: The SRM delivery service defines no support for securing the announcement and download of SRMs. It can therefore not guarantee that the HNEDs always have the latest and correct SRMs. It is up to the CP Systems to take care of that.

12.2 Functional Architecture

Figure 22 shows the SRM delivery functional architecture. The architecture includes logical interfaces between the SRM network functional components and the SRM Delivery Client on the HNED (SRM-x, see Table 31). These interfaces are part of the IPI-1 interface and defined in the following clauses. Interfaces between network functional components (e.g. between SRM Management and SRM Storage) and between the SRM Delivery CP System on the HNED are out of scope of the present document.



NOTE: All functions identified in the figure are logical rather than physical. No physical device is implied. The arrow direction indicates the main message flow.

Figure 22: SRM Delivery Functional Architecture

The SRM Storage holds the SRMs which are delivered to the HNED via the multicast or unicast download services. The SRM Management receives the SRMs from the CP System administrators, puts them on the SRM storage and generates the SRM announcement information accordingly. The SRM Download and Announcement Services and the SRM Delivery Client functionality are defined in the following clauses. SRM Storage and SRM Management are out of scope of the present document.

Table 31: SRM-x interfaces

Interface	Functionality
SRM-1	SD&S SRM announcement (see clause 12.4.1)
SRM-2	Dedicated SRM unicast announcement (see clause 12.4.2.1)
SRM-3	Dedicated SRM multicast announcement (see clause 12.4.2.2)
SRM-4	Unicast SRM download (see clause 12.5.1)
SRM-5	Multicast SRM download (see clause 12.5.2)

12.3 SRM specific identifiers

12.3.0 General

SRM specific identifiers are defined to differentiate between different SRMs in the delivery process and to indicate the CP System for which the SRM is issued.

12.3.1 CP System ID

SRMs are issued for a specific Content Protection System. The SRM delivery system uses the CP System ID defined in ETSI TS 101 162 [2] to identify the Content Protection System for which a SRM is issued. The CP System ID is also used in ETSI TS 102 770 [110] to identify the CP Systems for which SRMs are delivered over MPEG-2 transport streams.

12.3.2 CP System SRM ID

Some Content Protection Systems support different SRMs (e.g. different protocol versions, different compliance regimes) which have to be distributed in parallel. In order to support the individual announcement and download of such SRMs a CP System SRM ID can optionally be used in combination with the CP System ID. This CP System SRM ID shall be a binary string (hexadecimal coded) with a maximum length of 256 bytes. The usage of the CP System SRM ID is CP System specific and has to be defined by the CP System. However for the SRM delivery system it is required that SRMs with the same CP System ID which have to be delivered individually (dedicated announcement and download) shall have unique CP System SRM IDs so that the SRM delivery system can differentiate between them by a simple equal/not equal comparison.

12.4 SRM Announcement Services

12.4.0 General rules

SRM announcement services provide announcements for SRM download services or provide pointers to other SRM announcement services.

The announcements provide the list of CP System IDs and optional CP System SRM IDs (see clause 12.3) that are supported by the SRM download or announcement service and information on how to access the service. The list of CP System IDs and CP System SRM IDs can have a single entry, multiple entries or no entry. In the latter case the HNED has to access the service in order to know which CP System IDs and CP System SRM IDs are supported by the service. In case a CP System uses CP System SRM IDs and only the CP System ID is provided in the announcement the HNED has to access the service in order to get information about which CP System SRM IDs are supported by the service.

In case CP System SRM IDs are provided for a certain CP System ID by the SRM announcement and download services the SRM delivery client on the HNED shall provide the list of all announced CP System SRM IDs to the CP System specific functional block on the HNED. Based on this information the CP System specific functional block shall decide which SRM announcement and download services the HNED has to access in order to receive the relevant SRMs. The CP System specific functional block shall instruct the SRM delivery client to access these relevant services by providing the list of CP System SRM IDs in which it is interested in.

SRM announcements may include different types of version numbers (record version, announcement service version, FLUTE session version, SRM file version). For details on the version numbers and their usage see clause 12.6.

Note that multiple download or announcement services (e.g. multicast and unicast delivery) can be provided for a specific CP System ID and CP System SRM ID. The behaviour of the HNED in selecting a particular service in this case is implementation specific.

12.4.1 SD&S SRM Announcements (SRM-1 interface)

The entry point for all SRM services (announcement and download) is SD&S. SD&S SRM announcements are provided with the SRM Offering Record defined in clause 5.2.13.9. The SRM Offering Record can either directly announce SRM download services or can point to dedicated SRM announcement services.

12.4.2 Dedicated SRM Announcement services

12.4.2.0 General rules

A dedicated SRM announcement service provides a list of SRM download services for one or more CP System IDs and optional CP System SRM IDs.

Further indirection from the dedicated SRM announcement service, to other dedicated SRM announcement services is not supported.

Dedicated SRM announcement services are delivered via unicast using HTTP or via multicast using SAP.

Note that more than one Download Service might be announced for the same CP System ID or combination of CP System ID and CP System SRM ID. The behaviour of the HNED in selecting a particular download service in this case is implementation specific.

12.4.2.1 HTTP unicast SRM announcement service (SRM-2 interface)

Dedicated SRM unicast announcements are distributed using HTTP [39]. The service provides XML coded SRM download offering records reusing the SD&S SRM download service offering scheme as defined in clause 5.2.13.9. Table 32 lists the element of the SRM Download Record.

Dedicated unicast SRM announcement services are announced in SD&S (SRM announcement service offering) by providing the HTTP URL of the announcement, the list of CP System IDs and optional CP System SRM IDs that are handled by this announcement service and the announcement service version number (see clause 12.6 on the use of version numbers).

Table 32: SRM Download Record

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
SRMDownload	SRM Download Record (extending the OfferingBase from Table 11az).	O
SRMDownloadService (one entry per service)	SRM Download Service information (as defined in Table 11cm)	M

12.4.2.2 SAP multicast announcement service (SRM-3 interface)

Dedicated SRM multicast announcements are distributed using SAP [76]. The service provides SDP coded SRM download offerings records with the information as defined in Table 32. The SDP syntax for SRM announcements is defined in annex H.

Due to the limitations of SAP to 1 Kbyte for a single SDP message a SDP message shall announce only a single SRM download service. Several SRM download services shall be announced by separate SDP messages which can be delivered via the same SAP multicast session. The record version number (see clause 12.6 on version numbers) provided by the "o=" line of the SDP message (see clause H.2.1) is used to indicate a new version of a SDP message for a specific SRM download service.

Dedicated multicast SRM announcement services are announced in SD&S (SRM announcement service offering) by providing the SAP multicast address, port, optional source address (in case of source specific multicast), the list of CP System IDs, optional CP System SRM IDs that are handled by this multicast announcement service and the optional announcement service version number (see clause 12.6 for version numbers).

The HNED has to join the SAP multicast session in order to access the SRM announcement information distributed via this session.

12.5 SRM download services

12.5.0 Overview

SRM download services deliver the SRMs for specific CP System IDs to the HNED. The download service is transparent to the content of the SRMs.

HTTP unicast and FLUTE multicast download services are defined.

12.5.1 HTTP unicast SRM download service (SRM-4 interface)

Unicast SRM download services use HTTP [39] to download the SRM file for a specific CP System ID.

The SD&S or dedicated SRM announcement service offering provides the location of the SRM file together (URI) with the CP System ID and optional CP System SRM ID for which the SRM file is valid and the SRM file version (see clause 12.6.1).

Content encoding of the SRM files is not supported.

The HTTP server may use redirection to a different server location or ask for a delayed request (retry-after) to prevent overload conditions.

12.5.2 FLUTE multicast SRM download service (SRM-5 interface)

The FLUTE protocol defined in IETF RFC 3926 [70] and further detailed in clause 6 of ETSI TS 102 472 [65] and clause 10.6.2.2 of the present document is used for multicast SRM download services.

The SD&S or dedicated SRM announcement service offering provides the FLUTE session information (multicast address, port, TSI, optional source address), the list of CP System IDs, optional CP System SRM ID and SRM File version number supported by the service and the FLUTE session version number (see clause 12.6 on version numbers).

One or more SRM files can be delivered by a FLUTE session. A SRM FLUTE session runs as dynamic carrousel as defined in clause 6.2.1.5 of ETSI TS 102 472 [65]. This allows a HNED to join the session at any time to acquire the SRM file. SRM files can be updated and SRM files for new CP System IDs can be added during the session.

The FLUTE FDT is extended to provide the CP System ID, CP System SRM ID and SRM file version number for each SRM file as shown in Table 33. HNEDs can join the FLUTE session and check the FDT for CP System IDs for which they want to download SRM files. The SRM file version number shall be incremented each time the SRM file for a specific CP System ID is modified (see clause 12.6.1). A change of the SRM file version number will also result in a change of the FDT instance number. Modified versions of SRM files shall be sent with a different Transport Object Identifier (TOI) as defined in clause 6.1.12 of ETSI TS 102 472 [65].

Table 33: Extended SRM FLUTE File Delivery Table (FDT) structure

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
FDT-Instance-Attributes	Common Attributes for all the files described by the FDT instance	
Expires	expiry time of the FDT Instance.	M
Complete	when present and TRUE, signals that no new data will be provided in future FDT Instances within this session.	O
Content-Type	content type.	O
Content-Encoding	Content encoding.	O
FDT-Instance-Delivery-Attributes	Attributes related to the delivery of all files described by the FDT instance	
FEC-OTI-FEC-Encoding-ID	Identification of FEC algorithm.	O
FEC-OTI-FEC-Instance-ID	FEC instance depending on the FEC algorithm identification.	O
FEC-OTI-Maximum-Source-Block-Length	The maximum number of source symbols per source block.	O
FEC-OTI-Encoding-Symbol-Length	Length of encoding symbols in bytes.	O
File Attributes (one per file)		
Content-Type	MIME media type of content.	O
Content-Encoding	Compression.	O
Content-Location	Location of file.	M
Content-Length	Size of the content.	M
Content-MD5	Hash of the content (MD5).	O
CP-System-ID	CP System ID of the SRM file.	M
CP-System-SRM-ID	CP System SRM ID of the SRM file (of the CP Systems supports several types of SRM files)	O
SRM-File-Version	Version of the SRM file for download.	M
Content-Delivery-Attributes	Attributes related to the delivery of the file	
TOI	Transport Object Identifier.	M
Transfer-Length	Size of the transport object carrying the content.	O
Bandwidth-Requirement	Aggregate rate of sending packets to all channels.	O
FEC-OTI-FEC-Encoding-ID	Identification of FEC algorithm.	O
FEC-OTI-FEC-Instance-ID	FEC instance depending on the FEC algorithm identification.	O
FEC-OTI-Maximum-Source-Block-Length	The maximum number of source symbols per source block.	O
FEC-OTI-Encoding-Symbol-Length	Length of encoding symbols in bytes.	O

The use of a single multicast channel for SRM FLUTE sessions shall be supported. Multiple multicast channels for a SRM FLUTE session are not supported.

The "Compact No-Code FEC scheme" [73] (FEC Encoding ID 0) shall be supported for SRM FLUTE sessions. The Algorithm for Computing Source Block Structure defined in IETF RFC 3926 [70] shall be used. Other symbol encoding schemes are not be supported for SRM FLUTE sessions. If an error occurs during the download of a SRM file it can be recovered at a later time when it is repeated in the carrousel.

Content encoding of the SRM files is not supported.

12.6 Version Numbers

12.6.0 Overview of the different types of Version Numbers and their usage

Different types of version numbers are used by the SRM Announcement and Download Services. The different types of version numbers and their usage is defined in this clause. Figure 23 provides an overview on the use of the different version numbers.

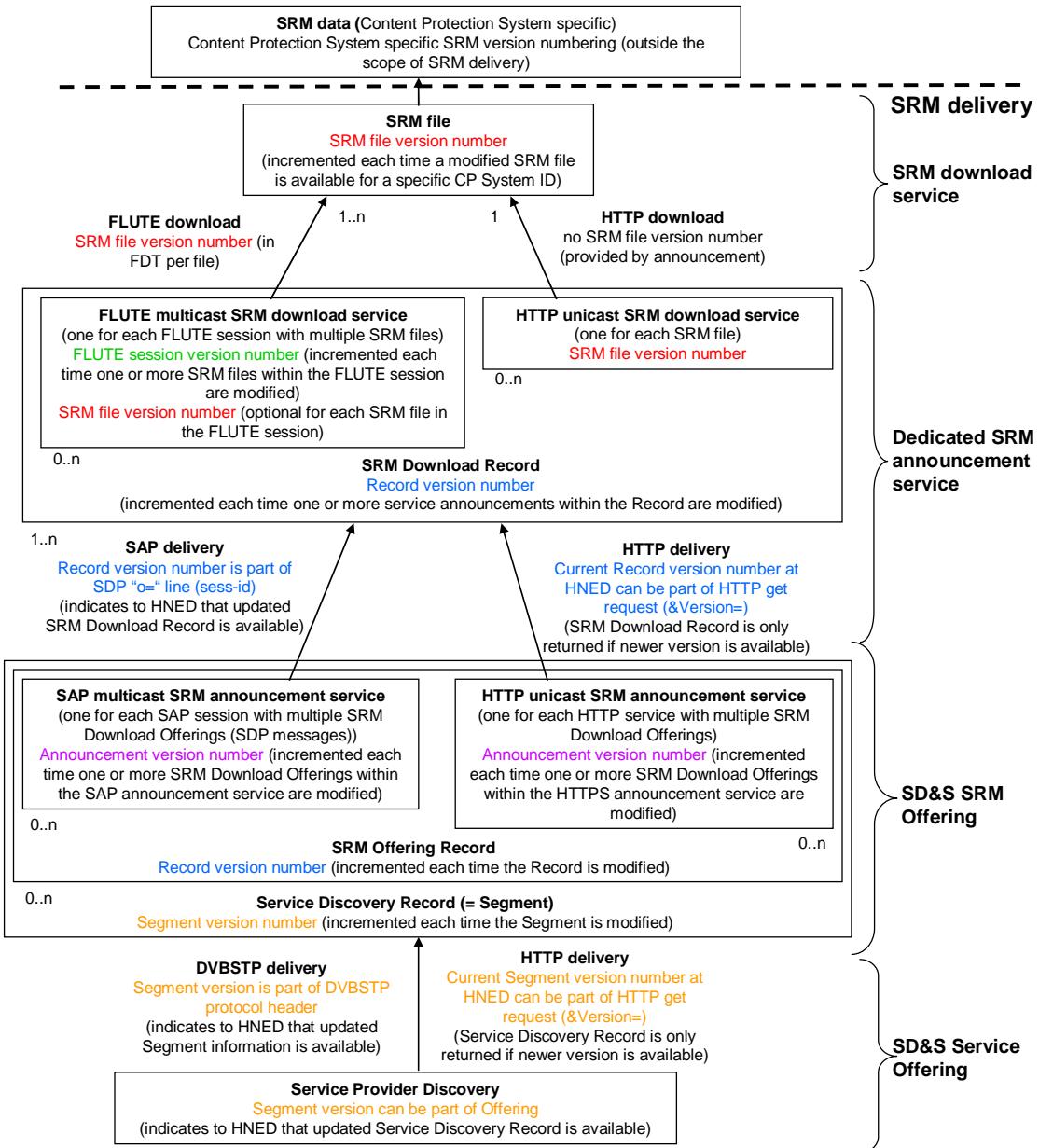


Figure 23: SRM version numbers

12.6.1 SRM File Version Number

A SRM file version number shall be provided in download service offerings for HTTP unicast SRM download services (SD&S SRM Offering Record or SRM Download Record) and in the FLUTE FDT for each SRM file delivered by the FLUTE multicast SRM download service. It may also be used in the download service offerings for FLUTE unicast download services.

The SRM file version number is specific to the SRM file for a dedicated CP System ID or combination of CP System ID and CP System SRM ID and shall be incremented (modulo 256) each time an update of that SRM file is available.

In case a SRM file for a specific CP System ID is delivered via FLUTE and HTTP, the SRM file version number in the FLUTE FDT and in the download service offering for the HTTP unicast SRM download services shall be the same for the same version of the SRM file. This provides a consistent check of the version of the SRM file over the different download services.

Note that the SRM file version number is not related to any version number within the SRM data itself. The SRM file version number is used to indicate the availability of updated SRM files within the SRM delivery and is generated by the SRM delivery service independently of any version number within the SRM data itself.

12.6.2 FLUTE Session Version Number

A FLUTE session version number can be provided in download service offerings for FLUTE multicast SRM download services. The FLUTE session version number shall be incremented (modulo 256) each time new or updated SRM files are available via the specific FLUTE download session.

A change of the FLUTE session number in the download service offering indicates to the HNED that new or updated SRM files are available from a SRM FLUTE download service. The HNED shall join the FLUTE session and check if new SRM files are available for the CP System IDs and CP System SRM IDs it is interested in. If the FLUTE session version number is not provided the HNED has to check the FLUTE session regularly for updates.

12.6.3 Record Version Number

Each SD&S SRM Offering Record and SRM Download Record has a record version number which indicates the version of this record. The record version number shall be incremented (modulo 256) each time the record is modified (i.e. new, updated or deleted SRM announcement or download service offerings).

The record version is provided by the version attribute in the SD&S OfferingBase type (clause 5.2.12.18, Table 11az) used by the SD&S SRM Offering Record (clause 5.2.13.9, Table 11cm) and the SRM Download Record (Table 32) and by the session version attribute of the SDP "o=" line (see clause H.2.1).

The record version number tells the HNED if the record has changed from a previous received version.

12.6.4 Announcement Service Version Number

Each SRM announcement service offering within an SD&S SRM Offering may have an announcement service version included. A dedicated SRM announcement service provides 1 or more SRM Download Records. The announcement service version number shall be incremented (modulo 256) each time SRM Download Records are updated, added to or removed from the dedicated SRM announcement service.

The use of the announcement service version number is optional for SRM multicast announcement service offerings and mandatory for SRM unicast announcement service offerings. If a HNED detects a change of an announcement service version number for a SRM announcement service it is interested in the HNED shall join this announcement service and check for updated information. If the announcement service version number is not provided the HNED has to check the announcement service regularly for updates.

12.6.5 Segment Version Number

Segment version numbers are specific for the SD&S delivery and are defined in clause 5.4.

A SD&S Segment provides one or more Service Offering records. The segment version number is incremented each time any of these Service Offering records is updated, removed or a new record is added.

13 Dynamic Service Management (DSM)

13.1 Overview

Dynamic Service Management is a feature to enable the HNED and/or users to make smarter decisions about which service to select out of a group of equivalent DVB services in order to provide an optimum service when multiple DVB services are offered to the users' home. A group of equivalent DVB services may include SD, HD, 3D and possibly multiple bitrate versions.

In order to provide the Dynamic Service Management functionality, clause 13 of the present document defines:

- A data model.
- A messaging structure.
- A message transport based on a peer to peer model (i.e. not client-server).
- A process to allocate a temporarily unique identifier to each HNED in a home.

Clause 5 of the present document contains the required SD&S extensions. The address of the DSM Manager shall be provided in the SD&S "RMSFUSDiscovery" element from the Service Provider where DSM is supported. Only one DSM Manager will be available for any service offering of one service provider and therefore only a single address will be provided.

In order to manage multiple HNEDs in a home it is necessary to allocate a unique HNED identifier (HNED_ID) to each HNED, the process to do this is described in clause 13.9.

The DSM functionality enables a decision about whether new service delivery requests from other HNEDs in the home (using the same access network connection) can be granted without compromising those HNEDs to which content is already delivered. In case of contention DSM defines the messaging functionality for some negotiation to take place for the home environment, using the IPI-1 interface.

Clause K.1 includes an analysis of the use cases where there are 2 HNEDs in a home, with some expanded examples to illustrate the exchange of message sequences. The DSM method can also be used in more complex multi-HNED home scenarios.

In Dynamic Service Management, the admission controls operate on a service layer requiring information exchanges and caching between the headend servers and the HNEDs, managed through a Dynamic Service Management Manager function. In order to enable this, suitable metadata shall be available to both, the Dynamic Service Management Manager and the HNED. It is the responsibility of the HNED implementation to manage access to the services based on the messaging provided. The policy logic of how to use the information about available equivalent services is out of scope of the present document and is defined by the HNED implementation.

13.2 DSM Functional Architecture

Two examples of functional architecture are shown in Figure 24 and Figure 25, these can be used as reference models for implementation of the DSM methods, however the practical implementations associated with actual deployments is not necessarily exposed.

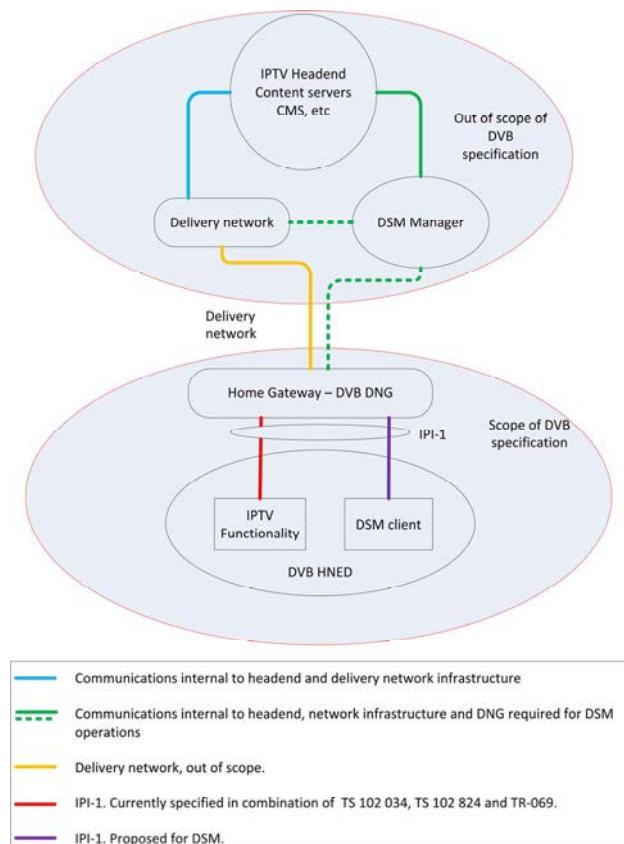


Figure 24: Example functional DSM architecture, DSM Manager resides in the Headend

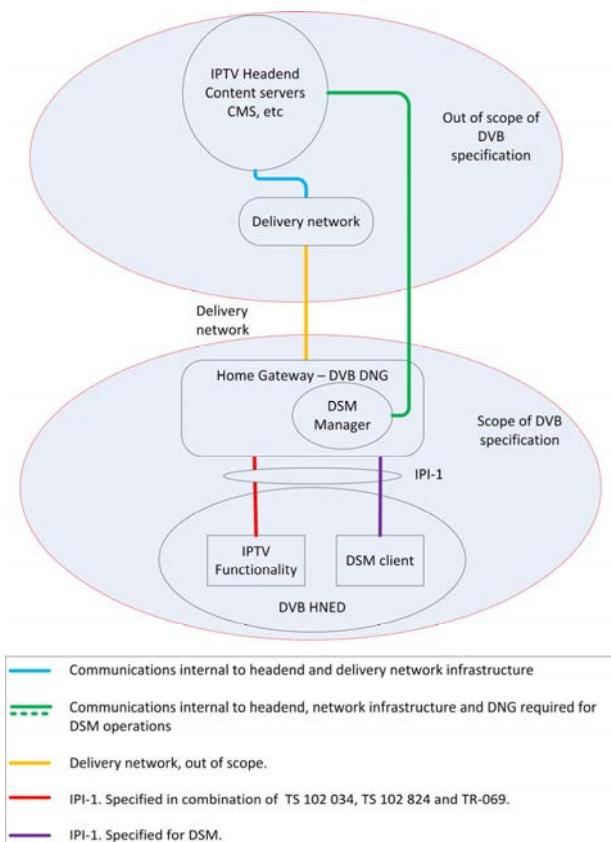


Figure 25: Example functional DSM architecture, DSM Manager resides in the DNG

13.3 Operating Assumptions

The structure of the data model and messaging is based on some assumptions about the services supported by the headend. The main assumptions are:

- All DVB equipment connected to the IP access network in the home is managed by the headend, and therefore the headend is assumed to have realtime information about the status of all HNEDs served by it and of all the services being delivered to those HNEDs.
- The headend manages the delivery of a set of DVB services to the home.
- The delivery bitrate on the access network may not be sufficient for delivery of multiple services to the home and should not vary in an unmonitored way with time, i.e. it shall be assumed to be quasi-static.
- A home may contain multiple HNEDs connected to the SP through a single DNG.
- HNEDs cannot communicate directly with each other within the home (that would represent "DVB HN/DLNA style Home Network" behaviour).
- The SP defines the actual DSM management "policy", assumed to include the options offered and the content of information and messaging to be offered to customers.
- It is not assumed that any data model will be maintained by the HNED, all settings will be stored on the server from where they can be queried or modified (if agreed with SP).
- Most of the functionalities required by the headend are already available (i.e. no additional to current requirements), although it may not be either aggregated nor used at present.
- The location of the DSM Manager is out of scope of the present document.
- A single point of storage of DSM data, on a DSM Manager, ensures consistency of HNED status and removes the need for frequent synchronization.

- The policy may be managed directly from the headend or locally in any of the HNEDs.
- The metadata (SD&S, BCG, etc.) provided to any HNED may only describe and expose the most appropriate instances of a content item to the HNED.
- For services supporting DSM the SD&S metadata shall indicate the intended usage of a service in an extension of the "IPService" field as shown in clause 5.

13.4 DSM Process

Figure 26 explains the basic DSM process. The left side of Figure 26 shows the HNED boot-up process, the asynchronous messaging required to maintain DSMM-HNED synchronization is shown in the centre of the flowchart, and the process shown on the right hand side shows the decision process associated with HNED initiated actions.

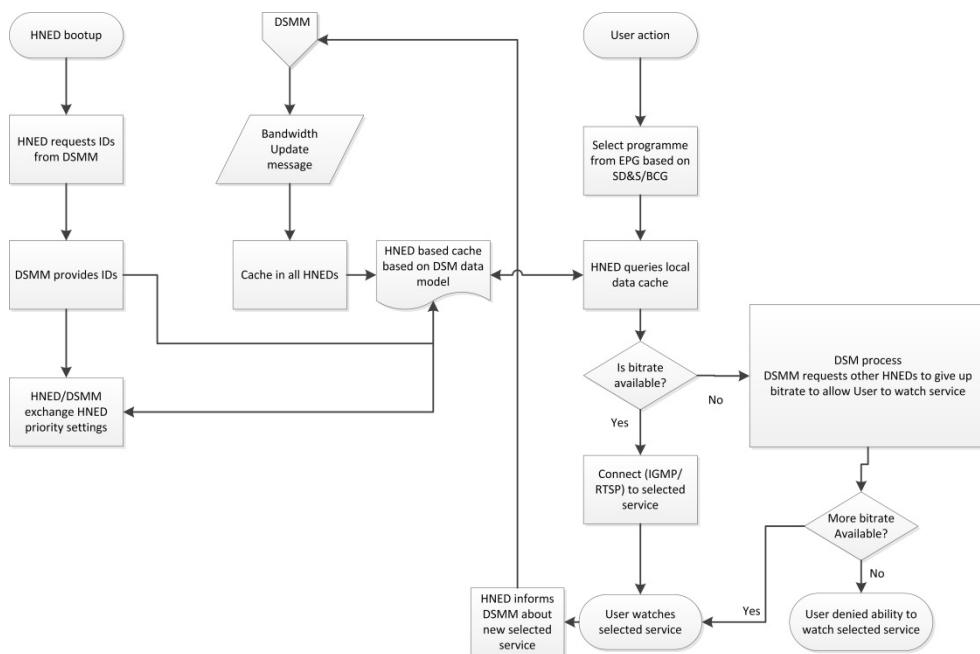


Figure 26: Basic DSM process

13.5 Data Model for information stored by the DSM Manager

13.5.1 DSM Data Model

The hierarchical nature of the data model structure allows data to be stored on a "per customer", "per HNED" and "per session" basis. The representation below shows the hierarchy of the fields required to describe the service status for a home, HNED and IP service delivery session. Since this is managed by the Service Provider and created within the headend, further definition of the data is out of scope of DVB and therefore of the present document.

Clause K.2 includes an XML schema for the data model which includes support for IPv4 and IPv6 and may be used for the implementation of this database.

The data model fields are profiled in Figure 27.

```

Customer {
    CustomerID
    TotalAvailableBitrate
    ServiceTypePriority
    ContentTypePriority
    HNED {
        HNED_ID
        HNEDpriority
        Session {
            SessionID
            ServiceBitrates {
                Bitrate
                Usages {
                    Usage
                }
            }
            ServiceID{
                DomainName
                ServiceName
            }
            EquivalentService {
                ServiceBitrates {
                    Bitrate
                    Usages {
                        Usage
                    }
                }
                EquivalentServiceID{
                    DomainName
                    ServiceName
                }
                EquivalentServiceLocation
            }
        }
    }
}

```

Figure 27: Data model structure

Support for the DSM service is optional for IPTV installations based on the present document. Where the DSM service is implemented the DSM Manager shall support all the fields appropriate for the service supported, for example, one or more ServiceTypePriority levels, and the HNED shall support all the elements of the data model.

Table 34: Profiling of Data Model fields

Field	Profiling	Status	Instances	Usage applied	
				DSMM	HNED
CustomerID	In combination with HNED_ID this describes the combination of HNEDs in the home per customer, there shall only be one CustomerID per access network connection and it shall be uniquely maintained within the SP domain.	M (Optional for DSM001)	1	RW	R
TotalAvailableBitrate	Indicates the total available bitrate for DVB services to the DNG which is connected both to the SP domain and to the HNEDs in the Home domain.	M	1	RW	R
ServiceTypePriority	This defines the priority of selected service types for the HNED, the supported types are as follows: <ul style="list-style-type: none"> • DeliveryType: <ul style="list-style-type: none"> – LMB. – CoD. LMB and CoD fields are integer based, with values of "1" = highest priority, "2" = lowest priority. The <field><value> combinations are detailed as below. If no values are provided for either of the type parameters then unqualified types within that group will have equal priority.	O	1 per field	RW	RW

Field	Profiling	Status	Instances	Usage applied	
				DSMM	HNED
	The priority value may be set by the HNED (locally) or the DSM Manager depending on the policy for the HNED within the home.				
ContentTypePriority	<p>SD, HD and 3D fields are integer based, with values of "1", "2" and "3" being defined. "1" has highest priority, "3" has lowest priority, etc.</p> <p>Defined contentTypes are:</p> <ul style="list-style-type: none"> • SD. • HD. • 3D. <p>If no values are provided for any or all of the types then the unqualified types within that group will have equal priority with value "3".</p> <p>The priority value may be set by the HNED (locally) or the DSM Manager depending on the policy for the HNED within the home.</p>	O	1 per field	RW	RW
HNED_ID	<p>Single identifier for each HNED in the home, this will be allocated by the DSM Manager. Each HNED shall have only one HNED_ID and it shall be unique in the scope of the CustomerID.</p> <p>This unique identification string allows DSM Manager to synchronize service negotiations with multiple HNEDs, this may be fixed only until the HNED is made inactive (powered off).</p>	M	1	RW	R
HNEDpriority	<p>Priority values applied to HNEDs determine the order of pre-emption and weight in decision making, the values 1 to 3 are defined as follows:</p> <ul style="list-style-type: none"> - A priority value of "1" gives the HNED the most significant weight in the system, there should only be a single HNED with priority "1" at any time, priority "2" and "3" HNEDs will be asked or required to give up bitrate to a priority "1" HNED if required. - A priority value of "2" means that the HNED may be requested to give up bitrate when required by a priority "1" device, but may request that a priority "3" HNED or another priority "2" HNED gives up bitrate when required. - A priority "3" HNED is expected to give up bitrate to either of a priority "1" or "2" HNED when required. <p>The priority value may be set by the HNED (locally) or the DSM Manager depending on the policy for the HNED within the home. If undefined for all HNEDs an equal priority shall be assumed.</p>	O	1	RW	RW
SessionID	In this context "Session" means IP content delivery session. There may be multiple sessions in progress at any time, and for each session the characteristics may be stored. It is assumed that the DSM Manager has access to all the current information for each open session.	M	0-n	RW	R

Field	Profiling	Status	Instances	Usage applied
				DSMM HNED
ServiceBitrates	All bitrates required for the service, unique per session for the current service session.	M	1 per session	RW R
Bitrate	Bitrate of the current service. The stream is identified by its usage.	M	1-n	RW R
Usages	List of different usages for the current service. One service can have more than one usage, e.g. FCC and PiP usage share the same stream. Available usages are: Main, SD, HD, 3D, FCC, PiP, DSMService.	M	1-n	RW R
ServiceID	Reference unique to content item for the current service, identical to the TextualIdentifier that is used in SD&S containing the domain and service names.	M	1 per session if required	RW R
ServiceID.DomainName	Unique DNS domain name registered by the SP providing the current service, as provided in the IPSERVICE element for the service.	M	1 per session	RW R
ServiceID.ServiceName	A unique host name for the current service within the SP's domain, as provided in the SD&S IPSERVICE element for the service.	M	1 per session	RW R
EquivalentService	Alternative service which is editorially the same in terms of content but different in terms of encoding or delivery. Reference unique to service and identical to that used in SD&S. Equivalent services can be identified from the Service element of the Package element.	M	0-n per session	RW R
EquivalentService.ServiceBitrates	All bitrates required for the equivalent service, unique per session for the equivalent service session.	M	1 per session	RW R
EquivalentService.Bitrate	Bitrate of the equivalent service. The stream is identified by its usage.	M	1-n	RW R
EquivalentService.Usages	List of different usages for equivalent service. One stream can have more than one usage, e.g. FCC and PiP usage share the same stream. Available usages are: Main, SD, HD, 3D, FCC, PiP, DSMService.	M	1-n	RW R
EquivalentServiceID	Reference unique to content item for the equivalent service, identical to that used in SD&S containing the domain and service names.	M	1 per equivalent service	RW R
EquivalentService.DomainName	Unique DNS domain name registered by the SP providing the equivalent service, as provided in the TextualIdentifier element in the SD&S IPSERVICE element for the service.	M	1 per equivalent session	RW R
EquivalentService.ServiceName	A unique host name for the equivalent service within the SP's domain, as provided in the TextualIdentifier element in the SD&S IPSERVICE element for the service.	M	1 per equivalent session	RW R
EquivalentServiceLocation	Connection URL at which the equivalent service can be found. The dvb14:ServiceLocation type is used, equal to the ServiceLocation as provided in the SD&S IPSERVICE element, described in clause 5.2.12.33.	O	1 per equivalent service	RW R
NOTE: No values are provided for the RET component of a service since this is a TCP service and does not have a maximum bitrate.				

In addition to the data model fields defined in Table 34 NegotiationSessionID and ProposedSessionID are used in the messages, these fields are used to support a DSM message sequence but are not stored outside of the the lifetime of that message sequence. They are defined in Table 35.

Table 35: Profiling of additional Session based ID fields

Field	Profiling	Status	Instances	Usage applied	
				DSMM	HNED
NegotiationSessionID	Defined by the entity (HNED or DSMM) which initiates a DSM message sequence. It shall be unique while the DSM message sequence is in progress but shall then be deleted. The lifetime is therefore the period until the DSM message sequence is completed.	M	1 per DSM message sequence	RW	RW
ProposedSessionID	The IP session ID which is created to identify the service for a proposed change. If that change is accepted the ProposedSessionID becomes the SessionID for the service to be stored in the DSMM.	M	1 per service proposal	RW	R
RequestedServiceID	Identifier for service (domain and service names), to be populated from SD&S IPService element for the service.	M	1 per service request	RW	R
RequestedServiceID.DomainName	Unique DNS domain name registered by the SP providing the service, as provided in the TextualIdentifier element of the SD&S IPService element for the service.	M	1 per service request	RW	R
RequestedServiceID.ServiceName	A unique host name for the service within the SP's domain, as provided in the TextualIdentifier element of the SD&S IPService element for the service.	M	1 per service request	RW	R
ProposedServiceID	Identifier for service (domain and service names), to be populated from SD&S IPService element for the service.	M	1 per service proposal	RW	R
ProposedServiceID.DomainName	Unique DNS domain name registered by the SP providing the service, as provided in the TextualIdentifier element of the SD&S IPService element for the service.	M	1 per service request	RW	R
ProposedServiceID.ServiceName	A unique host name for the service within the SP's domain, as provided in the TextualIdentifier element of the SD&S IPService element for the service.	M	1 per service request	RW	R

13.5.2 Equivalent Services

Equivalent services can be found in the Packages definitions. Multiple services (with the same editorial content) can belong to a single package service, allowing to link those services together. Identified by their TextualID, the DSMM can identify the type of the IPService (IP, Broadcast, etc.).

13.6 DSM Message Set

For an effective DSM service the DSM Manager shall asynchronously keep all the HNEDs informed about the available bitrate of the access network to the home and other issues related to the home network involving the HNEDs, therefore the DSMM shall be updated by the HNEDs after every service change about the actual service in use.

Also, in order to allow an HNED to calculate whether a service connection is viable within the constraints of the access network connection the maximum bitrate needed for any selected service described in the SD&S shall be provided in the DSM extension to the SD&S. This is supported by re-profiling the "MaxBitrate" element of the "IPService" element to be mandatory for services supporting DSM.

The detailed message descriptions are provided in clause 13.7. Some examples of the Use Cases and associated message sequences based on a home (defined by "CustomerID") having 2 HNEDs with each HNED having a locally unique identifier (HNED_ID) are described in Annex H. All messages refer to a single HNED only but a service change scenario may involve negotiation with several HNEDs in a home with multiple HNEDs.

The format of the messages allows extension of the messages in future, by addition of more parameter-value pairs.

The set of messages required is listed and profiled in Table 36, and the messages below are logically grouped. Where HNED numbers are specifically used, for example "HNED1", the numbers used are used in the same way as in the Use Cases.

Table 36: Overview of DSM Message Set

Message Type	From/to	Purpose of Message	Section ref	Comment
DSM001 - DSM004		Messages for identification and priority setting	13.7.1	
DSM001	HNED to DSMM	Request ID by HNED at boot-up	13.7.1.1	HNED requests ID from DSM Manager to identify HNED during service negotiations. This message shall also be interpreted by the DSM Manager as the method of announcement that the HNED has been switched to an active state from "Off".
DSM002	DSMM to HNED	Assignment of an ID	13.7.1.2	Identification of the HNED until re-boot.
DSM003	HNED to DSMM	Passing of pre-assigned HNED parameters to DSMM at boot-up.	13.7.1.3	
DSM004	DSMM to HNED	Confirming acceptance of HNED parameters by DSMM to HNED.	13.7.1.4	
DSM101		Assynchronous service delivery and HNED status updates from DSMM to HNEDs	13.7.2	
DSM101	DSMM to HNED	Available bitrate	13.7.2.1	Sent after identification of the HNED Sent to all HNEDs when any change in the remaining available bitrate to a home occurs.
DSM201 - DSM209		Messages directly associated with a service selection	13.7.3	Only required if there is insufficient bitrate to deliver the HNED2 request.
DSM201	HNED to DSMM	Change request	13.7.3.1	Message from HNED to DSM Manager when a service is selected and there is insufficient bitrate to deliver it.
DSM202	DSMM to HNED	Change proposal	13.7.3.2	Sent to HNED where change is proposed by DSM Manager, indicating what is offered. Note that capability to deliver this can be dependent on response from HNED1.
DSM203	HNED to DSMM	Change accept/refuse	13.7.3.3	Message from HNED accepting or refusing proposed service delivery change. Defined values are: <ul style="list-style-type: none">• "0" = Accept change.• "1" = Refuse change.

Message Type	From/to	Purpose of Message	Section ref	Comment
DSM204	DSMM to HNED	Change Confirmed/cancelled	13.7.3.4	Sent to HNED where change has been completed or cancelled. Defined values are: <ul style="list-style-type: none">• "0" = Change confirmed.• "1" = Change cancelled.
DSM205	HNED to DSMM	Service Change Acknowledge	13.7.3.5	Sent by all HNED involved in transaction to acknowledge completion
DSM206	HNED to DSMM	Service Change complete	13.7.3.6	Sent to DSM Manager to synchronize status when no DSM session has been necessary to enable service connection.
DSM301 - DSM308		Data value manipulation messages	13.7.4	Uses "parameter - value" pairs.
DSM301	HNED to DSMM	Query Value	13.7.4.1	Used by any HNED to query the settings of any field in the stored data structure in the DSM Manager. The argument will be the field to be queried, multiple fields can be queried using a space separated format, and a "QueryValue" with no argument should return all values stored for that HNED.
DSM302	DSMM to HNED	Return Value	13.7.4.2	The DSM Manager should return values of requested fields.
DSM303	HNED to DSMM	Set Value	13.7.4.3	Allows any HNED to modify settings stored in the DSM Manager for that HNED. This may only apply for some values. This message can be used to inform the DSM Manager in case of an autonomous service change by an HNED.
DSM304	DSMM to HNED	Set Value Success	13.7.4.4	Return message from DSM Manager for each request to change a field value.
DSM305	DSMM to HNED	Query Value	13.7.4.5	Used by the DSM Manager to query the settings of any field in the stored data structure in any HNED. The argument will be the field to be queried, multiple fields can be queried using a space separated format, and a "QueryValue" with no argument should return all values stored in that HNED.
DSM306	HNED to DSMM	Return Value	13.7.4.6	The HNED should return values of requested fields.
DSM307	DSMM to HNED	Set Value	13.7.4.7	Allows the DSM Manager to set the parameter values in any specific HNED.
DSM308	HNED to DSMM	Succesfull transaction	13.7.4.8	Indicates that the transaction was succesfull.

13.7 DSM messages

13.7.1 Overview

The message descriptions and Use Cases described in annex H are based on multiple HNEDs in a home; in the examples used to explain the message set there are 2 HNEDs in the home (defined by "CustomerID") with:

- HNED1 - the HNED already receiving a service.
- HNED2 - the HNED requesting to connect to a service.

The format of the messages allows future extension of the messages by addition of more parameter-value pairs.

NOTE: It is proposed that these messages will be represented in XML to allow definition of the fragments to be carried.

The structure and hierarchy of the messages is defined in clause 13.8 and the Use Cases in Annex K.1 include some examples of message sequence diagrams.

