Second Generation DVB Interactive Satellite System (DVB-RCS2)

Part 3: Higher Layers Satellite Specification

DVB Document A155-3

February 2020

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

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

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

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

The present document is part 3 of a multi-part deliverable covering the DVB Interactive Satellite System specification as identified below:

ETSI TS 101 545-1: "Overview and System Level specification";

ETSI EN 301 545-2: "Lower Layers for Satellite standard";

ETSI TS 101 545-3: "Higher Layers Satellite Specification";

ETSI TR 101 545-4: "Guidelines for Implementation and Use of ETSI EN 301 545-2";

ETSI TR 101 545-5: "Guidelines for the Implementation and Use of ETSI TS 101 545-3".

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.

Introduction

ETSI EN 301 790 [i.1] defines the first generation of DVB-RCS which is a system providing an interaction channel for satellite distribution systems. Together with its guidelines [i.3] and C2P specification for mesh [i.7] and [i.8] describes how such system can be built on the physical and MAC layers to provide an efficient way of turning a satellite broadcast TV into a full RCST solution capable of transporting IP traffic in a satellite-only system.

Since the original definition of DVB-RCS systems, several versions of the specification were issued, describing the requirements for the implementation of a system providing an interaction channel for satellite distribution systems.

The present document provides the higher layers for satellite the 2nd Generation Interactive DVB Satellite System (DVB-RCS2) and represents the third part of the multi-part specification of that system. The present document is the specification of the higher layers satellite architecture, signalling and functions required for the two way interactive satellite networks specified in [1] and is completed with its HLS guidelines.

The detailed specifications for these different layers are presented in the other part of this multi-part specification, introduced as normative references.

The requirements in the present document have been introduced to provide the best possible interoperability between terminals and hubs, defining the network functions as well as management and control capabilities to complement the lower layers of the system (up to layer 2) given in part 2 [1].

Clause 2 provides the references. Clause 3 provides the definitions, explains symbols and expands abbreviations. Clause 4 provides a reference system architecture that helps to understand the functional architecture of Higher Layers. Clause 5 specifies the concepts of OVN, SVNs and VFRs. Clause 6 specifies the SVN addressing for management and traffic. Clause 7 specifies the network layer functions, including network interfaces and forwarding, IPv4/IPv6 interface, routing function, quality of service and network control functions. Clause 8 provides recommendations for management signalling including the management reference architecture, signalling protocol and the specification of an RCST MIB parameters. Clause 9 specifies functions for interception traffic including PEP negotiation protocol. Clause 10 provides the description of control of motorized mount. Annex A and annex B are clauses reserved for the future inclusion of the RCST MIB and configuration file. Annex C provides the description of SDDP, for remote RCST SW image update. Annex D specifies the Dynamic Connectivity Protocol (DCP) for mesh profiles. Annex E provides the description of Antenna Alignment message data formats. Finally, annex F provides additional Bibliography.

1 Scope

The present document specifies the functional requirements for the higher protocol layers for the DVB-RCS2 satellite interactive system specified in [i.1]. The present document applies for the transparent star satellite network, mesh transparent overlay and mesh regenerative satellite networks as defined in [1], and it is concerned with RCSTs connecting LANs via satellite to other networks like e.g. the Internet, as an implementation of the lower layer protocol layers specified in [1].

The present document is normative for the user plane and control plane, and informative for the management plane. For the latter, the specifications are provided as recommendations to guide in aligning implementations of M and C, aiming at a future enhancement to become a normative specification also for the management plane. For this purpose, the specification provides abstraction models, and recommends protocols and managed objects and structures that relate to these models. The recommendations aim at minimizing the gap between early M and C implementations and a future normative specification for the management plane.

The current non-normative recommendations for the management plane are intended to be extended by implementation dependent adaptation to create bilateral interoperability. The recommendations aim at making such adaptation a simple task.

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 https://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 301 545-2: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite standard".

[2] ETSI TS 102 606: "Digital Video Broadcasting (DVB); Generic Stream Encapsulation (GSE) Protocol".

[3] Recommendation ITU-T X.693: "Information technology - ASN.1 encoding rules: XML Encoding Rules (XER)".

[4] ETSI EN 302 307-1: "Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2".

[5] ETSI TS 102 293: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; IP Interworking over satellite; Multicast group management; IGMP adaptation".

[6] IETF RFC 1812: "Requirements for IP Version 4 Routers", Baker, F., Ed., June 1995.

[7] IETF RFC 1886: "DNS Extensions to support IP version 6", S.Thomson, C. Huitema, December 1995.

[8] IETF RFC 1918: "Address Allocation for Private Internets", Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, February 1996.