13.7.2 Messages at boot time

13.7.2.1 DSM001 - HNED ID request - HNED to DSM Manager

```
MessageType=DSM001 {
  NegotiationSessionID
  HNEDPriority=<Value>
}
```

Table 37: DSM001 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM001" acts as request to DSM Manager for Customer and HNED IDs for the current active session.	M
NegotiationSessionID	An ID covering the transaction to obtain the Customer_ID and HNED_ID. This ID shall be set by the HNED, as defined in Table 35.	M
HNEDPriority	Carries value as defined in Table 34.	M

13.7.2.2 DSM002 - Assignment of IDs to HNED - DSM Manager to each HNED

```
MessageType=DSM002 {
  NegotiationSessionID
  CustomerID=<value>
  HNED_ID=<value>
}
```

Table 38: DSM002 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM002" carries IDs from DSM Manager to HNED which are necessary to synchronize DSM Manager and HNED for continued service negotiations.	M
NegotiationSessionID	An ID covering the transaction to obtain the Customer_ID and HNED_ID, as defined in Table 35. This ID shall be set by the HNED.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M

13.7.2.3 DSM003 - HNED ID exchange - HNED to DSM Manager

```
MessageType=DSM001 {
    HNED_ID=<Value>
    NegotiationSessionID
    HNEDPriority=<Value>
}
```

Table 39: DSM003 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM003" acts as a means to pass a pre-assigned (e.g. embedded) HNED_ID from the HNED to the DSMM at boot-up for the current active session.	M
HNED_ID	The identifier which has been pre-assigned to the HNED.	M
NegotiationSessionID	An ID covering the transaction to obtain the Customer_ID and HNED_ID, as defined in Table 35. This ID shall be set by the HNED.	M
HNEDPriority	Carries value as defined in Table 34.	M

13.7.2.4 DSM004 - HNED_ID Confirmation by DSMM - DSM Manager to each HNED

```
MessageType=DSM002 {
    NegotiationSessionID
    CustomerID=<value>
    HNED_ID=<value>
}
```

Table 40: DSM004 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM004" is used by the DSMM to confirm acceptance of the pre-assigned HNED_ID passed to it from the HNED in DSM003. carries IDs from DSM Manager to HNED which are necessary to synchronize DSM Manager and HNED for continued service negotiations.	M
NegotiationSessionID	The ID covering the transaction to obtain the Customer_ID and HNED_ID, as defined in Table 35. This ID shall be set by the HNED.	M
CustomerID	As defined in Table 34.	M
HNED_ID	The HNED_ID as passed from the HNED to the DSMM in DSM003. As defined in Table 34.	M

13.7.3 Status synchronization updates

13.7.3.1 DSM101 - Sychronisation of current status - DSM Manager to HNED

This message is used by the DSM Manager to synchronize the status settings of all the HNEDs as they are switched from off or standby to one of the active states, and also to be used as a method of asynchronously synchronizing the values held by the HNEDs and the DSM Manager in the event of a service status change, such as an access network bitrate change or HNED priority change.

```
MessageType=DSM101 {
    CustomerID {
        HNED_ID
        HNEDPriority
        ServiceTypePriority
        ContentModePriority
        TotalAvailableBitrate
    }
}
```

Table 41: DSM101 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM101" from DSM Manager to HNED to carry updates of delivery and service status values. This may be used whenever anything has changed, e.g. available bitrate, or an HNED is brought from off or out of standby. Message type "DSM101" also carries information about the HNED and service priorities where they have been set by the DSM Manager.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
HNEDPriority	As defined in Table 34.	O
ServiceTypePriority	As defined in Table 34.	O
ContentModePriority	As defined in Table 34.	O
TotalAvailableBitrate	As defined in Table 34.	M

13.7.4 Messages directly associated with a service selection

13.7.4.1 DSM201 - Change request - HNED to DSM Manager

```
MessageType="DSM201" {
    CustomerID {
        HNED_ID {
            NegotiationSessionID
            SessionID
            ServiceID{
                DomainName
                ServiceName
            }
            RequestedServiceID{
                DomainName
                ServiceName
            }
            RequestedServiceLocation
            RequestedServiceBitrate
        }
    }
}
```

Table 42: DSM201 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM201" from HNED to DSM Manager to carry the request from the HNED which wants to set up a new connection or change connections where a bitrate contention will exist if the simple change is carried out.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	SessionID associated with current service change transaction, as defined in Table 35.	M
SessionID	As defined in Table 34.	M
ServiceID	As defined in Table 34.	M
ServiceID.DomainName	As defined in Table 34.	M
ServiceID.ServiceName	As defined in Table 34.	M
RequestedServiceID	As defined in Table 35.	M
RequestedServiceID.DomainName	As defined in Table 35.	M
RequestedID.ServiceName	As defined in Table 35.	M
RequestedServiceLocation	Connection URL or IP address (IPv4 or IPv6) and port number, provided from SD&S.	O
RequestedServiceBitrate	A value provided in SD&S in "MaxBitrate" element of IPService.	M

13.7.4.2 DSM202 - Change proposal - DSM Manager to HNED

```
MessageType="DSM202" {
    CustomerID {
        HNED_ID {
            NegotiationSessionID
            ProposedSessionID
            ProposedServiceID {
                DomainName
                ServiceName
            }
            ProposedServiceBitrate
            ProposedServiceLocation
            Preference
        }
    }
}
```

Table 43: DSM202 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM202" from DSM Manager to HNED to carry requests from the DSM Manager to the HNED for which the service would be affected by the service changes proposed by the associated DSM201 message.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSession ID	SessionID associated with a service change transaction.	M
ProposedSessionID	Service delivery session ID for proposed service. If the message is used to terminate the service which an HNED is receiving, this field will be populated with "0".	M
ProposedServiceID	Service ID for proposed service. If the message is used to terminate the service which an HNED is receiving, this field will be populated with "0".	M
ProposedServiceID.DomainName	DomainName as defined in Table 35.	M
ProposedServiceID.ServiceName	ServiceName as defined in Table 35.	M
ProposedServiceBitrate	Service bitrate for proposed service. If the message is used to terminate the service which an HNED is receiving, this field will be populated with "0".	M
ProposedServiceLocation	Location for proposed service. If the message is used to terminate the service which an HNED is receiving, this field will be populated with "0".	O
Preference	Ranking number for services to be offered. A value of "1" marks highest preference, increasing values (2, 3, etc.) should be interpreted as reduced preference.	O

13.7.4.3 DSM203 - Change accept/refuse - HNED to DSM Manager

```
MessageType="DSM203" {
    CustomerID {
        HNED_ID {
            NegotiationSessionID

            ProposedServiceID {
                DomainName
                ServiceName
            }
            Response="Accept" | "Refuse"
        }
    }
}
```

Table 44: DSM203 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM203" from HNED to DSM Manager to accept or refuse the change proposal (DSM202).	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSession ID	SessionID associated with a service change transaction.	M
ProposedServiceID	ServiceID for proposed service which has been accepted or refused.	M
ProposedServiceID.DomainName	DomainName as defined in Table 35.	M
ProposedServiceID.ServiceName	ServiceName as defined in Table 35.	M
Response	Value = "Accept" "Refuse".	M

13.7.4.4 DSM204 - Change confirmed/cancelled - DSM Manager to HNED

```
MessageType="DSM204" {
  CustomerID {
    TotalAvailableBitrate
    HNED_ID {
      NegotiationSessionID
      ProposedSessionID
      Response="Confirmed" | "Cancelled"
    }
  }
}
```

Table 45: DSM204 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM204" from DSM Manager to HNED to inform that the change proposal will be carried out (confirmed) or will be cancelled.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSession ID	SessionID associated with a service change transaction, as defined in Table 35.	M
ProposedSessionID	Service delivery session ID for proposed service, as defined in Table 35.	M
Response	Value = "Confirmed" "Cancelled".	M

13.7.4.5 DSM205 - Service Change Acknowledge - HNED to DSM Manager

Sent by both HNEDs to DSM Manager to acknowledge that the transaction is complete and the negotiation session should be closed.

```
MessageType="DSM205" {
  CustomerID {
    HNED_ID {
      NegotiationSessionID
    }
  }
}
```

Table 46: DSM205 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM205" from HNED to DSM Manager to acknowledge that the transaction is complete and the negotiation session should be closed.	M
CustomerID	As defined Table 34.	M
HNED_ID	As defined Table 34.	M
NegotiationSession ID	SessionID associated with a service change transaction, as defined in Table 35.	M

13.7.4.6 DSM206 - Service Change complete - HNED to DSM Manager

Sent by a HNED when a service change has happened in which the DSM Manager was not involved to acknowledge that the service change transaction is complete. Note that since this is a single message with no associated negotiation session there is no "NegotiationSessionID" field.

It is assumed that "NegotiationSessionID" is used by the DSM Manager and all HNEDs involved to track the components of any service change.

```
MessageType="DSM206" {
CustomerID {
HNED_ID {
    SessionID
    ServiceID {
        DomainName
        ServiceName
    }
    ServiceBitrate
    ServiceLocation
}
}
}
```

Table 47: DSM206 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM206" from HNED to DSM Manager to acknowledge that the service change transaction is complete.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
SessionID	SessionID associated with a service change transaction	M
ServiceID	Service ID for a service the HNED has connected to.	M
ServiceID.DomainName	As defined in Table 35.	M
ServiceID.ServiceName	As defined in Table 35.	M
ServiceBitrate	Service bitrate for a service the HNED has connected to.	M
ServiceLocation	Location for proposed service the HNED has connected to.	O

13.7.5 Data value messages

13.7.5.1 DSM301 - Query value - HNED to DSM Manager

```
MessageType="DSM301" {
CustomerID {
    HNED_ID {
        NegotiationSessionID
        ParameterID
    }
}
}
```

Table 48: DSM301 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM301" from HNED to DSM Manager requesting current value of parameter.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID	Parameter for which value is requested.	M

13.7.5.2 DSM302 - Return value - DSM Manager to HNED

```
MessageType="DSM302" {
  CustomerID {
    HNED_ID {
      NegotiationSessionID
      ParameterID <Value>
    }
  }
}
```

Table 49: DSM302 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM302" from DSM Manager to HNED returning current value of parameter.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID <Value>	Parameter and current value.	M

13.7.5.3 DSM303 - Set value - HNED to DSM Manager

```
MessageType="DSM303"
  CustomerID {
    HNED_ID {
      NegotiationSessionID
      ParameterID <Value>
    }
  }
}
```

Table 50: DSM303 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
MessageType	Message type "DSM303" from HNED to DSM Manager containing new value of parameter to be set in DSM Manager. Multiple "ParameterID <Value>" pairs may be carried sequentially.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID <Value>	ParameterID and value to be set in DSM Manager.	M

13.7.5.4 DSM304 - Set value success - DSM Manager to HNED

```
MessageType="DSM304"
CustomerID {
    HNED_ID {
        NegotiationSessionID
        ParameterID
    }
}
```

Table 51: DSM304 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM304" from DSM Manager to HNED confirming that the new value of parameter has been set.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID	Parameter for which value has been set.	M

13.7.5.5 DSM305 - Query value - DSM Manager to HNED

```
MessageType="DSM305"
CustomerID {
    HNED_ID {
        NegotiationSessionID
        ParameterID
    }
}
```

Table 52: DSM305 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM305" from DSM Manager to HNED requesting current value of parameter.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID	Parameter for which value is requested.	M

13.7.5.6 DSM306 - Return value - HNED to DSM Manager

```
MessageType="DSM306"
CustomerID {
    HNED_ID {
        NegotiationSessionID
        ParameterID <Value>
    }
}
```

Table 53: DSM306 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM306" from HNED to DSM Manager returning current value of parameter.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID <Value>	Parameter and current value.	M

13.7.5.7 DSM307 - Set value - DSM Manager to HNED

```
MessageType="DSM307"
CustomerID {
    HNED_ID {
        NegotiationSessionID
        ParameterID Value
    }
}
```

Table 54: DSM307 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM307" from DSM Manager to HNED containing new value of parameter to be set in DSM Manager. Multiple "ParameterID <Value>" pairs may be carried sequentially.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID <Value>	ParameterID and value to be set in DSM Manager.	M

13.7.5.8 DSM308 - Succesfull transaction - HNED to DSM Manager

```
MessageType="DSM308"
CustomerID {
    HNED_ID {
        NegotiationSessionID
        ParameterID
    }
}
```

Table 55: DSM308 Message Profiling

Element/Attribute Name	Element/Attribute Description	Mandated/Optional
MessageType	Message type "DSM308" from HNED to DSM Manager confirming that the new value of parameter has been set.	M
CustomerID	As defined in Table 34.	M
HNED_ID	As defined in Table 34.	M
NegotiationSessionID	ID set by HNED of session associated with data value exchange, as defined in Table 35.	M
ParameterID	Parameter for which value has been set.	M

13.8 Message Structure and Transport

13.8.1 Structure of the messages

All messages shall be structured in the same way, to conform with the schema shown in clause 13.8.3. The elements for any message may be included in any order within the following rules:

- All sub-elements shall be grouped with their parent element.
- Elements which are not required may be omitted.
- Multiple DSM messages which may be associated from DSM Manager to HNED or vice versa may be combined in a single HTTP(S) payload string, for example, the response from the DSM Manager to an HNED to a DSM001 request could include a sequence of message types DSM002 and DSM101, and also DSM004 if the DSM Manager is used to set the HNED priority. If multiple DSM messages are carried all the elements of each DSM message shall be listed together.

13.8.2 Transport of the messages

Messages shall be exchanged between a single HNED within a home (defined by the combination of "CustomerID" and "HNED_ID") and the DSM Manager. The messages shall be transported over HTTP or HTTPS, as defined in IETF RFC 2616 [39]. The HTTP GET method shall be used for all message exchanges. As the delivery of DSM messages is based on a peer to peer model, the HTTP response is not used to carry the DSM response message, but the DSM response message is carried using another HTTP GET message. This means that the HNED shall host a HTTP server.

The HTTP messages shall contain the DSM messages defined in clauses 13.6 and 13.7 according to the rules defined in clause 13.8. Clause 13.8.3 describes the schema of the HTTP transport messages.

Optionally, message security and authentication shall be carried out using the methods defined in the DVB RMS/FUS (ETSI TS 102 824 [78]) specification.

13.8.3 Message Schema

As a result of the rules defined in clause 13.8 and the DSM message contents defined in clause 13.7 the HTTP message schema is as follows.

The message elements shall be prefixed using reserved characters as defined in IETF RFC 2396 [31] as follows:

```
Message type prefixed by "?"
  Message elements prefixed (hierarchically) as:
    Main identifiers (CustomerID, HNED_ID, NegotiationID) prefixed by "$"
      Element pre-fixed by "&"
    Message terminated by ";"
```

The general message schema is therefore as follows:

```
http://'SourceAddress:[<port]>'?'<MessageType> {'$CustomerID='<string>} {'$HNED_ID='<string>}
{'$NegotiationSessionID='<value>} {'&'<Element>'='<value>} {'&'<Element>'='<value>} {'&'<Child-
element >'='<value>} {'&'<Child-element >'='<value>}'{'&'<Element>'='<value>'}';;
```

Where:

```
SourceAddress = address
port = associated port number (optional)
MessageType = DSM message identifier, e.g. dsm101
CustomerID as defined in clause 13.5.1, this is not required for all messages
HNED_ID as defined in clause 13.5.1, this is not required for all messages
NegotiationSessionID = NegotiationID as defined in clause 13.5.1, this is not required for all
messages and may not be present
<Element> = Element-name as defined in clause 13.7 or as used during a DSM negotiation
<value> = Value as defined in clause 13.7 or as used during a DSM negotiation
';' = Message terminator
```

For example:

A DSM001 message might be:

```
'http://SourceAddress:[port]?MessageType=DSM001$NegotiationSessionID=ASDF1234
[$HNEDPriority=2];;
```

A DSM306 message returning the value of a parameter following a query might be:

```
'http://SourceAddress:[port]?MessageType=DSM306 $CustomerID=5678ad $HNED_ID=qwerty1
$NegoiationID=123098 &TotalDSMBitrate=3500500;;
```

A composite message containing DSM 002 and DSM101 may be:

```
'http://SourceAddress:[port]?MessageType=DSM002$CustomerID=5678ad$HNED_ID=qwerty1$NegoiationI
D=123098?DSM101$CustomerID=5678ad$HNED_ID=qwerty1$HNEDPriority=2$ServiceTypePriority=1$C
ontentModePriority=2$TotalAvailableBitrate=400050050;;
```

13.9 Setting of HNED Identifier (HNED_ID) for each HNED

Only one DSM Manager will be available for any service offering and therefore only a single URI will be provided.

The process by which the unique HNED_ID is set for each HNED in a home is not mandated in this present document.

From the SD&S metadata at first boot-up, as follows:

- HNED follows standard boot process defined in clause 8 to connect to the Service Provider SD&S service.
- The HNED acquires the RMSFUSDiscovery record from the SD&S record.
- The DSMPublic element of the SD&S "RMSFUSDiscovery" element from the Service Provider which supports DSM shall contain the address of the DSM Manager.
- Exchange of HNED_ID by one of the following options:
 - If the HNED_ID has not been pre-assigned then the HNED requests the HNED_ID information from the DSM Manager using the DSM001 message, as defined in clause 13.7.2.1. The DSM Manager returns the HNED_ID information as requested using the DSM002 message, as defined in clause 13.7.2.2.
 - If the HNED_ID has been pre-assigned then the HNED passes the HNED_ID information to the DSM Manager using the DSM003 message, as defined in clause 13.7.2.3. Acceptance of this HNED_ID will be confirmed by the DSMM using the DSM004 message.
- The DSM Manager sends a DSM101 Status Synchronization message to the HNED, as defined in clause 13.7.3.1.
- Normal HNED startup and operation then continues.

NOTE: The service provider may validate the HNED before exchanging the HNED_ID using means not specified in the present document.

Annex A (informative): MPEG-2 Timing Reconstruction

A.0 Overview

This annex describes one way in which RTP timestamps can be used to reconstruct an MTS that is encapsulated in RTP packets using IETF RFC 2250 [29] and transported over a jitter-inducing network e.g. IP or Ethernet. This description is for information only and is not a normative part of the present document.

The Transport Stream System Target Decoder (T-STD) is defined fully in ISO/IEC 13818-1 [52]. It is a conceptual decoder model used to define terms precisely and to model the decoding process. The input to the T-STD is a MTS. A MTS may contain multiple MPEG programs with independent time bases. However, the T-STD decodes only one program at a time.

Data from the MTS enters the T-STD at a piecewise constant rate. The i th byte enters at time $t(i)$. The time at which this byte enters the T-STD can be recovered from the input stream by decoding the input PCR fields, encoded in the MTS packet adaptation field of the program to be decoded and, by counting the bytes in the complete MTS between the successive PCRs of the program to be decoded. The value encoded in the PCR field indicates the time $t(i)$, where i refers to the byte containing the last bit of the PCR.

For all other bytes the input arrival time $t(i)$ is computed from $PCR(i'')$ and the transport rate at which the MTS arrives. The transport rate is determined as the number of bytes in the MTS between the bytes containing the last bit of two successive PCR fields of the same program plus one, divided by the difference between the time values encoded in these same two PCR fields (see also figure A.1):

$$t(i) = \frac{PCR(k-1)}{27\text{ MHz}} + \frac{i - i''}{R(i)} \quad (\text{A.1})$$

Where:

- i is the index of any byte in the MTS for $i'' < i < i'$.
- i'' is the index of the byte containing the last bit of the most recent PCR field applicable to the program being decoded.
- $PCR(k-1)$ is the time encoded in the PCR field in units of the 27 MHz system clock.
- $R(i)$ is the transport rate which is calculated as follows:

$$R(i) = \frac{(i' - i'') \times 27\text{ MHz}}{PCR(k) - PCR(k-1)} \quad (\text{A.2})$$

Where:

- i' is the index of the byte containing the last bit of the immediately following PCR applicable to the program being decoded.
- and $i'' < i \leq i'$.

Note that equation A.2 assumes that the transport rate between two successive PCRs is constant, but that the transport rate may change at any PCR. Note furthermore that the transport rate for multi-program transport streams is typically constant, but that the transport rate of a single-program transport stream may vary within the piece-wise constant rate concept defined by equation A.2. (See also ISO/IEC 13818-1 [52]).

A tolerance is specified for the PCR values. The PCR tolerance is defined as the maximum inaccuracy allowed in received PCRs. This inaccuracy may be due to imprecision in the PCR values or to PCR modification during remultiplexing. Note that it does not include errors in packet arrival time due to network jitter or other causes. The PCR tolerance is ± 500 ns. In the T-STD model, the inaccuracy will be reflected as an inaccuracy in the calculated transport rate $R(i)$ of equation A.2.

A.1 Clock recovery in a RTP receiver

It is assumed that a jitter-smoothing network adapter is inserted between a network's output and an MPEG-2 decoder. The network adapter exploits the RTP timestamps to achieve jitter smoothing. The MPEG-2 decoder is assumed to conform to the real-time MPEG-2 interface specification [53]. This interface requires an MPEG-2 decoder with more jitter tolerance than the idealized decoder of the System Target Decoder. The network adapter processes the incoming jittered bit stream and outputs a system stream whose actual byte delivery schedule conforms to the real-time specification.

Note that for immediate decoding the network adapter approach may not be necessary or cost effective. Instead a single stage of clock recovery can be used.

According to IETF RFC 2250 [29], each RTP packet contains a timestamp derived from the sender's 90 KHz clock reference. This timestamp is the *target transmission time* of the first byte of the RTP payload i.e. the "ideal" time that the packet should be fed into the IP network. It is assumed that the time between the last byte put in the RTP packet and the time value inserted as the RTP timestamp into the packet is constant. In this way the RTP timestamp is the time of the last byte that entered the RTP packet plus some constant delay. Note that the boundary of the IP network may still be somewhat vague and this may affect the jitter process i.e. the transmitter can also add some (scheduling and processing) jitter to the packet before it appears on the (IP) network. However, the receiver should be able to handle this additional jitter adequately.

In this regard, the difference between the (RTP) *target transmission time* and the (MPEG) *target delivery time* is a time constant plus the (constant) delay imposed on the delivery of the MTS to the RTP receiver. Both can be ignored, because they are constant, and hence for the RTP receiver the target transmission time is functionally equivalent to the target delivery time.

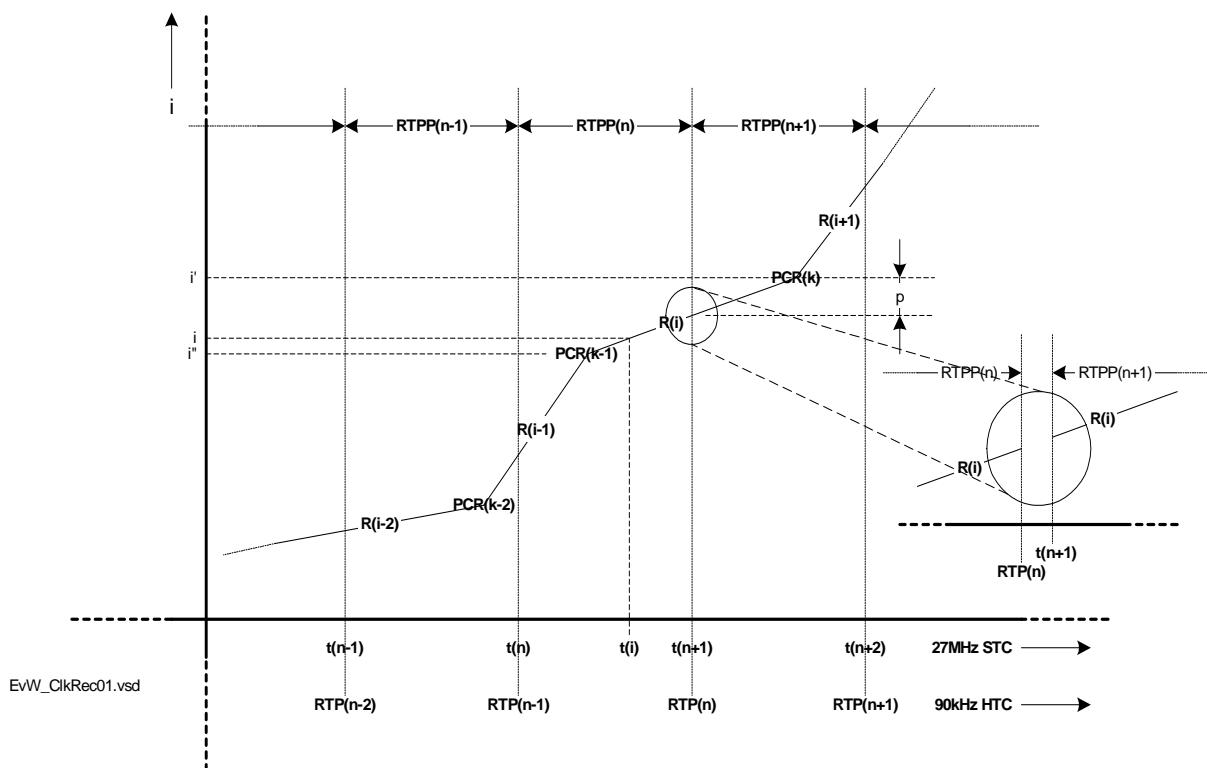


Figure A.1: Timing

In terms of the MPEG-2 system time clock, the first byte of the payload of *RTP Packet (n+1)*, referred to as RTPP(n+1) in figure A.1, enters the T-STD at time $t(n+1)$. Time $t(n+1)$ can be recovered as follows:

$$t(n+1) = \frac{PCR(k)}{27 \text{ MHz}} - \frac{p}{R(i)} \quad (\text{A.3})$$

where:

$n+1$	is the index of the RTP packet i.e. the value $n+1$ in RTPP($n+1$).
k	is the index of the first PCR in RTPP($n+1$).
p	is the number of bytes preceding the byte that contains the last bit of PCR(k).
$PCR(k)$	is the time encoded in the first PCR of the MPEG program that is selected as reference to reconstruct the MTS.
$R(i)$	is the transport rate of the transport stream between PCR($k-1$) and PCR(k) of the MPEG program that is selected as reference to reconstruct the MTS, as calculated by equation A.2.

The target transmission time $RTP(n)$ plus a constant delay, expressed in units of the 90 kHz Head-end Time Clock (HTC) of the sender corresponds to time value $t(n+1)$ of the first byte of RTPP($n+1$). Time value $t(n+1)$ is expressed in units of the 27 MHz MPEG-2 STC. In many, if not all cases, it is reasonable to assume that the drift between the HTC and the STC can be ignored for the duration of the transport stream contained in one RTP packet and between two consecutive RTP packets.

Therefore, if desired, it is also possible to map the value of any contained PCR to a 90 kHz value of the sender, as follows:

$$PCR(k) \approx RTP(n) + 90 \text{ kHz} \times \frac{(p+1)}{R(i)} \quad (\text{A.4})$$

The mapping information between the STC and the 90 kHz clock of the sender can be used to reconstruct the MPEG-2 transport stream at the receiver.

Note that there is an uncertainty of about 11 μs (1/90 kHz), due to the 90 kHz resolution of the RTP time stamps. This is perceived by the receiver as delivery jitter and conforms to the MPEG-2 real-time interface specification [53]. A well-constructed 27 MHz STC PLL should be able to remove this jitter.

Note that the RTP timestamps can be derived from an arbitrary 90 kHz HTC, which may be, but is not required to be, locked to the STC of one of the programs in the MTS.

A.2 Recommendation

To use this two-stage MTS reconstruction method based on RTP timestamps, it is recommended that the time between putting the last byte in the RTP packet and inserting the RTP timestamp value into the RTP packet is constant.

Annex B (informative): SD&S data model

Following restructuring, the text for this annex can now be found in clause 5.2.7: "Data Model (Informative)".

Annex C (normative): Schemas

C.1 SD&S XML schemas

C.1.1 Namespace

Following restructuring, the text for this clause can now be found in clause 5.2.8: "Metadata Namespace".

C.1.2 Simple types

Following restructuring, the text for this clause can now be found in clause 5.2.10: " XML Basic Types".

C.1.3 Complex types and attribute groups

Following restructuring, the text for this clause can now be found in clause 5.2.11: "XML Complex Types - Attribute Groups".

C.1.4 Element Types

Following restructuring, the text for this clause can now be found in clause 5.2.12: "XML Complex Types - Element Groups".

C.1.5 Schema

Following restructuring, the text for this clause can now be found in clause 5.2.13: "XML Main Types".

C.1.6 Multicasting SD&S XML documents

Following restructuring, the text for this clause can now be found in clause 5.4: "Transport mechanisms".

C.2 CDS XML Schemas

C.2.0 Introduction

The following clauses define the various types and elements that are used in the CDS XML schema. The full normative XML schema is available as the file dvb_metadata_iptv_cds_2008-1r3.xsd in archive ts_102034v020101p0.zip which accompanies the present document.

C.2.1 Namespace

The namespace for the CDS XML schema is urn:dvb:metadata:iptv:cds:2008-1.

C.2.2 Basic schema definitions

```
<?xml version="1.0" encoding="utf-8"?>
<! -- Created with Liquid XML Studio 1.0.8.0 (http://www.liquid-technologies.com) -->
<xsschema targetNamespace="urn:dvb:metadata:iptv:cds:2008-1"
  xmlns:cds="urn:dvb:metadata:iptv:cds:2008-1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:sdns="urn:dvb:metadata:iptv:sdns:2008-1"
  xmlns:hfp="http://www.w3.org/2001/XMLSchema-hasFacetAndProperty"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xss import namespace="urn:dvb:metadata:iptv:sdns:2008-1" schemaLocation=".//sdns_v1.4r13.xsd"/>
  <xss:annotation>
    <xss:documentation xml:lang="en">
      The present document defines XML schemas used for DVB IPTV Content Download Services
      (CDS) and is
    </xss:documentation>
  </xss:annotation>
</xsschema>
```

```

compatible with r1.4 of ETSI TS 102 034 and later using associations with
"sdns_v1.4r13.xsd"
  </xs:documentation>
</xs:annotation>
...
...
</xs:schema>

```

C.2.3 Download session description

```

<xs:complexType name="Download-Session-General-ParametersType">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="1" name="Service-Provider-Domain" type="sdns:DomainType"
/>
    <xs:element minOccurs="1" maxOccurs="1" name="Download-Session-ID" type="xs:nonNegativeInteger"
/>
    <xs:element minOccurs="1" maxOccurs="1" name="Download-Session-Version"
type="xs:nonNegativeInteger" />
    <xs:element minOccurs="0" maxOccurs="1" name="Content-Item-Format">
      <xs:simpleType>
        <xs:restriction base="xs:unsignedByte">
          <xs:enumeration value="0" />
          <xs:enumeration value="1" />
          <xs:enumeration value="2" />
          <xs:enumeration value="3" />
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="1" maxOccurs="1" name="Download-Session-Time-Information">
      <xs:complexType>
        <xs:attribute name="Start-Time" type="xs:dateTime" use="required" />
        <xs:attribute name="Stop-Time" type="xs:dateTime" use="optional" />
      </xs:complexType>
    </xs:element>
    <xs:element minOccurs="0" maxOccurs="1" name="Reception-Reporting">
      <xs:complexType>
        <xs:complexContent mixed="false">
          <xs:extension base="cds:Distribution-Of-Requests-Over-Time-And-ServersType">
            <xs:attribute default="0" name="Mode" use="optional">
              <xs:simpleType>
                <xs:restriction base="xs:unsignedByte">
                  <xs:enumeration value="0" />
                  <xs:enumeration value="1" />
                  <xs:enumeration value="2" />
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:extension>
        </xs:complexContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

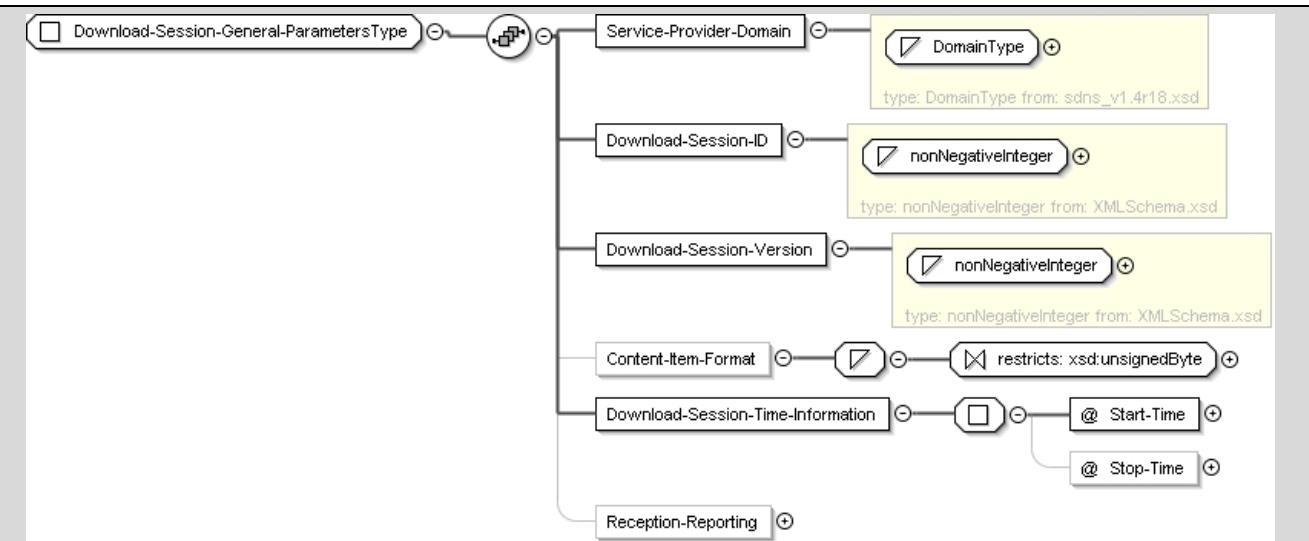


Figure C.1: Download-Session-General-ParametersType



Figure C.2: Reception-Reporting

```

<xs:element name="Unicast-Download-Session">
  <xs:complexType>
    <xs:complexContent mixed="false">
      <xs:extension base="cds:Download-Session-General-ParametersType">
        <xs:sequence>
          <xs:element minOccurs="1" maxOccurs="unbounded" name="File-Info">
            <xs:complexType>
              <xs:choice>
                <xs:element name="File-Server-Info" type="cds:File-Server-InfoType" />
                <xs:element name="File-Server-Chunk-Info" type="cds:File-Server-Chunk-InfoType" />
              </xs:choice>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:element>

```



Figure C.3: Unicast-Download-Session

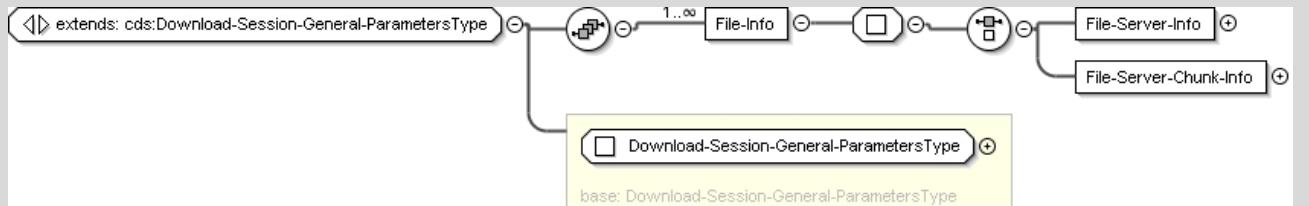


Figure C.4: Extended Download-Session-General-ParametersType

```

<xs:complexType name="Multicast-Download-SessionType">
  <xs:complexContent mixed="false">
    <xs:extension base="cds:Download-Session-General-ParametersType">
      <xs:sequence>
        <xs:element minOccurs="0" maxOccurs="unbounded" name="File-Reference">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:anyURI" />
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```
</xs:element>
<xs:element minOccurs="1" maxOccurs="1" name="IP-Multicast-Address-Source"
type="sdns:IPOrDomainType" />
<xs:element minOccurs="1" maxOccurs="1" name="Transport-Session-Identifier">
<xs:simpleType>
<xs:restriction base="xs:unsignedLong">
<xs:maxInclusive value="281474976710655" />
<xs:minInclusive value="0" />
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element minOccurs="0" default="1" name="Number-Of-Channels">
<xs:simpleType>
<xs:restriction base="xs:unsignedByte">
<xs:maxInclusive value="16" />
<xs:minInclusive value="1" />
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element maxOccurs="unbounded" name="Channel">
<xs:complexType>
<xs:attribute name="IP-Multicast-Address" type="sdns:IPType" use="required" />
<xs:attribute name="IP-Multicast-Port-Number" type="xs:unsignedShort" use="required" />
<xs:attribute name="Max-Bandwidth-Requirement" type="xs:positiveInteger" use="optional" />
/>
</xs:complexType>
</xs:element>
<xs:element minOccurs="0" default="0" name="FEC-Encoding-ID" type="xs:unsignedByte" />
<xs:element minOccurs="0" name="Recovery">
<xs:complexType>
<xs:complexContent mixed="false">
<xs:extension base="cds:Distribution-Of-Requests-Over-Time-And-ServersType">
<xs:attribute default="0" name="Mode" use="optional">
<xs:simpleType>
<xs:restriction base="xs:unsignedByte">
<xs:enumeration value="0" />
<xs:enumeration value="1" />
</xs:restriction>
</xs:simpleType>
</xs:attribute>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```



Figure C.5: Multicast-Download-SessionType

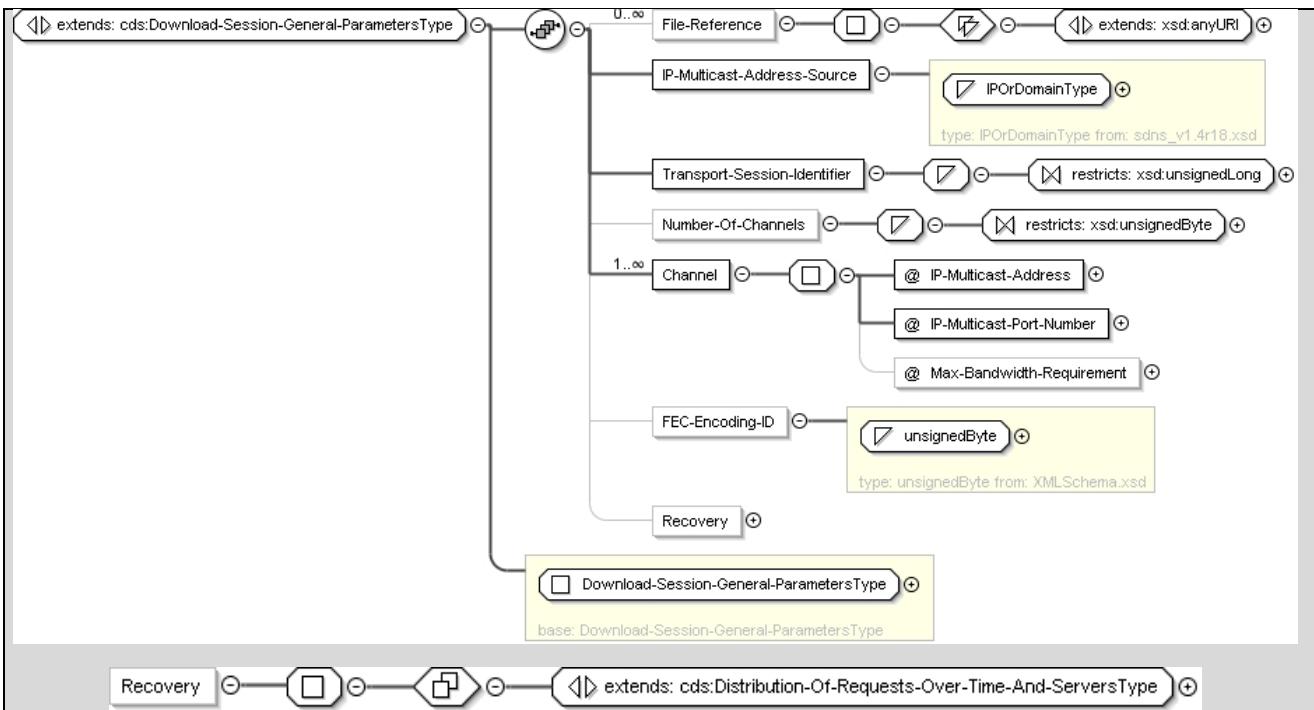


Figure C.6: Extended Download-Session-General-ParametersType

```
<xs:element name="Carousel-Multicast-Download-Session">
<xs:complexType>
  <xs:complexContent mixed="false">
    <xs:extension base="cds:Multicast-Download-SessionType" />
  </xs:complexContent>
</xs:complexType>
</xs:element>
```

See Figure C.5..

```
<xs:element name="Scheduled-Multicast-Download-Session">
<xs:complexType>
  <xs:complexContent mixed="false">
    <xs:extension base="cds:Multicast-Download-SessionType">
      <xs:sequence>
        <xs:element minOccurs="0" name="Completion-Poll-Response-Server">
          <xs:complexType>
            <xs:attribute name="IP-Address" type="sdns:IPOrDomainType" use="required" />
            <xs:attribute name="Port-Number" type="xs:unsignedShort" use="required" />
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
</xs:element>
```

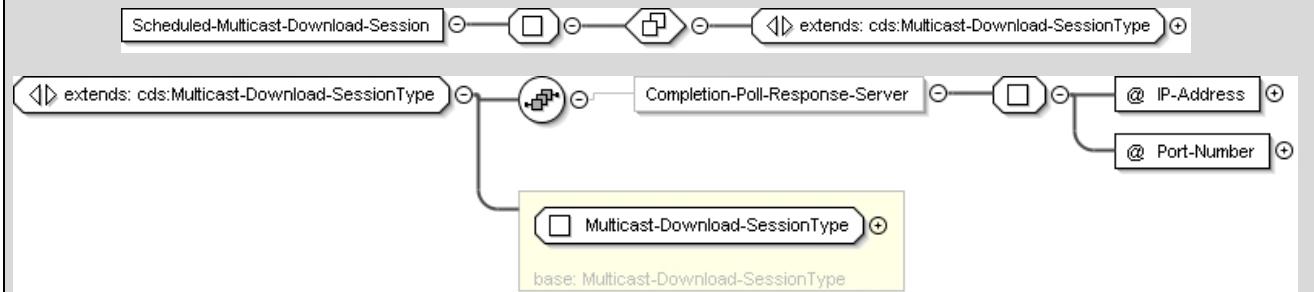


Figure C.7: Extended Multicast-Download-SessionType

```
<xs:complexType name="Distribution-Of-Requests-Over-Time-And-ServersType">
  <xs:sequence>
    <xs:element maxOccurs="unbounded" name="Server-URI" type="xs:anyURI" />
  </xs:sequence>
```

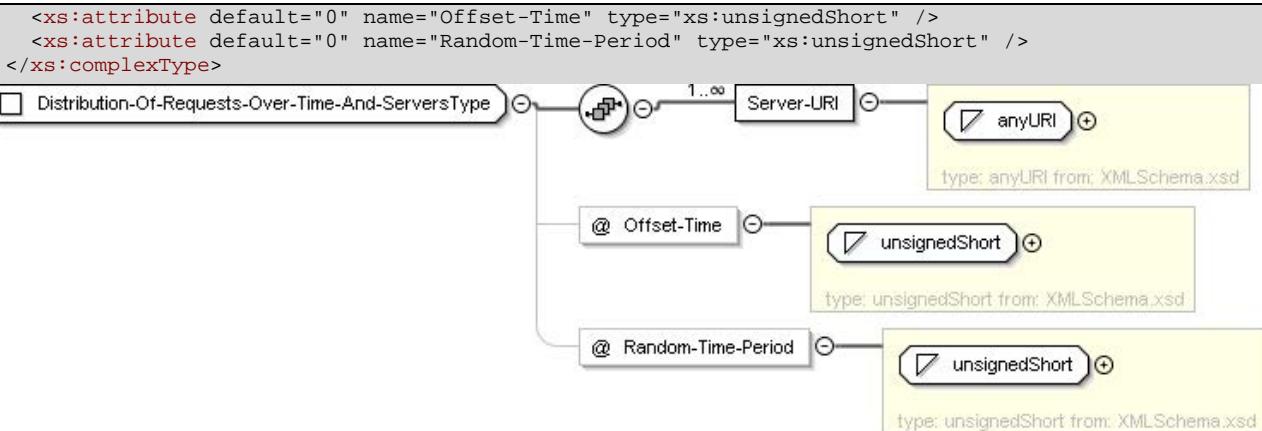


Figure C.8: Distribution-Of-Requests-Over-Time-And-ServersType

```

<xs:complexType name="File-InfoType">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="1" name="File-Reference" type="xs:anyURI" />
    <xs:element minOccurs="0" maxOccurs="1" name="File-Content-Typ" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="Content-Item-Format">
      <xs:simpleType>
        <xs:restriction base="xs:unsignedByte">
          <xs:enumeration value="0" />
          <xs:enumeration value="1" />
          <xs:enumeration value="2" />
          <xs:enumeration value="3" />
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="0" maxOccurs="1" name="File-Length" type="xs:unsignedLong" />
    <xs:element minOccurs="0" maxOccurs="1" name="File-Digest" type="xs:base64Binary" />
  </xs:sequence>
</xs:complexType>

```

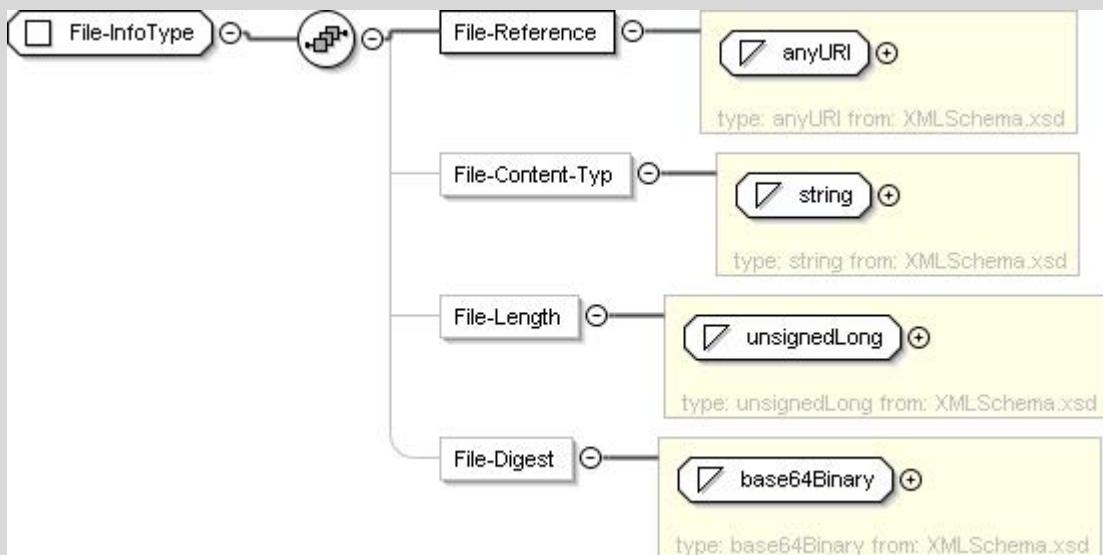


Figure C.9: File-InfoType

```

<xs:complexType name="File-Server-InfoType">
  <xs:complexContent mixed="false">
    <xs:extension base="cds:File-InfoType">
      <xs:sequence>
        <xs:element minOccurs="1" maxOccurs="unbounded" name="Server-Info">
          <xs:complexType>
            <xs:sequence>
              <xs:element minOccurs="1" maxOccurs="1" name="Server-Base-URI" type="xs:anyURI" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

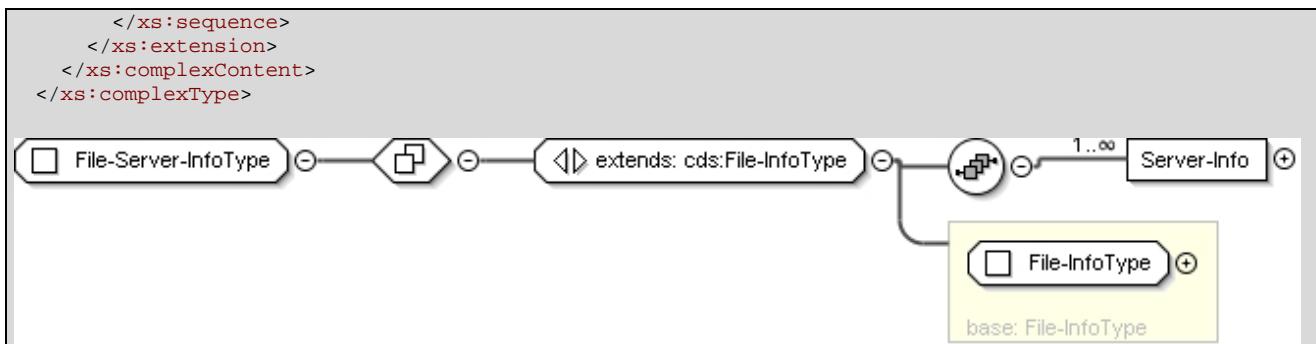


Figure C.10: File-Server-InfoType



Figure C.11: Server-Info

```

<xs:complexType name="File-Server-Chunk-InfoType">
  <xs:complexContent mixed="false">
    <xs:extension base="cds:File-InfoType">
      <xs:sequence>
        <xs:element minOccurs="1" maxOccurs="1" name="Chunk-Length" type="xs:unsignedLong" />
        <xs:element minOccurs="0" maxOccurs="unbounded" name="Chunk-Digest">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Digest" type="xs:base64Binary" />
              <xs:element name="Chunk-Number" type="xs:unsignedLong" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element minOccurs="1" maxOccurs="unbounded" name="Server-Info">
          <xs:complexType>
            <xs:sequence>
              <xs:element minOccurs="1" maxOccurs="1" name="Server-Base-URI" type="xs:anyURI" />
              <xs:element minOccurs="0" maxOccurs="1" name="Available-Chunk-List" type="cds:Available-Chunk-ListType" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
  
```

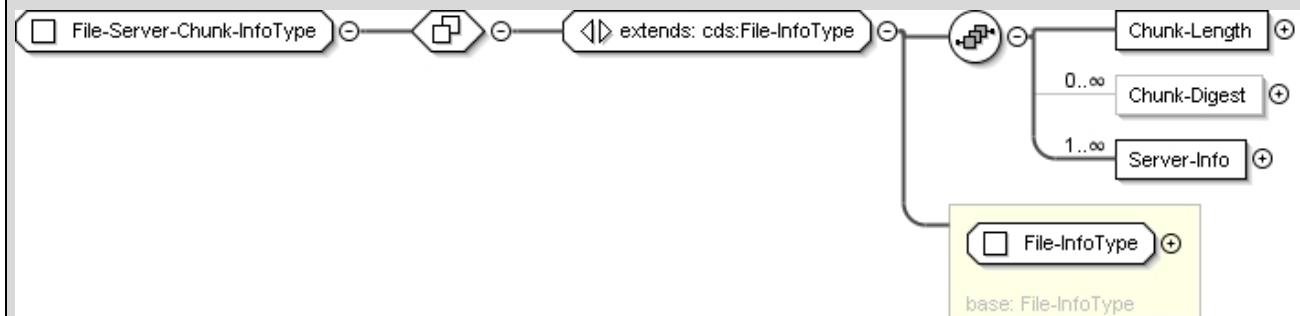
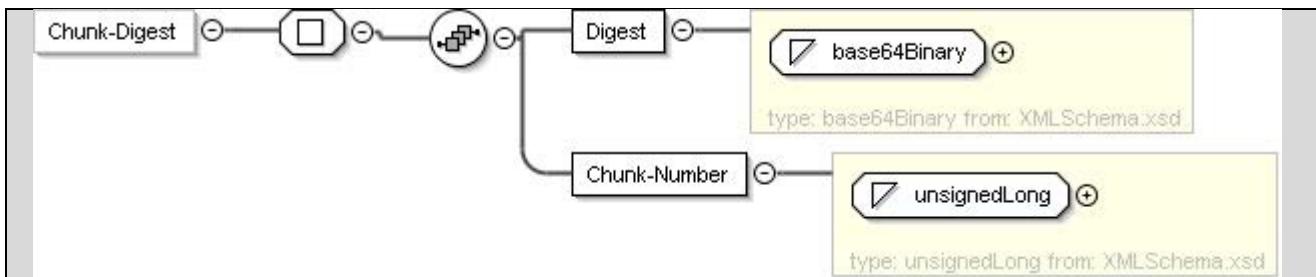
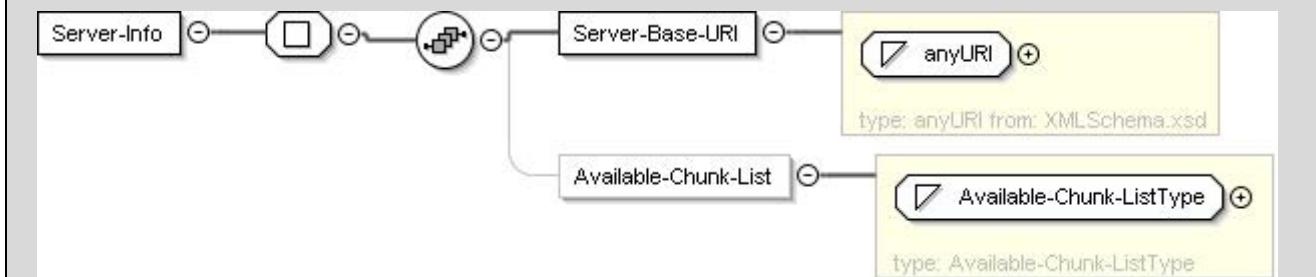


Figure C.12: File-Server-Chunk-InfoType

**Figure C.13: Chunk-Digest****Figure C.14: Server-Info**

```

<xs:simpleType name="Available-Chunk-ListType">
  <xs:list itemType="xs:positiveInteger" />
</xs:simpleType>
  
```

**Figure C.15: Available-Chunk-List**

C.2.4 Reception reporting message

```

<xs:element name="Content-Item-Reception-Report">
  <xs:complexType>
    <xs:complexContent mixed="false">
      <xs:extension base="cds:Basic-Reception-Report-Type">
        <xs:sequence minOccurs="1" maxOccurs="1">
          <xs:element minOccurs="1" maxOccurs="unbounded" name="File">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="File-URI" type="xs:anyURI" />
                <xs:element name="Download-Action">
                  <xs:simpleType>
                    <xs:restriction base="xs:string">
                      <xs:enumeration value="download" />
                      <xs:enumeration value="skipped" />
                    </xs:restriction>
                  </xs:simpleType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:element>
  
```

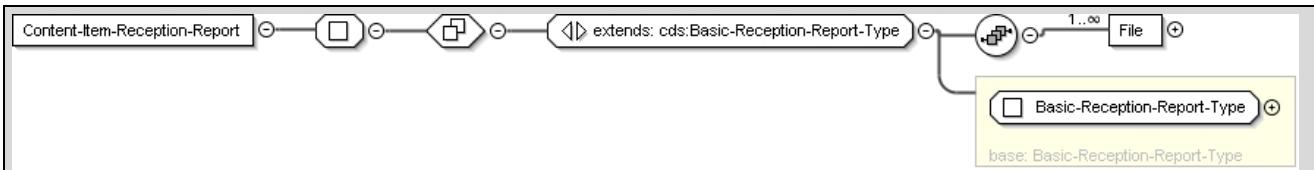


Figure C.16: Content-Item-Reception-Report

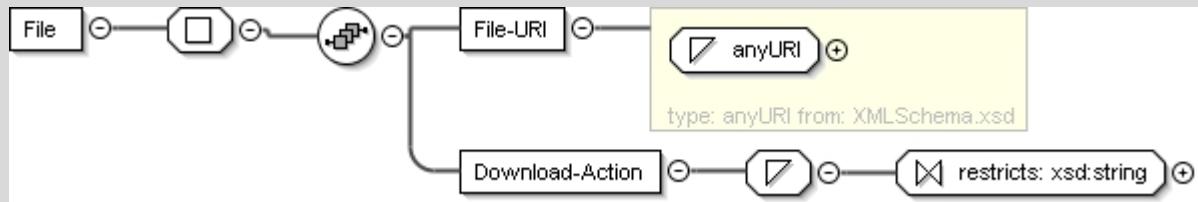


Figure C.17: File

```

<xs:element name="File-Reception-Report">
  <xs:complexType>
    <xs:complexContent mixed="false">
      <xs:extension base="cds:Basic-Reception-Report-Type">
        <xs:sequence minOccurs="1" maxOccurs="1">
          <xs:element minOccurs="1" maxOccurs="unbounded" name="File">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="File-URI" type="xs:anyURI" />
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:element>
  
```

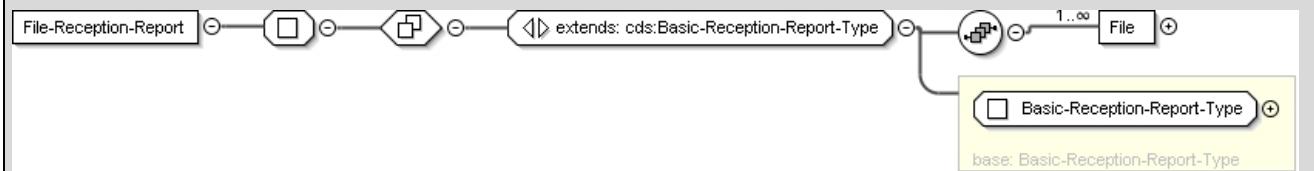


Figure C.18: File-Reception-Report



Figure C.19: File

```

<xs:element name="Chunk-Reception-Report">
  <xs:complexType>
    <xs:complexContent mixed="false">
      <xs:extension base="cds:Basic-Reception-Report-Type">
        <xs:sequence minOccurs="1" maxOccurs="1">
          <xs:element minOccurs="1" maxOccurs="unbounded" name="File">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="File-URI" type="xs:anyURI" />
                <xs:element minOccurs="1" maxOccurs="unbounded" name="Byte-Range"
type="cds:ByteRange" />
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:element>

```

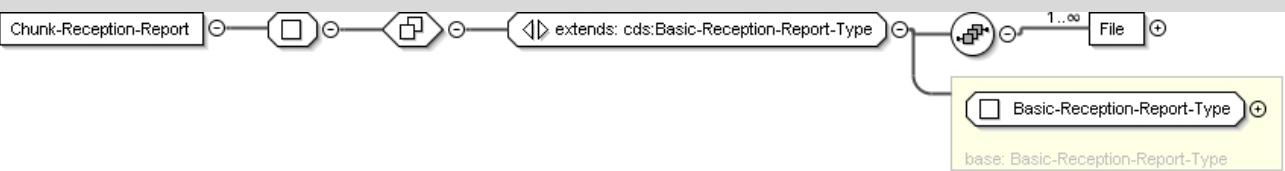


Figure C.20: Chunk-Reception-Report

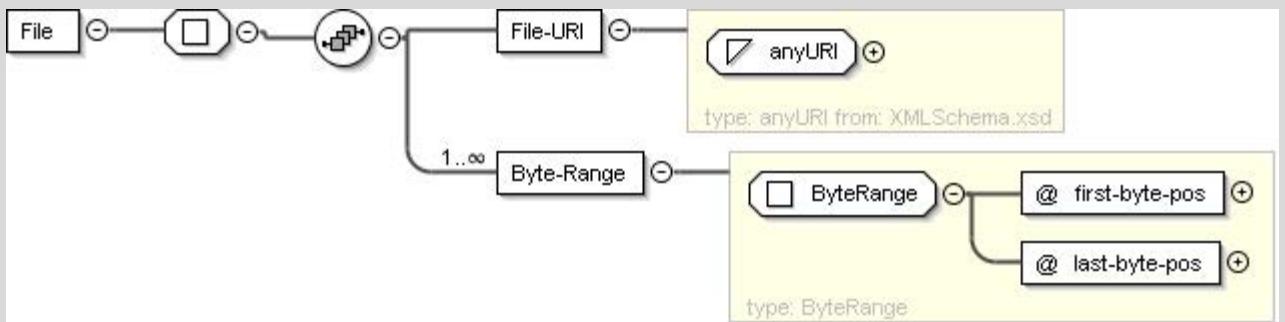


Figure C.21: File

```

<xs:complexType name="Basic-Reception-Report-Type">
  <xs:sequence>
    <xs:element name="Client-ID" type="xs:string" />
    <xs:element name="Push-Action" type="xs:boolean" />
    <xs:element name="CRID" type="xs:anyURI" />
    <xs:element name="Content-Version" type="xs:unsignedByte" />
    <xs:element name="Service-Provider-Domain" type="sdns:DomainType" />
    <xs:element name="Download-Session_ID" type="xs:nonNegativeInteger" />
    <xs:element name="Download-Session-Version" type="xs:nonNegativeInteger" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="ByteRange">
  <xs:attribute name="first-byte-pos" type="xs:unsignedLong" use="required" />
  <xs:attribute name="last-byte-pos" type="xs:unsignedLong" use="required" />
</xs:complexType>

```

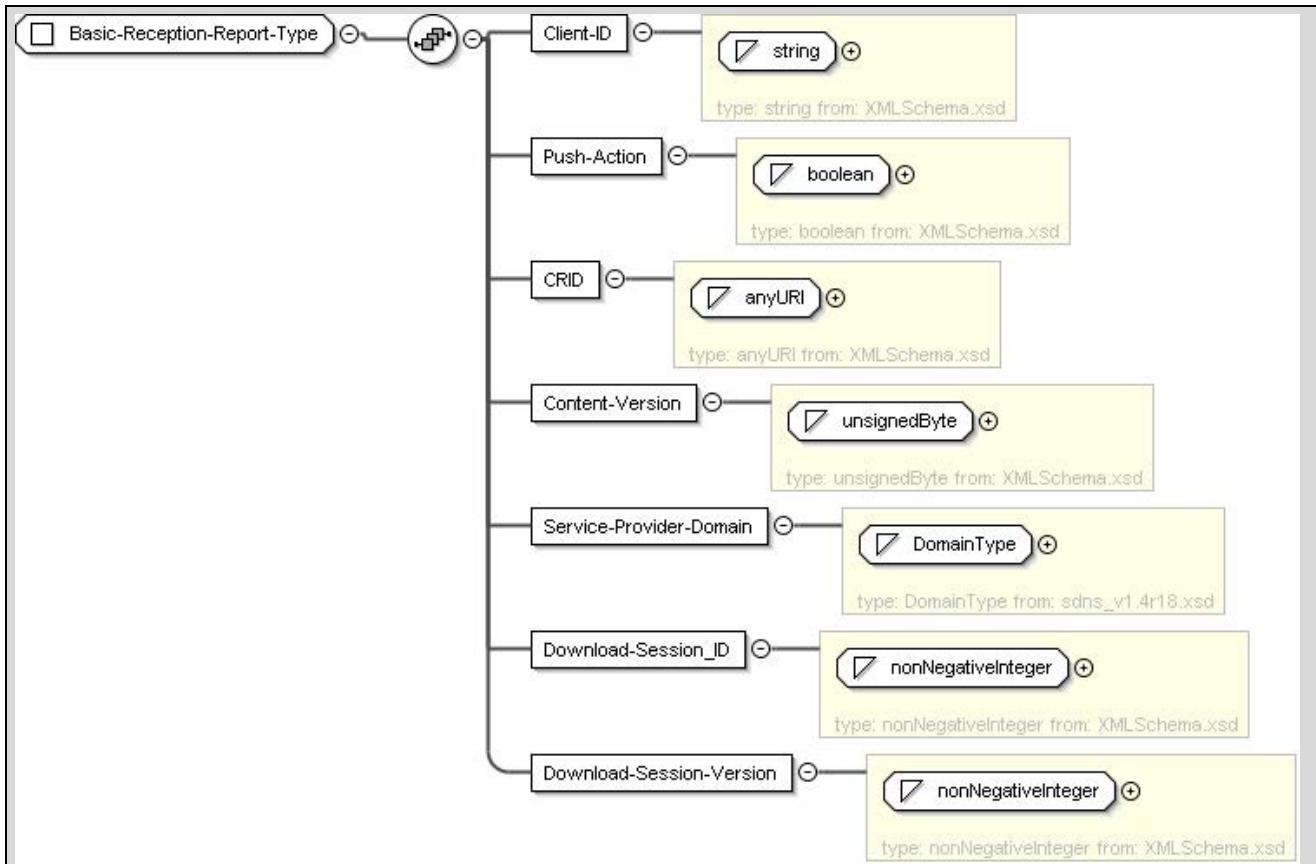


Figure C.22: Basic-Reception-ReportType

C.3 FLUTE FDT XML Schema for SRM

This clause defines FLUTE FDT XML schema for the FLUTE multicast SRM download service defined in clause 12.5.2. It supports the attributes defined in Table 33.

The base FLUTE FDT XML schema defined in IETF RFC 3926 [70] is not a valid schema. Therefore the XML schema defined in draft-ietf-rmt-flute-revised-07 is used as the base schema for the SRM extensions. This base schema is extended with the CP System ID, CP System SRM ID and SRM file version attributes as defined in Table 33.

```
<xs:element name="FDT-Instance" type="FDT-InstanceType" />
```



Figure C.23: FDT-Instance

```
<xs:complexType name="FDT-InstanceType">
    <xs:sequence>
        <xs:element name="File" type="FileType" maxOccurs="unbounded"/>
        <xs:any namespace="##other" processContents="skip" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="Expires" type="xs:string" use="required"/>
    <xs:attribute name="Complete" type="xs:boolean" use="optional"/>
    <xs:attribute name="Content-Type" type="xs:string" use="optional"/>
    <xs:attribute name="Content-Encoding" type="xs:string" use="optional"/>
    <xs:attribute name="FEC-OTI-FEC-Encoding-ID" type="xs:unsignedByte" use="optional"/>
    <xs:attribute name="FEC-OTI-FEC-Instance-ID" type="xs:unsignedLong" use="optional"/>
    <xs:attribute name="FEC-OTI-Maximum-Source-Block-Length" type="xs:unsignedLong"
use="optional"/>
```

```

<xs:attribute name="FEC-OTI-Encoding-Symbol-Length" type="xs:unsignedLong" use="optional"/>
<xs:attribute name="FEC-OTI-Max-Number-of-Encoding-Symbols" type="xs:unsignedLong" use="optional"/>
<xs:attribute name="FEC-OTI-Scheme-Specific-Info" type="xs:base64Binary" use="optional"/>
<xs:anyAttribute processContents="skip"/>
</xs:complexType>

```

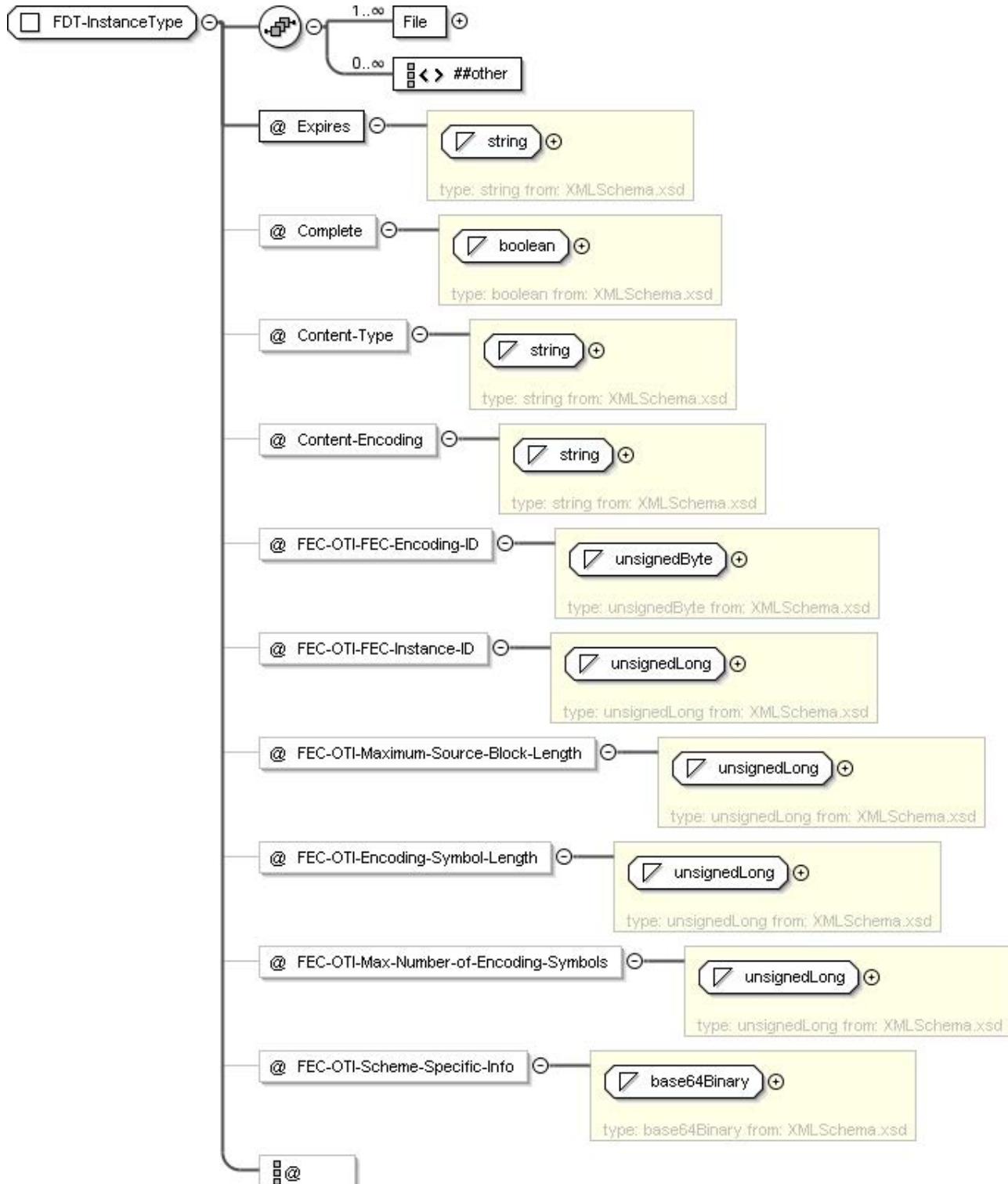


Figure C.24: FDT-InstanceType

```

<xs:complexType name="FileType">
  <xs:sequence>
    <xs:any namespace="##other" processContents="skip" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="Content-Location" type="xs:anyURI" use="required"/>
</xs:complexType>

```