[9] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration", S. Thomson, T. Narten, December 1998.

[10] IETF RFC 2465: "Management Information Base for IP Version 6: Textual Conventions and General Group", D. Haskin, S. Onishi, December 1998.

[11] IETF RFC 2863: "The Interfaces Group MIB", K. McCloghrie, F. Kastenholz, June 2000.

[12] IETF RFC 2933: "Internet Group Management Protocol MIB", K. McCloghrie, D. Farinacci, D. Thaler, October 2000.

[13] IETF RFC 3901: "DNS IPv6 Transport Operational Guidelines", A. Durand, J. Ihren, September 2004.

[14] IETF RFC 4241: "A Model of IPv6/IPv4 Dual Stack Internet Access Service", Y. Shirasaki, S. Miyakawa, T. Yamasaki, A. Takenouchi, December 2005.

[15] IETF RFC 4605: "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding (IGMP/MLD Proxying)", B. Fenner, H. He, B. Haberman, H. Sandick, August 2006.

[16] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)", T. Narten, E. Nordmark, W. Simpson, H. Soliman, September 2007.

[17] IETF RFC 1112: "Host Extensions for IP Multicasting".

[18] IETF RFC 1981: "Path MTU Discovery for IP version 6".

[19] IETF RFC 3140: "Per Hop Behavior Identification Codes".

[20] IETF RFC 4294: "IPv6 Node Requirements", Loughney, J., Ed., April 2006.

[21] ETSI EN 302 307-2: "Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 2: DVB-S2 Extensions (DVB-S2X)".

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 EN 301 790: "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems".

[i.2] ETSI TS 101 545-1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 1: Overview and System Level specification".

[i.3] ETSI TR 101 790: "Digital Video Broadcasting (DVB); Interaction channel for Satellite Distribution Systems; Guidelines for the use of EN 301 790".

[i.4] SatLabs System Recommendations.

NOTE: Available at www.satlabs.org.

[i.5] ETSI TR 101 545-5: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 5: Guidelines for the Implementation and Use of TS 101 545-3".

[i.6] ETSI TR 101 545-4: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 4: Guidelines for Implementation and Use of EN 301 545-2".

[i.7] ETSI TS 102 602: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Connection Control Protocol (C2P) for DVB-RCS; Specifications".

[i.8] ETSI TR 102 603: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Connection Control Protocol (C2P) for DVB-RCS; Background Information".

[i.9] Void.

[i.10] IETF RFC 6434: "IPv6 Node Requirements", E. Jankiewicz, Loughney, J., Narten, December 2011.

[i.11] Draft-ietf-behave-sctpnat-06.txt Stewart, R.: "Stream Control Transmission Protocol (SCTP) Network Address Translation", March 2012.

[i.12] "IPDR/SP Protocol Specification,Version 2.1" November 2004, IPDR Inc.

NOTE: Available at https://www.tmforum.org/resources/standard/ipdr-streaming-protocol-specifications-v2-1-reference-implementation-zipipdr_distribution_31_05_2005/

[i.13] IETF RFC 6204: "Basic Requirements for IPv6 Customer Edge Routers" April 2011.

[i.14] IETF RFC 791: "Internet Protocol", Postel, J., STD 5, September 1981.

[i.15] IETF RFC 792: "Internet Control Message Protocol", Postel, J., STD 5, September 1981.

[i.16] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers", Braden, R., STD 3, October 1989.

[i.17] IETF RFC 1142: "OSI IS-IS Intra-domain Routing Protocol", Oran, D., Ed., February 1990.

[i.18] IETF RFC 1350: "The TFTP Protocol (Revision 2)", Sollins, K., STD 33, July 1992.

[i.19] IETF RFC 2131: "Dynamic Host Configuration Protocol", Droms, R., March 1997.

[i.20] IETF RFC 2205: "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, September 1997.

[i.21] IETF RFC 2236: "Internet Group Management Protocol, Version 2", Fenner, W., November 1997.

[i.22] IETF RFC 2328: "OSPF Version 2", Moy, J., STD 54, April 1998.

[i.23] IETF RFC 2347: "TFTP Option Extension", Malkin, G. and A. Harkin, May 1998.

[i.24] IETF RFC 2348: "TFTP Blocksize Option", Malkin, G. and A. Harkin, May 1998.

[i.25] IETF RFC 2349: "TFTP Timeout Interval and Transfer Size Options", Malkin, G. and A. Harkin, May 1998.

[i.26] IETF RFC 2365: "Administratively Scoped IP Multicast", Meyer, D., BCP 23, July 1998.