```
<xs:attribute name="TOI" type="xs:positiveInteger" use="required"/>
<xs:attribute name="Content-Length" type="xs:unsignedLong" use="optional"/>
<xs:attribute name="Transfer-Length" type="xs:unsignedLong" use="optional"/>
<xs:attribute name="Content-Type" type="xs:string" use="optional"/>
<xs:attribute name="Content-Encoding" type="xs:string" use="optional"/>
<xs:attribute name="Content-MD5" type="xs:base64Binary" use="optional"/>
<xs:attribute name="FEC-OTI-FEC-Encoding-ID" type="xs:unsignedByte" use="optional"/>
<xs:attribute name="FEC-OTI-FEC-Instance-ID" type="xs:unsignedLong" use="optional"/>
<xs:attribute name="FEC-OTI-Maximum-Source-Block-Length" type="xs:unsignedLong"
use="optional"/>
    <xs:attribute name="FEC-OTI-Encoding-Symbol-Length" type="xs:unsignedLong" use="optional"/>
    <xs:attribute name="FEC-OTI-Max-Number-of-Encoding-Symbols" type="xs:unsignedLong"
use="optional"/>
        <xs:attribute name="FEC-OTI-Scheme-Specific-Info" type="xs:base64Binary" use="optional"/>
        <xs:attribute name="CP-System-ID" type="dvb12:CPSystemIDType"/>
        <xs:attribute name="CP-System-SRM-ID" type="dvb12:CPSystemSRMIDType" use="optional"/>
        <xs:attribute name="SRM-File-Version" type="dvb:Version"/>
    <xs:anyAttribute processContents="skip"/>
</xs:complexType>
</xs:schema>
```

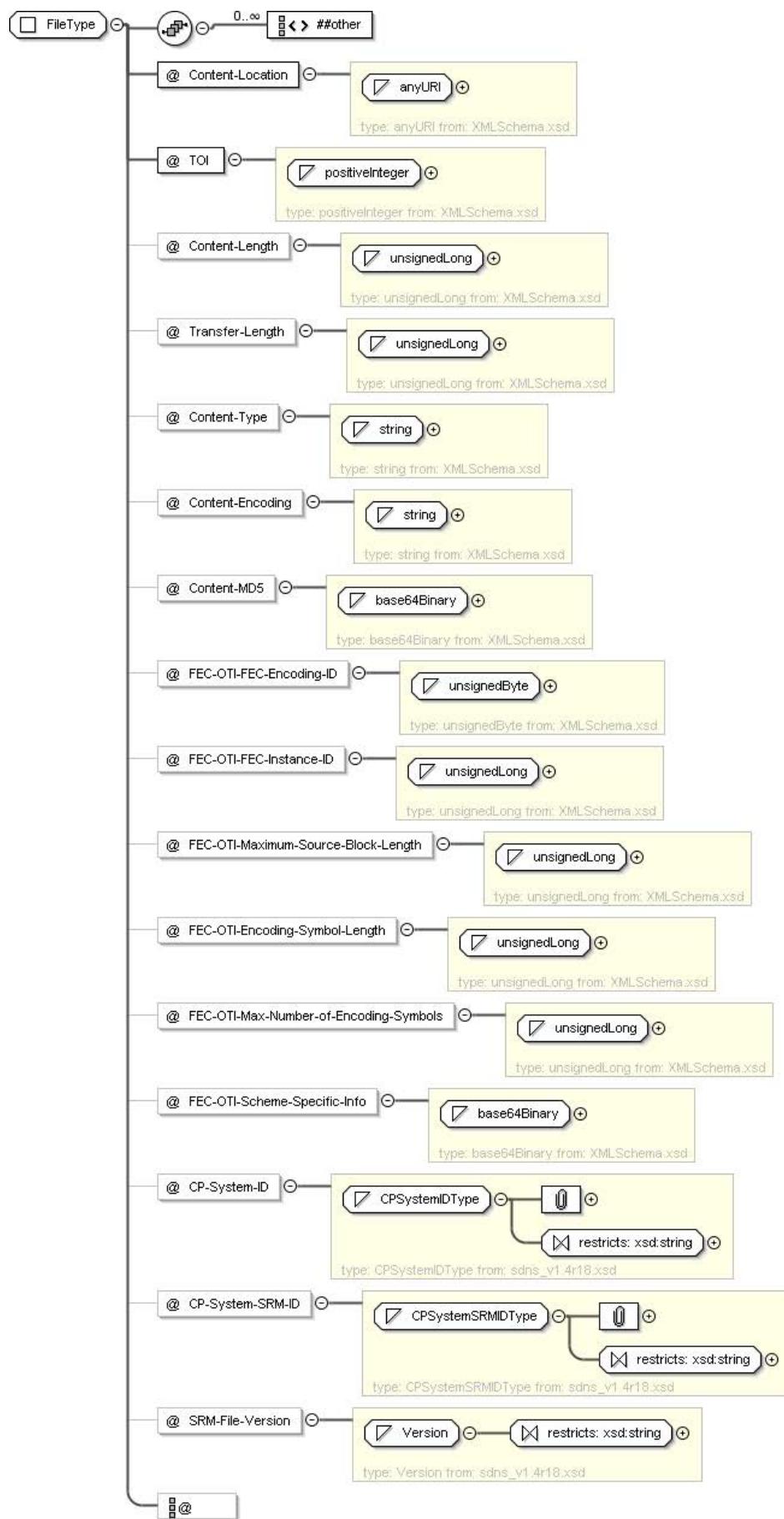


Figure C.25: FileType

Annex D (informative): Void

Annex E (normative): Application Layer Forward Error Correction

E.1 Introduction

This annex defines an optional protocol for Application Layer FEC (AL-FEC) protection of streaming media for DVB-IPTV services carried over RTP transport. This AL-FEC protocol is a layered protocol based on a combination of the following two forward error correction codes:

- a simple packet-based interleaved parity code, equivalent to a subset of the code defined in [66];
- the Raptor code, as defined in [64] and [65].

Note that the code defined in [66] is only applicable to the case of media carried within a single RTP flow. In this case, FEC repair packets may be sent in one (or more) layers, the first layer containing packets generated by the interleaved parity code and the optional second and subsequent layers containing packets generated by the Raptor code. Receivers process only packets from the layer or layers they support. A key property of the code defined in the present document is that simultaneous support of multiple layers is possible and FEC packets from these multiple layers can be combined at the receiver to achieve error correction performance which is better than any single layer alone.

Clause E.3 defines the first layer, based on [66].

Clause E.4 defines the subsequent layers, based on [64] and [65].

Clause E.5 describes hybrid decoding procedures which can make use of packets from all layers of the code.

Finally, clause E.6 defines complete FEC protocols for multicast and unicast video with both MPEG-2 Transport Stream encapsulation and direct transport of audio and video over RTP, constructed using the components described in the previous clauses.

E.2 Terms and Acronyms

Table E.1: Terms and Acronyms

Term/Acronym	Definition/Description
Bundle	Collection of Streams (a.k.a. Flows) that are collected into a single Source Block, and used to generate a single stream of Repair Symbols. For example, a low-bitrate audio stream might be bundled with a high-bitrate stream, providing better FEC protection than if it had not been bundled.
Flow	Another term for "Stream", used in the context of Bundles.
Intermediate Block	A block of data derived from the original Source Block data in the case of Raptor Encoder or the combination of Received Source Symbols and Repair Symbols in the case of Raptor Decoder.
Repair Symbol	A Symbol generated by the Raptor Encoder that is derived from Source Symbols.
Source Block	A block of source data over which the Raptor Encoder provides FEC repair information.
Source Symbol	The unit of data from a Source Block. All Source Symbols within a source block are the same size.
FEC	Forward Error Correction.
Encoding Symbol	A source symbol or a repair symbol.
Source Packet Information (SPI)	Information included in a source block related to or from a source packet.

Term/Acronym	Definition/Description
FEC Streaming Configuration Information	Information which controls the operation of the FEC Streaming Framework.
FEC Payload ID	See [48].
Source FEC Payload ID	See [48].
Repair FEC Payload ID	See [48].
FEC Object Transmission Information	See [48].
FEC Encoding ID	See [48].
Content Delivery Protocol	See [48].

E.3 SMPTE 2022-1-based code

SMPTE 2022-1 [66] based coding may be applied for streams which meet the requirements of SMPTE 2022-2 [67].

All requirements of [66] and [67] shall apply, with the modifications and exceptions as shown in Table E.2. Modifications/exceptions are classified as follows:

- (R) Additional requirement (normative).
- (E) Exception (normative).
- (N) Note (informative).

Table E.2: Modification/exceptions to [66] and [67]

Clause from [66] and [67]	Modification/exception
[66] 7.1 RTP/UDP/IP Layer	(E) The SSRC of the source stream shall be chosen randomly (with collision detection) per the requirements of [21]. RTCP CNAME field should be used to associate the FEC streams with the source streams.
[66] 7.1 RTP/UDP/IP Layer	(E) The initial value of the sequence number for the source stream shall be random per [21].
[66] 7.1 RTP/UDP/IP Layer	(E) The source packets have a zero CC field.
[66] 8 FEC Scheme	(N) The term "FEC Scheme" used here does not have the same meaning as "FEC Scheme" in the present document or in [64].
[66] 8.1 FEC Packet Arrangement	(E) When used with multiple layers, then the $L \times D$ block of packets protected by one or more FEC packets shall be wholly contained within a single source block of the Raptor code.
[66] 8.1 FEC Packet Arrangement	(E) Only the first (interleaved) FEC stream shall be supported.
[66] 8.3 FEC Packet RTP Header Format	(E) The FEC stream should use the PT number specified in SD&S which defaults to 96, the same value as in the SMPTE 2022-1 specification [66].
[66] 8.3 FEC Packet RTP Header Format	(E) The SSRC of the FEC stream shall be 0. RTCP CNAME field should be used to associate the FEC streams with the source streams.
[66] 8.3 FEC Packet RTP Header Format	(E) The initial value of the sequence number for the FEC stream should be random per [21] and it shall be one higher than the sequence number in the previously transmitted FEC packet.
[66] 7.1 (or [66] 8.2) FEC buffer Overhead and Latency Implications	(E) The limits defined in this clause shall not apply. Receivers shall support values of L and D within the restrictions $L \times D \leq 400$ and $L \leq 40$ (L is the length of burst protection - in packets). Receivers may also support values of L and D outside this range.
[66] 8.4 FEC Header Format	(R) The D bit shall be set to 0.
[66] 8.4 FEC Header Format	(R) The SNBase ext bits shall be ignored by receivers.
[66] 8.5 FEC Traffic Shaping Issues	(E) The requirements of this clause shall not apply.
[66] 8.6 Reorder Tolerance	(E) The requirement for reordering capability of minimum 10 packets before applying FEC does not apply.
[66] annex B Non Block Aligned FEC Arrangement	(E) If hybrid decoding procedures are supported (clause E.5.2), the sending arrangement described in this annex shall not be used.

NOTE: The DVB AL-FEC base layer conforms to [66] with the restrictions/exceptions listed in Table E.2.

E.4 Raptor code

E.4.1 Introduction

The FEC Building Block [48] defined by the IETF Reliable Multicast working group describes an approach to the present document of protocols using FEC but separates the definition of the protocol from the present document of the FEC code itself. In the language of the FEC Building Block, separate specifications are provided for "Content Delivery Protocols" and for "FEC Schemes", the former defining the protocols and the latter defining the actual FEC codes. The FEC Building Block describes rules that both kinds of specification shall follow so that they can be used together and so it provides the "glue" between Content Delivery Protocols and FEC Schemes.

Following this approach, this clause is organized as a number of modular components. These are then combined to form complete protocols suitable for the DVB-IPTV services. These components include:

- An FEC Streaming Framework, equivalent to that defined in ETSI TS 126 346 [64], which provides an overall protocol framework for the application of FEC to media streams. This is described in clause E.4.2.
- A number of FEC Schemes, which define protocol components according to the IETF FEC Building Block [48] suitable for various classes of application and which define how the Raptor FEC code is applied for streaming applications. These are defined in clause E.4.3.

Complete protocol specifications for multicast and unicast video with both MPEG-2 Transport Stream encapsulation and direct transport of audio and video encapsulated in RTP are then described in clause E.5. In both cases, the construction is based on the building blocks described above.

E.4.2 FEC Streaming Framework

E.4.2.1 Introduction

This clause defines a framework for the definition of CDPs, in the sense of the FEC Building Block, which provides for FEC protection of streamed data flows over UDP. This clause does not define a complete Content Delivery Protocol, but rather defines only those aspects that are expected to be common to all Content Delivery Protocols that support streaming data over UDP.

The framework defined in this clause is not specific to a single streaming application protocol. The framework provides FEC protection for application protocol flows over UDP and for combined protection of multiple such flows. For example, multiple RTP flows may be protected together with the associated RTCP flows and potentially also other related flows such as security protocol packets.

Content Delivery Protocols which use this framework shall provide for communicating two kinds of information from sender to receiver:

- FEC Streaming Configuration Information.
- FEC Object Transmission Information.

FEC Streaming Configuration Information is information independent of the FEC Scheme being used that is needed by the FEC Streaming Framework, e.g. the definition of the UDP flows that are protected by the FEC Streaming Framework. The FEC Streaming Configuration Information is defined in this clause and the means to transport it (for example with Service Discovery Information) shall be defined by each Content Delivery Protocol.

FEC Object Transmission Information is information which is specific to a particular FEC Scheme. The FEC Object Transmission Information is defined by each FEC Scheme. Content Delivery Protocols shall define a means to transport the FEC Object Transmission Information from sender to receiver.

The architecture outlined above is illustrated in figure E.1.

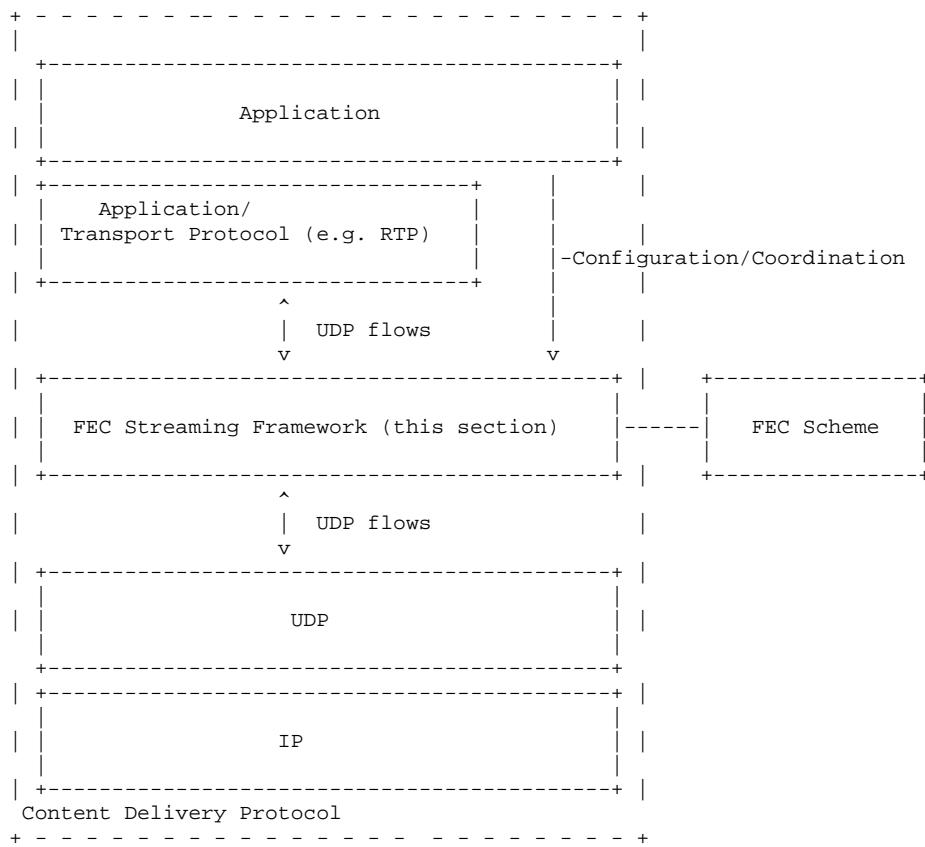


Figure E.1: FEC Streaming Framework Architecture

E.4.2.2 Procedural overview

E.4.2.2.1 General

The mechanism defined in this clause consists of three components:

- (i) Construction of a "source block" from source media packets belonging to one or several UDP packet flows. The UDP flows may include, for example, RTP and RTCP packets and also other protocols related to the stream.
- (ii) Optional extension of source packets to indicate the source block and the position within the source block occupied by the data from and related to the source packet.
- (iii) Definition of repair packets, sent over UDP, which can be used by the FEC decoder to reconstruct missing portions of the source block.

The protected data may be from several different UDP flows that are protected jointly. In general, multiple source blocks will be constructed for a stream; each source block is constructed from different sets of source packets. For example, each source block may be constructed from those source packets related to a particular segment of the stream in time.

A receiver supporting this streaming framework shall support the packet format for FEC Source packets and shall also support the packet format for FEC Repair packets.

This clause does not define how the sender determines which source packets are included in which source blocks. A specific Content Delivery Protocol may define this mapping or it may be left as implementation dependent at the sender, possibly including some memory constraints at receivers. However, a CDP specification shall define how a sender communicates to the receiver the maximum length of time that the sender will allow between a source packet and a repair packet that protects that source packet.

At the sender, the mechanism processes original UDP packets to create:

- (i) A stored copy of the original packets in the form of one or more "source block(s)". The source block is a logical block of data to which the FEC code will subsequently be applied. It is constructed by concatenating "Source Packet Information" (SPI) for each source packet. Generally, the SPI for a packet contains a short identifier for the flow the packet belongs to, a length indicator for the packet, the UDP payload and possible padding bytes.
- (ii) FEC Source packets for transmission to the receiver.

The FEC Streaming Framework uses the FEC encoder specified by the FEC Scheme in use to generate the desired quantity of repair symbols from a source block. These repair symbols are then sent using the FEC repair packet format to the receiver. The FEC Repair packets are sent to a UDP destination port different from any of the original UDP packets' destination port(s) as indicated by the FEC Streaming Configuration Information.

The receiver recovers original source packets directly from any FEC Source packets received. The receiver also uses the received FEC Source Packets to construct a stored copy of the original packets in the same source block format as constructed at the sender.

If any FEC Source packets related to a given source block have been lost, then this copy of the source block at the receiver will be incomplete. If sufficient FEC source and FEC Repair packets related to that source block have been received, the FEC Framework may use the FEC decoding algorithm defined by the FEC Scheme to recover a (hopefully, but not necessarily, complete) copy of the source block. The SPI for the missing source packets can then be extracted from the completed parts of the source block and used to reconstruct the source packets to be passed to the application.

The receiver of FEC Source packets shall be able to identify the source block and the position within the source block occupied by the SPI derived from each packet. This information is known as FEC Source Packet Identification Information and may be communicated in several ways. The FEC Source Packet Identification Information may be encoded into a specific field within the FEC Source packet format defined in this Annex, called the Source FEC Payload ID field. The exact contents and format of the Source FEC Payload ID field are defined by the FEC Scheme. Alternatively, the FEC Scheme or CDP may define how the FEC Source Packet Identification Information is derived from other fields within the source packets. This clause defines the way that the Source FEC Payload ID field, if used, is appended to source packets to form FEC Source packets.

The receiver of FEC Repair packets shall also be able to identify the source block and the relationship between the contained repair data and the original source block. This information is known as FEC Repair Packet Identification information. This information shall be encoded into a specific field, the Repair FEC Payload ID field, the contents and format of which are defined by the FEC Scheme.

Any FEC Schemes to be used in conjunction with this framework shall be a systematic FEC Scheme and shall be based on source blocks. The FEC Scheme may define different FEC Payload ID field formats for FEC Source packets and FEC Repair packets.

E.4.2.2.2 Sender Operation

It is assumed that the sender has constructed or received original data packets for the session. These may be RTP, RTCP or other UDP packets. The following operations describe a possible way to generate compliant FEC Source packet and FEC repair packet streams:

- 1) A source block is constructed as specified in clause E.4.2.3.2, by concatenating the SPI for each original source packet. In doing so, the Source FEC Packet Identification Information of the FEC Source packet can be determined and included in the Source FEC Payload ID field, if used. In the SPI the identity of the packet's UDP flow is marked using a short "UDP flow ID", defined in this Annex. The association of UDP flow specifications to UDP flow IDs is defined by the FEC Streaming Configuration Information.
- 2) The FEC Source packet is constructed according to clause E.4.2.3.3. The identity of the original flow is maintained by the source packet through the use of the same UDP ports and IP addresses which have been advertised by the Content Delivery Protocol (for example using DVB Service Discovery), as carrying FEC Source packets generated from an original stream of a particular protocol (e.g. RTP, RTCP, etc.). The FEC Source packet generated is sent according to normal UDP procedures.

- 3) The FEC encoder generates repair symbols from a source block and the FEC Streaming Framework places these symbols into FEC Repair packets, to be conveyed to the receiver(s). These repair packets are sent using normal UDP procedures to a unique destination port to separate them from any of the source packet flows. The ports to be used for FEC Repair packets are defined in the FEC Streaming Configuration Information.

E.4.2.2.3 Receiver Operation

The following describes a possible receiver algorithm, when receiving an FEC source or repair packet:

- 1) If an FEC Source packet is received (as indicated by the UDP flow on which was received):
 - a) The original source packet is reconstructed by removing the Source FEC Payload ID, if used. The resulting packet may be buffered to allow time for the FEC repair.
 - b) The Source FEC Packet Identification Information is determined, either from the Source FEC Payload ID, if used, or by other means.
 - c) The SPI for the resulting packet is placed into the source block according to the Source FEC Packet Identification Information and the source block format described in clause E.4.2.3.2. The IP addresses and UDP ports the packet was received on/sent from are used to determine the UDP flow ID within the SPI.
- 2) If an FEC Repair packet is received (as indicated by the UDP flow on which it was received), the contained repair symbols are associated with a source block according to the Repair FEC Payload ID.
- 3) If at least one source packet is missing and at least one repair packet has been received for a source block then FEC decoding may be desirable. The FEC decoder determines if the source block constructed in step 1 plus the associated repair symbols received in step 2 contains enough symbols for decoding of any or all of the missing source symbols in the source block and, if so, performs a decoding operation.
- 4) Any SPI that was reconstructed during the decoding operation is then used to reconstruct the missing source packets and these are buffered as normal received source packets (see step 1a above).

NOTE: The above procedure may result in a situation in which not all original source packets are recovered.

E.4.2.3 Protocol Specification

E.4.2.3.1 General

This clause specifies the protocol elements for the FEC Streaming Framework. The protocol consists of three components which are described in the following clauses:

- 1) Construction of a source block from source packets. The FEC code will be applied to this source block to produce the repair data.
- 2) A format for packets containing source data.
- 3) A format for packets containing repair data.

The operation of the FEC Streaming Framework is governed by certain FEC Streaming Configuration Information. This configuration information is also defined in this clause. A complete protocol specification that uses this framework shall specify the means to determine and communicate this information between sender and receiver.

E.4.2.3.2 Structure of Source Block

This clause defines the layout of the source block. A source block consists of the concatenation of SPI for at least one original source UDP packet.

Let:

- n be the number of UDP packets in the source block. n may be determined dynamically during the source block construction process.
- T be the source symbol size in bytes. Note: this information is provided by the FEC Scheme as defined in clause E.4.2.3.6.

<i>i</i>	the index to the (<i>i</i> +1)-th UDP packet to be added to the source block, $0 \leq i < n$.
$R[i]$	denote the number of octets of the UDP payload of the <i>i</i> -th UDP packet.
$l[i]$	be a length indication associated with the <i>i</i> -th UDP packet - the nature of the length indication is defined by the FEC Scheme.
$L[i]$	denote two octets representing the value of $l[i]$ in network byte order (high order octet first) of the <i>i</i> -th UDP packet.
$f[i]$	denote an integer "UDP flow ID" identifying the UDP flow from which the <i>i</i> -th packet was taken.
$F[i]$	denote a single octet representing the value of $f[i]$.
$s[i]$	be the smallest integer such that $s[i] \times T \geq (l[i]+3)$. Note $s[i]$ is the length of $SPI[i]$ in units of symbols of size T bytes.
$P[i]$	denote $s[i] \times T - (l[i]+3)$ zero octets.

NOTE: $P[i]$ are padding octets to align the start of each UDP packet with the start of a symbol.

$SPI[i]$ be the concatenation of $F[i], L[i], R[i]$ and $P[i]$.

Then, the source block is constructed by concatenating $SPI[i]$ for $i = 0, 1, 2, \dots, n-1$. The source block size, S , is then given by sum $\{s[i] \times T, i=0, \dots, n-1\}$.

Source blocks are identified by integer SBNs and symbols within a source block by integer ESIs. This clause does not specify how SBNs are allocated to source blocks. Symbols are numbered consecutively starting from zero within the source block. Each source packet is associated with the ESI of the first symbol containing SPI for that packet. Thus, the ESI value associated with the *j*-th source packet, $ESI[j]$, is given by:

$$ESI[j] = 0, \text{ for } j=0 \quad (\text{E.1})$$

$$ESI[j] = \text{sum}\{s[i], i=0, \dots, (j-1)\}, \text{ for } 0 < j < n \quad (\text{E.2})$$

The Source FEC Packet Identification Information consists of the identity of the source block and the ESI associated with the packet.

A UDP flow is uniquely defined by an IP source and destination address and UDP source and destination port values. The assignment of UDP flow ID values to UDP flows is part of the FEC Streaming Configuration Information.

E.4.2.3.3 Packet format for FEC Source packets

The packet format for FEC Source packets shall be used to transport the payload of an original source UDP packet. As depicted in figure E.2, it consists of the original UDP packet, followed, optionally, by the Source FEC Payload ID field, if used.

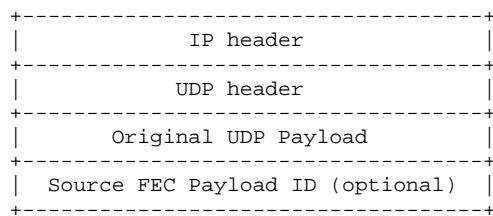


Figure E.2: Structure of FEC Source Packets

The IP and UDP header fields shall be identical to those of the original source packet. The Original UDP Payload field shall be identical to the UDP payload of the original source packet. The UDP payload of the FEC Source packet shall consist of the Original UDP Payload followed by the Source FEC Payload ID field.

The Source FEC Payload ID field, if present, contains information required for the operation of the FEC algorithm, in particular for the derivation of the Source FEC Packet Identification Information. The format of the Source FEC Payload ID and the derivation of the Source FEC Packet Identification Information are defined by the FEC Scheme. Note that the FEC Scheme or CDP may define a means to derive the Source FEC Packet Identification Information from other information in the source packet (for example the RTP Sequence number). In this case the Source FEC Payload ID field described here is not appended to the packet and the Source FEC packet is identical in every way to the original Source packet.

E.4.2.3.4 Packet Format for FEC Repair packets

The packet format for FEC Repair packets is shown in figure E.3. The UDP payload consists of a Repair FEC Payload ID field and one or more repair symbols generated by the FEC encoding process.

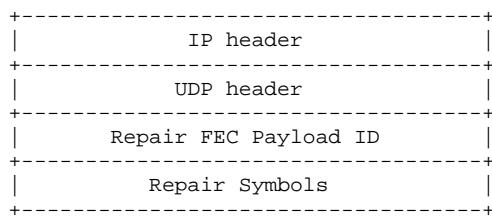


Figure E.3: FEC Repair packet format

The Repair FEC Payload ID field contains information required for the operation of the FEC algorithm. This information is defined by the FEC Scheme. The format of the Repair FEC Payload ID field is defined by the FEC Scheme.

Any number of whole repair symbols may be contained within an FEC Repair packet, subject to packet size restrictions or other restrictions defined by the FEC Scheme. The number of repair symbols within a packet can be determined from the symbol length and the packet length. Partial repair symbols shall not be included in FEC repair packets.

E.4.2.3.5 FEC Streaming Configuration Information

The FEC Streaming Configuration Information is information that the FEC Streaming Framework needs in order to apply FEC protection to the UDP flows. A complete Content Delivery Protocol specification for streaming that uses the framework specified here shall include details of how this information is derived and communicated between sender and receiver.

The FEC Streaming Configuration Information includes identification of a number of UDP packet flows. Each UDP packet flow is uniquely identified by a tuple { Source IP Address, Destination IP Address, Source UDP port, Destination UDP port }.

A single instance of the FEC Streaming Framework provides FEC protection for all packets of a specified set of source UDP packet flows, by means of one or more UDP packet flows containing repair packets. The FEC Streaming Configuration Information includes, for each instance of the FEC Streaming Framework:

- 1) Identification of the UDP packet flow(s) carrying FEC Repair packets, known as the FEC repair flow(s).
- 2) For each source UDP packet flow protected by the FEC repair flow(s):
 - a) Identification of the UDP packet flow carrying source packets.
 - b) An integer identifier, between 0 and 255, for this flow. This identifier shall be unique amongst all source UDP packet flows which are protected by the same FEC repair flow.
- 3) The FEC Scheme that is to be applied.

Multiple instances of the FEC Streaming Framework, with separate and independent FEC Streaming Configuration Information, may be present at a sender or receiver. A single instance of the FEC Streaming Framework protects all packets of all the source UDP packet flows identified in (2) above i.e. all packets on those flows shall be FEC Source packets as defined in clause E.4.2.3.3. A single source UDP packet flow shall not be protected by more than one FEC-SF instance.

A single FEC repair flow provides repair packets for a single instance of the FEC-SF. Other packets shall not be sent within this flow i.e. all packets in the FEC repair flow shall be FEC repair packets as defined in clause E.4.2.3.4 and shall relate to the same FEC Streaming Framework instance.

The FEC Streaming Framework shall be informed of the symbol size to be used for each source block. This information may be included in the FEC Streaming Configuration Information or it may be communicated by other means, for example within the FEC Repair Payload ID field. A complete Content Delivery Protocol specification SHALL specify how this information is communicated between sender and receiver.

E.4.2.3.6 FEC Scheme requirements

In order to be used with this framework, an FEC Scheme shall:

- adhere to the requirements of IETF RFC 5052 [48];
- be systematic;
- be based on source blocks which are non-overlapping and contiguous within the stream;
- specify how the SBN and ESI associated with a source packet are derived or communicated from sender to receiver (for example, within the Source FEC Payload ID field);
- specify how the symbol length is derived or communicated from sender to receiver (for example, as part of the FEC Object Transmission Information);
- specify how the length indication, $l[i]$, included in the Source Packet Information, is derived from a UDP packet;
- specify how the Source Packet Information length, $s[i]$, is derived from a UDP packet.

E.4.3 FEC Schemes for streaming

E.4.3.1 Raptor FEC Scheme for arbitrary packet flows

E.4.3.1.0 Introduction

This clause defines an FEC Scheme for Raptor protection of arbitrary packet flows over UDP.

E.4.3.1.1 Formats and Codes

E.4.3.1.1.1 FEC Object Transmission Information

This FEC Object Transmission Information elements for this FEC Scheme and their value ranges are as follows:

Maximum Source Block Length

A non-negative integer less than 2^{16} , in units of symbols.

Encoding Symbol Size

A non-negative integer less than 2^{16} , in units of bytes.

An encoding format for this information in a 4 octet field is defined in figure E.4.

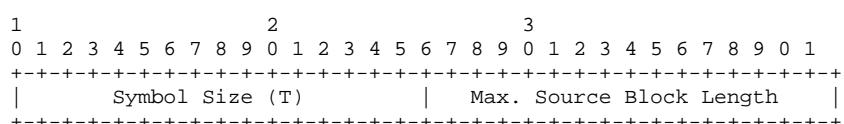


Figure E.4: Encoded Common FEC Object Transmission Information for Raptor FEC Scheme for arbitrary packet flows

E.4.3.1.1.2 FEC Payload ID

E.4.3.1.1.2.1 Source FEC Payload ID

The Source FEC payload ID is composed as follows.

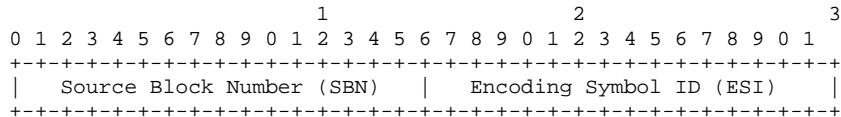


Figure E.5: Source FEC Payload ID format for Raptor FEC Scheme for arbitrary packet flows

Source Block Number (SBN), (16 bits): An integer identifier for the source block that the source data within the packet relates to.

Encoding Symbol ID (ESI), (16 bits): The starting symbol index of the source packet in the source block.

The interpretation of the ESI is defined by the FEC Streaming Framework (see clause E.4.2).

E.4.3.1.1.2.2 Repair FEC Payload ID

The structure of the Repair FEC Payload ID is defined in figure E.6.

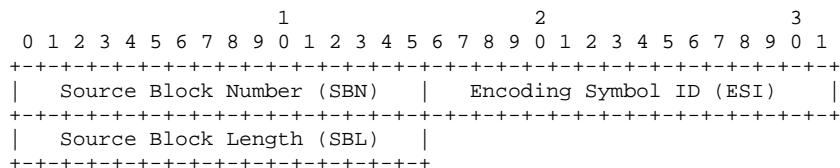


Figure E.6: Repair FEC Payload ID

Source Block Number (SBN), (16 bits): An integer identifier for the source block that the repair symbols within the packet relate to.

Encoding Symbol ID (ESI), (16 bits): Integer identifier for the encoding symbols within the packet.

Source Block Length (SBL), (16 bits): The number of source symbols in the source block.

The interpretation of the SBN, ESI and SBL is defined by the FEC Code Specification according to clause E.4.3.1.3.

E.4.3.1.2 Procedures

This FEC Scheme uses the procedures of the framework defined in clause E.4.2.2 to construct a source block to which the FEC code can be applied. The sender shall allocate SBNs to source blocks sequentially, wrapping around to zero after SBN $2^{16}-1$.

During the construction of the source block as per clause E.4.2.3.2:

- The length indication, $l[i]$, included in the Source Packet Information for each packet shall be the UDP payload length.
- The value of $s[i]$ in the construction of the Source Packet Information for each packet shall be the smallest integer such that $s[i] \times T \geq (l[i]+3)$.

E.4.3.1.3 FEC Code specification

The Raptor FEC encoder defined in clause E.7 shall be used. The source block passed to the Raptor FEC encoded shall consist of the Source Block constructed according to clause E.4.2.3.2 extended with zero or more padding symbols such that the total number of symbols in the source block is equal to the Maximum SBL signalled in the FEC Object Transmission Information. Thus the value of the parameter K used by the FEC encoded is equal to the Maximum SBL for all blocks of the stream. Padding symbols shall consist entirely of bytes set to the value zero.

The symbol size, T , to be used for source block construction and the repair symbol construction are equal to the Encoding Symbol Size signalled in the FEC Object Transmission Information. The parameter T shall be set such that the number of source symbols in any source block is at most $K_{MAX} = 8\,192$.

The Maximum SBL parameter - and hence the number of symbols used in the FEC Encoding and Decoding operations - shall be set to one of the values specified in clause E.7. Recommended derivation of other parameters is presented in clause E.4.3.1.6.

E.4.3.1.4 Encoding packet construction

As described in clause E.4.2.3.4, each repair packet contains the following information:

- Source Block Number (SBN).
- Encoding Symbol ID (ESI).
- Source Block Length (SBL).
- Repair symbol(s).

The number of repair symbols contained within a repair packet is computed from the packet length. The ESI value placed into a repair packet is given by the following formula:

$$\text{ESI}_{\text{repair}} = I_{\text{repair}} + K \quad (\text{E.3})$$

Where I_{repair} is the index of the repair symbol in the sequence of repair symbols generated according to clause E.7, where the first repair symbol has index 0, the second index 1, etc. and K is the number of source symbols (equal to the Maximum SBL parameter).

The SBL field of the Repair FEC Payload ID field shall be set to the number of symbols included in the Source Packet Information of packets associated with the source block i.e. before padding to the Maximum SBL.

E.4.3.1.5 Transport

This clause describes the information exchange between the Raptor encoder/decoder and any transport protocol making use of Raptor forward error correction for streaming.

The Raptor encoder for streaming requires the following information from the transport protocol for each source block:

- The symbol size, T , in bytes.
- The number of symbols in the source block, K .
- The Source Block Number (SBN).
- The source symbols to be encoded.

The Raptor encoder supplies the transport protocol with encoding packet information consisting, for each repair packet, of:

- Source Block Number (SBN).
- Encoding Symbol ID (ESI).
- Source Block Length (SBL).
- repair symbol(s).

The transport protocol shall communicate this information transparently to the Raptor decoder.

A suitable transport protocol is defined in the present document.

E.4.3.1.6 Example parameters

E.4.3.1.6.1 Parameter derivation algorithm

This clause provides recommendations for the derivation of the transport parameter T . This recommendation is based on the following input parameters:

- B the maximum source block size, in bytes. For further explanation, see below.
- A the symbol alignment factor, in bytes, i.e. symbol size T is a multiple of A .
- P the maximum repair packet payload size (not including Repair FEC Payload ID), in bytes, which shall be multiple of A .
- K_{MAX} the maximum number of source symbols per source block. As defined in clause E.7, $K_{MAX} = 1\,281$.
- K_{MIN} a minimum target on the number of symbols per source block.
- G_{MAX} a maximum target number of symbols per repair packet.

A requirement on these inputs is that $\text{ceil}(B/P) \leq K_{MAX}$. Based on the above inputs, the transport parameter T is calculated as follows:

Let:

$$G = \min\{\text{ceil}(P \cdot K_{MIN}/B), P/A, G_{MAX}\} \quad (\text{E.4})$$

- the approximate number of symbols per packet

$$T = \text{floor}(P/(A \cdot G)) \cdot A \quad (\text{E.5})$$

The value of T derived above should be considered as a guide to the actual value of T used. It may be advantageous to ensure that T divides into P , or it may be advantageous to set the value of T smaller to minimize wastage when full size repair symbols are used to recover partial source symbols at the end of lost source packets (as long as the maximum number of source symbols in a source block does not exceed K_{MAX}). Furthermore, the choice of T may depend on the source packet size distribution, e.g. if all source packets are the same size then it is advantageous to choose T so that the actual payload size of a repair packet P'' , where P'' is a multiple of T , is equal to (or as few bytes as possible larger than) the number of bytes each source packet occupies in the source block.

Recommended settings for the input parameters, A , K_{MIN} and G_{MAX} are as follows:

$$A = 16 \quad K_{MIN} = 640 \quad G_{MAX} = 10$$

E.4.3.1.6.2 Examples

The above algorithm leads to transport parameters as shown in Table E.3, assuming the recommended values for A , K_{MIN} and G_{MAX} and $P = 1\,424$.

Table E.3: Example parameters settings

Max source block size B	G	Symbol size T	$G \cdot T$
16 KB	10	128	1 280
32 KB	10	128	1 280
128 KB	7	192	1 344
256 KB	4	352	1 408

E.4.3.2 Raptor FEC Scheme for a single sequenced packet flow

E.4.3.2.0 General

This clause defines an FEC Scheme for FEC protection of a single packet flow in which source packets each carry a unique sequence number. Such a packet flow is called a "sequenced flow". A primary example would be FEC protection of an RTP flow containing an MPEG-2 Transport Stream within which all data for the service is multiplexed. In this case the RTP Sequence Numbers can be used to derive the Source FEC Packet Identification Information.

Compared to the FEC Scheme defined in clause E.4.3.1, the primary advantage of this scheme is that it does not modify source packets in any way. As a result this FEC scheme can be used in the presence of legacy equipment which would not recognize source packets which had been modified according to the schemes defined in clause E.4.3.1.

In this FEC Scheme, the role played by the Source FEC Payload ID in the scheme of clause E.4.3.1 is replaced by the sequence number. The sequence numbers of packets within each flow to be protected shall be incremented by one for each packet in the stream.

The size of the Source Packet Information within a given Source Block for each packet within a given sequenced flow shall be the same and is derived from the size of the FEC Repair packets, which shall also all be the same size for a given source block.

E.4.3.2.1 Formats and Codes

E.4.3.2.1.1 FEC Object Transmission Information

See clause E.4.3.1.1.1.

E.4.3.2.1.2 FEC Payload ID

E.4.3.2.1.2.1 Source FEC Payload ID

The Source FEC Payload ID field is not used by this FEC Scheme. Source packets are not modified by this FEC Scheme.

E.4.3.2.1.2.2 Repair FEC Payload ID

The Repair FEC Payload ID for this FEC scheme consists of two parts:

- an optional RTP header for the DVB AL-FEC enhancement layer;
- a Repair FEC Payload ID Field for the DVB AL-FEC enhancement layer.

The RTP header shall only be added if the SD&S flag FECEnhancementLayer@TransportProtocol is present for this FEC enhancement layer and the SD&S flag FECEnhancementLayer@TransportProtocol signals RTP/AVP as transport protocol. If the SD&S flag FECEnhancementLayer@TransportProtocol is not present or the SD&S flag FECEnhancementLayer@TransportProtocol signals UDP/FEC, the RTP header shall not be added.

An HNED shall only join/request an AL-FEC enhancement layer if it supports the reception of the signalled Repair FEC Payload ID.

All the fields in the RTP header of DVB AL-FEC packets are used according to IETF RFC 3550 [21], with for some of them further clarification as follows:

Marker bit:	The marker bit shall be set 1 for the last protection RTP packet sent for each source block, and otherwise set to 0.
Timestamp:	The timestamp rate shall be 10 kHz and shall be set to a time corresponding to the packet's transmission time. The timestamp value has no use in the actual FEC protection process and is only set to a value to produce reasonable resolution for arrival measuring and jitter calculation.
Sequence number:	Is set in accordance with IETF RFC 3550 [21]. The sequence number is primarily used to detect losses of the protection RTP packets.
Payload type (PT):	If SD&S is used for service discovery, it is dynamically allocated using FECEnhancementLayer@PayloadTypeNumber in the SD&S. If the SD&S attribute FECEnhancementLayer@PayloadTypeNumber is not present the transmitter may use any dynamic payload number between 96 and 128 and the receiver shall ignore this PT field.
SSRC:	One SSRC is used per source SSRC. The SSRC used by the protection payload format shall be different the one used by the source RTP packets. The binding of the source SSRC to the repair SSRC shall be performed using the RTCP SDES CNAME, which shall be identical for the two SSRCs.

The Repair FEC Payload ID Field format for this FEC Scheme is shown in figure E.7.

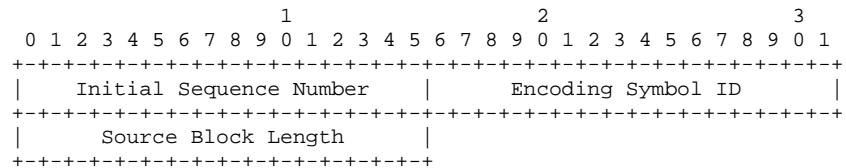


Figure E.7: Repair FEC Payload ID Field format

Initial Sequence Number (Flow i ISN) - 16 bits

This field specifies the lowest 16 bits of the sequence number of the first packet to be included in this sub-block. If the sequence numbers are shorter than 16 bits then the received Sequence Number shall be logically padded with zero bits to become 16 bits in length respectively.

Encoding Symbol ID (ESI) - 16 bits

This field indicates which repair symbols are contained within this repair packet. The ESI provided is the ESI of the first repair symbol in the packet.

Source Block Length (SBL) - 16 bits

This field specifies the length of the source block in symbols.

E.4.3.2.2 Procedures

E.4.3.2.2.0 General

This FEC Scheme uses the procedures of the framework defined in clause E.4.2 to construct a source block to which the FEC code can be applied. The sender shall allocate SBNs to source blocks sequentially, wrapping around to zero after SBN $2^{16}-1$.

During the construction of the source block as per clause E.4.2.3.2:

- The length indication, $l[i]$, included in the Source Packet Information for each packet shall be dependent on the protocol that is carried. Rules for RTP are specified below in clause E.4.3.2.2.3.
- The value of $s[i]$ in the construction of the Source Packet Information for each packet shall be equal to the number of repair symbols placed in each repair packet, which shall be the same for all repair packets of a block.

E.4.3.2.2.1 Derivation of Source FEC Packet Identification Information

The Source FEC Packet Identification Information for a source packet is derived from the sequence number of the packet and information received in any Repair FEC packet belonging to this Source Block. Source blocks are identified by the sequence number of the first source packet in the block. This information is signalled in all Repair FEC packets associated with the source block in the ISN field.

The length of the Source Packet Information (in bytes) for source packets within a source block is equal to length of the payload containing encoding symbols of the repair packets (i.e. not including the Repair FEC Payload ID) for that block, which shall be the same for all repair packets. The Source Packet Information Length (*SPIL*) in symbols is equal to this length divided by the Encoding Symbol Size (which is signalled in the FEC Object Transmission Information).

The set of source packets which are included in the source block is determined from the ISN and SBL as follows:

Let:

I be the Initial Sequence Number of the source block.

L_P be the Source Packet Information Length in symbols.

L_B be the Source Block Length in symbols.

Then, source packets with sequence numbers from I to $I + L_B/L_P - 1$ inclusive are included in the source block.

Note that if no FEC Repair packets are received then no FEC decoding is possible and it is unnecessary for the receiver to identify the Source FEC Packet Identification Information for the source packets.

The ESI for a packet is derived from the following information:

- The sequence number, N_s , of the packet.
- The Source Packet Information Length for the source block, L_P .
- The Initial Sequence Number of the source block, I .

Then the ESI for packet with sequence number N_s is determined by the following formula:

$$ESI = (N_s - I) \cdot L_P \quad (E.6)$$

Note that all repair packet associated to a given Source Block shall contain the same SBL and ISN.

E.4.3.2.2.2 Derivation of repair packet ESIs

The ESI for a repair packet indicates which repair symbols the packet contains. This is given directly by the ESI field of the Repair FEC Payload ID.

E.4.3.2.2.3 Procedures for RTP flows

In the specific case of RTP packet flows, then the RTP Sequence Number field shall be used as the sequence number in the procedures described above.

The length indication included in the Source Packet Information shall be the RTP payload length plus the length of the CSRCs, if any, and the RTP padding bytes, if any. Note that this length is always equal to the UDP payload length of the packet, minus 12.

E.4.3.2.3 FEC Code specification

The requirements of clause E.4.3.1 apply.

E.4.3.2.4 Example parameters

E.4.3.2.4.1 Parameter derivation algorithm

It is recommended that the algorithm of clause E.4.3.1.6.1 is used.

In the case of RTP streams carrying MPEG-2 Transport Streams, then the maximum repair packet size should be set to

$$P = \text{ceil}((n \cdot 188 + 15)/A) \cdot A \quad (E.7)$$

Where n is the nominal number of 188 byte TS packets per IP Source packet.

The maximum source block size is determined by application configuration at the sender.

E.4.3.2.4.2 Examples

The above algorithm leads to transport parameters for MPEG-2 Transport Streams as shown in Table E.4, assuming the recommended values for A , K_{MIN} and G_{MAX} .

Table E.4: Example parameters settings

Maximum packets per protection period	Nominal TS packets per IP packet	Maximum Packet Size, P	Maximum Source Block Size, B	G	Symbol size T
100	7	1 344	134 400	7	192
200	7	1 344	268 800	4	336
300	7	1 344	403 200	3	672
400	7	1 344	537 600	2	672

E.5 FEC decoder

E.5.1 Decoder requirements (normative)

E.5.1.1 Minimum decoder requirements

FEC decoders that are compliant to this annex shall support processing of the SMPTE 2022-1 [66] packets. This means that whenever:

- 1) an SMPTE 2022-1 FEC packet has been received; **and**
 - 2) all but one of the media packets protected by this FEC packet have been received within the previous *max-block-size* source packets and/or within a time window beginning *max-block-size-time* before the current time; **and**
 - 3) the time at which the remaining media packet is useful to the media decoder has not passed,
- then**, the SMPTE 2022-1 decoding operation shall be applied and the resulting recovered packet passed to the media decoder.

The above requirement applies independently of the arrival time or order of the packets involved.

NOTE: The parameters *max-block-size* and *max-block-size-time* are part of the FEC Configuration Information and are discussed further in clause E.6.

E.5.1.2 Enhanced decoder requirements

FEC decoders may additionally support Raptor FEC packets. In this case, if a receiver receives a mathematically sufficient set of encoding packets (which may include both SMPTE 2022-1 FEC packets and Raptor FEC packets) for reconstruction of a source block within the previous *max-block-size* source packets and/or within a time window beginning *max-block-size-time* before the current time then the decoder shall recover the entire source block. Note that the example decoder procedures described in clause E.5.2 fulfil this requirement and thus a decoder is compliant to this Annex only if it can successfully decode given any set of packets with which the example decoder can also decode.

E.5.2 Hybrid decoding procedures (informative)

E.5.2.1 Outline

In the case that a receiver receives FEC repair packets from multiple layers, including packets generated according to the codes of both clauses E.3 and E.4, then combined decoding may be provided. This clause outlines procedures which may be followed to achieve this.

Combined decoding proceeds in 3 steps:

Step 1: SMPTE 2022-1 decoding

In this step, the packets encoded according to SMPTE 2022-1 [66], together with the received source packets, are processed as usual to recover zero or more source packets.

Step 2: Raptor decoding

In this step, if source packets are still missing, then packets encoded according to Raptor, together with the received source packets and any source packets which were recovered in Step 1, are processed using standard Raptor decoding procedures (for example as described in [65]) to recover zero or more source packets.

Step 3: Hybrid decoding

In this step, if source packets are still missing, then remaining (unprocessed) SMPTE 2022-1 [66] packets are converted to a form in which they can be added to the Raptor decoding process, and Raptor decoding is then continued.

Conversion of SMPTE 2022-1 packets and their use in Raptor decoding are described in the following clauses.

E.5.2.2 Conversion of SMPTE 2022-1 packets

The objective of this conversion operation of SMPTE 2022-1 packets is to convert them into a form such that they can be included in the Raptor decoding process. According to SMPTE 2022-1, each FEC packet is constructed by applying a protection operation, based on the exclusive OR operation (XOR), to a number, D , of the source packets (the "protected packets"). The UDP payload of the SMPTE 2022-1 packet contains the following data:

- An RTP header for the SMPTE 2022-1 packet.
- An FEC header containing:
 - The Length Recovery field, which is the XOR of the unsigned network-ordered 16-bit representation of the lengths of the protected packets in bytes minus 12 (for the fixed RTP header), i.e. the sum of the lengths of all the following if present: the CSRC list, header extension, RTP payload, and RTP padding.
 - The PT Recovery field, which is the XOR of the Payload Type (PT) fields in the RTP headers of the protected packets.
 - The Timestamp Recovery field, which is the XOR of the Timestamp fields in the RTP headers of the protected packets.
- The XOR of the CSRC list, header extension, RTP payload and RTP padding of the protected packets.

After the SMPTE 2022-1 [66] decoding, if all missing source packets associated with an SMPTE 2022-1 [66] FEC packet have been recovered, it is not necessary to perform the conversion operation for that SMPTE 2022-1 [66] FEC packet. However, if there are still remaining unrecovered protected packets, a conversion operation is needed for each such SMPTE 2022-1 [66] FEC packet. The conversion is achieved by concatenating the following fields to form a "virtual" Raptor repair packet payload i.e. the virtual Source Packet Information that includes in addition to the virtual payload also the fields for the UDP flow ID, the length indication field, and padding:

- A single zero byte.
- A two byte length indication, which is equal to the XOR of the unsigned network-ordered 16-bit representation of the lengths of the unrecovered protected packets in bytes minus 12 (for the fixed RTP header). This is equal to the XOR of the Length Recovery field in the SMPTE 2022-1 [66] FEC header and the 16-bit representation of the lengths of the received protected packets in bytes minus 12.
- A two-bit field, which is equal to the XOR of the RTP Version fields of the unrecovered protected packets. This is equal to zero if the number of unrecovered protected packets is even and 2 otherwise.
- A seven (7) bit field, equal to the XOR of the RTP Padding (P), Extension (X), CSRC Count (CC) and Marker (M) fields of the unrecovered protected packets. This is equal to the XOR of the concatenated P, X, CC and M fields in the SMPTE 2022-1 RTP header and the concatenated P, X, CC and M fields of the received protected packets.
- A seven (7) bit field equal to the XOR of the RTP PT fields of the unrecovered protected packets. This is equal to the XOR of the PT Recovery field in the SMPTE 2022-1 FEC header and the PT fields of the received protected packets.
- A 16-bit field equal to the XOR of the RTP Sequence Number fields of the unrecovered protected packets. The Sequence Numbers of the unrecovered protected packets can be explicitly calculated based on the *SNbase*, *offset* and *NA* fields of the SMPTE 2022-1FEC header.
- A 32-bit field equal to the XOR of the RTP Timestamp (TS) fields of the unrecovered protected packets. This is equal to the XOR of the TS Recovery field in the SMPTE 2022-1 FEC header and the TS fields of the received protected packets.
- A 32-bit field equal to the XOR of the RTP SSRC fields of the unrecovered protected packets. This is equal to zero if the number of unrecovered protected packets is even and equal to the SSRC of the stream otherwise.

- The XOR of the CSRC lists, header extensions, RTP payloads and RTP paddings of the unrecovered protected packets,. This is equal to the XOR of all the bits in the SMPTE 2022-1 FEC packet except its RTP and FEC headers and all the bits in the received protected packets except their 12-byte fixed RTP headers (padded as necessary). Note that a header extension and CSRC list are never present in an SMPTE 2022-1 FEC packet, independent of the values of the X and CC fields in its RTP header.
- A number of zero-valued padding bytes, such that the total length of the "virtual" repair packet payload is equal to the length of the other Raptor repair packet payloads (which are all required to be the same according to clause E.4.3.2.5).

The resulting "virtual" repair packet payload is then equal to the XOR of the Source Packet Information of the unrecovered protected packets.

E.5.2.3 Extension of Raptor decoding

A possible Raptor decoding algorithm is described in clause C.7 of [65] in terms of a Gaussian Elimination process upon a matrix **A**. If decoding is not possible without use of the SMPTE 2022-1 [66] packets, then this decoding process will fail during the second phase described in clause C.7 of [65]. At this point, the matrix **A** has less than L non-zero rows (Note, the symbol L here denotes the number of intermediate symbols of the Raptor code as defined in [65], not the L value associated with the SMPTE 2022-1 [66] packets).

Let G be the number of symbols per packet (which can be calculated as the Raptor repair packet payload size divided by the symbol size). Then each "virtual" Raptor repair packet constructed above consists of exactly G new symbols, each of which is the XOR of exactly N_s source symbols (which we call the "unrecovered protected symbols"), where N_s is the number of unrecovered protected packets associated with the SMPTE 2022-1 [66] FEC packet from which the "virtual" Raptor repair packet was constructed.

For each such new symbol, a new row is added to the decoding matrix **A**. This row is constructed as follows:

- The row is initialized to zero.
- For each of the N_s unrecovered protected symbols, the *LTEnc* generator is used to determine the set of intermediate symbols whose sum is equal to the unrecovered protected symbol. For each such intermediate symbol a "1" is XORed into the appropriate position of the new row.

Phase two of the decoding process is then continued with these additional rows and symbols.

E.6 FEC Content Delivery Protocols

E.6.0 Introduction

This clause defines several complete FEC Content Delivery Protocols, making use of the components defined in the foregoing clauses.

E.6.1 Multicast MPEG-2 Transport Stream over RTP

E.6.1.0 Introduction

This clause defines a Content Delivery Protocol for FEC protected multicast delivery of MPEG-2 Transport Streams over RTP.

E.6.1.1 Control protocols

FEC Configuration information shall be delivered using the DVB Service Discovery mechanisms as described in clause 5. The DVB Broadcast Discovery record may contain the multicast address(es) and port(s) for one or more FEC layers. Receivers may choose which layers to join depending on capability and local configuration.

When the Raptor layer is provided, the Flow ID within the Source Packet Information for the MPEG-2 TS flow shall be zero.

E.6.1.2 Transport protocol

The MPEG-2 Transport Stream shall be transported according to clause 7.1.1.

FEC protection of the MPEG-2 Transport Stream may be provided according to clauses E.3 and E.4. When a Raptor layer is provided, the FEC Scheme defined in clause E.4.3.2 shall be used.

E.6.2 Unicast MPEG-2 Transport Stream over RTP

E.6.2.0 Introduction

This clause defines a Content Delivery Protocol for FEC protected unicast delivery of MPEG-2 Transport Streams over RTP.

E.6.2.1 Control protocols

The receiver shall indicate in the Transport header of the RTSP SETUP request which FEC layers are requested by supplying port numbers that should be used for the FEC repair packets. Only requested FEC layers shall be sent to the receiver.

The server may supply the FEC parameters *max-block-size*, *max-block-size-time* and *FEC Object Transmission Information* in the Transport header of the RTSP SETUP response.

The Flow ID for the MPEG-2 TS flow shall be zero.

E.6.2.2 Transport protocol

The MPEG-2 Transport Stream shall be transported according to clause 7.1.1.

FEC protection of the MPEG-2 Transport Stream may be provided according to clauses E.3 and E.4 above. When a Raptor layer is provided, the FEC Scheme defined in clause E.4.3.2 shall be used.

E.6.3 Generic multicast video (informative)

E.6.3.0 Introduction

This clause defines a Content Delivery Protocol for FEC protected multicast delivery of arbitrary audio/video streams (for example H.264 encapsulated in RTP).

E.6.3.1 Control protocols

FEC Configuration information shall be delivered using the DVB Service Discovery mechanisms as described in clause 5. The DVB Broadcast Discovery record may contain the multicast address(es) and port(s) for one or more FEC layers. Receivers may choose which layers to join depending on capability and local configuration.

E.6.3.2 Transport protocols

The audio/video stream is assumed to be carried by one or more UDP flows. FEC protection of these UDP flows may be provided using the procedures of clause E.4.2.2 and in particular the FEC Scheme defined in clause E.4.3.1.

E.6.4 Generic unicast video (informative)

E.6.4.0 Introduction

This clause defines a Content Delivery Protocol for FEC protected unicast delivery of arbitrary audio/video streams (for example H.264 encapsulated in RTP). This clause is provided to describe how FEC can be applied to future extensions to the DVB-IPTV Handbook which address direct encapsulation of audio/video streams in RTP.

E.6.4.1 Control protocols

The receiver shall indicate in the Transport header of the RTSP SETUP request which FEC layers are requested by supplying port numbers that should be used for the FEC repair packets. Only requested FEC layers shall be sent to the receiver.

The server may supply the FEC parameters *max-block-size*, *max-block-size-time* and *FEC Object Transmission Information* in the Transport header of the RTSP SETUP response.

E.6.4.2 Transport protocols

The audio/video stream is assumed to be carried by one or more UDP flows. FEC protection of these UDP flows may be provided using the procedures of clause E.3 and in particular the FEC Scheme defined in clause E.4.

E.6.5 MIME Types definitions for AL-FEC

Two MIME media subtypes have been registered with IANA (<http://www.iana.org/>) for DVB-IPTV AL-FEC:

- "application/vnd.dvb.ipvt.alfec-base" to identify the Base layer;
- "application/vnd.dvb.ipvt.alfec-enhancement" to identify the Enhancement layer(s).

These two MIME types shall be used when the description of DVB-IPTV services using FEC layers require MIME type usage (e.g. with SDP).

E.7 Raptor explicit encoding sequences

The Raptor code defined in this annex is defined in terms of explicit encoding operation sequences which shall be applied to generate repair symbols from source symbols.

NOTE: The FEC code which results from these encoding sequences is identical to that generated by the procedures described in annex C of [65]. As a result, the example decoder procedures described in [65] may be used.

The Maximum Source Block Size used with the FEC Schemes defined in clause E.4.3 shall be one of the following values:

- 101, 120, 148, 164, 212, 237, 297, 371, 450, 560, 680, 842, 1 031, 1 139 and 1 281.

Explicit encoding operation sequences are provided for each of the block sizes indicated above, supporting highly efficient implementation of encoders for the Raptor code for these block sizes.

This clause describes the notation used for the encoding sequences. The encoding sequences are provided as text files attached to the present document.

Each text file consists of two parts, a "pre-coding" section and a "repair symbol encoding" section. The two sections of the file are separated by a blank line.

The encoding sequence assumes that the data to be encoded is stored in a (virtual) block of memory. Each virtual memory location stores a complete symbol. At the start of the process, the source symbols are assumed to be stored consecutively in memory locations 0 to K -1 inclusive, where K is the block size.

Additional working memory locations are required to be available up to and including memory location L -1, where L is given in the following table for each value of K . Note that the L value here is exactly the value of L calculated according to annex C of [65]. The additional working memory shall be initialized to zero.

K	L
101	127
120	149
148	181
164	197
212	251
237	277
297	337
371	419
450	499
560	613
680	739
842	907
1 031	1 103
1 139	1 213
1 281	1 361

Figure E.8: Total memory requirement in symbols (L) for different block sizes

Each line of the "pre-coding" section of the text file consists of a series of memory location indices (in decimal notation), separated by spaces and each optionally preceded by the character ">". Each line is interpreted as follows:

Let:

- A be a working register which stores one symbol.
- n be the number of memory location entries on the line.
- m_i be the ith entry of the line, for $i = 0, \dots, n-1$.
- $C[x]$ be the symbol at memory location x.
- 0** be the zero symbol (all bits are zero).
- \oplus be the bitwise exclusive OR operation.

The following algorithm should be followed for each line in sequence:

```

A := 0
FOR i = 0 to n-1
  IF  $m_i$  is preceded by ">" THEN
     $C[m_i] := C[m_i] \oplus A$ 
  ELSE
    A := A  $\oplus C[m_i]$ 
  ENDIF

```

Each line of the "repair symbol encoding" section of the file lists the memory locations which shall be XORed together to produce a repair symbol, the first line providing the list for the repair symbol with ESI K, the second for the repair symbol with ESI K+1 etc.

For example, when included within the pre-coding section of the file, the line:

4 8 3 5 > 7 6 > 10

Would result in the following symbol assignments:

$$C[7] := C[7] \oplus C[4] \oplus C[8] \oplus C[3] \oplus C[5]$$

and:

$$C[10] := C[10] \oplus C[6] \oplus C[4] \oplus C[8] \oplus C[3] \oplus C[5]$$

Annex F (normative): RTP Retransmission Solution

F.1 Introduction

This annex defines an option for an HNED to provide immediate feedback (FB) using RTCP and then an RET server to retransmit the missing packets. This mechanism can be used instead of the optional AL-FEC solution or in combination with an AL-FEC solution, to provide for protection against packet loss of RTP streams. It can be used both for unicast services (CoD and Broadcast TV service with trick mode) and multicast (Live Media Broadcast service).

F.2 Terms and Acronyms

See clauses 3.1 and 3.2 of the present document.

F.3 Retransmission (RET) architecture

F.3.0 Introduction

The Retransmission (RET) architecture clause describes how RTP retransmission works for unicast and multicast services, as defined in other parts of the present document.

F.3.1 RET for CoD/MBwTM service

The simplest retransmission architecture is for unicast CoD and Media Broadcast with Trick Mode (CoD/MBwTM), as shown in figure F.1. This architecture contains two components: an HNED with an RTP client for media and an RTP client for repair and a CoD/MBwTM streamer with an RTP media and RTP RET server function. If the HNED uses SSRC multiplexing then it is the same RTP client for both media and repair. The RET server may not be in the same physical box as the CoD/MBwTM server. The Retransmission repair consists of 3 steps:

- 1) The CoD/MBwTM data stream is unicast over RTP (1, in the figure) with a packet loss.
- 2) Upon RTP packet loss detection by the HNED, the RET client in the HNED sends an RTCP FB message to the RET server (2).
- 3) The server responds to the RTCP FB message by retransmitting the requested packet (called a RET packet) over RTP to the RET client (3).

The unicast RTP RET packets can be regarded as a separate RTP stream which is one-to-one associated with the original unicast RTP stream composed of the original packets. This is important when you consider the concept of RTP sessions, as described in [21], which are each distinguished by a full, separate space of SSRC identifiers. If the RTP source coincides with the RTP retransmission server, as shown in figure F.1, then the original and retransmission streams are combined into a single RTP session with different SSRC identifiers only if the same transport addresses are used.

DVB RET recommends the use of SSRC multiplexing for a CoD/MBwTM stream and associated RET stream, resulting in a single RTP session. If session multiplexing is used the DVB RET server shall use an SSRC identical to the SSRC in the original stream as defined in IETF RFC 4588 [85].

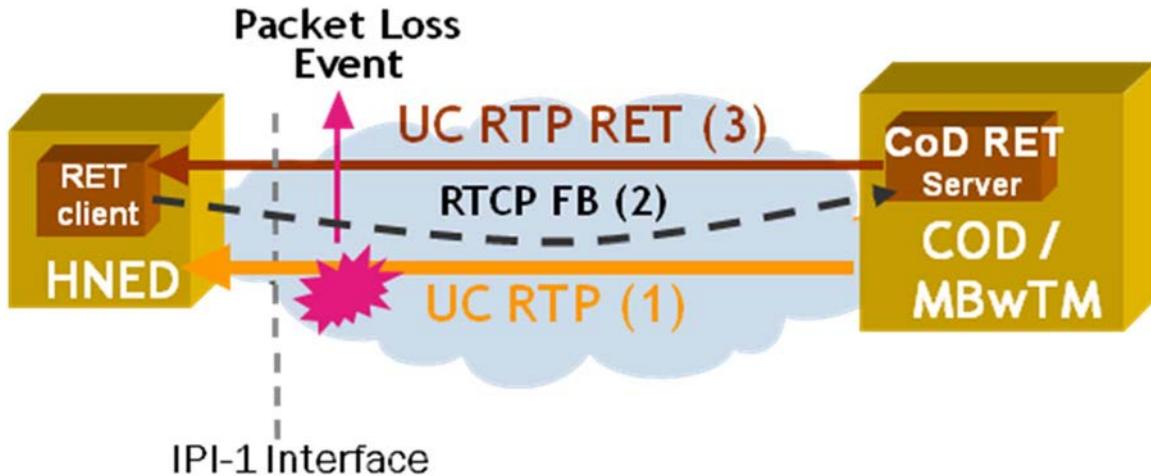


Figure F.1: RET Architecture and messaging for CoD/MBwTM services overview

F.3.2 RET for LMB service

F.3.2.0 RET architecture for LMB service

RTP retransmission for Live Media Broadcast (LMB) is more complex than for CoD/MBwTM because the media stream is multicast whilst the repair stream can be multicast or unicast. Figures F.2 and F.3 show the elements and communication flows involved in a RET architecture for LMB service. In this architecture, there can be several DVB LMB RET servers which handle unicast RTCP (FB) messaging from the RET clients, typically each server acting as an RTCP target for a subset of the HNEDs. RET enabled LMB services use SSM multicast with unicast feedback as discussed in IETF RFC 5760 [111].

A packet loss event may take place anywhere in the network: Downstream from the DVB LMB RET server (see figure F.2) and upstream from the DVB LMB RET server (see figure F.3). The packet loss event upstream of the DVB LMB RET servers can be repaired by adding a retransmission client to the server and use the same retransmission mechanism to repair the packet loss (see Figure F.3). Note that the scope of the present document is the IPI-1 interface and hence communication between DVB LMB RET servers and any retransmission server positioned deeper upstream in the network is not addressed in the present document.

There are two ways for repairing the packet loss event for LMB services:

- Unicast (see Figure F.2).
- Multicast (see Figure F.3).

The unicast repair method works similarly to the CoD/MBwTM case. The HNED detects packet loss, transmits a FB message, and the response is a unicast RET packet. The SSRC used by the LMB RET server shall be identical to the SSRC in the original MC RTP session (IETF RFC 4588 [85]).

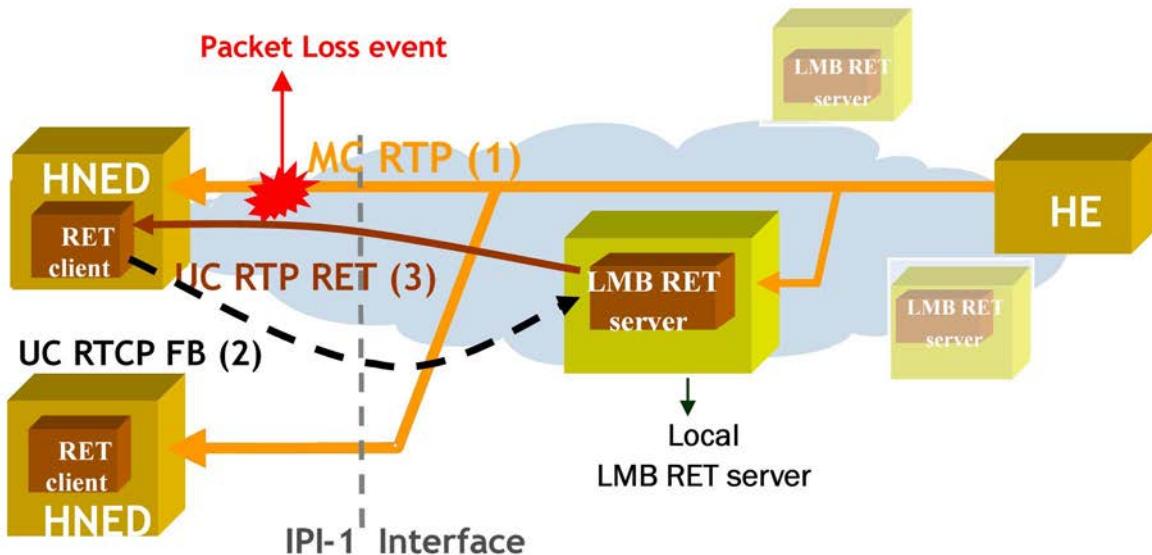


Figure F.2: RET Architecture and messaging for LMB services: unicast retransmission

Figure F.3 shows the multicast repair method for LMB services based on a packet loss event that has taken place upstream of the DVB LMB RET server, impacting many HNEDs. The LMB RET server does not need the RTCP FB message from the HNEDs to know about the packet loss as the LMB RET server itself can detect this packet loss. The LMB RET server, having detected the loss, requests the impacted HNEDs to not transmit the FB message by sending itself an RTCP Feed Forward (FF) message over multicast (step 2 in figure F.3) so preventing "NACK storms." The RET packet, once it has been made available to the LMB RET server, is then sent to the impacted HNEDs (step 3) also over multicast. This mechanism assumes that the RET clients respect some minimum waiting time between packet loss detection and RET requesting, either through randomization of waiting times (see IETF RFC 4585 [84]) or a more advanced mechanism as explained in clause F.7.2.

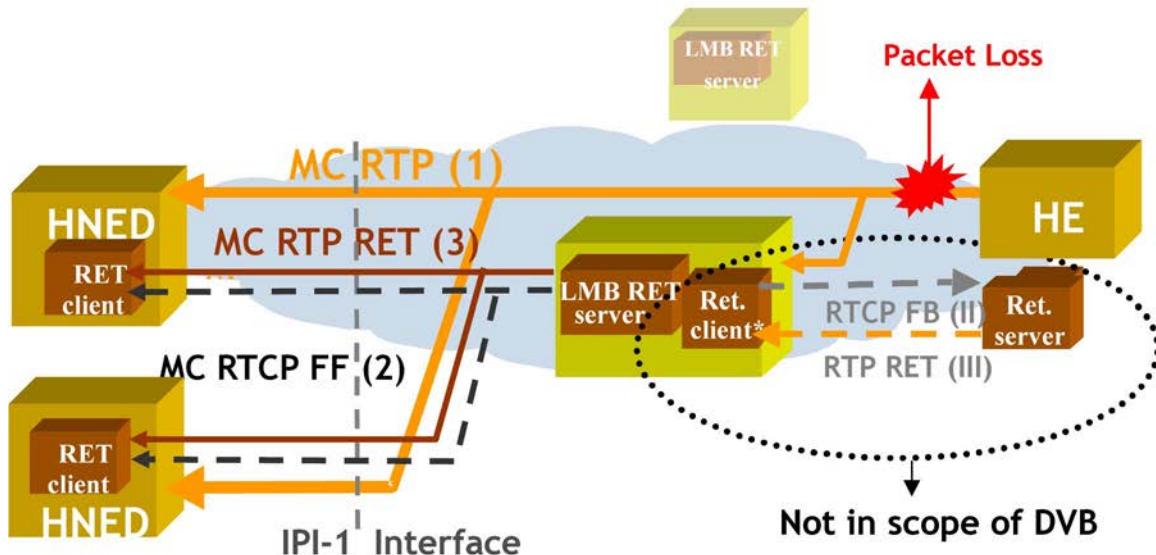


Figure F.3: RET Architecture and messaging for LMB services: MC retransmission and MC NACK suppression

The LMB RET server does not usually coincide with the Head End (HE) acting as the RTP media source, and retransmissions can occur both unicast (default) and multicast. This results at IPI-1 in an original multicast RTP session plus 2 associated RTP Retransmission sessions, which gives 2 RTP sessions if only unicast repair is used and 3 if both multicast and unicast repair are used.

The Multicast RTP RET session differs from the original Multicast RTP session because of a different source IP (the IP address of the LMB RET server), a different destination port and/or group Multicast IP address. The default retransmission repair being unicast, all the unicast and optional multicast repair parameters including availability shall be configured or signalled to the RET client. The multicast repair session functions just like any other SSM stream, for example, using the "join" methods of IPv4 or IPv6 to get the MC RTP RET stream.

F.3.2.1 RTP Sessions for the RET Enabled LMB service

Whenever a RET-enabled HNED connects to a RET-enabled LMB service, along with the establishment of an RTP session for the original multicast stream, a new unicast RTP RET session should be autonomously established.

The "media source SSRC" and/or the destination transport address of the unicast RTCP FB packets issued by the HNEDs indicate to the LMB RET server from which original RTP stream a packet is requested for retransmission. This results in, for a service with unicast and multicast repair, $N + 2$ RTP sessions where N is the number of serviced RET clients. Specifically the $N + 2$ RTP sessions are:

- 1) The original RTP MC session, which is a source-specific multicast (SSM) with the headend being the source, in which the DVB LMB RET server acts both as receiver (receiving the MC RTP stream) and as an RTCP target (receiving the unicast RTCP reports of the HNEDs).
 - 2) N x unicast RET RTP sessions (one for each RET-enabled HNED): the LMB RET server acts as RTP sender/source.
 - 3) (optional) A source-specific multicast RET RTP session where the LMB RET server acts as the source. This source-specific multicast may also be used by the LMB RET server for distributing the RTCP Feed Forward messages for NACK suppression in the original multicast RTP session (see clause F.5.2).

F.4 RTCP signalling by RET-enabled HNEDs

F.4.0 RTCP reports

The HNED's RTCP reports for RET enabled LMB services are always transmitted in unicast towards the DVB LMB RET server that shall also be the RTCP target [112]. The LMB RET server shall never return the reports towards the HNEDs except when the LMB RET server forwards the RTCP FF message (see clause F.5.2).

The following clauses describe the RTCP reports that can be transmitted by an HNED and shall be supported by a RET-enabled HNED for both RET-enabled CoD and LMB services.

F.4.1 RTCP FB message

The protocol that is used by an HNED for requesting retransmission is RTCP. The format of the Generic NACK transport layer FB message as specified in IETF RFC 4585 [84] will be used for packet retransmission requests, as shown in Figures F.4 and F.5. The HNED shall support the timing rules set forth in IETF RFC 4585 [84].

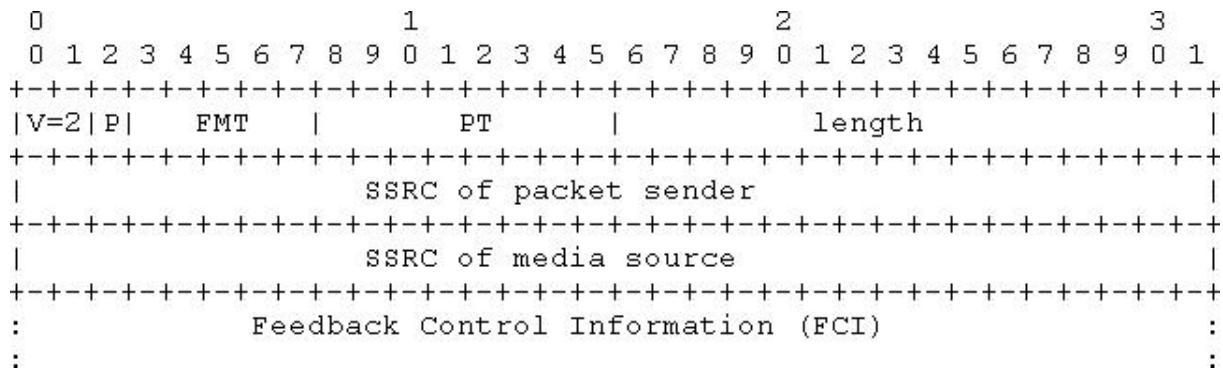


Figure F.4: Packet format for RTCP FB message

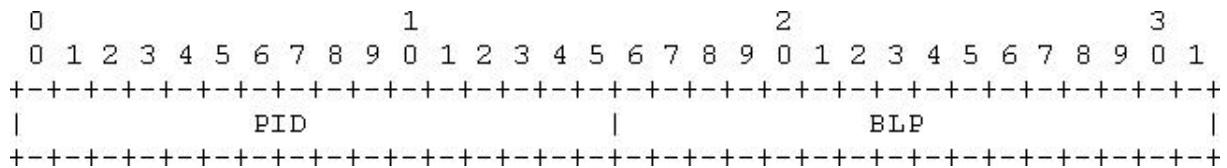


Figure F.5: Format of the Generic NACK put in the FCI field in the RTCP FB message

The PT in the RTCP FB message is filled in as "RTPFB" (value 205) and the Feedback Message Type (FMT) field in the RTCP FB message shall be 1.

The Feedback Control Information (FCI) field in the RTCP FB message contains at least one Generic NACK and may contain more than one.

The format of the generic NACK is shown in figure F.5. The Packet ID (PID) field refers to the sequence number of the first reported lost packet. The bitmask of following lost packets (BLP) field allows for reporting losses of any of the 16 RTP packets immediately following the RTP packet indicated by the PID (see IETF RFC 4585 [84] for a thorough definition). This allows a single Generic NACK to report up to 17 (consecutive) packet losses.

The RTCP messages issued by the HNED are always unicast towards the network, even for LMB services. The transport address for the RTCP messaging (destination IP address and UDP destination port) is obtained by the HNED through the configuration methods as explained in clause F.6.

The "SSRC of packet sender" in the RTCP FB message has the SSRC value used by the HNED in the original RTP session for LMB services. The "SSRC of media source" is the SSRC of the headend used for the LMB service for which the RTCP Feedback message reports packet loss.

Note: When multiple LMB services have the same media source SSRC, for example when LMB streams are sourced from different LMB SPs, the "SSRC of media source" in the RTCP Feedback message might not uniquely define the LMB service. This means that the HNED needs to be configured with different transport addresses for the unicast RTCP FB packets associated with these LMB services. Once configured, the combination of the "SSRC of media source" and the RTP RET session transport address of the IP/UDP/RTCP FB packet uniquely defines the LMB service for which the RTCP Feedback message reports packet loss.

F.4.2 RTCP RR, RTCP SDES and RTCP BYE packets

F.4.2.0 Introduction

A RET-enabled HNED shall support the RTCP Source Description (SDES) packet, RTCP Receiver Reports (RR), and RTCP BYE packet as defined by the formats in [21].

F.4.2.1 RTCP SDES Packet

The SDES packet shall only contain the CNAME item with the format following [21].

The SDES packet can be sent by the RET-enabled HNED in two different RTP sessions: in the original RTP session (multicast or unicast), and in the unicast RTP RET session. The CNAME, identifying the HNED shall be identical for the two RTP sessions.

The support by the HNED for the SDES packet is mandatory for the original MC RTP session. An HNED, for the RTP RET session, may support sending RTCP, and when it is enabled to do so it shall always send the RR combined with an SDES as a compound message (see [84], clause 3.1).

F.4.2.2 RTCP RR Packet

The RR contains the reception quality data of an RTP session as defined by [21].

The RET-enabled HNED shall support sending RR packets that contain reception quality data on the RTP packets received in the original RTP session, both for LMB and CoD services. This RR reporting may be disabled with the attribute dvb-disable-rtcp-rr.

The RET-enabled HNED may support sending RR that contain reception quality data on unicast RTP RET packets. The HNED is not allowed to send RTCP packets for a RET stream before RTCP packets for the original session have been sent.

When an HNED sends RTCP reporting data on both the original and RET packets, it may do so by including the RET RR and original RR into the same compound RTCP report or using two separate sessions, depending on configuration. When including the RET RR and original RR into the same compound RTCP report, the HNED uses one and the same SSRC but when using a separate session the HNED may use either different SSRCs for the RTCP reports in the two sessions or the same SSRC.

F.4.2.3 RTCP BYE packet

When a participant wishes to leave a RTP session, a BYE packet shall be transmitted to inform the other participants of this event as defined in [21]. A BYE packet shall be sent on an SSRC collision.

A BYE packet shall only be sent for LMB services by the HNED if it has been configured through the parameter "dvb-enable-bye" and when configured should only be sent if RTCP FB or SDES/RR have already been exchanged by the HNED in the original RTP session with the RTCP Target.

F.4.3 RTCP messaging types

An HNED shall be able to support both compound and non-compound RTCP FB packets for the original RTP session. A compound RTCP packet shall contain an SDES, an RR and FB messages (see [84]), while a non-compound (reduced size) RTCP packet contains only RTCP FB message(s) (see [113]). The use of both types of RTCP packets enables the split between longer term statistical information and retransmission repair information. [113] provides more information on reduced size RTCP messaging.

SD&S or RTSP configuration determines the message type when requesting retransmissions. When the HNED uses non-compound RTCP FB messages, the frequency of sending compound packets for statistical reporting is governed by [21]. DVB recommends that for compound reporting for statistical purposes, this frequency be once every 5 s.

The BYE packet for the original RTP session, when used, is always sent out in compound format containing at least one SDES and the BYE packet, as per [21]. The RR shall also be included if RR reporting is enabled.

RTCP compound statistical reporting (comprising SDES +RR) may also be disabled through configuration with the "dvb-disable-rtcp-rr" attribute.

For the RTP RET session non-compound reporting by the HNED is forbidden.

F.5 RTCP signalling towards RET-enabled HNEDs

F.5.0 Introduction

The following clauses describe the RTCP packets that shall be supported by a RET-enabled HNED.

F.5.1 The RTCP SDES/SR packets

An HNED shall be able to receive RTCP Sender Report (SR) and RTCP SDES packets in the original multicast RTP session from the RTP multicast source.

A DVB LMB/CoD RET server may send RTCP SR and RTCP SDES packets in the unicast RTP RET session.

A DVB LMB RET server may send RTCP SR and RTCP SDES packets in the multicast RTP RET session.

F.5.2 The RTCP Feed Forward (FF) message (LMB service only)

The RTCP FF message is an RTCP FB message relayed by the LMB RET server downstream. The RTCP FB message originated either at an "upstream RTP client" or at immediate reporting HNEDs:

- An upstream RTP client means the client is located upstream from the LMB RET server so it is able to detect upstream packet losses impacting all HNEDs serviced by the LMB RET server and receiving the LMB service. Figure F.3 shows such an upstream client.

- Immediate reporting HNEDs is a subset of HNEDs that are configured to report missing packets immediately, thus reporting before all the other RET-enabled HNEDs serviced by the same LMB RET server. Their SSRCs are distinguishable from the SSRC of non-immediate reporting HNEDs (see clause F.7.2).

The relayed messages are now called RTCP FF messages because they are multicast back to the HNEDs in the opposite direction to the RTCP FB messages issued by the HNEDs. The sending of the RTCP FF message to the HNEDs assists in preventing or reducing NACK storms. The operation of the LMB RET Server, when handling such a RTCP FB message originating from an upstream client or a set of immediate reporting HNEDs, is that of an RTP translator that "simply forwards RTCP packets unmodified" as described in clause 7.2 of [21].

The typical event sequence when a RTCP FF message is relayed by the RTCP target/LMB RET server is:

- There is a packet loss event on an upstream link or on a downstream aggregated link impacting several HNEDs serviced by the LMB RET server.
- An RTCP FB message is sent by an upstream RTP client and/or by all immediate reporting HNEDs receiving the LMB service, indicating packet loss to the RTCP target/LMB RET server.
- **Upstream packet loss:** The LMB RET server, acting as RTP translator, translates the transport address of RTCP FB message and forwards it as an RTCP FF message in the MC RTP RET session. The LMB RET server discards any RTCP FB messages received by immediate reporting HNEDs.
- **Downstream packet loss event impacting all or a large subset of HNEDs:** The RTCP target will get RTCP FB messages of all immediate reporting HNEDs, but it needs to forward only one FB message as FF message in the MC RTP RET session.
- The LMB RET server transmits in the MC RTP RET session the RET packet(s) as indicated by the RTCP FF message. Note that in the case of upstream packet loss, this is only done once the missing packets are available at the LMB RET server.

The different logical functionalities: upstream client, translator and LMB RET server may or may not be implemented in the same physical entity. The SSRC of the upstream client is signalled through the parameter "dvb-ssrc-upstream-client".

The format of the RTCP FF messages is the RTCP Generic NACK transport layer FB message as specified in [84]. The feedback control information field in the RTCP FF message shall contain at least one NACK and may contain more than one.

The "packet sender SSRC" field in the FF message is the "upstream-client" SSRC or the SSRC of an immediate reporting HNED. The "media source SSRC" field is the same as found in the originating RTCP FB message and will have the SSRC value as in the original RTP MC packets.

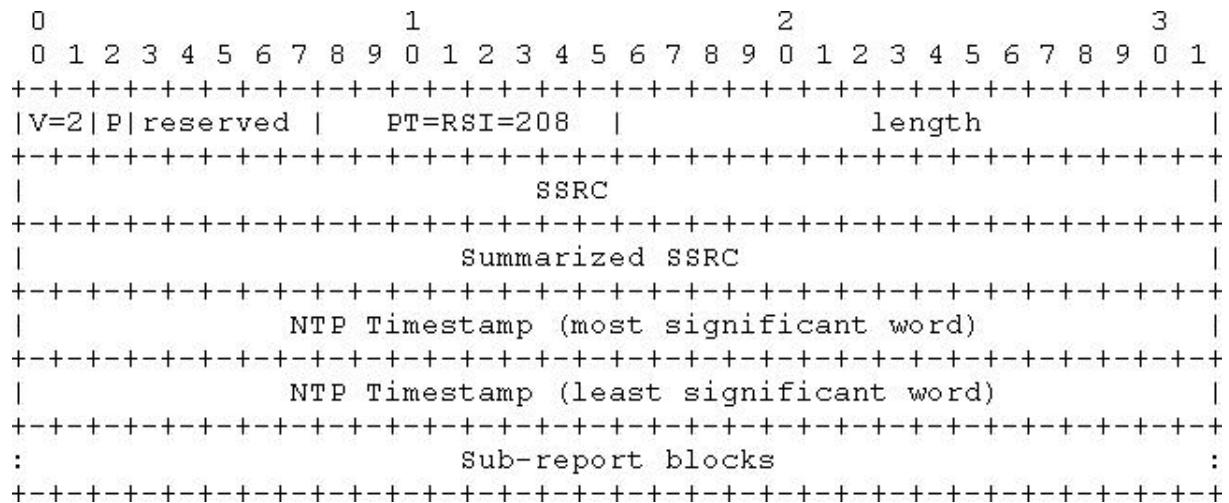
The RTCP FF message is sent from the LMB RET server anticipating the loss detection of a certain packet by the HNED. The LMB RET server shall send this message in the MC RTP RET session.

When the HNED receives this message, it should not send out an RTCP FB message asking for retransmission of those packets as indicated in the received RTCP FF message. If, after time "dvb-t-ret" (see clause F.7) as defined in SD&S, not all the expected RET packets have been received then the HNED may send an RTCP FB message.

F.5.3 The RTCP Receiver Summary Information (RSI) packets(LMB service only)

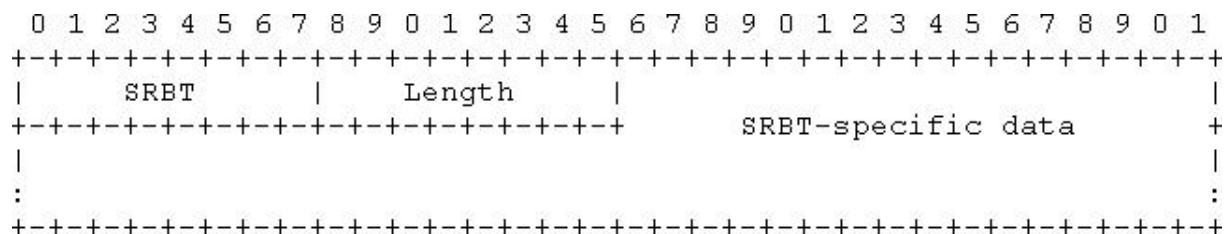
The RTCP RSI packets are RTCP packets that signal information towards the HNEDs relating to the original MC RTP session. In general, these packets convey information which otherwise could be retrieved by the HNEDs if multicast distribution of HNED's RTCP packets were allowed in the original MC RTP session.

The RTCP RSI packet has the format as defined in Figure F.6.

**Figure F.6: Format of RSI packet**

- Length: 16 bits: the length of the RTCP packet in 32-bit words minus one, including the header and any padding.
- SSRC: 32 bits: The SSRC, which equals the SSRC in the original RTP MC stream packets.
- Summarized SSRC: 32 bits: The SSRC (of the Media Sender) of which this report contains a summary; this is generally the same value as found in the previous SSRC field.
- Timestamp: 64 bits: Indicates the wallclock time when this report was sent. Wallclock time (absolute date and time) is represented using the timestamp format of the Network Time Protocol (NTP), which is in seconds relative to 0h UTC on 1 January 1900. Its format is similar to the time stamp in the RTCP sender reports. The timestamp value is used to enable detection of duplicate packets, reordering and to provide a chronological profile of the feedback reports.

Four sub-reports are defined in the present document, which the RET-enabled HNED shall be able to parse and interpret. The sub-reports all share the following format:

**Figure F.7: Generic Format of RSI Packet**

- SRBT: 8 bits: Sub-Report Block Type. The sub-report block type identifier. The values for the sub-report block types can be:
 - 0: IP4 Unicast Feedback Address; this is the address of the LMB RET server to which the RTCP (FB) messages shall be addressed.
 - 1: IP6 Unicast Feedback Address.
 - 2: DNS name for Unicast Feedback: this is the address of the LMB RET server, being the RTCP target to which the RTCP (FB) messages shall be addressed.
 - 8: SSRC collision list.
 - 11: "Receiver Bandwidth".
- Length: 8 bits: The length of the sub-report in 32-bit words.

- SRBT-specific data: <Length*4 - 2> octets: This field contains type-specific information based upon the SRBT value.

The sub-report block type 0,1 or 2 has the following format.

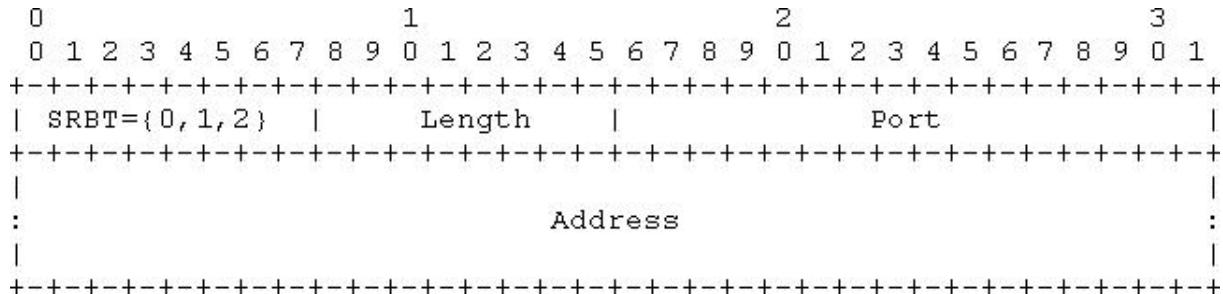


Figure F.8: Format of RSI Packet with sub-report block type equal to 0,1 or 2

- Length: 8 bits: The length of the sub-report block in 32-bit words. This is 2 for an IPv4 address (Total length = 4 + 4 = 2*4 octets) and 5 for an IPv6 address (Total length = 4 + 16 = 5 * 4 octets). For a DNS name, the length field indicates the number of 32-bit words making up the string plus 1 byte and any additional padding required to reach the next word boundary.
- Port: 2 octets: The port number to which the HNEDs send RTCP reports.
- Address: 4 octets (IPv4), or 16 octets (IPv6) or n octets (DNS name). The address to which receivers send RTCP reports. A DNS name is an arbitrary length string that is padded with null bytes to the next 32 bit boundary. The string shall be UTF-8 encoded.

The sub-report type 8 has the following format:

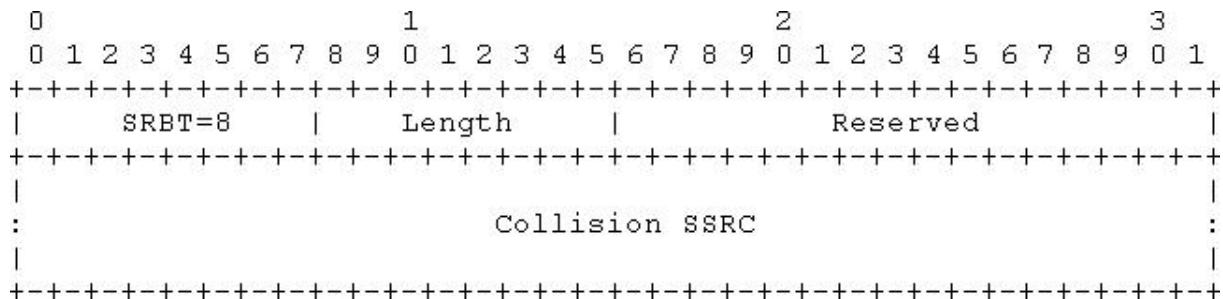


Figure F.9: Format of RSI Packet with sub-report block type equal to 8

- Length: 8 bits: The length of the sub-report block in 32-bit words.
- The collision SSRC sub-report provides a mechanism to report SSRC collisions amongst the group. In the event that a non-unique SSRC is discovered based on the tuple [SSRC,CNAME], the collision is reported in this block and the affected nodes shall reselect their respective SSRC identifiers. The "Collision SSRC" is a n × 32 bits field; this field contains a list of SSRCs that are duplicated within the group.

This sub-report is used when multiple HNEDs independently choose the same SSRC for the LMB original RTP session. This SSRC collision is not detected by the HNEDs, rather by the network elements such as the RTCP target, by looking at the (SSRC, CNAME) and/or the transport addresses used by the HNEDs. The "SSRCcollision list" RSI packet signals such an SSRC collision and advertises the HNED SSRCs for which a collision is detected. When an HNED receives such a packet, and it recognizes its own SSRC in the "collision SSRC" list then it shall adapt its SSRC, only sending an RTCP BYE packet when RTCP BYEs are enabled in SD&S.

In case the HNEDs are configured not to use the SDES (including CNAME) packets for their RTCP reporting in the original MC RTP session, SSRC collision may also be detected based on the tuple [SSRC, transport address].

The sub-report type 11 has the following format:

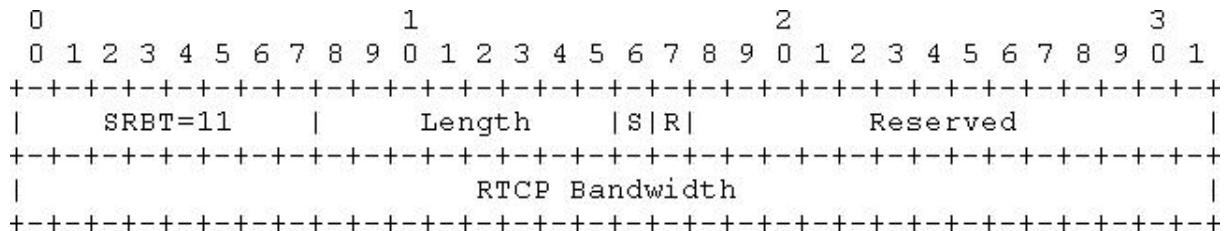


Figure F.10: Format of RSI packet with sub-report block type equal to 11

- Length: 8 bits: The length of the sub-report block in 32-bit words.
- Sender (S): 1 bit: Shall be set to 0.
- Receivers (R): 1 bit.

Shall be set to 1 and explicitly indicates that the contained bandwidth value applies to each RET-enabled HNED.

- Reserved: 14 bits.

Shall be set to zero upon transmission and ignored upon reception.

- RTCP Bandwidth: 32 bits.

This field indicates the maximum bandwidth allocated per HNED for sending RTCP data relating to the original RTP session. This is a fixed-point value with the binary point in between the second and third bytes. The value represents the bandwidth allocation per-receiver in kilobits per second with values in the range $0 \leq BW < 65536$.

The information in the RSI packets always relates to the original multicast RTP session, but they can be distributed either in the original multicast RTP session or in the multicast RTP RET session (with a source address of the LMB RET server address), but never in both multicast RTP sessions. By default the RSI messages are transmitted in the original multicast RTP session. When they are transmitted in the multicast RTP RET session, this is indicated by means of the "dvb-rsi-mc-ret" attribute.

The configuration of both the RTCP target/LMB RET server address and the RTCP bandwidth use SD&S Broadcast Discovery Records as well as RSI. The LMB RET server address may also be signalled via DHCP. If the RSI packets are received, the HNED shall use the information in these packets so overriding SD&S or DHCP.

F.6 Retransmission Format and RTP Retransmission Session SSRC and transport address

F.6.1 Retransmission Format

The HNED shall support RET packets with a 2-byte RET payload format header containing the original sequence number as defined in IETF RFC 4588 [85]. This format increases the IP packet size in two bytes and this should be considered when packetizing original media to avoid IP level fragmentation.

The sequence number in the RTP header of the retransmission packet shall follow the standard definition of being one higher than the sequence number of the preceding packet sent in the retransmission stream. The retransmission packet timestamp in the RTP header shall be set to the timestamp of the original packet. The SSRC shall be the same as the SSRC of the original packet if retransmission session multiplexing is used. The Payload Type in the RTP header of the RET packets is dynamically assigned and configured in the HNED. The RTP payload section in the RET packet is identical to the original packet.

F.6.2 Some Observations on Retransmission Transport Addresses and SSRC Identifiers

F.6.2.1 Unicast services (CoD and MBwTM)

The IP address and port numbers of the original RTP and retransmitted RTP packets are recommended to be identical, resulting in a single RTP session.

The SSRC of the RTP retransmission packets shall be different from the SSRC of the RTP original packets if RTP retransmission and RTP original packets are transported in the same session. This allows the HNED to distinguish among RET and original packets based on the SSRC.

F.6.2.2 LMB service

When using unicast RET repair for LMB, the SSRC of the RTP retransmission packet shall have the same value as the SSRC of the MC RTP original packets. This is recommended in cases where it is required to distinguish original from RET packets, for example for network monitoring.

When an HNED sends RTCP packets in a RTP RET session, it may use an SSRC different from the one it uses for RTCP reporting in the original RTP session.

NOTE: One can overcome typical NAT arrangements like "port restricted cone" (see [86]) and avoid opening an additional "pinhole" in the firewall for the RET RTP and RTCP packets transmitted by the LMB RET server in the retransmission session by:

- Having the retransmission server using the same destination port/address for the RTP packets in the retransmission session as the source port/address of the RTCP (FB) messages issued by the HNED.
- Having the retransmission server using the same source port/address for the RTP packets in the retransmission session as the destination port/address of the RTCP (FB) messages issued by the HNED. The latter is signalled to the HNED by means of the RTCPReporting@DestinationPort parameter (SD&S).
- Having the retransmission server multiplexing the RET RTP and RTCP on the same port as per [113].

In the case that the LMB RET server sends the RTP and RTCP packets in the RTP RET session to the same destination transport address, the combination of the Marker value and expected Payload Type value in the RET RTP packet header will be different from the possible Packet Type values in the RTCP packets. This allows the HNED to distinguish between incoming RTP and RTCP packets in the unicast RTP RET session.

When a system is deployed as described above, the UDP destination port of RTCP packets issued by the HNED in the retransmission session shall be different from the port of the RTCP packets issued by the HNED in the original multicast session. This is necessary to allow the LMB RET server to distinguish between RTCP messages received in the original multicast RTP session and RTCP messages received in the RTP retransmission session. The UDP destination port of RTCP packets issued by the HNED in the retransmission session is signalled by means of the Retransmission_session @DestinationPortForRTCPReporting parameter. When sent over multicast, the multicast group address of the multicast RET packets may be identical to the one of the original multicast packets, but using a different source IP address.

The source IP address of the MC RTP RET packets may be different from the source IP address of the unicast RTP RET packets so allowing the LMB RET server for unicast repair to be different from LMB RET server for multicast repair.

F.7 Retransmission Requesting Behaviour of RET-enabled HNED

F.7.0 General

A RET-enabled HNED will buffer incoming RTP packets over a certain time duration, providing time for packet loss detection, RET requesting and packet repair. The buffering delay is a fixed value and is determined based on some RET timing parameters which are described in this clause separately for CoD/MBwTM and for LMB services.

If an RTP packet is received, which may be a RET packet or an original packet, which carries a payload which was already received in a RET packet or in an original packet, than this RTP packet shall be discarded by the HNED. This behaviour of the HNED mirrors the behaviour of an RTP receiver that shall drop duplicate received RTP packets as defined in [21].

F.7.1 CoD/MBwTM RET (requesting) Timing Parameters

The RET timing parameters for CoD/MBwTM as signalled via RTSP are:

rtx-time

"rtx-time" is the amount of time a packet is available for retransmissions in milliseconds. This is defined in [85]. This value represents a meaningful maximum for the buffering delay as a result of RET.

dvb-t-ret

A RET-enabled HNED may issue multiple retransmission requests for the same packet loss event in the original RTP session, to take into account loss of RET packets or RTCP FB messages.

"dvb-t-ret" is defined as the minimum time in milliseconds a receiver should wait for a requested repair packet per retransmission request before issuing another retransmission request for the same packet(s). This time period has as starting point the sending of the retransmission request. This parameter is optional but the HNED shall be able to support this parameter if signalled. If the parameter is not signalled the HNED shall then choose an appropriate delay time with which failed retransmissions are retried. This delay time may be based on observing the time that elapses between sending out an RTCP FB for a single packet loss and the time of reception of the requested RET packet at the HNED and could be dynamically adapted (see [85], clause 6.3).

- "rtx-time" will determine how many retransmission attempts the HNED may perform, taking into account the "dvb-t-ret" parameter.
- "dvb-t-ret" is determined by round trip time (RTT) between the HNED and RET server and the RET server performance in processing the HNED generated RTCP FB messages. This could be set to a maximum anticipated value under normal circumstances.

Note that, the following relationship shall be valid:

- "rtx-time" > "dvb-t-ret" > average RTT.

The RET buffer delay shall be chosen by the HNED between:

- minimum value= "dvb-t-ret".
- maximum value= "rtx-time".

An HNED shall restrict the maximum bandwidth that is allowed for the RTCP reporting. For this, two parameters are defined:

ttr-int

"ttr-int" as defined by IETF RFC 4585 [84] defines the minimum interval between two regular full compound RTCP packets in milliseconds for the RTP session. If "ttr-int" is not specified, a default value of 0 is assumed.

Full compound RTCP packets include Receiver Reports. RTCP packets containing only FB messages are not subject to the "ttr-int" restriction.

rtpc-bandwidth

The "rtpc-bandwidth" XML parameter indicates the maximum amount of bandwidth that can be consumed by the HNED for its RTCP reporting. The default value is 5 % of the original stream bandwidth. If SDP is used, this parameter can be signalled using the "b=RR:<bandwidth-value>" bandwidth modifier as described in IETF RFC 3556 [83].

F.7.2 LMB RET (requesting) Timing Parameters

The RET timing parameters for RET-enabled LMB as distributed by SD&S include those defined in the previous clause F.7.1.

For CoD, a RET-enabled HNED may always transmit an RTCP FB message immediately upon packet loss detection, provided the "rtpc-bandwidth" value is not violated. For LMB, two parameters are defined that determine the window in which the HNED may issue an RTCP FB message upon packet loss detection: "dvb-t-wait-min" and "dvb-t-wait-max". This results in a more scalable LMB RET solution for those cases where a single multicast packet loss event impacts many HNEDs causing NACK storms. An additional bitmask "dvb-ssrc-bitmask" can be configured at the HNED that makes an HNED an immediate reporter by setting the "dvb-t-wait-min" and "dvb-t-wait-max" parameter values to zero.

The RET-enabled HNED shall behave as follows when requesting retransmission for LMB services:

When a packet loss is detected, the HNED sends out a RET request after waiting for an interval time which is randomly selected between "dvb-t-wait-min" and "dvb-t-wait-max." This time interval is called the "waiting time."

"dvb-t-wait-min," "dvb-t-wait-max" and "dvb-ssrc-bitmask" are configured with SD&S. "dvb-t-wait-min" can be zero and "dvb-t-wait-max" can be set equal to "dvb-t-wait-min" and "dvb-t-wait-max" \geq "dvb-t-wait-min." The default value for all of these parameters is zero.

The following applies when SD&S signals "dvb-t-wait-min" with a value different from zero:

The HNED shall not send the RTCP FB message after the waiting period has elapsed with "dvb-t-wait-min" \leq waiting period \leq "dvb-t-wait-max" if one of the following events occurs during the waiting time:

- An RTCP FF message is received from the LMB RET server advertising the packet loss detected by the HNED.
- The missing original packet(s) is/are received.
- RET packet(s) associated with the missing RTP packet(s) is/are received.

However, if an RTCP FF message was received and "dvb-t-ret" has elapsed since the reception of the first RTCP FF message then the HNED may issue an RTCP FB message, provided all of the following conditions are met:

- No additional RTCP FF message arrived reporting the same packet loss as the first received RTCP FF message.
- The expected RET packets have not arrived.
- The original missing packets have not arrived.

As long as RTCP FF messages are received from the LMB RET server reporting the same loss, the HNED shall not send an RTCP FB message.

If an RTCP FF message was received by the HNED prior to the packet loss detection by the HNED, the HNED shall wait for at least "dvb-t-ret" starting from the reception of the FF message before issuing itself an RTCP FB message, if still required.

For non-zero "dvb-t-wait-min" values signalled by SD&S, a 32-bit wide bitmask (signalled as dvb-ssrc-bitmask) may also be used to cope with packet loss occurring downstream of the LMB RET server affecting several HNEDs serviced by the server.

The "dvb-ssrc-bitmask" makes a small subset of HNEDs immediate reporters, and at least one RTCP FB message issued by these HNEDs may be translated and forwarded by the LMB RET server as an RTCP FF message downstream over the RET SSM to all HNEDs (see clause F.5.2).

If the "dvb-ssrc-bitmask" is provided by SD&S, the RET-enabled HNED shall compare, on a bit per bit basis, its own 32-bit SSRC which it uses in the original multicast RTP session with the 32-bit SSRC carried in the original MC RTP stream, on those bit positions that have the value 1 in the bit mask. If the two SSRC identifiers have the same values on all the non-zero "dvb-ssrc bitmask" bit positions, the HNED is an immediate reporter, which means that its "dvb-t-wait-min" and "dvb-t-wait-max" equal zero, and hence overrule any SD&S signalled "dvb-t-wait-min" and "dvb-t-wait-max" parameter values.

As the HNEDs select their SSRC randomly, on average the ratio of immediate reporting HNEDs to all RET-enabled HNEDs is $(1 / (2^N))$ with N the number of "1"s in the bit mask ($0 \leq N \leq 32$). For example, if there are two non-zero values in the bit mask, this means that on average 1 out of 4 HNEDs will be an immediate reporter.

If the "dvb-t-wait-min" parameter is configured to be zero or not provisioned in SD&S then the LMB RET server should issue no RTCP FF messages. When packet loss detection occurs, the HNED shall send out an RTCP FB message after a time interval randomly selected between 0 and "dvb-t-wait-max".

F.8 Configuration method and configuration parameters

RET-enabled LMB use SD&S to configure the RET client while CoD uses RTSP to configure the RET client. The exception to this is the initial IP address of the LMB RET servers that can be configured in three different ways:

- 1) DHCP RTP Retransmission Server Address option

DHCP should be used at start up to get a list of IP addresses of LMB RET servers as described in clause 8.1.1.10 for IPv4 and in clause 8.1.2.4.10 for IPv6. These IP addresses are the same for all LMB services. The servers shall be in the order of priority from first to last server to connect to. The method for connecting to the server and assuring its operation is vendor specific.

- 2) SD&S

SD&S may also contain LMB RET server addresses which can be specified per LMB service. These addresses overrule the LMB RET server address obtained from DHCP for the specific LMB service where SD&S contains a value.

- 3) RSI messages

The RSI messages with sub report block type equal to 0,1 or 2 that may be distributed in the RET SSM group to signal the new address of an LMB RET server. The LMB RET server address signalled in an RSI is only valid for a specific SSM group (LMB service), being the original SSM group associated with the RET SSM. The LMB RET server address signalled through RSI takes precedence over the LMB RET server address(es) that may be configured via SD&S for that specific service, and also takes precedence over the LMB RET server address(es) that may be configured via DHCP.

If SD&S records are updated with new LMB RET server addresses after an RSI message then the new SD&S values for the LMB RET server will take preference over addresses in the RSI message.

Note that LMB RET server addresses signalled via DHCP or RSI can be different for different access service regions as they can be distributed locally via the DHCP server or via the operational LMB RET server (RSI).

F.9 QoS Priority settings

The RTP RET packets take over video bearer priority of corresponding original RTP packets (which is DSCP 0b100010 or 0b100100). All RTCP packets issued by the HNED have voice/video signalling priority setting (DSCP 0b011010). The RTCP packets that are transmitted to the HNEDs are considered to be of the video bearer traffic type with appropriate priority setting.

F.10 DVB RET and AL-FEC services combined

The DVB Application Layer FEC and the DVB Application Layer RET are services that both protect for packet losses. They are defined separately and there is no dependency between the two solutions.

If a SP would like to use both packet loss recovery methods for the same LMB and/or CoD/LMBwTM service the FEC and RET protection services may be combined.

The RET mechanism as explained in the present document, is then applied only to the original RTP data streams. RET on FEC repair streams shall never be used so the RTCP FB messages always identify a packet missing from the original RTP stream rather than the FEC repair stream.

F.11 Mapping of DVB-specific RET attributes and parameters in SDP

"dvb-t-ret" and "dvb-disable-rtcp-rr" may be included in the SDP description both for LMB and for CoD services.

"dvb-t-ret" can only be specified as media level parameter in the SDP description in the m-line associated with the original RTP packet flow.

"dvb-disable-rtcp-rr" is a session or media level attribute both for the original RTP and the unicast retransmission RTP flows.

For RET-enabled LMB services the following media level parameters may also be included in the SDP file in the m-line associated with the original RTP session: "dvb-t-wait-min", "dvb-t-wait-max", "dvb-ssrc-bitmask", "dvb-ssrc-upstream-client", "dvb-rsi-mc-ret" and "dvb-enable-bye".

Examples of SDP descriptions for a RET-enabled CoD and for a RET-enabled LMB RTP session - including the DVB RET parameters/attribute defined in this annex - will be provided in the guidelines document ETSI TS 102 542 [i.5] .

Annex G (normative): CDS Related Information

G.1 CDS Related Extensions to Other Specifications

G.1.0 Introduction

CDS Announcement requires extension of the BCG as well as extension of TVA. The BCG OnDemandProgram Type and the on-demand decomposed binary locator are extended in order to differentiate between streaming and download modes and with content download specific information. A new BCG type *PushDownloadType* is introduced. Relevant specifications are expected to be updated in their next releases. To provide a consistent CDS specification in the present document, these extensions are collected in this clause.

G.1.1 Usage and Extensions of OnDemandProgramType for pull download service

G.1.1.0 Introduction

The OnDemandProgramType as defined in ETSI TS 102 822-3-1 [60], clause 6.4.2 may be used to announce CDS-based delivery of content items in pull download service mode. This clause defines the usage and extensions for this type in order to support CDSs.

The XML syntax for the extended OnDemandProgramType is defined in clause G.1.1.

G.1.1.1 Delivery Mode Extension

In order to indicate the different modes of content delivery a new attribute is introduced as an extension to the OnDemandProgramType: the DeliveryMode attribute signals the delivery mode, namely streaming or download.

DeliveryMode	This attribute indicates the delivery mode. It can have the values "streaming" or "download". If the attribute is not provided streaming delivery is assumed.
--------------	---

If the DeliveryMode is not present, or the DeliveryMode signals "streaming", then a streaming delivery service as specified in ETSI TS 102 539 [62], clause 6.7 is defined.

If the DeliveryMode is present and it signals "download", a pull download service mode is defined. The other attributes of the OnDemandProgramType shall be interpreted as defined in the following clauses.

G.1.1.2 Usage of TVA OnDemandProgramType attributes for CDS pull download

If the DeliveryMode signals the download mode, then the OnDemandProgramType attributes shall be used as specified in this clause.

All attributes that are defined in ETSI TS 102 822-3-1 [60], clause 6.4.2 for the OnDemandProgramType are applicable for CDSs.

The following attributes have a specific usage for delivery mode "download":

ProgramURL	This element specifies a URI for the content download session. This URI can be a unicast or a multicast URI to download session description in SDP or XML format (see clause 10.3.2).
StartOfAvailability	This element specifies the time and date from which on the content item is available for download. If this parameter is not provided the content is already available for download and the value of "now" shall be assumed.
EndOfAvailability	This element specifies the time and date from which the content is no longer available for download. If not present, then the value of "indefinitely" shall be assumed.
NOTE: In case of scheduled multicast download start and end of availability may be the same indicating that a HNED shall join the multicast session only at that specified date and time.	

G.1.1.3 Content Version Number Extension

The ContentVersion attribute allows to signal updated versions of a downloadable content item. A new version of a content item may for example be issued in case of errors in the files of the content item that prevent the correct play out of the content item.

ContentVersion	The attribute indicates the version of the downloadable content. The version number counts from 0 to 255 with an overflow from 255 to 0.
NOTE: This content version number is not intended to be used to signal changed versions of the content item itself (e.g. new, removed or updated scenes). Such changes will result in a new content item with a different CRID.	

If the DeliveryMode signals the download mode, the attribute shall be used as defined in clause 10.6.6 of the present document.

If the DeliveryMode signals the streaming mode, then the ContentVersion attribute shall be ignored by the HNED.

If the parameter is not provided a content version number of 0 shall be assumed.

G.1.1.4 Expiry Time Extension

If the DeliveryMode signals the download mode the ExpiryTime attribute allows the SP to define an expiry time for the downloaded content item. A HNED shall automatically remove the content item from the CDS HNED storage at the expiry time (see clause 10.7).

ExpiryTime	The attribute defines the time when the content item expires and shall be removed from the CDS HNED storage.
------------	--

If the DeliveryMode signals the streaming mode, then the ExpiryTime attribute shall be ignored by the HNED.

If the parameter is not provided no expiry time shall apply to the downloaded content item.

G.1.1.5 Early Play Out Indication Extension

If the DeliveryMode signals the download mode the EarlyPlayout attribute allows to indicate if the play out of the content item can start while the download is still ongoing, i.e. before the content item is completely available on the CDS HNED.

EarlyPlayout	The attribute indicates if the play out of the content item can start while the download is still ongoing. If EarlyPlayout is "true" play out may start while the content item is downloaded. If EarlyPlayout is "false" play out shall not start before the content item is completely downloaded.
--------------	---

If the DeliveryMode signals the streaming mode, then the EarlyPlayout attribute shall be ignored by the HNED.

If the parameter is not provided it shall be assumed as "false".

G.1.1.6 Extended OnDemandProgramType XML Schema