[i.27] IETF RFC 2453: "RIP Version 2", Malkin, G., STD 56, November 1998.

[i.28] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification", Deering, S. and R. Hinden, December 1998.

[i.29] IETF RFC 2464: "Transmission of IPv6 Packets over Ethernet Networks", Crawford, M., December 1998.

[i.30] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", Nichols, K., Blake, S., Baker, F., and D. Black, December 1998.

[i.31] IETF RFC 2475: "An Architecture for Differentiated Service", Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. WeRcs2, December 1998.

[i.32] IETF RFC 2663: "IP Network Address Translator (NAT) Terminology and Considerations", Srisuresh, P. and M. Holdrege, August 1999.

[i.33] IETF RFC 2750: "RSVP Extensions for Policy Control", Herzog, S., January 2000.

[i.34] IETF RFC 3086: "Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification", Nichols, K. and B. Carpenter, April 2001.

[i.35] IETF RFC 3135: "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations", Border, J., Kojo, M., Griner, J., Montenegro, G., and Z. Shelby, 2001.

[i.36] IETF RFC 3260: "New Terminology and Clarifications for Diffserv", Grossman, D., April 2002.

[i.37] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, July 2003.

[i.38] IETF RFC 3376: "Internet Group Management Protocol, Version 3", Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, October 2002.

[i.39] IETF RFC 3411: "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", D. Harrington, R. Presuhn, B. Wijnen, December 2002.

[i.40] IETF RFC 3449: "TCP Performance Implications of Network Path Asymmetry", Balakrishnan, H., Padmanabhan, V., Fairhurst, G., and M. Sooriyabandara, BCP 69, December 2002.

[i.41] IETF RFC 3810: "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Vida, R., Ed., and L. Costa, Ed., June 2004.

[i.42] IETF RFC 4026: "Provider Provisioned Virtual Private Network (VPN) Terminology", Andersson, L. and T. Madsen, March 2005.

[i.43] IETF RFC 4292: "IP Forwarding Table MIB", Haberman, B., April 2006.

[i.44] IETF RFC 4326: "Unidirectional Lightweight Encapsulation (ULE) for transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)", Fairhurst and B. Collini-Nocker, 2005.

[i.45] IETF RFC 4443: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", Conta, A., Deering, S., and M. Gupta, Ed., March 2006.

[i.46] IETF RFC 4594: "Configuration Guidelines for DiffServ Service Classes", Babiarz, J., Chan, K., and F. Baker, August 2006.

[i.47] IETF RFC 4601: "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, August 2006.

[i.48] IETF RFC 4607: "Source-Specific Multicast for IP", Holbrook, H. and B. Cain, August 2006.

[i.49] IETF RFC 4608: "Source-Specific Protocol Independent Multicast in 232/8", Meyer, D., Rockell, R., and G. Shepherd, BCP 120, August 2006.

[i.50] IETF RFC 4787: "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", Audet, F. and C. Jennings, BCP 127, January 2007.

[i.51] IETF RFC 5135: "IP Multicast Requirements for a Network Address Translator (NAT) and a Network Address Port Translator (NAPT)", Wing, D. and T. Eckert, BCP 135, February 2008.

[i.52] IETF RFC 5163: "Extension Formats for Unidirectional Lightweight Encapsulation (ULE) and the Generic Stream Encapsulation (GSE)", Fairhurst, G. and B. Collini-Nocker, April 2008.

[i.53] IETF RFC 5340: "OSPF for IPv6", Coltun, R., Ferguson, D., Moy, J., and A. Lindem, July 2008.

[i.54] IETF RFC 5382: "NAT Behavioral Requirements for TCP", Guha, S., Ed., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, BCP 142, October 2008.

[i.55] IETF RFC 5424: "The Syslog protocol", Gerhards R., March 2009.

[i.56] IETF RFC 5508: "NAT Behavioral Requirements for ICMP", Srisuresh, P., Ford, B., Sivakumar, S., and S. Guha, BCP 148, April 2009.

[i.57] IETF RFC 5597: "Network Address Translation (NAT) Behavioral Requirements for the Datagram Congestion Control Protocol", Denis-Courmont, R., BCP 150, September 2009.

[i.58] IETF RFC 5625: "DNS Proxy Implementation Guidelines", Bellis, R., BCP 152, August 2009.

[i.59] IETF RFC 5728: "The SatLabs Group DVB-RCS MIB", Combes, S., Amundsen, P., Lambert, M., Lexow, H-P, March 2010.