```

<annotation>
  <documentation xml:lang="en">Extended OnDemandProgramType for TM-IPI CDS</documentation>
</annotation>

<simpleType name="DeliveryModeType">
  <restriction base="string">
    <enumeration value="streaming" />
    <enumeration value="download" />
  </restriction>
</simpleType>

<complexType name="OnDemandProgramType">
  <complexContent mixed="false">
    <extension base="tva:ProgramLocationType">
      <sequence>
        <element minOccurs="0" name="PublishedDuration" type="duration" />
        <element minOccurs="0" name="StartOfAvailability" type="dateTime" />
        <element minOccurs="0" name="EndOfAvailability" type="dateTime" />
        <element minOccurs="0" name="FirstAvailability" type="tva:FlagType" />
        <element minOccurs="0" name="LastAvailability" type="tva:FlagType" />
        <element minOccurs="0" name="ImmediateViewing" type="tva:FlagType" />
        <element minOccurs="0" maxOccurs="1" name="DeliveryMode" type="tva:DeliveryModeType" />
        <element minOccurs="0" maxOccurs="1" name="ContentVersion" type="unsignedByte" />
        <element minOccurs="0" maxOccurs="1" name="ExpiryTime" type="dateTime" />
        <element minOccurs="0" maxOccurs="1" name="EarlyPlayout" type="tva:FlagType" />
      </sequence>
      <attributeGroup ref="tva:fragmentIdentification" />
      <attribute name="metadataOriginIDRef" type="tva:TVAIDRefType" use="optional" />
      <attribute ref="xml:lang" use="optional" />
      <attribute name="serviceIDRef" type="tva:TVAIDRefType" use="optional" />
    </extension>
  </complexContent>
</complexType>

```

G.1.2 PushDownloadType for CDS push download service

G.1.2.1 Background and Semantics

A new type PushDownloadType is added to TV Anytime, ETSI TS 102 822-3-1 [60]. The PushDownloadType initiates download and storage of the referenced content item to the CDS HNED storage. Subject to any filtering criteria that may be applied by the HNED, the CDS HNED shall autonomously join the announced download session and download the content item to its local storage for any content item that is announced by the PushAction to be stored. Metadata related to this content item may be provided together with the content data as part of the download (see clause 10.4). The PushDownloadType is part of the instance description metadata and based on the ProgramLocationType defined in ETSI TS 102 822-3-1 [60], clause 6.4.2. The extension of the ProgramLocationType is provided in clause G.1.3.

Table G.1: PushDownloadType

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
Program	TVA CRID reference type defined in ETSI TS 102 822-3-1 [60], clause 6.4.2.	M
ProgramURL	URI defined in ETSI TS 102 822-3-1 [60], clause 6.4.2. This element specifies a locator for the content download session description for the content item. The locator can be a unicast or a multicast URI to a download session description in SDP or XML format (see clause 10.3.2).	O
InstanceMetadataID	TVA instance metadata ID type as defined in ETSI TS 102 822-3-1 [60], clause 6.4.2.	O
InstanceDescription	TVA instance description type as defined in ETSI TS 102 822-3-1 [60], clause 6.4.2.; can contain information on the content item (e.g. title, genre, AV attributes).	O
PublishedDuration	The advertised duration of the programme as defined in ETSI TS 102 822-3-1 [60], clause 6.4.2.	O

Element/Attribute Name	Element/Attribute Description	Mandated/ Optional
StartOfAvailability	Time and date from which on the content item is available for download. If this parameter is not provided the content is already available for download and the value of "now" shall be assumed.	O
EndOfAvailability	Time and date from which the content is no longer available for download. If not present, then the value of "indefinitely" shall be assumed.	O
ContentVersion	The attribute indicates the version of the downloadable content. The version number counts from 0 to 255 with an overflow from 255 to 0 (see clause G.1.1.3).	O
ExpiryTime	The attribute defines the time when the content item expires and shall be removed from the CDS HNED storage (see clause G.1.1.4).	O

G.1.2.2 PushDownloadType XML Schema

```

<annotation>
  <documentation xml:lang="en">New PushDownloadType for TM-IPI CDS</documentation>
</annotation>

<complexType name="PushDownloadType">
  <complexContent mixed="false">
    <extension base="tva:ProgramLocationType">
      <sequence>
        <element minOccurs="0" name="PublishedDuration" type="duration" />
        <element minOccurs="0" name="StartOfAvailability" type="dateTime" />
        <element minOccurs="0" name="EndOfAvailability" type="dateTime" />
        <element minOccurs="0" maxOccurs="1" name="ContentVersion" type="unsignedByte" />
        <element minOccurs="0" maxOccurs="1" name="ExpiryTime" type="dateTime" />
      </sequence>
      <attributeGroup ref="tva:fragmentIdentification" />
      <attribute name="metadataOriginIDRef" type="tva:TVAIDRefType" use="optional" />
      <attribute ref="xml:lang" use="optional" />
      <attribute name="serviceIDRef" type="tva:TVAIDRefType" use="optional" />
    </extension>
  </complexContent>
</complexType>

```

G.1.3 Extended ProgramLocationTableType

G.1.3.0 Introduction

The ProgramLocationType as defined in ETSI TS 102 822-3-1 [60], clause 6.7.1 is extended in order to include the PushDownloadType as a valid program location.

G.1.3.1 PushDownloadProgram Extension

The PushDownloadProgram includes CDS push download announcements into the BCG program location table. The attribute is of the type PushDownloadType.

PushDownload	A list of content items pushed to the user device at the request and under the control of the SP
--------------	--

G.1.3.2 Extended ProgramLocationTableType XML Schema

```

<annotation>
  <documentation xml:lang="en">Extended ProgramLocationType for TM-IPI CDS</documentation>
</annotation>

<complexType name="ProgramLocationTableType">
  <sequence>
    <element minOccurs="0" maxOccurs="unbounded" name="Schedule" type="tva:ScheduleType" />
    <element minOccurs="0" maxOccurs="unbounded" name="BroadcastEvent" type="tva:BroadcastEventType" />
    <element minOccurs="0" maxOccurs="unbounded" name="OnDemandProgram" type="tva:OnDemandProgramType" />
    <element minOccurs="0" maxOccurs="unbounded" name="OnDemandService" type="tva:OnDemandServiceType" />
    <element minOccurs="0" maxOccurs="unbounded" name="PushDownload" type="tva:PushDownloadType" />
  </sequence>
  <attribute name="metadataOriginIDRef" type="tva:TVAIDRefType" use="optional" />
  <attribute ref="xml:lang" use="optional" />
</complexType>

```

G.1.4 Extended On-demand decomposed binary locator

An Extended On-demand decomposed binary locator is introduced in order to provide the necessary parameters for pull download services. The Extended On-demand decomposed binary locator is based on the On-demand decomposed binary locator defined in ETSI TS 102 323 [59], clause 7.3.2.3.5.

The locator format for the Extended On-demand decomposed binary locator is 0x04. The syntax of the Extended On-demand decomposed binary locator is a superset of the On-demand decomposed binary locator to include CDS-based service modes.

The syntax of the Extended On-demand decomposed binary locator is defined in Table G.2.

Table G.2: Extended On-demand decomposed binary locator

Syntax	No. of bits	Identifier
extended_on-demand_decomposed_binary_locator() {		
reserved	6	uimsbf
availability_start_date	9	uimsbf
availability_end_date	9	uimsbf
availability_start_time	16	uimsbf
availability_end_time	16	uimsbf
content_version	8	uimsbf
expiry_time	16	uimsbf
expiry_date	9	uimsbf
reserved	1	uimsbf
delivery_mode	1	bslbf
Early_playout	1	bslbf
URI_length	12	uimsbf
for (i=0; i<URI_length; i++) {		
URI_byte	8	uimsbf
}		
}		

delivery_mode: The delivery mode for the content. The supported modes are:

0: Streaming

1: Download

The same semantics as specified in clause G.1.1.1 shall apply.

If the delivery_mode is 0, i.e. streaming mode, then the semantics for the fields shall be identical to the ones specified in ETSI TS 102 323 [59], clause 7.3.2.3.5. The **content_version**, **early_playout**, **expiry_date** and **expiry_time** fields shall be set to 0 and shall be ignored by the receiver.

If the delivery_mode is 1, i.e. download mode, then the following semantics apply:

availability_start_date: The first date on which the on-demand content pointed to by this locator becomes available download delivery. This field uses Universal Co-ordinated Time (UTC) as the time reference. It shall be encoded as the number of days from the beginning of the year indicated by the year_offset field in the enclosing structure. The value zero indicates the 1st of January of that year.

NOTE 1: The size of this field allows the encoded date to extend into the year following that encoded in the year_offset field.

availability_end_date: The first date on which the content pointed to by this locator is no longer available for download delivery. This field uses Universal Co-ordinated Time (UTC) as the time reference. It shall be encoded as the number of days from the beginning of the year indicated by the year_offset field in the enclosing structure. The value zero indicates the 1st of January of that year.

NOTE 2: The size of this field allows the encoded date to extend into the year following that encoded in the year_offset field.

availability_start_time: The time at which the on-demand content pointed to by this locator becomes available for download delivery. This field uses UTC as the time reference. This is encoded as the number of 2 s periods since midnight.

availability_end_time: The first time at which the on-demand content pointed to by this locator is no longer available for download delivery. This field uses UTC as the time reference. This is encoded as the number of 2 s periods since midnight.

NOTE 3: The duration of the on-demand content is signalled elsewhere in the TV-Anytime metadata and therefore does not need to be encoded in the locator.

content_version: The version of the downloadable content. The version number counts from 0 to 255 with an overflow from 255 to 0. The receiver shall interpret this field in the same way as the ContentVersion attribute specified in clause G.1.1.

early_playout: This flag indicates if the content play out can start while the download is still ongoing.

early_playout = "1": play out may start before the content item is completely downloaded.

early_playout = "0": play out shall not start before the content items is completely downloaded

expiry_date: The date on which the on-demand content pointed to by this locator expires and shall be deleted from the local storage of the HNED (see clause 10.7). This field uses Universal Co-ordinated Time (UTC) as the time reference. It shall be encoded as the number of days from the beginning of the year indicated by the year_offset field in the enclosing structure. The value zero indicates the 1st of January of that year.

NOTE 4: The size of this field allows the encoded date to extend into the year following that encoded in the year_offset field.

expiry_time: The time at which the on-demand content pointed to by this locator expires and shall be deleted from the local storage of the HNED (see clause 10.7). This field uses UTC as the time reference. This is encoded as the number of 2-second periods since midnight.

URI_length: The number of URI_bytes present in the following field.

URI_bytes: A sequence of bytes representing a URI compliant string. The string shall include a valid URI scheme at the start. The URI points to a download session description according to clause 10.3.2.

G.1.5 ProgramURL and Locator URIs for files located on CDS HNED storage

Media files being part of content items located on the CDS HNED storage (e.g. after a successful push download) shall be referenced from the BCG metadata (e.g. Program URL of OnDemandProgramType) and locators (e.g. URI locator, URI of Extended On-demand decomposed binary locator) by using the URI scheme defined in clause 10.3.3.

G.2 SDP syntax

G.2.0 General

This clause defines the SDP syntax of the CDS session descriptions parameters defined in clause 10.5.3. The SDP syntax is defined based on IETF RFC 4566 [75]. CDS specific usage of the standard SDP parameters defined in IETF RFC 4566 [75] and new CDS specific parameters are defined.

For unicast download sessions the SDP grouping framework as defined in IETF RFC 3388 [81] is used if alternative server locations for a file have to be defined. A new CDS specific semantic for groups is introduced. FLUTE specific SDP parameters for multicast download sessions are based on the definitions in ETSI TS 102 472 [65], clause 6.1.3.

G.2.1 SDP message structure

A single SDP message contains the description for a single CDS download session of a content item, which includes one or more files to be downloaded. The SDP message provides all the necessary information to locate and download these files. A CDS download session is completed when all the referenced files have been downloaded.

The SDP starts with a session level section followed by one or more media descriptions as defined below. The order of the lines shall be used as defined in IETF RFC 4566 [75].

G.2.2 General parameters

G.2.3.0 Mapping to standard SDP parameters

Clause 10.5.3 defines general parameters that have to be supported for CDS. They apply to any type of CDS download session. This clause defines how they are mapped to the standard SDP parameters in Table G.3. In addition new CDS specific SDP parameters are defined.

Table G.3: CDS usage of standard SDP parameters

SDP Line	IETF RFC 4566 [75] attribute definition	DVB CDS usage
Protocol Version	v=0	Mandatory as in IETF RFC 4566 [75]
Origin	o=<username> <sess-id> <sess-version> <nettype> <addrtype> <unicast-address>	mandatory <username> is set to the Service-Provider-ID <sess-id> is set to the Download-Session-ID <sess-version> is set to the Download-Session-Version <nettype> is set to "IN" <addrtype> is set to "IP4" or to "IP6" <unicast-address> as in IETF RFC 4566 [75]
Session Name	s=<session-name>	Mandatory as in IETF RFC 4566 [75]
Session Description	i=<session-description>	optional as in IETF RFC 4566 [75]
URI	u=<URI>	not used
Email Address	e=<email-address>	not used
Phone Number	p=<phone-number>	not used
Connection Data	c=<nettype> <addrtype> <connection address>	mandatory <nettype> is set to "IN" <addrtype> is set to "IP4" or to "IP6" <connection-address> see unicast and multicast download parameters for specific usage

SDP Line	IETF RFC 4566 [75] attribute definition	DVB CDS usage
Bandwidth	b=<bwtype>:<bandwidth>	optional see multicast download parameters below for specific usage
Timing	t=<start-time> <stop-time>	mandatory The parameter provides the Download-Session-Time-Information.
Repeat Times	r=<repeat interval> <active duration> <offsets from start-time>	not used
Time Zone	z=<adjustment time> <offset> <adjustment time> <offset>	not used
Encryption Keys	k=<method>:<encryption key>	not used
Attributes	a=<attribute>:<value>	None of the standard attributes defined in IETF RFC 4566 [75] are used. Grouping specific attributes as defined in IETF RFC 3388 [81] are used. For CDS specific attributes see below
Media description	m=<media> <port> <proto> <fmt> ...	mandatory see unicast and multicast download parameters for specific usage

NOTE: The session name and session description can be freely defined within the scope of their definitions in IETF RFC 4566 [75].

G.2.3.1 SP domain, download session ID and download session version

The SP name, download session ID and download session version shall be provided at the session level.

The <username> field of the "o=" line is used for the Service-Provider-Domain.

The <sess-id> field of the "o=" line is used for the Download-Session-ID.

The <sess-version> field of the "o=" line is used for the Download-Session-Version.

The usage of the attribute is:

For IPv4 usage: o=<Service-Provider-Domain> <Download-Session-ID> <Download-Session-Version> IN IP4 <unicast-address>

For IPv6 usage: o=<Service-Provider-Domain> <Download-Session-ID> <Download-Session-Version> IN IP6 <unicast-address>

<unicast-address>: IPv4 address or IPv6 address or fully qualified domain name of the server that generated the session

G.2.3.2 Content item format

One content item format parameter should be defined at the session level. The Content-item-format is specified by the following syntax:

```
Content-item-format="a=x-dvb-cds-content-item-format:" c-format
c-format="0" | "1" | "2" | "3"
0: Defined by Content-Type of first file in the list of files in the content item description
1: MPEG-2 Transport Stream
2: MPEG-2 Transport Stream with associated BCG metadata
3: MPEG-2 Transport Stream encapsulated in DVB File Format
```

The usage of the attribute is:

```
a=x-dvb-cds-content-item-format:<Content-Item-Format>
<Content-Item-Format>: format of the content item
```

G.2.3.3 Download session mode

Exactly one download session mode parameter shall be defined at the session level. The Download-Session-Mode is specified by the following syntax:

```
Download-session-mode="a=x-dvb-cds-mode:" d-mode
d-mode="SMD" | "CMD" | "UD"
SMD: Scheduled Multicast Download
CMD: Carousel Multicast Download
UD: Unicast Download
```

The usage of the attribute is:

```
a=x-dvb-cds-mode:< Download-Session-Mode>
< Download-Session-Mode>: mode of download session
```

G.2.3.4 Download session time information

Download session time information shall be provided at the session level. The "t=" line is used to provide Download-Session-Time-Information.

The usage of the attributes is as defined in IETF RFC 4566 [75].

```
t=<Download-Session-Time-Information@Start-Time> [<Download-Session-Time-Information@End-Time>]
```

G.2.3.5 Reception reporting server

One or more reception reporting servers can be provided at the session level. The Reception-Reporting-Server-URI is specified by the following syntax:

```
Reception-Reporting-Server-URI="a=x-dvb-cds-rr-server:" uri
uri=Uniform Resource Identifier as defined in IETF RFC 3986 [79]
```

The usage of the attribute is:

```
a=x-dvb-cds-rr-server:<Reception-Reporting-Server-URI>
```

One "a=x-dvb-cds-rr-server:" line shall be provided per reception reporting server.

G.2.3.6 Reception reporting mode

Reception reporting mode can be provided at the session level. It is specified by the following syntax:

```
Reception-Reporting-Mode="a=x-dvb-cds-rr-mode:" rr-mode
rr-mode="0" | "1" | "2"
0: Content item reporting only
1: Content item and file reporting
2: Content item, file and chunk reporting
```

The usage of the attribute is:

```
a=x-dvb-cds-rr-mode:<Reception-Reporting-Mode>
```

G.2.3.7 Reception reporting offset time and random time period

Reception reporting offset time and random time period can be provided at the session level. They are specified by the following syntax:

```
Reception-Reporting-Time="a=x-dvb-cds-rr-time:" dtime [SP dtime]
dtime= integer representing time in milliseconds
```

The usage of the attribute is:

```
a=x-dvb-cds-rr-time:<Reception-Reporting-Offset-Time> <Reception-Reporting-Random-Time-Period>
```

G.2.4 Unicast download parameters

G.2.4.0 Introduction

This clause defines the SDP parameters used for the description of a unicast content download session. First the SDP syntax for the unicast specific CDS download session parameters as defined in clause 10.5.3 is provided. The use of grouping is defined in clause G.2.4.8. The structure of a SDP message for a multicast download session is defined in clause G.2.4.9.

G.2.4.1 File Reference

The files that are downloaded are defined by their <path-absolute> *relative reference*.

The file reference absolute is specified by the following syntax:

```
File-Reference="a=x-dvb-cds-file-reference:" Path-Absolute
Path-Absolute= <path-p-absolute> relative reference as defined in clause 10.5.2.
```

The attribute shall be provided for each file in the media description. In case grouping is used the attribute is defined in the primary media description (see clause G.2.4.8).

The usage of the attribute is:

```
a=x-dvb-cds-file-reference:<File-Reference>
```

G.2.4.2 File Length

The length of a file is specified by the following syntax:

```
File-Length="a=x-dvb-cds-file-length:" Length
Length = integer defining the length in bytes
```

In case of single server file download the attribute may be provided for the file in the media description. In case of multiple server file download the attribute shall be provided for the file in the media description. In case grouping is used the attribute is defined in the primary media description (see clause G.2.4.8).

The usage of the attribute is:

```
a=x-dvb-cds-file-length:<File-Length>
```

G.2.4.3 File Digest

The MD5 digest of a file is specified by the following syntax:

```
File-Digest="a=x-dvb-cds-file-digest:" digest
digest = base64
```

The attribute may be provided for the file in the media description. In case grouping is used the attribute is defined in the primary media description (see clause G.2.4.8).

The usage of the attribute is:

```
a=x-dvb-cds-file-digest:<File-Digest>
```

G.2.4.4 Chunk Length

The common length of the chunks of a file is specified by the following syntax:

```
Chunk-Length="a=x-dvb-cds-chunk-length:" Length
Length = integer defining the length in bytes
```

In case of multiple server file download the attribute shall be provided for the file in the media description. The attribute is not used for single server file download. The attribute is defined in the primary media description (see clause G.2.4.8).

The usage of the attribute is:

```
a=x-dvb-cds-chunk-length:<Chunk-Length>
```

G.2.4.5 Chunk Digest

The MD5 digest of a chunk and its number (position within the file counted from 1 to n) is specified by the following syntax:

```
Chunk-Digest="a=x-dvb-cds-chunk-digest:" int digest
digest-list = digest 1*[SP digest]
```

In case of multiple server file download the attribute may be provided for each chunk of the file in the media description. The attribute is not used for single server file download. The attribute is defined in the primary media description (see clause G.2.4.8).

The usage of the attribute is:

```
a=x-dvb-cds-chunk-digest:<Chunk-Number> <Chunk-Digest>
```

G.2.4.6 Server Base URI and File Content Type

The base URI of a server location where the file is available shall be provided by c-line and the m-line.

The <connection address> field of the c-line shall be set to the server address part of the base URI (IPv4 address or IPv6 address or fully qualified domain name). The <nettype> field of the c-line shall be set fixed to "IN". The <addrtype> field of the c-line shall be set fixed to "IP4" or to "IP6".

The <port> field of the m-line shall be set to the optional port part of the base URI. In case the port is not provided it is set to the HTTP default port of 80. The <proto> field of the m-line shall be set fixed to "TCP/HTTP". The <media> field shall be set to the main media type of the content type of the file as defined (e.g. video, application). The <fmt> field shall be set to the subtype of the content type of the download file as defined in clause 10.4.2 (e.g. mp2t, xml). In case the mime type is provided the fields shall be set to "*".

The attributes shall be provided for each file in the media description. In case several server locations are provided for a file grouping shall be used as defined in clause G.2.4.8.

The usage of the attributes is:

```
For IPv4 usage: c=IN IP4 <Server-Base-URI@Address>
For IPv6 usage: c=IN IP6 <Server-Base-URI@Address>

m=<File-Content-Type@MainTyp> <Server-Base-URI@Port> TCP/HTTP <File-Content-Type@Subtype>
```

G.2.4.7 Available Chunk List

The list of available chunks of a file at a server location is specified by the following syntax:

```
Available-Chunk-List="a=x-dvb-cds-available-chunk-list:" chunk-list
chunk-list = chunk|chunk-range 1*[SP chunk|chunk-range]
chunk-range = chunk "-" chunk
Chunk = integer
```

In case of multiple server file download the attribute may be provided for each server location. In case it is not provided all chunks of the file are available at that server location. The attribute is not used for single server file download. The attribute is defined in each media description.

The usage of the attribute is:

```
a=x-dvb-cds-available-chunk-list:<Available-Chunk-List>
```

G.2.4.8 Grouping of media lines

The grouping framework as defined in IETF RFC 3388 [81] shall be used in order to define alternative or multiple server locations for a file that has to be downloaded. For each server location a media description shall be used and shall be identified by the mid-attribute as defined in IETF RFC 3388 [81]. The media descriptions that belong to a single file are grouped together using the group-attribute as defined in IETF RFC 3388 [81]. A new semantic "X-DVB-CDS-AS" (alternative server) is defined for the group-attribute. It indicates that the media descriptions of a group define alternative server locations. This can be alternative servers for a single server download or locations of file chunks for multiple server downloads.

The first media description of a group is the primary media description and contains parameters that apply for the whole group (e.g. File-Absolute-Path).

If at least one file has alternative server locations grouping has to be used for all files in the SDP message.

Each group is defined by a group attribute at the session level. The group attributes lists the media descriptions that are members of the group.

```
a=group:X-DVB-CDS-AS 1*<id>
id: token
```

The mid-attribute has to be defined for each media description if grouping is used. It provides a unique identifier for each media description.

```
a=mid:<id>
id: token
```

G.2.4.9 SDP message structure for unicast download session

Each file that has to be downloaded within the session is defined by a media description or a group of media descriptions. Grouping is used in case alternative server locations are provided for a single server file download or for a multiple server file download. File absolute path, mime type, file length, file digest, file chunk length and file chunk digest information is provided per file in the media description. In case of grouping they are provided in the primary media description. Server base URI and available chunk list information is provided per media description.

A unicast download SDP starts with session level fields in the order listed below where the values for origin (o=) and connection (c=) slightly differ depending on whether IPv4 addresses or IPv6 addresses are being used.

```
v=0
For IPv4:o=<Service-Provider-Domain> <Download-Session-ID> <Download-Session-Version> IN IP4
<unicast-address>
For IPv6:o=<Service-Provider-Domain> <Download-Session-ID> <Download-Session-Version> IN IP6
<unicast-address>
s=<session name>
i=<session description> (optional)
a=x-dvb-cds-content-item-format:<Content-Item-Format>
a=x-dvb-cds-mode:UD
a=x-dvb-cds-rr-server:<Reception-Reporting-Server-URI> (0..n)
```

```
a=group:X-DVC-CDS-AS 1*<id> (0..n)
t=<Download-Session-Time-Information@Start-Time> [<Download-Session-Time-Information@End-Time>]
```

The session level information is followed by one or more media descriptions, one for each file and server location, with fields in the following order:

Media description without grouping and primary media description of a group:

```
m=<File-Content-Type@MainTyp> <Server-Base-URI@Port> TCP/HTTP <File-Content-Type@Subtype>
a=x-dvb-cds-file-reference:<File-Reference>
For IPv4: c=IN IP4 <Server-Base-URI@Address>
For IPv6: c=IN IP6 <Server-Base-URI@Address>
a=mid:<id> (in case of grouping)
a=x-dvb-cds-file-length:<File-Length> (optional for single server file download)
a=x-dvb-cds-file-digest:<File-Digest> (optional)
a=x-dvb-cds-file-chunk-length:<File-Chunk-Length> (not used for single server file download)
a=x-dvb-cds-file-chunk-digest:<File-Chunk-Digest> (optional for multiple server file download)
a=x-dvb-cds-available-chunk-list:<Available-Chunk-List> (optional for multiple server file download)
```

All other media descriptions of a group:

```
m=<File-Content-Type@MainTyp> <Server-Base-URI@Port> TCP/HTTP <File-Content-Type@Subtype>
For IPv4: c=IN IP4 <Server-Base-URI@Address>
For IPv6: c=IN IP6 <Server-Base-URI@Address>
a=mid:<id>
a=x-dvb-cds-available-chunk-list:<Available-Chunk-List> (optional)
```

Example of a unicast download session description with a single server file download of two files with no alternative server locations and no reception reporting using IPv4 addresses:

```
v=0
o=provider.org 1234 1 IN IP4 135.27.66.45
s= Example1
i= Example session 1
a=x-dvb-cds-content-item-format:1
a=x-dvb-cds-mode:UD
t= 3034423619 3042462419
m=video 80 TCP/HTTP mp2t
c=IN IP4 server.provider.org
a=x-dvb-cds-file-reference:/content/video1.mp2t
a=x-dvb-cds-file-length:160607052
a=x-dvb-cds-file-digest: Q2h1Y2sgSW50ZWdyaxR5IQ==
m=application 80 TCP/HTTP xml
c=IN IP4 server.provider.org
a=x-dvb-cds-file-reference:/content/meta1.xml
```

Example of a unicast download session description with a multiple server and a single server file download with two alternative server locations and reception reporting using IPv4 addresses:

```
v=0
o=provider.org 1240 1 IN IP4 135.27.66.45
s= Example2
i= Example session 2
a=x-dvb-cds-content-item-format:1
a=x-dvb-cds-mode:UD
a=x-dvb-cds-rr-server:rr1.provider.org
a=x-dvb-cds-rr-server:rr2.provider.org
a=group:X-DVB-CDS-AS 1 2
a=group:X-DVB-CDS-AS 3 4
t= 3034423619 3042462419
m=video 80 TCP/HTTP mp2t
c=IN IP4 server1.provider.org
a=mid:1
a=x-dvb-cds-file-reference:/content/video1.mp2t
a=x-dvb-cds-file-length:160607052
a=x-dvb-cds-file-digest: Q2h1Y2sgSW50ZWdyaxR5IQ==
a=x-dvb-cds-file-chunk-length:50000000
a=x-dvb-cds-file-chunk-digest: We14fgTT5DSwqGH44fGzr3== aa3f4GHj76fGHCB86AqwDD==
asdd23EsWQ65DFVmLkkJS8== ASq34fDD5gRGdSSw34D214==
a=x-dvb-cds-available-chunk-list:1-2 3
m=video 80 TCP/HTTP mp2t
a=mid:2
c=IN IP4 server2.provider.org
a=x-dvb-cds-available-chunk-list:1 3 4
m=application 80 TCP/HTTP xml
c=IN IP4 server3.provider.org
```

```
a=mid:3
a=x-dvb-cds-file-reference:/content/metal.xml
m=application 80 TCP/HTTP xml
c=IN IP4 server4.provider.org
a=mid:4
```

G.2.5 Multicast download parameters

G.2.5.0 Introduction

This clause defines the SDP parameters used for the description of a multicast content download session. The same SDP structure is used for scheduled and carousel multicast download. FLUTE is used for multicast download and the SDP FLUTE parameters defined in ETSI TS 102 472 [65], clause 6.1.3 are used for the description of the FLUTE specific information. First the SDP syntax for the multicast specific CDS download session parameters as defined in clause 10.5.3 is provided. The structure of a SDP message for a multicast download session is defined in clause G.2.5.13.

G.2.5.1 File Reference

For each file within the Flute session that has to be downloaded the <path-absolute> *relative reference* (see clause 10.5.2) of the file can be provided at the session level. If no such parameter is provided all files of the Flute session have to be downloaded to the HNED. The same "a=x-dvb-cds-file-REFERENCE :" attribute as defined in clause G.2.4.1 for the unicast file reference is used.

Note, that in contrast to the definition in clause G.2.4.1 the line is used at the session level and all files indicated by such lines have to be downloaded.

The usage of the attribute is:

```
a=x-dvb-cds-file-reference:<File-Reference>
```

G.2.5.2 Multicast channel source address

The source address of the FLUTE multicast channels is provided at the session level by the "a=source-filter" attribute as defined in ETSI TS 102 472 [65], clause 6.1.13.1.1. Depending on the usage of IPv4 addresses or IPv6 addresses, this definition slightly differs:

```
For IPv4 usage: a=source-filter: incl IN IP4 * <IP-Source-Address>
For IPv6 usage: a=source-filter: incl IN IP6 * <IP-Source-Address>
```

G.2.5.3 Transport Session Identifier

The transport session identifier is provided at the session level by the "a=flute-tsi:" attribute as defined in ETSI TS 102 472 [65], clause 6.1.13.1.4.

```
a=flute-tsi:<Transport-Session-Identifier>
```

G.2.5.4 FEC Encoding ID

The FEC encoding ID is provided at the session level by the "a=FEC-declaration:" attribute as defined in ETSI TS 102 472 [65], clause 6.1.13.1.6. The fec-inst-id parameter is not used. The fec-ref parameter is set to "0" as the "a=fec:" line per media is not supported.

If the FEC encoding ID is not provided the compact no-code FEC scheme is assumed.

```
a=FEC-declaration:0 <FEC-Encoding-ID>
```

G.2.5.5 Numbers of channels

The number of channels is provided at the session level by the "a=flute-ch:" attribute as defined in ETSI TS 102 472 [65], clause 6.1.13.1.2.

```
a=flute-ch:<Number-Of-Channels>
```

G.2.5.6 Multicast Address

The address of each multicast channel is provided by a c-line per media description. The <nettype> and <addrtype> fields of the c-line are able to support either IPv4 addresses or IPv6 addresses.

```
For IPv4 usage: c=IN IP4 <IP-Multicast-Address>
For IPv6 usage: c=IN IP6 <IP-Multicast-Address>
```

G.2.5.7 Multicast Port Number

The port number of each multicast channel is provided by a m-line per media description. The <media>, <proto> and <fmt> field of the m-line are fixed Flute specific values.

```
m=application <IP-Multicast-Port-Number> flute/udp *
```

G.2.5.8 Maximum bandwidth

The maximum bandwidth used by each multicast channel can be provided by a b-line per media description. The TIAS bandwidth modifier as defined in IETF RFC 3890 [80] shall be used.

```
b=TIAS <Max-Bandwidth>
```

G.2.5.9 Completion poll response server address and port number

Completion poll information is provided at the session level. The completion poll response server address and port number are provided by the following syntax:

```
Completion-Poll-Server="a=x-dvb-cds-cp-server:" nettype SP addrtype SP unicast-address SP port
    nettype=network type; fixed value "IN" as only IP networks are supported by the current
        specification
    addrtype=address type; "IP4" or "IP6"    unicast-address=IP address of completion poll response
    server
    port=server port for completion poll response
```

The usage of the attribute is for IPv4 addresses:
`a=x-dvb-cds-cp-server:IN IP4 <Completion-Poll-Response-Server-Address> <Completion-Poll-Response-Server-Port-Number>`

The usage of the attribute is for IPv6 addresses:
`a=x-dvb-cds-cp-server:IN IP6 <Completion-Poll-Response-Server-Address> <Completion-Poll-Response-Server-Port-Number>`

G.2.5.10 Recovery server base URI

One or more recovery server base URIs can be provided at the session level. The recovery server base URI is provided by the following syntax:

```
Recovery-Server="a=x-dvb-cds-rec-server:" uri
    uri= Uniform Resource Identifier as defined in IETF RFC 3986 [79]
```

The usage of the attribute is:

```
a=x-dvb-cds-rec-server:<Recovery-Server-Base-URI>
```

One "a=x-dvb-cds-recovery-server:" line shall be provided per recovery server.

G.2.5.11 Recovery mode

Recovery mode can be provided at the session level. It is provided by the following syntax:

```
Recovery-Mode="a=x-dvb-cds-rec-mode:" rec-mode
    rec-mode="0" | "1"
    0: CDS file repair mode
    1: IPDC like file repair mode
```

The usage of the attribute is

```
a=x-dvb-cds-rec-mode:<Recovery-Mode>
```

G.2.5.12 Recovery offset time and random time period

Recovery offset time and random time period can be provided at the session level. They are specified by the following syntax:

```
Recovery-Time="a=x-dvb-cds-rec-time:" dtime [SP dtime]
dtime= integer representing time in milliseconds
```

The usage of the attribute is:

```
a=x-dvb-cds-rec-time:<Recovery-Offset-Time> <Recovery-Random-Time-Period>
```

G.2.5.13 SDP message structure for multicast download session

The list of files that have to be downloaded from the FLUTE session as part of the CDS session is provided by "a=x-dvb-cds-file :" lines at the session level, one line per file. If this information is not provided all files of the FLUTE session have to be downloaded.

Each multicast channel of the FLUTE session is defined by a media description which starts with an "m=" line and is terminated by either the next "m=" line or by the end of the session description.

A multicast download SDP starts with session level fields in the order listed below where the values for origin (o=), attributes (a=) and connection (c=) slightly differ depending on whether IPv4 addresses or IPv6 addresses are being used.

v=0

```
For IPv4: o=<Service-Provider-Domain> <Download-Session-ID> <Download-Session-Version> IN IP4
<unicast-address>
For IPv6: o=<Service-Provider-Domain> <Download-Session-ID> <Download-Session-Version> IN IP6
<unicast-address>
s=<session name>
i=<session description> (optional)
a=x-dvb-cds-content-item-format:<Content-Item-Format>
a=x-dvb-cds-mode:CMD|SMD
a=x-dvb-cds-rr-server:<Reception-Reporting-Server-URI> (0..n)
a=x-dvb-cds-rr-time:<Reception-Reporting-Offset-Time> <Reception-Reporting-Random-Time-Period>
(optional)
For IPv4: a=source-filter: incl IN IP4 * <IP-Source-Address>
For IPv6: a=source-filter: incl IN IP6 * <IP-Source-Address>
a=flute-tsi:<Transport-Session-Identifier>
a=FEC-declaration:0 <FEC-Encoding-ID> (optional)
a=flute-ch:<Number-Of-Channels>
For IPv4: a=x-dvb-cds-cp-server:IN IP4 <Completion-Poll-Response-Server-Address> <Completion-Poll-
Response-Server-Port-Number> (optional)
For IPv6: a=x-dvb-cds-cp-server:IN IP6 <Completion-Poll-Response-Server-Address> <Completion-Poll-
Response-Server-Port-Number> (optional)
a=x-dvb-cds-rec-server:<Recovery-Server-Base-URI> (0..n)
a=x-dvb-cds-rec-mode:<Recovery-Mode> (optional)
a=x-dvb-cds-rec-time:<Recovery-Offset-Time> <Recovery-Random-Time-Period> (optional)
a=x-dvb-cds-file-reference:<File-Reference> (0..n)
t=<Download-Session-Time-Information@Start-Time> [<Download-Session-Time-Information@End-Time>]
```

The session level information is followed by one or more media descriptions, one for each multicast channel, with fields in the following order:

```
m=application <IP-Multicast-Port-Number> flute/udp *
For IPv4: c=IN IP4 <IP-Multicast-Address>
For IPv6: c=IN IP6 <IP-Multicast-Address>
b=TIAS <Max-Bandwidth> (optional)
```

Example of a carousel multicast download session with 2 FLUTE channels without reception reporting and file repair using IPv4 addresses. All files of the FLUTE sessions are downloaded:

```
v=0
o=provider.org 5678 2 IN IP4 135.27.66.45
s= Example3
```

```
i= Example session 3
a=x-dvb-cds-content-item-format:0
a=x-dvb-cds-mode:CMD
a=source-filter: incl IN IP4 * 135.27.66.40
a=flute-tsi:1234765
a=flute-ch:2
t= 3034423619 3042462419
m=application 1200 flute/udp *
c=IN IP4 227.124.5.3
b=TIAS 500
m=application 1200 flute/udp *
c=IN IP4 227.124.5.4
b=TIAS 1000
```

Example of a scheduled multicast download session with 3 FLUTE channels with Raptor FEC, reception reporting and file repair using IPv4 addresses. The listed files are downloaded:

```
v=0
o=provider.org 6123 1 IN IP4 135.27.66.45
s= Example4
i= Example session 4
a=x-dvb-cds-content-item-format:1
a=x-dvb-cds-mode:SMD
a=x-dvb-cds-rr-server:r1.provider.org
a=x-dvb-cds-rr-server:r2.provider.org
a=x-dvb-cds-rr-time:100 50
a=source-filter: incl IN IP4 * 135.27.66.40
a=flute-tsi:123456
a=FEC-declaration:0 1
a=flute-ch:3
a=x-dvb-cds-cp-server:IN IP4 135.27.60.4 300
a=x-dvb-cds-rec-server:recl.provider.org
a=x-dvb-cds-rec-mode:0
a=x-dvb-cds-rec-time:200 30
a=x-dvb-cds-file-reference:/content/video1.mp2t
a=x-dvb-cds-file-reference:/content/meta1.xml
t= 3034423619
m=application 1200 flute/udp *
c=IN IP4 227.124.6.3
b=TIAS 500
m=application 1200 flute/udp *
c=IN IP4 227.124.6.4
b=TIAS 1000
m=application 1200 flute/udp *
c=IN IP4 227.124.6.5
b=TIAS 1000
```

G.3 DVB-MCAST URI scheme

G.3.0 Overview

The DVB-MCAST URI scheme is defined to identify resources provided via an IP multicast channel. It provides a means to locate the multicast channel carrying the resource and also to specify information concerning the application layer transport protocol which will be used to carry the data over that multicast channel (e.g. SAP, DVBSTP).

Clause G.3.1 defines the basic scheme. Clauses G.3.2 and G.3.3 define the specific extensions and usage of the scheme for referencing download session descriptions as defined in clause 10.5 using the DVBSTP and SAP protocols.

Additional application layer transport protocols specific extensions and usage might be defined in the future or in other specifications that make use of the DVB-MCAST URI scheme.

G.3.1 Basic DVB-MCAST URI scheme

The basic DVB-MCAST URI scheme defined in this clause provides the client with the information required to join an IP multicast channel. Only the minimum set of parameters required by a multicast connection protocol are included in the scheme. By optionally providing the type of the application layer transport protocol, the client will be able to provide the data from the multicast channel to the appropriate application. The scheme might be extended for application layer transport protocol specific usage.

The basic DVB-MCAST URI scheme is defined as follows:

```
'dvb-mcast:// [ src-host '@' ] mcast-addr ':' port ['?payload=' PayloadID]
src-host          = source host (for source specific multicast)
mcast-addr       = multicast address
port              = port
PayloadID         = payload-type
payload-type      = "sap" | "dvbstp"
```

The mcast-addr shall specify the multicast address the client has to join and the port shall specify the UDP destination port when receiving the multicast data stream.

The src-host is an optional syntax element referring to the unicast IP address of the source of the multicast data. This is only meaningful in case Source Specific Multicast (SSM) as defined in IETF RFC 4607 [104] is supported.

G.3.2 DVB-MCAST URI scheme for DVBSTP

The basic DVB-MCAST URI scheme defined in clause G.3.1 is extended in order to reference DVBSTP protocol specific elements, namely specific SPs, PTs and segments transported. The DVBSTP SP ID, Payload ID and Segment ID are defined as part of the Query component of the URI as they provide non-hierarchical information to locate a specific segment distributed on the DVBSTP multicast channel.

Note that a session version number is not provided in the URI scheme as always the latest version of a segment distributed over the multicast channel shall be used.

In order to reference a specific session description within the XML segment the CDS Download Session ID can be provided within the fragment part of the URI. The fragment syntax is not specific to the DVBSTP delivery but to the delivered media, the CDS XML session description in this case.

The DVB-MCAST URI scheme for DVBSTP is defined as follows:

```
'dvb-mcast:// [ src-host '@' ] mcast-addr ':' port '?payload=dvbstp' [&service-provider='
ServiceProviderID'] ['&dvbstp-payload=' DVBSTPPayloadID] ['&segment=' SegmentID] ['#? dvb-cds-
session-id=' Download-Session-ID]

src-host          = source host (for source specific multicast)
mcast-addr       = multicast address
port              = port
ServiceProviderID = IP address
DVBSTPPayloadId = 2*2 HEXDIG; any hex number from 0x00 to 0xff
SegmentId        = 4*4 HEXDIG; any hex number from 0x0000 to 0xffff
Download-Session-ID = DecimalString
```

In order to access the specified resource the device has to join the multicast group provided by the mcast-addr and port and optional src-host in the URI. It compares all the parameters provided in the query component of the URI against the corresponding DVBSTP protocol fields and extracts all the segments that match. The parameters in the query component of the URI are optional. In case a parameter is not provided the corresponding field in the DVBSTP protocol will not be used for the comparison.

In case a Download Session ID is provided in the fragment component of the URI, the device has to search all the extracted segments for the session description with the specific Download Session ID.

G.3.3 DVB-MCAST URI scheme for SAP

The basic DVB-MCAST URI scheme defined in clause G.3.1 is extended in order to reference SDP data provided via the SAP protocol. The PT is set to 'sap'. No further information has to be provided in the query part of the URI as no further payload identification is provided by SAP.

In order to reference a specific session description within the SDP information the CDS Download Session ID can be provided within the fragment part of the URI. The fragment syntax is not specific to the SAP delivery but to the delivered media, the SDP session description in this case.

The DVB-MCAST URI scheme for SAP is:

```
'dvb-mcast:// [ src-host '@' ] mcast-addr ':' port '?payload=sap' ['#? sdp-session-id=' Download-
Session-ID]

Download-Session-ID = unsigned Integer
```

In case a Download Session ID is provided in the fragment component of the URI, the device has to search all the SDP information delivered over the multicast channel for the session description with the specific Download Session ID.

Annex H (normative): SDP syntax for SRM announcement services

H.0 General

This annex defines the SDP syntax for the SAP multicast SRM announcement service defined in clause 12.4.2.2. The information provided by SDP is similar to the one provided by the SRM Download Record defined in Table 32.

The SDP syntax is defined based on IETF RFC 4566 [75]. SRM specific usage of the standard SDP parameters defined in IETF RFC 4566 [75] and new SRM specific parameters are defined.

FLUTE specific SDP parameters for multicast download sessions are based on the definitions in ETSI TS 102 472 [65], clause 6.1.3.

The Augmented BNF Syntax as defined in IETF RFC 5234 [27] is used to define new parameters.

H.1 SDP message structure

A single SDP message contains the description for a single SRM Download Service. The SDP message provides all the necessary information to access the SRM Download Service, the CP System IDs supported by the Download Service and the service version.

The SDP starts with a session level section followed by a single media description. The order of the lines shall be as defined in IETF RFC 4566 [75].

H.2 General Parameters

H.2.0 Mapping to standard SDP parameters

Table 32 lists the parameters that have to be provided for SRM Download Services.

This clause defines how the parameters that are not specific for a SRM download mode are mapped to the standard SDP parameters in Table H.1. In addition new SRM specific SDP parameters are defined.

Table H.1: SRM usage of standard SDP parameters

SDP Line	IETF RFC 4566 [75] attribute definition	DVB CDS usage
Protocol Version	v=0	Mandatory as in IETF RFC 4566 [75]
Origin	o=<username> <sess-id> <sess-version> <nettype> <addrtype> <unicast-address>	Mandatory <username> registered domain name of the SRM download service provider <sess-id> as in IETF RFC 4566 [75] <sess-version> record version number of the SRM Download Record <nettype> is set to "IN" <addrtype> is set to "IP4" or "IP6" <unicast-address> as in IETF RFC 4566 [75]
Session Name	s=<session-name>	Mandatory as in IETF RFC 4566 [75]
Session Description	i=<session-description>	optional as in IETF RFC 4566 [75]
URI	u=<URI>	not used
Email Address	e=<email-address>	not used
Phone Number	p=<phone-number>	not used
Connection Data	c=<nettype> <addrtype> <connection address>	mandatory <nettype> is set to "IN" <addrtype> is set to "IP4" or "IP6" <connection-address> see unicast and multicast SRM download service parameters for specific usage
Bandwidth	b=<bwtype>:<bandwidth>	not used

SDP Line	IETF RFC 4566 [75] attribute definition	DVB CDS usage
Timing	t=<start-time> <stop-time>	not used
Repeat Times	r= <repeat interval> <active duration> <offsets from start-time>	not used
Time Zone	z=<adjustment time> <offset> <adjustment time> <offset>	not used
Encryption Keys	k=<method>:<encryption key>	not used
Attributes	a=<attribute>:<value>	None of the standard attributes defined in IETF RFC 4566 [75] are used. see unicast and multicast SRM download service parameters below for specific usage
Media description	M=<media> <port> <proto> <fmt>	mandatory see unicast and multicast SRM download service parameters below for specific usage

NOTE: The session ID, session name and session description can be freely defined within the scope of their definitions in IETF RFC 4566 [75].

H.2.1 Domain name and Record version number

The domain name of the SRM download service provider and record version number of the SRM Download Record (see clause 12.6.4) shall be provided by the "o=" line at the session level.

The <username> field of the "o=" line is used for the domain name.

The <sess-version> field of the "o=" line is used for the record version.

The usage of the "o=" line is:

```
For IPv4: o=<service-provider-domain> <sess-id> <record-version> IN IP4 <unicast-address>
For IPv6: o=<service-provider-domain> <sess-id> <record-version> IN IP6 <unicast-address>

<service-provider-domain>: FQDN; registered domain name of the SRM download service provider
<sess-id>: unique session ID as defined in IETF RFC 4566 [75]
<record-version>: 2 HEXDIG; SRM Download Record version number (see clause 12.6.4)
<unicast-address>: IPv4 address or IPv6 address or fully qualified domain name of the server that generated the session as defined in IETF RFC 4566 [75]
FQDN as defined in IETF RFC 4466 [75]
```

H.2.2 SRM ID

The SRM ID identifies the CP System (CP System ID and optional CP System SRM ID) and SRM file version number of the SRM that is available for download:

```
SRM-ID = "a=x-dvb-srm-id:" cp-system-id "," [cp-system-srm-id] "," [srm-file-version]

cp-system-id = 4HEXDIG; CP System ID
cp-system-srm-id = 1*256(HEXDIG HEXDIG); CP System SRM ID
srm-file-version = 2HEXDIG; SRM file version
HEXDIG as defined in IETF RFC 5234 [27]
```

The SRM ID line is included in the media section of the announcements.

A single SRM ID line shall be included in each HTTP unicast SRM download announcement. The cp-system-id and srm-file-version parameter are required. The cp-system-srm-id parameter is optional.

A Flute multicast SRM download announcement may have one more SRM ID lines. In case it has SRM ID lines it shall have a SRM ID line for each SRM file delivered by the FLUTE session. The cp-system-id parameter is required. The srm-file-version and cp-system-srm-id parameters are optional.

H.3 HTTP unicast SRM download service parameters

H.3.0 Introduction

This clause defines the SDP parameters used for the description of a HTTP unicast SRM download service.

HTTP unicast SRM download specific parameters are included in a single media section.

H.3.1 HTTP URI

For the unicast SRM download the URI of the download file has to be provided. As the URI includes the server IP address or domain name, the connection address in the "c=" line shall not be used. As the "c=" is mandatory for SDP, the connection address shall be set to "0.0.0.0" and ignored by the receiver. The "c=" line shall be part of the media description and its value differs depending on whether IPv4 addresses or IPv6 addresses are being used:

```
For IPv4: c=IN IP4 0.0.0.0
For IPv6: c=IN IP6 0.0.0.0.0.0.0.0
```

The port sub-field provided in the "m=" line shall not be used as the port is provided by the URI (if no port is provided by the URI the default port for the protocol is used). The port sub-field shall be set to "*" and ignored by the HNED. The <media> sub-field shall be set to "application", the <proto> sub-field to "HTTP/TCP" and the <fmt> sub-field to "srm". The "m=" line has the following syntax:

```
m=application * HTTP/TCP srm
```

The URI of the SRM file is specified by the following syntax:

```
SRM-File-URI = "a=x-dvb-srm-file-uri:" srm-file-uri
srm-file-uri = Uniform Resource Identifier as defined in IETF RFC 3986 [79]
```

A SRM file URI shall be provided for each HTTP unicast SRM download service.

H.3.2 Complete SDP syntax for HTTP unicast SRM Download Service

The complete SDP syntax for the announcement of a HTTP unicast SRM Download Service is as follows where the values for origin (o=), and connection (c=) slightly differ depending on whether IPv4 addresses or IPv6 addresses are being used.