[i.60] IEEE MAC-48™: "Test procedures and requirements for alternating-current cable terminations used on shielded cables having laminated insulation rated 2.5 KV through 765 KV or extruded insulation rated 2.5 KV through 500 KV".

[i.61] IEEE 802™-2001: "IEEE Standard for Local and Metropolitan Area Networks: "Overview and architecture".

[i.62] IEEE 802.1Q™: "IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks", August 2011.

[i.63] IEEE 802.1D™-2004:"IEEE Standard for Local and Metropolitan Area Networks-Media access control (MAC) Bridges".

[i.64] IETF RFC 1034: "Domain names - concepts and facilities", P.V. Mockapetris, November 1987.

[i.65] IETF RFC 1035: "Domain names - implementation and specification", P.V. Mockapetris, November 1987.

[i.66] IETF RFC 1155: "Structure and identification of management information for TCP/IP-based internets", M.T. Rose, K. McCloghrie, May 1990.

[i.67] IETF RFC 1157: "Simple Network Management Protocol (SNMP)", J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin, May 1990.

[i.68] IETF RFC 1213: "Management Information Base for Network Management of TCP/IP-based internets:MIB-II", K. McCloghrie, M. Rose, March 1991.

[i.69] IETF RFC 1901: "Introduction to Community-based SNMPv2", J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996.

[i.70] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions", S. Alexander, R. Droms, March 1997.

[i.71] IETF RFC 2570: "Introduction to Version 3 of the Internet-standard Network Management Framework", J. Case, R. Mundy, D. Partain, B. Stewart, April 1999.

[i.72] IETF RFC 2575: "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", B. Wijnen, R. Presuhn, K. McCloghrie, April 1999.

[i.73] IETF RFC 2702: "Requirements for Traffic Engineering Over MPLS", D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, September 1999.

[i.74] IETF RFC 2784: "Generic Routing Encapsulation (GRE)", D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000.

[i.75] IETF RFC 3031: "Multiprotocol Label Switching Architecture", E. Rosen, A. Viswanathan, R. Callon, January 2001.

[i.76] IETF RFC 3270: "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen, May 2002.

[i.77] IETF RFC 3410: "Introduction and Applicability Statements for Internet-Standard Management Framework", J. Case, R. Mundy, D. Partain, B. Stewart, December 2002.

[i.78] IETF RFC 3412: "Message Processing and Dispatching for the Simple Network", J. Case, D. Harrington, R. Presuhn, B. Wijnen, December 2002.

[i.79] IETF RFC 3413: "Simple Network Management Protocol (SNMP) Applications".

[i.80] IETF RFC 3414: "User-based Security Model (USM) for version 3 of the Simple Network", U. Blumenthal, B. Wijnen, December 2002.

[i.81] IETF RFC 3415: "View-based Access Control Model (VACM) for the Simple Network Management", B. Wijnen, R. Presuhn, K. McCloghrie, December 2002.

[i.82] IETF RFC 3416: "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", R. Presuhn, Ed, December 2002.

[i.83] IETF RFC 3417: "Transport Mappings for the Simple Network Management Protocol (SNMP)", R. Presuhn, Ed, December 2002.

[i.84] IETF RFC 3418: "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", R. Presuhn, Ed, December 2002.

[i.85] IETF RFC 3419: "Textual Conventions for Transport Addresses", M. Daniele, J. Schoenwaelder, December 2002.

[i.86] IETF RFC 3489: "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, March 2003.

[i.87] IETF RFC 3513: "Internet Protocol Version 6 (IPv6) Addressing Architecture", R. Hinden, S. Deering, April 2003.

[i.88] IETF RFC 3584: "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard", R. Frye, D. Levi, S. Routhier, B. Wijnen, August 2003.

[i.89] IETF RFC 3596: "DNS Extensions to Support IP Version 6", S. Thomson, C. Huitema, V. Ksinant, M. Souissi, October 2003.

[i.90] IETF RFC 3633: "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", O. Troan, R. Droms, December 2003.

[i.91] IETF RFC 3635: "Definitions of Managed Objects for the Ethernet-like Interface Types", J. Flick, September 2003.

[i.92] IETF RFC 3826: "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", U. Blumenthal, F. Maino, K. McCloghrie, June 2004.

[i.93] IETF RFC 4008: "Definitions of Managed Objects for Network Address Translators (NAT)", R. Rohit, P. Srisuresh, R. Raghunarayan, N. Pai, C. Wang, March 2005.

[i.94] IETF RFC 4022: "Management Information Base for the Transmission Control Protocol (TCP)", R. Raghunarayan, Ed, March 2005.

[i.95] IETF RFC 4023: "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)", T. Worster, Y. Rekhter, E. Rosen, Ed., March 2005.