```
v=0
For IPv4: o=<service-provider-domain> <sess-id> <record-version> IN IP4 <unicast-address>
For IPv6: o=<service-provider-domain> <sess-id> <record-version> IN IP6 <unicast-address>
s=<session-name>
i=<session-description>
m=application * HTTP/TCP srm
a=x-dvb-srm-id:<cp-system-id>,<cp-system-srm-id>,<srm-file-version>
For IPv4: c=IN IP4 0.0.0.0
For IPv6: c=IN IP6 0.0.0.0.0.0.0.0.0
a=x-dvb-srm-file-uri:<srm-file-uri>
```

Below is an example for a HTTP unicast SRM Download Service announcement using IPv4 addresses:

```
v=0
o=provider.org 356 2 IN IP4 135.27.66.45
s=Example1
i=Example for HTTP unicast SRM Download Service announcement
m=application * HTTP/TCP srm
a=x-dvb-srm-id:0002,,06
c=IN IP4 0.0.0.0
a=x-dvb-srm-file-uri:http://srm.provider.org/cp-system-02.dat
```

H.4 FLUTE multicast SRM download service parameters

H.4.0 Introduction

This clause defines the SDP parameters used for the description of a FLUTE multicast SRM download service.

FLUTE multicast SRM download parameters are included in a single media section.

H.4.1 FLUTE Session Version

The FLUTE session version number (see clause 12.5.2) is specified by the following syntax:

```
SRM-FLUTE-Session-Version="a=x-dvb-srm-FLUTE-session-version:" flute-session-version
    flute-session-version = 2HEXDIG; FLUTE session version (see clause 12.5.2)
    HEXDIG as defined in IETF RFC 5234 [27]
```

The FLUTE session version number is optional.

H.4.2 FLUTE Session parameters

For the multicast SRM download service FLUTE session parameters have to be provided. SDP FLUTE parameters as defined in ETSI TS 102 472 [65], clause 6.1.3 and also used for CDS multicast download sessions (see clause G.2.5) are used. As a SRM FLUTE session supports only a single multicast channel and the "Compact No-Code FEC scheme", only the following FLUTE parameters are supported:

- Multicast channel source address (see clause G.2.5.2); optional
- Transport Session Identifier (see clause G.2.5.3); required
- Multicast Address (see clause G.2.5.6); required
- Multicast Port Number (see clause G.2.5.7); required

The <media> sub-field of the "m=" line shall be set to "application", the <proto> sub-field to "FLUTE/UDP" and the <fmt> sub-field to "srm".

H.4.3 Complete SDP syntax for FLUTE multicast SRM Download Service

The complete SDP syntax for the announcement of a FLUTE multicast SRM Download Service is as follows where the values for origin (o=), attributes (a=) and connection (c=) slightly differ depending on whether IPv4 addresses or IPv6 addresses are being used.

```
v=0
For IPv4: o=<username> <sess-id> <record-version> IN IP4 <unicast-address>
For IPv6: o=<username> <sess-id> <record-version> IN IP6 <unicast-address>
s=<session-name>
i=<session-description>
m=application <IP-Multicast-Port-Number> FLUTE/UDP srm
a=x-dvb-srm-id:<cp-system-id>,<cp-system-srm-id>,<srm-file-version>
a=x-dvb-srm-id:<cp-system-id>,<cp-system-srm-id>,<srm-file-version>
.
.
.
a=x-dvb-srm-FLUTE-session-version:<flute-session-version>
For IPv4: a=source-filter: incl IN IP4 * <IP-Source-Address>
For IPv6: a=source-filter: incl IN IP6 * <IP-Source-Address>
a=flute-tsi:<Transport-Session-Identifier>
For IPv4: c=IN IP4 <IP-Multicast-Address>
For IPv6: c=IN IP6 <IP-Multicast-Address>
```

Below is an example for a FLUTE multicast SRM Download Service announcement with 3 different SRM files in the FLUTE session using IPv4 addresses:

```
v=0
o=provider.org 134 1 IN IP4 135.27.66.45
s=Example2
i=Example for FLUTE multicast SRM Download Service announcement
m=application 1200 FLUTE/UDP srm
a=x-dvb-srm-id0002,,
a=x-dvb-srm-id0012,,
a=x-dvb-srm-id003A,,
a=x-dvb-srm-FLUTE-session-version:0F
a=source-filter: incl IN IP4 * 135.27.66.40
a=flute-tsi:12345
c=IN IP4 227.124.5.4
```

Annex I (normative): Server-based Fast Channel Change for DVB-IPTV Systems

I.1 Scope

Annex I contains the specification for an optional extension to the present DVB-IPTV specification which facilitates a faster rendering when moving from one multicast LMB service to another or joining a multicast LMB service, i.e. it enables Fast Channel Change (FCC). Annex I is not a necessary part of the DVB-IPTV system, but is provided to enhance performance of an otherwise functional system.

The specification provided is not necessarily restricted to use with DVB-IPTV systems, but may be fully or partially applicable to other forms of DVB broadcast services.

In order to implement the specifications in the present document, extensions to the platform will be required in both servers and clients over and above those needed for the most basic of multicast DVB-IPTV service delivery as described in the present document. These extensions may include additions to both hardware and software capabilities. In any implementation where these extensions are not available in either the client, the server, or both, then the overall DVB-IPTV service is not affected, but the rapid switching between services is not available and the channel change time is exactly as it would have been if the basic LMB service described in the present document was provided (i.e. without FCC).

It shall be noted that a specific ordering of the MPEG-2 TS packets transported in the LMB service (PAT/PMT, ECM/EMM, etc.) may facilitate a more efficient demultiplexing, descrambling and decoding pipeline at the HNED. This applies both to the LMB service without FCC and to the LMB service enhanced with FCC. MPEG-2 TS packet ordering in the IP multicast stream is under control of the head-end, implementation-dependent and outside the scope of the present document.

I.2 Server-based FCC: detailed specification

I.2.1 Introduction

The present document describes a solution by which the typical delay for an LMB service acquisition process is reduced by means of having a DVB FCC client interact with a DVB FCC server prior to the normal LMB connection process. It is based on RTP/RTCP and has many commonalities with the DVB LMB RET solution. Annex I addresses the DVB FCC solution based on a client-server paradigm, and is only applicable to LMB services that are transported over RTP.

I.2.2 DVB server-based FCC solution principle

The DVB server-based FCC solution operates as follows:

- the DVB FCC server caches the most recent data transported in the multicast of each LMB service;
- prior to connecting to the LMB service by means of joining a multicast, the HNED makes a request to a DVB FCC server;
- the server "bursts" the RTP data from its cache to the requesting HNED. This burst will start with a RAP. This eliminates any waiting time that is generally present when the HNED connects directly to a primary multicast of the LMB service, resulting in the improved response time of the Fast Channel Change Service;
- while the data is being "burst", at some point in time the FCC server cache will have no more cached data to transmit, and around that time, the HNED will join the primary multicast of the LMB service.

There are dedicated RTCP RAMS FB messages exchanged between the HNED and the FCC server for requesting, controlling and terminating the burst.

I.2.3 DVB server-based FCC and DVB LMB RET

The DVB server-based FCC solution has many commonalities with DVB LMB RET unicast repair because both solutions leverage the same protocol/architecture concepts. The main aspects of these common protocol/architecture concepts are specified in:

IETF RFC 4585 [84]: Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF).

IETF RFC 4588 [85]: RTP Retransmission Payload Format.

IETF RFC 5760 [111]: RTCP Extensions for Single-Source Multicast Sessions with Unicast Feedback.

The DVB server-based FCC solution leverages IETF RFC 6285 [116], also referred to as RAMS (Unicast-Based Rapid Acquisition of Multicast RTP Sessions). RAMS specifies the interactions between an RTP receiver and a "Retransmission Server", and defines new RAMS RTCP FeedBack messages (RAMS-R, -I and -T) for controlling the burst process.

This RAMS "Retransmission server" is responsible for sending the RTP burst (resulting in the FCC experience) but also for sending retransmissions in response to retransmission requests. IETF RFC 6285 [116] stipulates that RTP retransmissions and RTP burst packets are transmitted in one and the same unicast RTP (retransmission) session, with the RTP burst packets formatted with a retransmission payload header (IETF RFC 4588 [85]).

DVB server-based FCC will not deviate from these rules, which means that when both the RET and FCC services are offered for a DVB LMB service, and a HNED makes use of both these services:

The DVB LMB RET server and DVB FCC server coincide and are one and the same. This server will be referred to in this text as the DVB FCC (/LMB RET) server.

NOTE: This requirement stems from the fact that in IETF RFC 6285 [116], the "retransmission server" involved in the bursting process is also the one responding to retransmission requests by means of retransmissions. As the "IETF retransmission server" and the "DVB retransmission server" both host the RTCP Feedback Target logical entity, and for a given SSM RTP session and DVB-HNED, there can only be one active Feedback Target, this requirement is a logical consequence.

Unicast RET packets and FCC burst packets are transported by the DVB FCC (/LMB RET) server in the same unicast RTP retransmission session and are both formatted with a retransmission payload header as specified in IETF RFC 4588 [85].

It shall be stressed that the DVB LMB RET service and the DVB server-based FCC service remain decoupled in the sense that the DVB LMB RET service may be provided without DVB server-based FCC service and vice-versa.

However, DVB does recommend that server-based FCC service is combined with LMB RET, specifically because there is no penalty for any of the network, client or server implementation in deploying the DVB LMB RET service "on top of" the DVB server-based FCC service. In this section the focus is on the DVB server-based FCC solution, but because of the inherent ties into the LMB RET solution, there will also be some specific text in this annex with regard to unicast packet loss repair of the LMB RET solution. This text is provided in *italics*, and can be discarded where the FCC service is operated without support for LMB RET unicast repair. If both FCC and LMB RET services are offered, both the normative text in the RET specification and in the FCC specification in the present document shall be followed.

I.2.4 Server-based FCC architecture and terminology

I.2.4.1 Server-based FCC architecture

Figure I.1 represents a high level view of the DVB server-based FCC architecture.

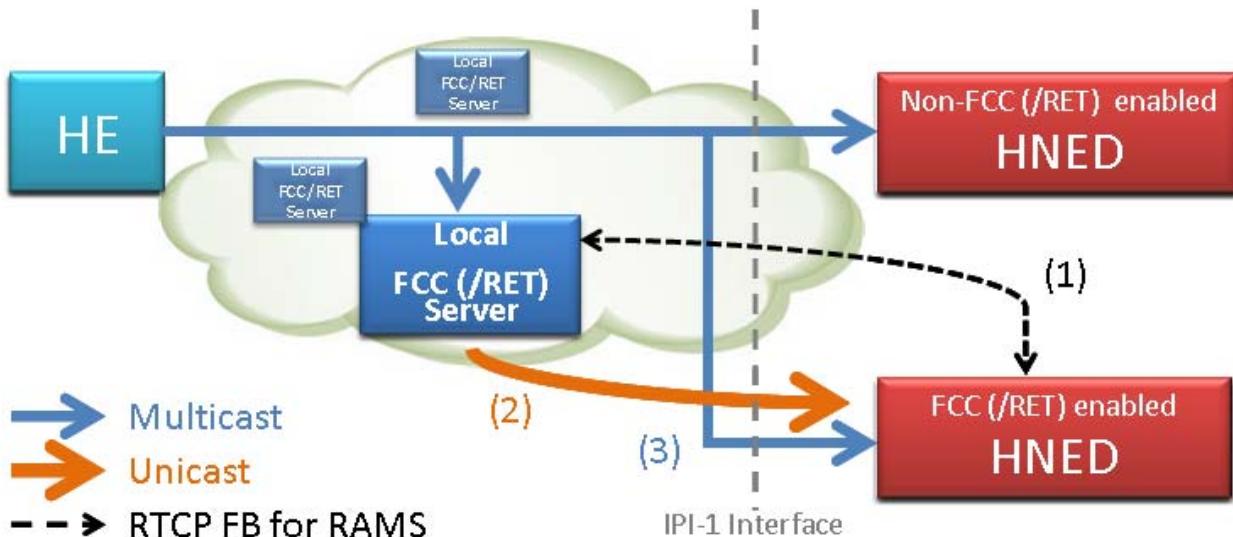


Figure I.1: DVB server-based FCC

The DVB server-based FCC solution relies on the RAMS protocol specified in IETF RFC 6285 [116].

When an end-user selects an LMB service ("a channel zap"), the DVB FCC client in the HNED requests a unicast RTP burst from a DVB FCC server by means of a RAMS-Request (RAMS-R) RTCP FB message. If the request is not accepted, the DVB FCC server will send a RAMS-Information (RAMS-I) RTCP message containing a non-service response, and then the HNED resorts to the normal LMB service connection process. When accepting the request, the DVB FCC server starts bursting (i.e. forwarding at a higher rate than the streaming rate) unicast data from its cache that holds the most recent data of the LMB service starting with a Random Access Point, along with a RAMS-I RTCP message. This message may be used to signal to the DVB FCC client when the DVB FCC client should issue a multicast join command to connect to the LMB service. In this case the DVB FCC server will cease bursting the cached data at that point, as the unicast RTP stream has caught-up with the multicast stream carrying the LMB service data. Before or after reception of the first multicast packets of the LMB service by the DVB FCC client, it sends a RAMS-Termination (RAMS-T) message to the DVB FCC server, requesting it to terminate the RTP burst.

I.2.4.2 IETF and DVB terminology

IETF RFC 6285 [116] uses the term "retransmission server" to indicate the server that is responsible for the RAMS messaging interaction with the RTP receiver and for the RTP burst transmission.

In the present document, "DVB FCC server", "DVB FCC/LMB RET server" or "DVB FCC (/LMB RET) server" terminology is applied, each being the equivalent of the IETF "retransmission server". When "DVB FCC server" is used, there is no LMB RET service available. When "DVB FCC/LMB RET server" is used, both FCC and LMB RET services are available.

The general term used throughout the remainder of this annex will be "DVB FCC (/LMB RET) server", to highlight that this annex describes the DVB FCC service solution, but bearing in mind that the same server is called LMB RET server (in annex F) when the DVB LMB RET service is also provided. Similarly, in the remainder of the present document, the term "DVB FCC (/RET) client" is used.

The choice not to use the IETF "retransmission server" term in the present document is made in order to differentiate "DVB server-based FCC service" from "DVB LMB RET service", for which annex F has already introduced the term "retransmission server".

I.2.5 FCC/ (LMB RET) unicast repair RTP sessions

A DVB FCC (/RET) client that makes use of the DVB FCC service, is engaged in:

A primary RTP multicast session, where the HNED is an SSM RTP receiver and the FCC (/RET) client sends its RTCP messages unicast to the RTCP FB target of that SSM, a logical entity that is part of the DVB FCC(LMB RET) server, and defined in IETF RFC 5760 [111]. These RTCP messages sent by the HNED are:

- the RAMS-Request RTCP FB message for requesting a burst,
- *the NACK RTCP FB message when the LMB RET service is activated and supported,*
- the other more generic RTCP messages (RTCP RR, RTCP SDES, RTCP Bye), as explained in the LMB RET annex, clause F.4 of the present document.

NOTE: In DVB RET terminology (defined in annex F of the present document) the primary RTP multicast session is named "original RTP multicast session".

A unicast retransmission session where the burst/retransmission source logical entity of the DVB FCC server sends the RTP burst packets, and in which the RAMS-I and RAMS-T messages are exchanged, as well as the RTCP SR/RR, RTCP SDES and RTCP Bye messages, pertaining to this session. *When the LMB RET service is present, the unicast RTP RET (RET service) packets are also transmitted in this unicast retransmission session.*

I.2.6 RAMS RTCP FB signalling for DVB FCC

Following IETF RAMS IETF RFC 6285 [116], an FCC client-enabled HNED shall support the RAMS-R, RAMS-I and RAMS-T RTCP FB messages. Figure I.2 depicts the basic RAMS FB message interactions between the DVB FCC (/RET) client and the DVB FCC (LMB RET) server.

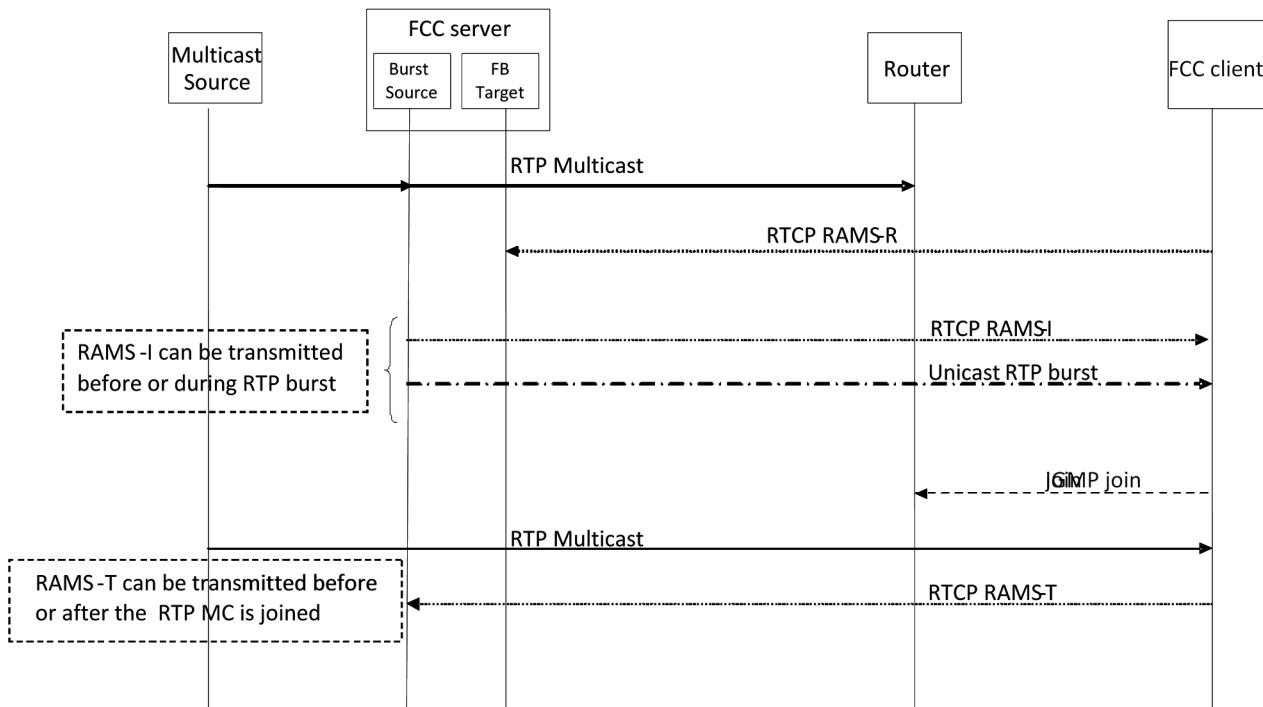


Figure I.2: Basic RAMS messaging between DVB FCC(/RET) client and DVB FCC (LMB RET) server

The formats of the RAMS messages are described in clause I.2.7.

The FCC (/RET) client in the HNED starts the RAMS interaction by issuing a RAMS-R message towards the FB target logical entity that is part of the FCC/LMB RET) server.

The FCC(/LMB RET) server is required to transmit at least one RAMS-I message, and when accepting the request, it also starts bursting the RTP data from its cache. In that case, the RAMS-I message shall include a field indicating the RTP sequence number (SN) of the first packet transmitted in the unicast burst.

The FCC(/RET) client needs to transmit a RAMS-T message, explicitly requesting the FCC (/LMB RET) server to stop the FCC burst. When the FCC client starts receiving the multicast stream prior to sending the RAMS-T message, the RAMS-T message shall include the field containing the RTP SN of the first packet received in the primary multicast stream.

See the IETF RAMS IETF RFC 6285 [116] for a detailed overview of the RAMS protocol interaction, including possible corner cases.

Figure I.3 shows the (basic) RAMS messaging between FCC(/RET) client and FCC(/LMB RET) server, and also (optional) Exchange of RAMS-R update RTCP FB message, allowing an FCC(/RET) client to request adjusting the bursting rate with optionally a corresponding response by the FCC(/LMB RET) server (including a RAMS-I update RTCP FB message).

NOTE: RAMS-R update and RAMS-I update messages have the same format definitions as respectively the RAMS-R and RAMS-I messages.

DVB LMB RET interactions (only present when the LMB RET service is offered) where the FCC/RET client issues an RTCP FB NACK message to the FB target logical entity of the FCC/LMB RET server, with the latter responding with one or several Retransmission Packets. DVB LMB RET service may be used by the HNED to request missing packets detected in the multicast stream or in the unicast burst. This could be for example a gap that may have occurred between the end of the unicast burst and the start of reception of the primary multicast stream by the HNED.

Transmission of RTCP Bye from the HNED FCC(/RET) client towards the FB target logical entity (in the primary RTP multicast session) and towards the burst/retransmission source logical entity of the FCC (/LMB RET) server (in the unicast retransmission session), when the HNED no longer wants to receive the LMB service (e.g. user zaps away). In this particular example the unicast burst was already terminated.

Not indicated in the figure: RTCP RR, RTCP SR and RTCP SDES messages are also exchanged between the FCC(/RET) client and the FCC(/LMB RET) server -in both the multicast and the unicast retransmission session-, and the rules apply as stipulated in the LMB RET annex, clause F.4.2.

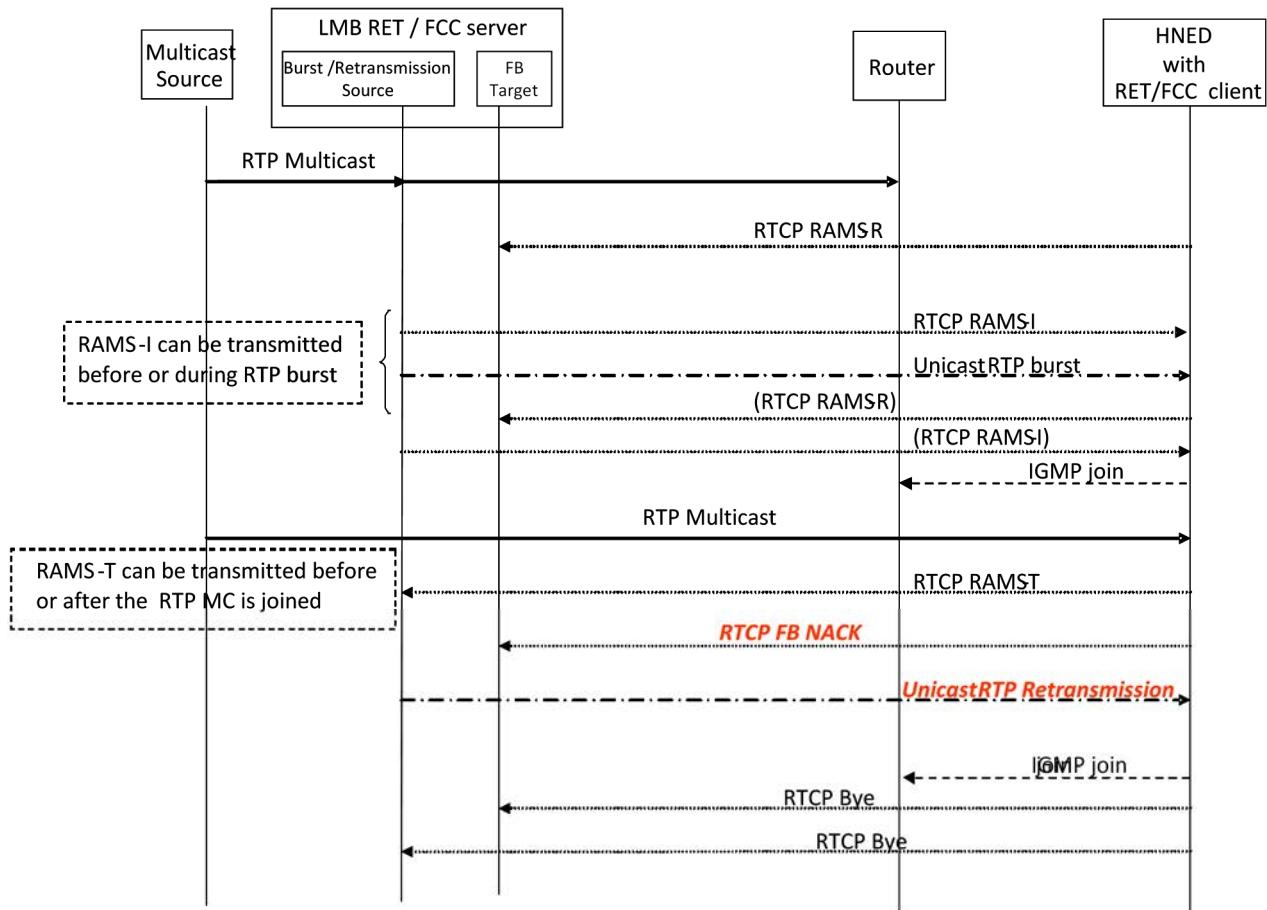


Figure I.3: Basic RAMS messaging extended with RET messaging and RTCP Bye

I.2.7 RAMS RTCP FB message formats

I.2.7.1 RAMS RTCP FB message format

The RAMS RTCP FB message formats follow the RTCP FB message format as defined in IETF RFC 4585 [84].

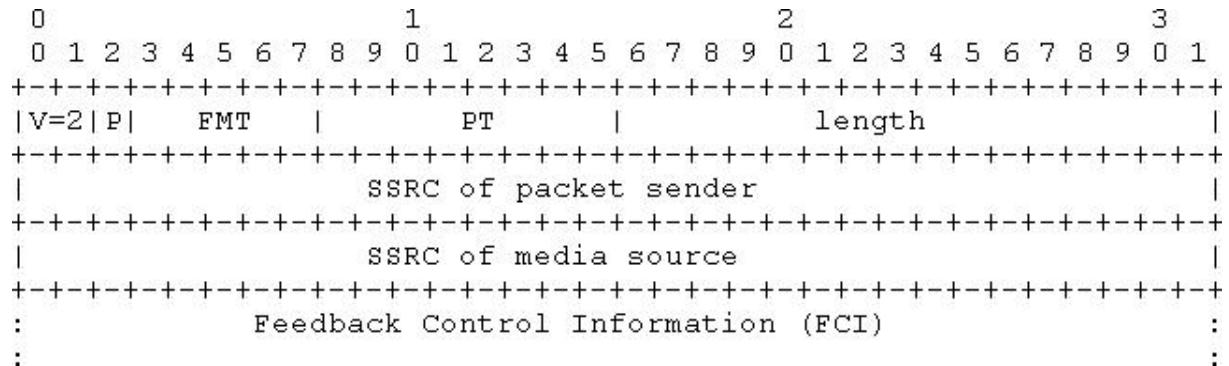


Figure I.4: Generic Packet format for RTCP FB message

Each feedback message has a fixed-length field for version, padding, feedback message type (FMT), payload type (PT), length, SSRC of packet sender, SSRC of media source as well as a variable-length field for feedback control information (FCI).

In RAMS messages, the PT field is set to RTPFB (205) and the FMT field is set to RAMS (6).

Individual RAMS messages are identified by an 8-bit sub-field called Sub Feedback Message Type (SFMT), which is always the first field of the FCI information for RAMS. The second field is a 24 bit reserved field (for alignment).

With two exceptions (see further, RAMS-I), all subsequent information (sub-)fields in the FCI field are encoded as TLV elements as described below, and depicted in Figure I.5.

Type: A single-octet identifier that defines the type of the parameter represented in this TLV element.

Length: A two-octet field that indicates the length (in octets) of the TLV element excluding the Type and Length fields, and the 8-bit Reserved field between them. Note that this length does not include any padding that is required for alignment.

Value: Variable-size set of octets that contains the specific value for the parameter.

If a TLV element does not fall on a 32-bit boundary, the last word shall be padded to the boundary using further bits set to 0.

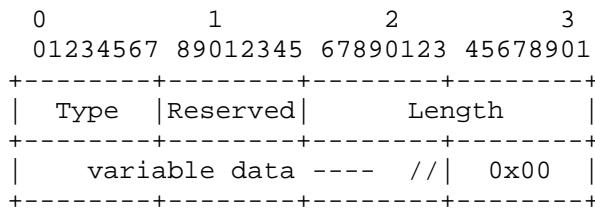


Figure I.5: Format for TLV elements in RAMS messages

Dedicated TLV elements are specified in this section, but note that private TLV elements may be defined too [116].

I.2.7.2 Feedback Control Information for RAMS-R

The RAMS Request message is identified by SFMT=1. The FCI field shall contain only one RAMS Request.

The RAMS IETF RFC 6285 [116] has defined four TLV elements that can be embedded in the RAMS Request:

- Requested Media Sender SSRC (type = 1): Optional TLV element that in DVB system is only used when the HNED does not know the media sender SSRC of the primary multicast RTP stream carrying the LMB service. The length field shall be zero (i.e. there is no value field). When this TLV is present, the FCC server will ignore the media sender SSRC specified in the header of the RAMS-R message. This TLV shall not be used by the HNED when the SSRC values of the primary multicast streams are signalled in SD&S.

When the FCC server cannot use the media sender SSRC field in the RAMS-R message to identify the primary multicast stream, the transport address of the RAMS-R shall provide that information, requiring a different tuple of FCC server IP address and port number for the Feedback Target entity for each primary multicast, when SSRCs are not signalled in SD&S.

- Min RAMS Buffer Fill Requirement (32 bits) (type = 2): Optional TLV element that denotes the minimum milliseconds of data that HNED desires to have in its buffer before allowing the data to be consumed by the application.
- Max RAMS Buffer Fill Requirement (32 bits) (type = 3): Optional TLV element that denotes the maximum milliseconds of data that HNED can buffer without losing the burst data due to buffer overflow.
- Max Receive Bitrate (64 bits) (type = 4): Optional TLV element that denotes the maximum bitrate (in bits per second) that the HNED can process the unicast burst. This rate should include whatever knowledge the HNED has that would provide an upper bound on the unicast burst bitrate. The limits may include local receiver limits as well as network limits that are known to the receiver.

I.2.7.3 Feedback Control Information for RAMS-I

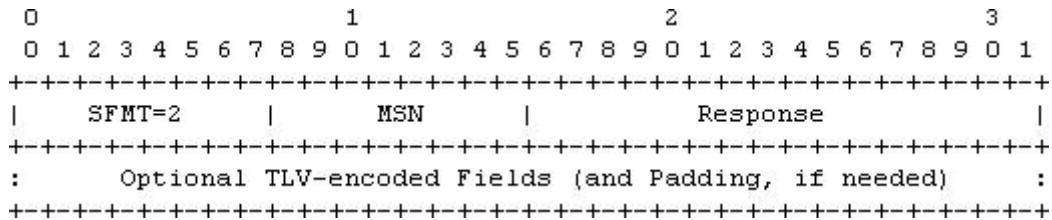


Figure I.6: FCI field syntax for the RAMS Information message

The following fields are defined for the RAMS-I:

- SFMT (8 bits): Value is 2 for RAMS-I.
 - Message Sequence Number (8 bits): Mandatory field that denotes the sequence number of this RAMS-I message. During rapid acquisition, multiple RAMS-I messages (RAMS-I update) may be sent and/or the same RAMS-I message may be repeated. The first RAMS-I message shall have an MSN value of 0. This value shall not be changed if the same RAMS-I message is sent to the same HNED multiple times for redundancy purposes. If a new information is conveyed in a new RAMS-I message update, the MSN value shall be incremented by one.
 - Response (16 bits): Mandatory field that denotes the RS response code for this RAMS-I message. Possible response codes are defined in [116].

The TLV elements defined for RAMS-I are:

- Media Sender SSRC (32 bits) (type = 31): Optional TLV element that specifies the media sender SSRC of the unicast burst stream. While this information is already available in the message header, it may be useful to repeat it in an explicit field. For example, if the feedback target that received the RAMS-R message is associated with a single primary multicast stream but the requested media sender SSRC does not match the SSRC of the RTP stream associated with this feedback target, the FCC server should include this TLV element in the initial RAMS-I message to let the HNED know that the media sender SSRC has changed. If the two SSRCs match, there is no need to include this TLV element.
 - RTP Seqnum of the First Packet (16 bits) (type = 32): TLV element that specifies the RTP sequence number of the first packet that will be sent in the retransmission session. This allows the HNED to know whether one or more packets sent by the FCC (/LMB RET) server have been dropped at the beginning of the retransmission session. This field is only present if the RAMS request was accepted by the FCC (/LMB RET) server.
 - Earliest Multicast Join Time (32 bits) (type = 33): Optional TLV element that specifies the time difference (i.e. delta time, expressed in ms) between the arrival of the first RTP packet and the earliest time instant when the HNED could join the primary multicast session. A zero value in this field means that the HNED can join the primary multicast session right away.

NOTE 1: If the RAMS request has been accepted, this field should be sent at least once, so that the HNED knows when to join the primary multicast session. If the burst request has been rejected as indicated in the Response field, this field may be omitted or set to 0. In that case, it is up to the HNED when or whether to join the primary multicast session.

- Burst Duration (32 bits)(type = 34): Optional TLV element that denotes the duration of the burst, i.e. the delta difference between the first and the last burst packet, that the FCC(/LMB RET) is planning to send (in ms). In the absence of additional stimulus, the FCC(/LMB RET) server will send a burst of this duration. However, the burst duration may be modified by subsequent events, including changes in the primary multicast stream and reception of RAMS-T messages.

The FCCC(LMB RET) server shall terminate the flow in a deterministic timeframe, even if it does not get an RAMS-T or a BYE from the HNED.

- Max Transmit Bitrate (64 bits)(type = 35): Optional TLV element that denotes the maximum bitrate (in bits per second) that will be used for the burst.

NOTE 2: the initial RAMS-I message should precede the unicast burst or be sent at the start of the burst.
 Subsequent RAMS-I message(s) may be sent during the unicast burst and convey changes in any of the fields.

I.2.7.4 Feedback Control Information for RAMS-T

The RAMS Termination message is identified by SFMT=3. The FCI field shall contain only one RAMS Termination. Only one TLV field is defined for the RAMS-T.

If prior to sending the RAMS-T message the HNED has already joined the primary multicast session and received at least one RTP packet from the multicast session, the HNED includes the sequence number of this first RTP packet in the RAMS-T message. With this information, the FCC(/LMB RET) server can decide when to terminate the unicast burst.

If the HNED issues the RAMS-T message before it has joined and/or begun receiving RTP packets from the primary multicast session, the HNED does not specify any sequence number in the RAMS-T message, which indicates the FCC(/LMB RET) server shall stop the burst immediately.

The only TLV defined for RAMS-T is:

- Extended RTP Seqnum of First Multicast Packet (32 bits) (type = 61): conditionally optional TLV element that specifies the extended RTP sequence number of the first multicast packet received by HNED. If no RTP packet has been received from the primary multicast session, this field is not present.

I.2.8 HNED RTCP reporting for DVB FCC (/LMB RET)

For both the primary multicast session and the retransmission session, the HNED follows the RTCP reporting rules as defined by the early feedback profile AVPF [84], with the exception that the first RAMS-R message can be sent right at the beginning.

Similar as in the case for DVB RET, a DVB FCC(/RET) client and server shall support reduced size RTCP reporting. The parameter "RTCPReporting@rtcpssize" allows to signal to the HNEDs with SD&S whether the HNED may use reduced size RTCP reporting in the primary multicast session. However, the FCC(/RET) client shall transmit the RAMS-R and the Bye packet, when used in the primary multicast session, together with a SDES message. Note that reduced size reporting is only allowed and applicable for the primary multicast session. This means that:

- The DVB FCC(/LMB RET) server shall send RAMS-I in (full) compound message format, i.e. including an SDES and SR message.
- The DVB FCC(/LMB RET) client of the HNED shall send RAMS-T in (full) compound message format, i.e. including an SDES and RR message.

NOTE: Issuing of RTCP RR messages by the HNED may be disabled through the "dvb-disable-rtcp-rr" attribute.

DVB recommends that for compound reporting for statistical purposes (comprising the SDES and RR message), this frequency be once every 5 seconds.

A BYE packet shall only be sent by the HNED if it has been configured through the parameter "dvb_enable- bye". DVB recommends the use of Bye for FCC(/RET) deployment.

The BYE packet for the primary multicast RTP session and retransmission session, when used, is always sent out, together with an SDES, and also an RR if RR-reporting is enabled.

I.2.9 FCC RTP burst

I.2.9.0 General

As defined in IETF RAMS IETF RFC 6285 [116], the RTP burst packets shall be formatted following IETF RFC 4588 [85], i.e. have the RTP retransmission payload header. *When the LMB RET service is offered in addition to the DVB-FCC server-based method, the RET packets shall also be formatted as specified in IETF RFC 4588 [85].* The bit rate used during the burst is entirely determined by the FCC(/LMB RET) server but may be calculated based on the information retrieved from RTCP RAMS-R message and dynamically adapted based on tracking other RTCP messages exchanged during the bursting process. This is outside the scope of the present document.

I.2.9.1 Terminating the burst

A FCC(LMB RET) client that wishes to terminate the burst, can do this for two reasons:

- The FCC(LMB RET) client will be joining or has recently joined the associated primary multicast, and hence sends out the RAMS-T message. This is part of the normal RAMS process.
- The HNED is no longer interested in the primary multicast and associated burst (e.g. the end-user switched to a different LMB service while the burst was still received). In this case the FCC(LMB RET) client shall transmit an RTCP Bye message to the FCC(LMB RET) server, both in the primary multicast session and in the retransmission session, even when the FCC(LMB RET) client already issued a RAMS-T message. Note that sending the RAMS-T message may be omitted by the FCC(LMB RET) client, when the HNED transmits the Bye messages whilst still receiving the RTP burst.

I.2.9.2 Burst packet loss recovery

There may be packet loss occurring in the RTP unicast burst, or resulting from a non-seamless "switch over" from the unicast burst to the primary multicast stream by the HNED.

If the DVB LMB RET service is offered, the HNED FCC/RET client can request the missing packet(s) by issuing (an) RTCP FB NACK message(s) to the FCC/LMB RET server. In this message each reported missing packet is identified by means of the "media sender SSRC" -being the SSRC present in the primary multicast RTP stream- and a sequence number that is retrieved from the gap detected by the HNED by inspecting the RTP payload header field of the unicast RTP burst packets carrying the original RTP sequence number (OSN), i.e. the corresponding RTP SN in the primary multicast session.

When an FCC(RET) client issues a RAMS-R for receiving a burst and AL-FEC is used to protect the LMB service, this burst contains only the RTP data without the AL-FEC parity packets. This is aligned with the LMB RET specification which forbids RET sessions on AL-FEC streams (clause F.10).

When the LMB service and its associated AL FEC stream(s) are sent on different RTP SSM sessions (different transport address), it would require at least two dedicated RAMS interactions and at least two dedicated bursts in parallel. If this occurs, then the client needs to synchronize two different RAMS sessions which adds complexity to the client and the additional burst will cause significant bandwidth usage so compromising the speed of the channel change. DVB therefore does not allow FCC burst packet loss recovery by means of AL-FEC.

I.2.10 Retransmission session transport address and SSRC identifiers

The following recommendations and rules apply for both DVB server-based FCC and LMB RET.

NOTE: These rules deviate from the rules specified in the RET specification in annex F, clauses F.4.2.2 and F.6.2.2.

The SSRC used by the FCC(LMB RET) server in the retransmission session comprising the burst shall be the same as the SSRC used by the head-end in the primary multicast session, as stipulated in IETF RFC 4588 [85].

The SSRC identity used by the HNED in the retransmission session (and indicated in the "SSRC" field of the RTCP SDES, RR, Bye or RAMS-T messages exchanged with the Retransmission/Burst source entity) may or may not be different from the SSRC identity it uses in primary multicast session (as indicated in the corresponding SSRC field of the RAMS-R, NACK, SDES, RR and Bye messages exchanged with the FB target).

One can overcome typical NAT arrangements like "port restricted cone" and avoid opening an additional "pinhole" in the firewall for the RTP and RTCP packets transmitted by the FCC(LMB RET) server in the retransmissions session when the following three rules are fulfilled:

- The destination port/address of the RTP packets sent in the retransmission session have the same value as the source port/address of the RTCP FB RAMS-R (*and NACK, when DVB RET service is used*) messages.
- The source port/address of the RTP packets sent in the retransmission session have the same value as the destination port/address of the RTCP FB RAMS-R (*and NACK, when DVB RET service is used*) messages. The latter is signalled to the HNED by means of the SD&S RTCPReporting@DestinationPort parameter.

- The RTP and RTCP packets transmitted by the FCC(/LMB RET) server in the retransmission session are multiplexed on the same port as per IETF RFC 5761 [113].

When a system is deployed in the way as described above, the UDP destination port of RTCP packets issued by HNED in retransmission session shall be different from the destination port of the RTCP packets issued by the HNED in the primary multicast session. This is necessary to allow the FCC(/LMB RET) server to distinguish between RTCP messages received in the primary multicast RTP session and RTCP messages received in the RTP retransmission session. The UDP destination port of RTCP packets issued by HNED in retransmission session is signalled by means of the SD&S Retransmission_session @DestinationPortForRTCPReporting parameter.

In the case that the FCC(/LMB RET) server sends the RTP and RTCP packets in the RTP Retransmission session to the same destination transport address, the combination of the RTP Marker value and expected Payload Type value in the RTP packet header shall be different from the possible Packet Type values in the RTCP packets. This allows the HNED to distinguish between incoming RTP and RTCP packets in the retransmission session (see [113]).

I.2.11 RTSP and FCC

Similar as for LMB and LMB RET, RTSP may be used for connection set-up prior to the RAMS-interaction for DVB server-based FCC. However there are a few subtle points:

- the core idea of the RAMS-interaction and RTP Burst is to accelerate the LMB acquisition process. Setting-up each RTP session by means of RTSP will delay again the LMB acquisition process, and hence reduces the FCC service value;
- as a single RTP retransmission session is used for LMB RET and FCC service, the required bandwidth for the RTP burst (at the start of the session) and the retransmission service (after the burst is terminated) are typically very different. There is no way to signal this and unless this highly variable bandwidth consumption is implicitly known to monitoring systems, care should be taken if RTSP is used mainly because of bandwidth monitoring/reservation purposes.

It is therefore recommended to NOT use RTSP to set-up/tear down retransmission sessions when FCC service is used. As the RAMS-R is sent in the primary multicast session, and as any significant delay by which the RAMS-R can be sent to the FCC(/LMB RET) server will impact the FCC experience, it is also recommended to NOT use RTSP for setting-up/tearing down the primary multicast sessions for FCC-enabled LMB services.

I.2.12 QoS Priority settings

The RTP packets in the retransmission session take over video bearer priority of corresponding RTP packets in the primary multicast session (which is DSCP 0b100010 or 0b100100). All RTCP packets have voice/video signalling priority setting (DSCP 0b11010).

I.2.13 FCC (/LMB RET) Service discovery

The DVB configuration method for the FCC (/LMB RET) parameters is no different from what is defined for LMB RET.

The FCC (/LMB RET) client is configured via SD&S. The exception to this is the initial IP address of the FCC(/LMB RET) server(s) that can be configured in three different ways:

- By means of DHCP FCC(/LMB Retransmission Server) Address option. DHCP should be used at start up to get a list of IP addresses of FCC(/LMB RET) servers as described in clause 8.1.1.10. These IP addresses are the same for all LMB services. The servers shall be in the order of priority from first to last server to connect to. The method for connecting to the server and assuring its operation is vendor specific.
- Via SD&S. SD&S may also contain FCC(/LMB RET) server addresses which can be specified per LMB service. These addresses overrule the FCC(/LMB RET) server address obtained from DHCP for the specific LMB service where SD&S contains a server address value.

- By means of RTCP RSI messages The Receiver Summary Information RTCP messages are defined in annex F. The RSI messages with sub report block type equal to 0, 1 or 2 may be distributed over the SSM to signal the new address of an FCC(/LMB RET) server. The FCC(/LMB RET) server address signalled in an RSI is only valid for a specific LMB service. The LMB RET server address signalled through RSI takes precedence over the FCC(/LMB RET) server address(es) that may be configured via SD&S for that specific service, and also takes precedence over the FCC(/LMB RET) server address(es) that may be configured via DHCP.

NOTE 1: The RSI messages with sub report block type 0,1,2 signal the address and port of the Feedback Target logical entity (to which the RAMS-R and NACK messages are addressed). All other relevant FCC(/LMB RET) service parameter information is still retrieved from SD&S.

NOTE 2: Annex F specifies that the RSI can be sent either in the SSM of the primary multicast session, or in the SSM of the multicast LMB RET.

If SD&S records are updated with new FCC(/LMB RET) server addresses after an RSI message signalling an FCC(/LMB RET) server address, then the new SD&S values for the FCC(/LMB RET) server will take preference over addresses in the RSI message.

NOTE 3: FCC(/LMB RET) server addresses signalled via DHCP or RSI can be different for different access service regions as they can be distributed locally via the DHCP server or via the operational FCC(/LMB RET) server in the multicast LMB RET session (RSI message).

I.2.14 SD&S FCC (/LMB RET) parameters overview

A set of parameters related to the HNED configuration for DVB server-based FCC is defined for integration in the SD&S broadcast discovery records. The FCC parameters are grouped under the "ServerBasedEnhancementServiceInfo" element in the SD&S discovery records.

When a LMB RET service is offered together with the server-based FCC for a specific LMB service, and an HNED makes use of both services, the HNED should ignore any SD&S signalled RET parameters when present -defined and grouped under "RTPRetransmission" element -, and use only the SD&S signalled "ServerBasedEnhancementServiceInfo" FCC/RET parameters.

When an HNED makes use of RET services-only (and no server-based FCC), it should retrieve and use the "RTPRetransmission" SD&S parameters when present, and if not present, it should retrieve and use the "ServerBasedEnhancementServiceInfo" SD&S parameters.

It is the responsibility of the service provider to make the values of the parameters consistent across the two parameter sets ("RTPRetransmission" and "ServerBasedEnhancementServiceInfo") when both are signalled in SD&S, and the service provider wants a RET-only enabled HNED and FCC(RET)-enabled HNED to make use of the same parameter values.

More specifically, the parameters that enable the configuration of an FCC (/LMB RET) client shall be listed in the SD&S broadcast discovery records under:

- /BroadcastDiscovery/ServiceList/SingleService/ServiceLocation/IPMulticastAddress/ServerBasedEnhancementServiceInfo/ EnhancementService

This element indicates whether RET-only, FCC-only or "FCC and RET" services are provided. Values are "FCC" and "RET".

- "/BroadcastDiscovery/ServiceList/SingleService/ServiceLocation/IPMulticastAddress/ ServerBasedEnhancementServiceInfo/RTCPReporting"

The following "RTCPReporting" parameters apply for server-based FCC (*and for LMB RET with unicast-only repair when used in conjunction with server-based FCC*):

- RTCPReporting@DestinationAddress
- RTCPReporting@DestinationPort
- RTCPReporting@rtcp-bandwidth
- RTCPReporting@rtcp-rsize

- RTCPReporting@ trrint
- RTCPReporting@dvb-disablertcp-rr
- *RTCPReporting@dvb-enable-bye*
- RTCPReporting@dvb-rsi-mc-ret
 - "BroadcastDiscovery/ServiceList/SingleService/ServiceLocation/IPMulticastAddress/ServerBasedEnhancement ServiceInfo/Retransmission_session"

The following "Retransmission_session" parameters apply for server-based FCC (*and for LMB RET with unicast-only repair when used in conjunction with server-based FCC*):

- Retransmission_session@SourcePort
- Retransmission_session@DestinationPort
- Retransmission_session@rtx-time
- Retransmission_session@rtcp-mux
- Retransmission_session @DestinationPortForRTCPReporting
- Retransmission_session@trr-int
- Retransmission_session@RTPPayloadTypeNumber
- Retransmission_session@RTSPControlURL

The "/BroadcastDiscovery/ServiceList/SingleService/ServiceLocation/IPMulticastAddress/ServerBasedEnhancementServiceInfo/MulticastRET" attributes (defined in clause 5.2.12.16) are not relevant for server-based FCC, apart from the fact that when such a multicast packet loss repair service is enabled for LMB RET, this IP multicast may be used to transfer the RTCP RSI messages that are defined both for LMB RET and FCC service. When this is the case, this is signalled in RTCPReporting@dvb-rsi-mc-ret.

Annex J (normative): Companion stream Fast Channel Change for DVB-IPTV Systems

J.1 Scope

Annex J contains the specification for an optional extension to the present DVB-IPTV specification which facilitates in general a faster rendering when moving from one multicast LMB DVB-IPTV service to another or joining a multicast LMB DVB-IPTV service, i.e. it enables faster channel change but with a quality reduction in terms of a lower quality or resolution during the first second(s) of display. Annex J is not a necessary part of the DVB-IPTV system, but is provided to enhance performance of an otherwise functional system.

In order to implement the specification in the present document, extensions to the platform will be required in both Head End and HNED over and above those needed for the most basic of multicast DVB-IPTV service delivery as described in clause 7.3.1 Multicast Services. These extensions may include additions to both hardware and software capabilities. In any implementation where these extensions are not available in either the client, the Head End, or both, then the overall DVB-IPTV service is not affected, but the rapid switching of service is not available and the channel change time is exactly as it would have been if the basic service described in clause 7.3.1 Multicast Services were provided.

It shall be noted that a specific ordering of the MPEG-2 TS packets transported in the LMB service (PAT/PMT, ECM/EMM, etc.) may facilitate a more efficient demultiplexing, descrambling and decoding pipeline at the HNED. This applies both to the LMB service without companion stream FCC and to the LMB service enhanced with companion stream FCC. MPEG-2 TS packet ordering in the IP multicast stream is under control of the Head End, implementation-dependent and outside the scope of the present document.

J.2 Overview

The companion stream Fast Channel Change (FCC) solution is based on the following technique: a "tune-in" companion stream is sent along with the original stream of the LMB service. This companion stream helps the HNED during the channel change process to retrieve and render the LMB service more rapidly.

With this solution the LMB service is encoded and streamed in its original format, plus encoded and streamed in a companion format with a lower resolution and/or quality (and hence lower bit rate) than the original LMB. The HNED acquires both the main LMB stream and its companion stream, and this can result in an earlier display compared to an HNED that acquires (only) the normal/main LMB service. This is achieved by generating an encoded companion video stream with the following characteristics:

- A higher Random Access Point (RAP) frequency (or a smaller Group of Pictures (GoP) size) for the video stream, as compared to the LMB stream. This provides a higher chance for the HNED to receive a RAP in a shorter time frame.
- (Optionally) a lower video buffering time: the HNED video buffer will be filled faster when it retrieves the data from the companion stream.

Figure J.1 presents a high-level view of the system, with the Head End (HE) representing here the encoding and multicast streaming source of the original LMB service stream and the companion stream.

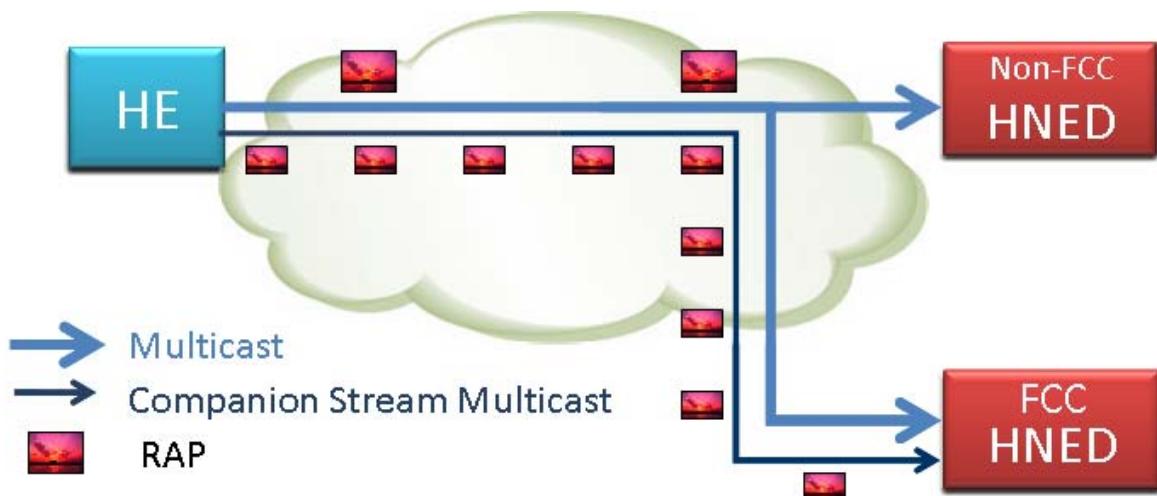


Figure J.1: High-level view of companion stream FCC

As depicted in Figure J.1, this FCC solution is transparent to HNEDs that do not support the companion stream FCC service.

J.3 Principles and examples (Informative)

J.3.0 Introduction

This clause presents in detail how both the RAP frequency and Buffering impact channel change time for a typical DVB LMB service, and how the companion stream FCC solution can help reducing the channel change time for the LMB service .

J.3.1 Normal channel change, RAP and buffer filling delays

Figure J.2 depicts a channel change process with a specific focus on the RAP waiting time and the video decoder buffer delay.

The HNED starts receiving data for the new service from the "Zap" arrow point, which in the example is close to the middle of the transmission of a compressed "I" picture.

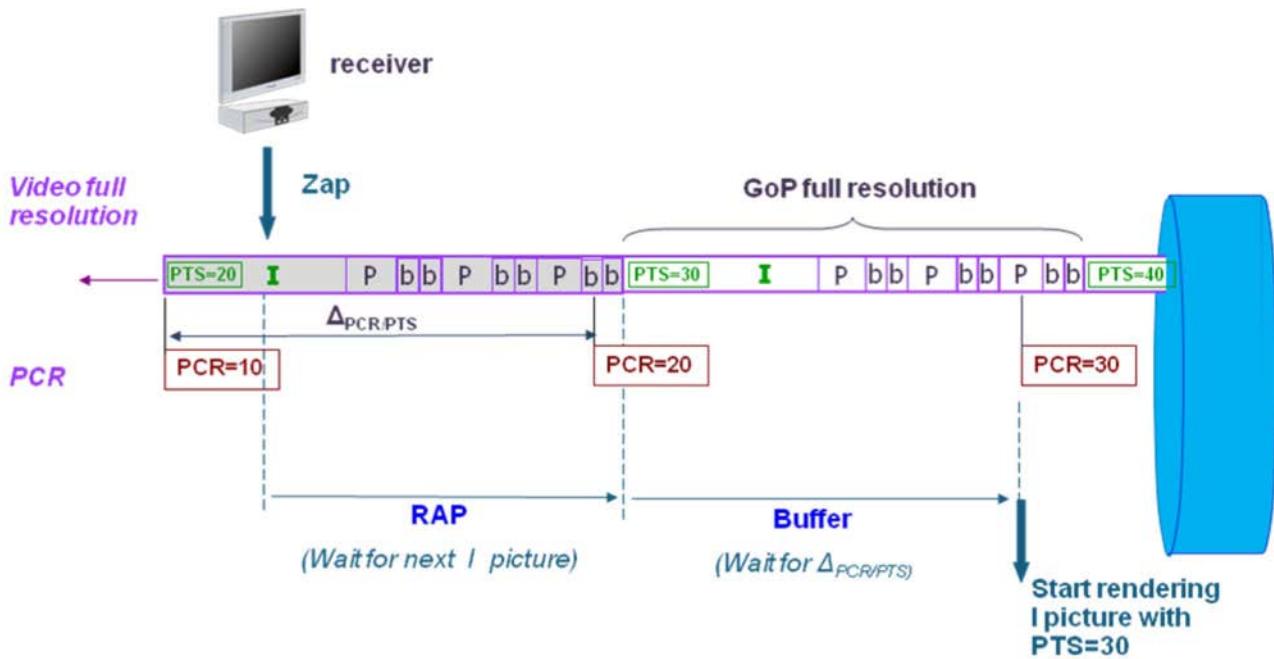


Figure J.2: Channel change process: RAP and Buffer delays

In Figure J.2, the decoder buffer delay for a given access unit is indicated with the $\Delta_{PCR/PTS}$ term. This is the delay of the Program Clock Reference (PCR) at the beginning of the decoder buffer loading of an access unit with respect to its Presentation Time Stamp (PTS) which represents the time that the decoded access unit will be rendered. In the example, the compressed "I" picture with PTS=20 is sent before the PCR=20 packet, and their relative time difference is this $\Delta_{PCR/PTS}$.

This decoder buffer delay ($\Delta_{PCR/PTS}$) is implicitly related to the end to end delay from the input to the encoder to the output or presentation from the decoder which, according to the "MPEG-2 systems timing model" in ISO/IEC 13818-1 [52] is a constant value determined by the encoding process. The encoder ensures that a given access unit of the stream can be decoded with a decoder buffer size fixed to $\Delta_{PCR/PTS}$ (in units of time): in other words it ensures that no access unit will take longer to be buffered than $\Delta_{PCR/PTS}$. The $\Delta_{PCR/PTS}$ is generally no longer than the GoP length.

In Figure J.2, when the HNED changes channel:

- It will first wait for the "RAP" time corresponding to the next compressed "I" picture.
- Then when this "I" picture is received, it checks the corresponding PTS (PTS=30) and has to wait for the decoder "Buffer" time which corresponds to a PCR=30, before starting the picture rendering process.

J.3.2 Channel change with companion stream, RAP delay-only improvement

The companion stream is used at first to improve the RAP waiting time delay by configuring a shorter GoP.

In order to maintain the synchronization of both services presentation, the corresponding frames in the two streams shall have the same frame rate, be based on the same Program Clock and have the same Presentation Time Stamps. For that the LMB service stream encoding and companion stream encoding are based on the same constant end to end delay, which means that the delay from the input to the encoder to the presentation from the decoder for the two streams is the same.

Figure J.3 depicts an original LMB service stream with an additional companion stream, carrying respectively the full and low resolution formats. In this example the companion stream has a GoP length which is half the length of the full resolution stream.

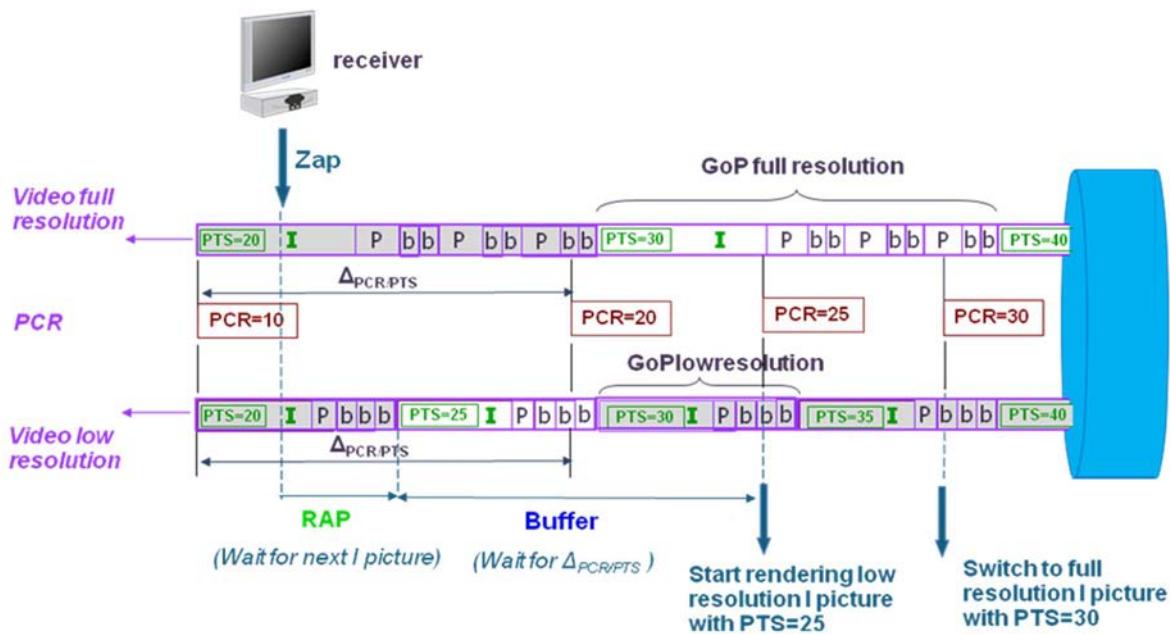


Figure J.3: Companion Stream FCC process: RAP delay-only improvement

When a companion stream FCC capable HNED changes or selects a LMB service:

- It will (initially) connect to both the LMB service stream and its companion stream.
- It will wait for the "RAP" time corresponding to the next compressed "I" picture, in both the full-resolution and the low-resolution streams. Most of the time a compressed "I" picture will appear first in the low resolution companion stream (as indicated in Figure J.3).
- Then the buffer is filled normally until the rendering of the low resolution stream can start (the decoder "Buffer" time). This is indicated in Figure J.3 by the "Start rendering" arrow which indicates the rendering of low resolution compressed "I" picture with a PTS=25, carried out when PCR=25. Compared to Figure J.2, the RAP time has been improved.
- (Partially) in parallel with the previous step, the data received from the high resolution stream is also being buffered, as soon as a RAP is detected.
- Finally the "Switch" arrow at PCR=30 shows when the full resolution stream is ready to be presented (it is the equivalent of Figure J.2 "Start rendering" arrow): at this time the low-resolution video is no longer rendered (the HNED can unsubscribe from the multicast companion stream) and the full-resolution video is displayed; the channel change process is finished.

J.3.3 Channel Change with companion stream, RAP and buffer delay improvements

Figure J.4 depicts the companion stream (low resolution) and an original LMB service stream (full resolution). The difference with Figure J.3 is that the original LMB service is encoded with a constant end to end delay "end-to-end-delay-full-res" which leads, for a given access unit, to the decoder buffer delay " $\Delta_{PCR/PTSfull-res}$ " whereas the companion stream is encoded with a shorter constant end to end delay "end-to-end-delay-low-res" which leads, for a given access unit, to the decoder buffer delay " $\Delta_{PCR/PTSlow-res}$ ".

In order to have a synchronized presentation of these two services, the companion stream encoding is delayed compared to the original LMB service encoding. This delay is equal to the difference between the constant values of the end to end delay resulting from the encoding process of each of the two streams ("end-to-end-delay-full-res" - "end-to-end-delay-low-res"). Indeed we know from the "MPEG-2 systems timing model" in ISO/IEC 13818-1 [52] that the end to end delay is a constant value. So when the low resolution stream is encoded with a lower end to end delay compared to the full resolution stream, the pictures in the low resolution stream would be presented well before the corresponding pictures of the full resolution stream.

To synchronize the presentation of the two streams it is necessary to delay the low resolution stream encoding compared to the full resolution stream encoding. Note that the delay is on the encoding process, but the two encoding processes make use of a single STC (System Time Clock) which results in the PCR alignment between the full resolution stream and the delayed low resolution stream.

When looking at Figure J.4, the compressed "I" picture with PTS=20 of the two streams are not transported at the same time anymore (compared to Figure J.3, because of this encoding delay). After being buffered in the video decoders they resynchronize themselves (as the buffer decoder delays configured by the encoders are such that the difference between the end to end delays used to encode them equals this transport delay).

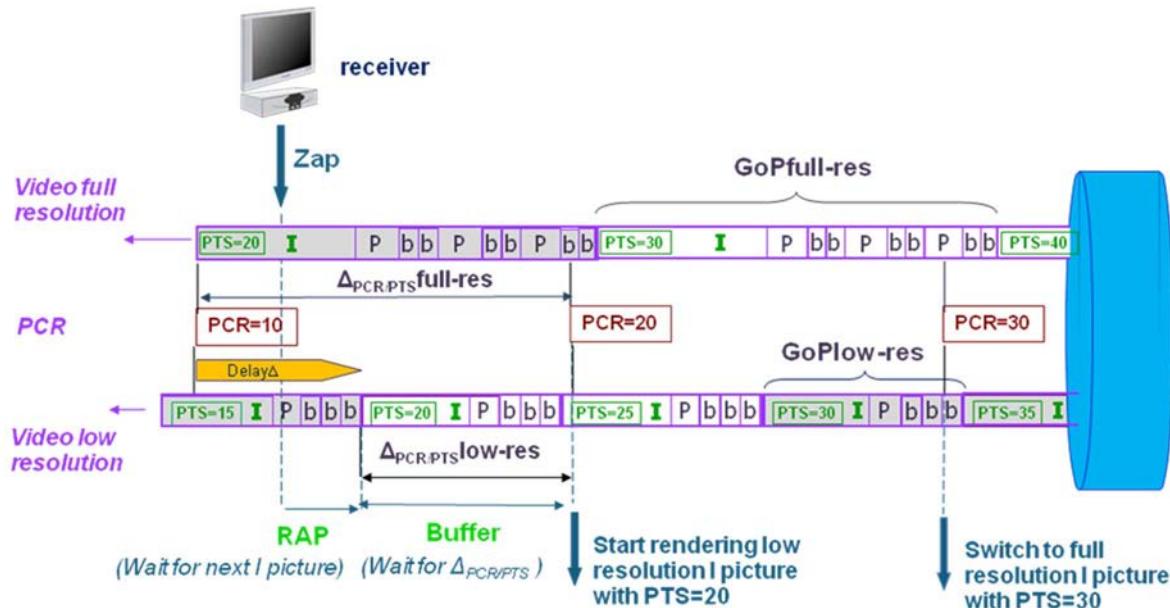


Figure J.4: Companion Stream FCC process: RAP and Buffer delay improvements

When a companion stream FCC capable HNED changes or selects a LMB service:

- It will (initially) connect to both the LMB service stream and its companion stream.
- It will wait for the "RAP" time corresponding to the next compressed "I" picture, in both the full-resolution and the low-resolution streams. Most of the time, a compressed "I" picture will appear first in the low resolution companion stream (as indicated in Figure J.3).
- Then it fills the video decoder buffer and waits the " $\Delta_{PCR/PTS\text{low-res}}$ " (decoder Buffer time) which is shorter than the " $\Delta_{PCR/PTS\text{full-res}}$ ". This is indicated in Figure J.4 by the "Start rendering" arrow which indicates the rendering of the low resolution compressed "I" picture with a PTS=20, carried out at PCR=20. Compared to Figure J.3, the Buffering time is reduced.
- (Partially) in parallel with the previous step, the data received from the high resolution stream is also being buffered, as soon as a RAP is detected.
- Finally the "Switch" arrow at PCR=30 shows when the full resolution stream is ready to be presented (it is the equivalent of Figure J.2 "Start rendering" arrow): at this time the low-resolution video is no longer rendered (the HNED can unsubscribe from the multicast companion stream) and the full-resolution video is displayed; the channel change process is finished. Note that compared to Figure J.3, the companion stream service is presented over a longer time period to the end-user and this is because the presentation of the new service is faster.

J.4 HNED behaviour

For an HNED that makes use of the companion stream FCC service, the channel change process is as follows:

- After a channel change request from the end-user, the HNED disconnects from the previous LMB service and joins both the new LMB service multicast stream and its companion multicast stream.
- The HNED waits for a RAP picture in both streams:
 - If the first received RAP picture belongs to the original LMB service stream, the HNED processes that stream for rendering, and disconnects from the companion stream. The channel change is effective. In this case the companion stream did not enable faster rendering.
 - If the first received RAP picture belongs to the companion stream, the HNED begins to process that stream in order to render that stream. When the RAP picture of the original service stream is received, the HNED starts processing that stream as well and the HNED stops to process the companion stream as soon as it has processed all the access units which have to be presented before the corresponding RAP picture (with the same PTS) that is received first in the original stream. At this time the HNED can disconnect from the companion stream. The HNED display will switch between the companion stream and the original stream at the presentation time (PTS) of the RAP picture received from the original service.

NOTE: Whether the companion low-resolution stream carries audio or not, it is recommended to decode audio only from the original service. In the same way the HNED recovers Program Clock from the original LMB service PCR.

J.5 Companion Stream Encoding and HNED requirements (Normative)

For the transition between original and companion streams to be seamless at display, the encoding process of the two streams shall use:

- The same frame rate.
- A single unique Program Clock.

Furthermore the following requirements shall be met:

- Corresponding frames in the two streams shall have the same Presentation Time Stamp.
- When the two streams have different decoder buffering delays, this shall be compensated by delaying the companion stream encoding process versus the original stream encoding process.

An HNED supporting the companion stream FCC method shall be capable of:

- Connecting to two multicast streams simultaneously (the normal LMB service stream and its companion stream).
- Processing the two encoded streams simultaneously, which requires the implementation of two video decoder instances in the HNED (each compliant to ETSI TS 101 154 [58]) dedicated to the video decoding of the original LMB service and its associated companion stream.

J.6 Companion stream-based FCC: Extension of the SD&S Broadcast Discovery Record (Normative)

The original LMB service and the FCC companion stream shall be carried in separate MPEG-2 TSs and delivered in different IP multicast sessions. The FCC companion stream shall use the same transport as the original LMB service (i.e. both shall use either MPEG2TS/UDP or MPEG2TS/RTP).

The "Usage" element within the IPService (clause 5.2.13.2) XML structure shall provide information on how the IP Service can be "consumed" by the HNED. The values are defined in clause 5.2.10.

For signalling the companion stream FCC service, SD&S shall make use of the "Linked Service" element of the IPService element (clause 5.2.13.2) for nesting the companion stream service metadata. The companion stream service metadata shall contain the "Usage" element where the "FCC" value shall be among the listed values.

Annex K (informative): Dynamic Service Management Use Cases

K.1 Example Use Cases and the Associated Message Sequences for Dynamic Service Management Service

K.1.0 Assumptions

The Use Cases described below show the possible DSM behaviour in response to a subset of the possible combinations of service change requests and other HNED DSM Manager interactions.

It is assumed that:

- The HNED_ID is allocated when the HNED powers up from the off state, and that the HNED priority is also set at that time.
- Those values are retained by the HNED in any of the standby states.

As in the previous analysis, HNED1 is assumed to have the highest priority and HNED2 a lower.

K.1.1 Use Case UC1 - Switching on from Standby and requesting a first service with sufficient bandwidth

HNED at power-up.

This applies to all HNEDs, the HNED is powered to an on state from the off state. This change is independent of changes of all other HNEDs. There is sufficient bandwidth for two HD services delivered simultaneously.

The sequence is:

- 1) Power on for both HNEDs (HNED1 and HNED2).
- 2) DVB-IPTV boot procedure (discover domain, SD&S addresses including DSMM address).
- 3) DSM sequence:
 - a) Request DSM ID = DSM001.
 - b) Receive DSM ID = DSM002.
 - c) Assynchronous bitrate update (DSM101) sent to both HNEDs.
- 4) HNEDs request services successfully.
- 5) Assynchronous bitrate update (DSM101) sent to both HNEDs.

This is expanded below as a DSM message sequence.

Table K.1

From/to	Message	Message Type	Result
To HNED1 and HNED2	DSM announcement		DSM announcement in SD&S information
HNED1 to DSMM	HNED_ID request	DSM001	Request for an ID
DSMM to HNED1	HNED ID assignment	DSM002	Assignment of the ID to HNED1 including priority setting(2)
DSMM to HNED1	Bitrate availability	DSM101	DSMM informs HNED1 of new available bitrate
HNED2 to DSMM	HNED_ID request	DSM001	Request for an ID
DSMM to HNED2	HNED ID assignment	DSM002	Assignment of the ID to HNED2 including priority setting(2)
DSMM to HNED2	Bitrate availability	DSM101	DSMM informs HNED2 of new available bitrate
HNED1 to DSMM	Change Request	DSM201	HNED1 asks for a new or a different service
DSMM to HNED1	Change Confirmed/cancelled	DSM204	Change confirmed by DSM Manager
Service connection is made to HNED1			
HNED2 to DSM Manager	Service Change Complete	DSM205	Service change/setup completed
HNED2 to DSMM	Change Request	DSM201	HNED2 asks for a new or a different service
DSMM to HNED2	Change Confirmed/cancelled	DSM204	Change confirmed by DSM Manager
Service connection is made to HNED2			
HNED2 to DSM Manager	Service Change Complete	DSM205	Service change/setup completed
DSMM to HNED1	Bitrate availability	DSM101	DSMM informs HNED1 of new available bitrate
DSMM to HNED2	Bitrate availability	DSM101	DSMM informs HNED2 of new available bitrate

When a HNED switches between services (channel change) and there is no need for more bandwidth (ex.: HD to HD, SD to SD) or if bandwidth is released (ex.: HD to SD), then a HNED internal calculation could be made, with a simple notification to the DSMM. Otherwise, a request should be made to the DSMM.

K.1.2 Use Case UC2 - change of service, sufficient bandwidth

Two HNEDs are in the home, both powered on and both are already consuming services. The lower priority HNED2 switches service. Because HNED2 does not need more bandwidth only an internal calculation is needed. There is sufficient bandwidth for two HD services simultaneously.

Sequence:

- 1) After HNED2 has switched to Active, the user selects a service to watch on HNED2, calculation is made to work out whether the bitrate fits into the available bandwidth.
- 2) Calculation outcome is positive, HNED2 will request the service.
- 3) HNED2 will inform the DSMM about the service change: DSM206.
- 4) Background update message is sent to both HNED1 and HNED2.

Table K.2

From/to	Message	Message Type	Result
1) User selects a service 2) HNED2 calculates whether the services bitrate fits in the available bandwidth(DSM101)			Enough bandwidth available, HNED2 can request the service
Service request from HNED2	appropriate request to make connection to TV service		Headend evaluates whether there is sufficient bitrate to that home Since "YES" then connection is made without DSM Manager negotiation
HNED2 to DSM Manager	Service Change Complete	DSM206	Since HNED2 does not need interaction (proposal) with the DSMM, the DSMM should be informed afterwards about the service change
DSMM to HNED1	Bitrate availability	DSM101	DSMM informs HNED1 of new available bitrate. Background update message
DSMM to HNED2	Bitrate availability	DSM101	DSMM informs HNED2 of new available bitrate. Background update message

K.1.3 Use Case UC3 - HNED2 Requesting a service - DSM negotiation needed

HNED1 is active and is receiving an HD service, HNED2 is switched from standby to active and would also like to connect to an HD service selected from the SD&S. HNED2 calculates that there is insufficient bitrate for the service to be delivered without disrupting the service to HNED1.

An SD equivalent is available for the service being received by HNED1, HNED1 is requested to change HD to SD by the DSMM but refuses to change denying HNED2 the ability to connect to the HD service selected and requested.

There is an SD equivalent of the service HNED2 wants to connect to, and enough bitrate to make the connection to the SD service. Based on the calculation done by the DSMM the DSMM requests HNED2 to change the request to the SD service. HNED2 agrees and connects to the SD service.

Table K.3

From/to	Message	Message Type	Result
	HNED2 selects HD service and calculates that bitrate is not sufficient for HD service request		
HNED2 to DSMM	Change request	DSM201	Request service connection
DSMM to HNED1	Change proposal	DSM202	Request change HD to SD
HNED1 to DSMM	Change accept/refuse	DSM203	Response = "Refuse" HNED1 refuses to change
DSMM to HNED2	Change proposal	DSM202	HD connection not possible, HNED2 requested to connect to SD equivalent
HNED2 to DSMM	Change accept/refuse	DSM203	Response = "Accept" HNED2 agrees to connect to SD service
HNED2 to Headend	HNED2 requests service connection		HNED2 uses Multicast or Unicast service
Service connection is made to HNED2, HNED1 is unaffected			
HNED2 to DSMM	Service Change Acknowledge	DSM205	HNED2 informs DSMM that service is being delivered
DSMM to HNED1	Status synchronization	DSM101	DSMM informs HNED1 of new available bitrate
DSMM to HNED2	Status synchronization	DSM101	DSMM informs HNED2 of new available bitrate

K.1.4 Use Case UC4 - HNED1 Requesting a service - DSM negotiation needed

2 HNEDs in the home, HNED2 active, higher priority HNED1 requests a change of service but without sufficient bandwidth available. HNED2 is asked to change to free needed bandwidth.

Sequence:

- 1) User selects a service to watch, calculation is made to work out whether the bitrate fits in the available bandwidth.
- 2) Calculation outcome is negative, HNED1 will ask the DSMM for the service: DSM201.
- 3) DSMM will communicate to HNED2 with a change proposal to ask for an alternative service: DSM202.
- 4) HNED2 will accept the alternative solution and connect to the new service: DSM203.
- 5) DSMM will confirmed the change to HNED1: DSM204.
- 6) HNED1 will connect to the service.
- 7) HNED1 confirms a successful service change: DSM205.
- 8) DSMM will inform the HNEDs about the new bandwidth availability : DSM101.

Table K.4

From/to	Message	Message Type	Result
HNED1 to DSMM	Change Request	DSM201	HNED1 asks for a new or a different service
DSMM to HNED2	Change Proposal	DSM202	DSMM will propose an alternative service to lower priority HNED2
HNED2 to DSMM	Change Accept	DSM203	HNED2 will accept the new service
Service request from HNED2	Multicast or Unicast request to make connection to TV service		HNED will make the necessary request for a service connection
HNED2 to DSMM	Service Change Acknowledge	DSM205	to acknowledge completion of service change
DSMM to HNED1	Change Confirmed	DSM204	DSMM will confirmed that HNED1 can connect to the new service
Service request from HNED1	Multicast or Unicast request to make connection to TV service		HNED will make the necessary request for a service connection
HNED1 to DSMM	Service Change Acknowledge	DSM205	to acknowledge completion of service change
DSMM to HNED1	Bitrate availability	DSM101	DSMM informs HNED1 of new available bitrate. Background update message
DSMM to HNED2	Bitrate availability	DSM101	DSMM informs HNED2 of new available bitrate. Background update message

K.1.5 Use Case UC5 - HNED2 queries data value from DSMM

HNED2 queries the value of one of the fields held by the DSM Manager for that HNED, e.g. the connected "ServiceID".

Table K.5

From/to	Message	Message Type	Result
HNED2 to DSMM	Data value query, payload = "ServiceID"	DSM301	
DSMM to HNED2	Return value	DSM302	Payload carries data field value currently held by DSMM
HNED2 to DSMM		DSM308	End of transaction

K.2 Example implementation XML Schema for DSM Datamodel

This annex contains a textual copy of the schema defined to support the data model elements as defined in clause 13 of the present document. It may be used in a DSM Manager or HNED implementation to support the data model structure.

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

    <!-- Data Model -->
    <xsd:element name="DataModel">
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="Customer" type="CustomerType" />
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>

    <xsd:complexType name="CustomerType">
        <xsd:sequence>
            <xsd:element name="CustomerID" type="xsd:string" />
            <xsd:element name="TotalAvailableBitrate" type="xsd:long" />
            <xsd:element name="ServiceTypePriority" type="DeliveryModeType" />
            <xsd:element name="ContentTypePriority" type="ContentTypeType" />
            <xsd:element name="HNEDDescription" type="HNEDDescriptionType" minOccurs="1"
maxOccurs="unbounded" />
        </xsd:sequence>
    </xsd:complexType>

    <!-- Support elements and attributes for datamodel and for message elements -->
    <xsd:complexType name="HNEDDescriptionType">
        <xsd:sequence>
            <xsd:element name="Session" type="SessionType" minOccurs="1" maxOccurs="unbounded" />
        </xsd:sequence>
        <xsd:attribute name="HNED_ID" type="xsd:integer" />
        <xsd:attribute name="HNEDPriority" type="xsd:integer" />
    </xsd:complexType>

    <xsd:complexType name="SessionType">
        <xsd:sequence>
            <xsd:element name="ServiceID" type="TextualIdentifier" />
            <xsd:element name="ServiceBitrates" type="ServiceBitratesType" />
            <xsd:element name="EquivalentService" type="EquivalentServiceType" minOccurs="1"
maxOccurs="unbounded" />
        </xsd:sequence>
        <xsd:attribute name="SessionID" type="xsd:integer" />
    </xsd:complexType>

    <xsd:complexType name="DeliveryModeType">
        <xsd:annotation>
            <xsd:documentation>
                Value restricted to "1" (high) or "2" (low) if present.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:attribute name="LMB" type="xsd:integer" default="2" />
        <xsd:attribute name="CoD" type="xsd:integer" default="2" />
    </xsd:complexType>

    <xsd:complexType name="ContentTypeType">
        <xsd:attribute name="SD" type="xsd:integer" default="3" />
        <xsd:attribute name="HD" type="xsd:integer" default="3" />
        <xsd:attribute name="Is3D" type="xsd:integer" default="3" />
    </xsd:complexType>

    <xsd:complexType name="EquivalentServiceType">
        <xsd:sequence>
            <xsd:element name="EquivalentServiceID" type="TextualIdentifier" />
            <xsd:element name="ServiceBitrates" type="ServiceBitratesType" />
            <xsd:element name="EquivalentServiceLocation" type="ServiceLocation" />
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="ServiceBitratesType">
        <xsd:sequence minOccurs="1" maxOccurs="unbounded" >
            <xsd:element name="Bitrate" type="xsd:integer" />
        </xsd:sequence>
    </xsd:complexType>

```

```
<xsd:sequence>
  <xsd:element name="Usage" type="UsageType" minOccurs="1" maxOccurs="unbounded" />
</xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="UsageType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="FCC" />
    <xsd:enumeration value="PiP" />
    <xsd:enumeration value="Main" />
    <xsd:enumeration value="HD" />
    <xsd:enumeration value="SD" />
    <xsd:enumeration value="3D" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="TextualIdentifier">
  <xsd:attribute name="DomainName" type="DomainType" use="optional" />
  <xsd:attribute name="ServiceName" type="Service" use="required" />
</xsd:complexType>
<xsd:complexType name="ServiceLocation">
  <xsd:choice maxOccurs="1">
    <xsd:element name="IPMulticastAddress" type="dvb:McastType" />
    <xsd:element name="RTSPURL" type="dvb:RTSPURLType" />
  </xsd:choice>
</xsd:complexType>
</xsd:complexType>
<xsd:simpleType name="DomainType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="((.|\\n|\\r)*)(\\.\\.|\\n|\\r)*+" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="Service">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="(.|\\n|\\r)+" />
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>
</xsd:schema>
```

Annex L (informative): Bibliography

- ISO/IEC 15802-3:1998: "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks Common specifications - Part 3: Media Access Control (MAC) Bridges".
- IETF RFC 2597: "Assured Forwarding PHB Group".
- IETF RFC 3246: "An Expedited Forwarding PHB (Per-Hop Behavior)".
- IETF RFC 3454: "Preparation of Internationalized Strings ("stringprep")".
- IETF RFC 1213: "Management Information Base for Network Management of TCP/IP-based internets: MIB-II".
- IETF RFC 2011: "SNMPv2 Management Information Base for the Internet Protocol using SMIv2".
- IETF RFC 2013: "SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2".
- IETF RFC 2863: "The Interfaces Group MIB".
- ISO 8601: "Data elements and interchange formats - Information interchange - Representation of dates and times".
- ISO/IEC 13818-2 (1996): "Information technology - Generic coding of moving pictures and associated audio information: Video".
- ISO/IEC 13818-3 (1998): "Information technology - Generic coding of moving pictures and associated audio information - Part 3: Audio".
- IETF RFC 3208: "PGM Reliable Transport Protocol Specification".
- draft-begec-fecframe-interleaved-fec-scheme-00 (July 2008): "1-D Interleaved Parity FEC Scheme for FEC Framework".
- draft-watson-fecframe-raptor-00 (July 2008): "Raptor FEC Schemes for FECFRAME".
- draft-ietf-rmt-flute-revised-08.txt: "FLUTE - File Delivery over Unidirectional Transport".
- ETSI TS 101 547: "Digital Video Broadcasting (DVB); Frame Compatible Plano-stereoscopic 3DTV".
- IEEE 802-2001: "IEEE Standard for local and metropolitan area networks: overview and architecture".
- IEEE 1394: "IEEE Standard for High Performance Serial Bus".
- IETF RFC 826: "An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware".
- IETF RFC 1042: "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks".

History

Document history		
V1.1.1	March 2005	Publication
V1.2.1	September 2006	Publication (Withdrawn)
V1.3.1	October 2007	Publication
V1.4.1	August 2009	Publication
V1.5.1	May 2014	Publication
V1.5.2	December 2014	Publication
V2.1.1	April 2016	Publication