[i.96] IETF RFC 4113: "Management Information Base for the User Datagram Protocol (UDP)", B. Fenner, J. Flick, June 2005.

[i.97] IETF RFC 4188: "Definitions of Managed Objects for Bridges", K. Norseth, Ed., E. Bell, Ed. September 2005.

[i.98] IETF RFC 4271: "A Border Gateway Protocol 4 (BGP-4)", Y. Rekhter, Ed., T. Li, Ed., S. Hares, Ed. January 2006.

[i.99] IETF RFC 4293: "Management Information Base for the Internet Protocol (IP)", S. Routhier, Ed. April 2006.

[i.100] IETF RFC 4364: "BGP/MPLS IP Virtual Private Networks (VPNs)", E. Rosen, Y. Rekhter, February 2006.

[i.101] IETF RFC 5036: "LDP Specification", L. Andersson, Ed., I. Minei, Ed., B. Thomas, Ed. October 2007.

[i.102] IETF RFC 5790: "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", H. Liu, W. Cao, H. Asaeda, February 2010.

[i.103] IETF RFC 2579: "Textual Conventions for SMIv2".

[i.104] IETF RFC 4001: "Textual Conventions for Internet Network Addresses".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Allocation Channel (AC): set of timeslots identified by one Assignment ID that represents a portion of the retun link capacity that is assigned by the NCC to one or more streams of an RCST

assignment identifier: identifier used to indicate the association of a timeslot to the access method and possibly a specific RCST, as well as a specific channel for that RCST

NOTE: Each timeslot is associated with an Assignment ID in the control signalling from NCC to RCST.

assigment ID: identifier composed of the Channel_ID and Logon_ID used in the TBTP2 for allocating MF-TDMA resources to data streams

Behaviour Aggregate (BA): aggregate of packets that share the same network forwarding behaviour

NOTE: Within a Connectivity Aggregate (CA), the traffic of a TC constitutes a Behaviour Aggregate (BA).

Connection Control Protocol (C2P): layer1-2 connection control protocol supporting the regenerative and mesh overlay networking control signalling between the RCST and the NCC

Connectivity Aggregate (CA): comprises the traffic to be sent over a single connectivity channel as the output of a L3 routing or L2 forwarding decision

Connectivity Channel (CC): transmission channel that support a shared transmission from one transmitter to one or several receivers

NOTE: The set of receivers may be limited to only one, like for transparent star (the RCSTs and the gateways).

control plane: part of the layered RCS network architecture that provides the communications for control signalling information

Dedicated Access service (DA service): control plane entity that is defined for each DA allocation channel and that regulates RCST behaviour while forwarding data traffic on the corresponding DA allocation channel (DA-AC)

NOTE: The DA service corresponds to the utilization of a DA-AC.

Differentiated Services Code Point (DSCP): IPv4 header Type Of Service octet or IPv6 Traffic Class octet when interpreted in conformance with the definition given in IETF RFC 2475 [i.31]

Digital Video Broadcasting Return Channel by Satellite (DVB-RCS): architecture for an interaction (or return) channel using satellite links and forming an Interactive Network (DVB-RCS2-S)

Dynamic Connectivity: mechanism defined as the capability to establish, modify, or release links between RCSTs and gateways based upon events occurring on traffic/control or management level

Dynamic Connectivity Protocol (DCP): layer1-2 dynamic connectivity protocol supporting the regenerative and mesh overlay networking control signalling between the RCST and the NCC

feeder: transmits the forward link signal

NOTE: The forward link signal is a standard satellite digital video broadcast (DVB-S or DVB-S2) uplink, onto which are multiplexed the user data and/or the control and timing signals needed for the operation of the Satellite Interactive Network (DVB-RCS2).

Forward Link (FL): satellite link from the NCC and Feeder to the RCSTs DVB-RCS2

Gateway (GW): system that receives the RCST return link signals, and provides the next-hop bi-directional network-layer interface for traffic sent using a star connection

NOTE: In the Star Topology, this includes the functionality of the Feeder that provides the forward link.

Generic Stream Encapsulation (GSE): encapsulation format defined in the Lower layers for use with continuous mode transmission. This is a particular subset of GSE

HID: hardware ID IEEE MAC-48 [i.60], a 6 Byte identifier that is permanently associated with a single RCST

Higher Layers: set of RCS network functions that are defined in the present document

NOTE: These layers perform functions relating to the operation of the network-layer and higher layers and define the interfaces presented to the attached LAN interface(s).

Higher Layer service (HL service): per-hop treatment of Layer 3 PDUs characterized by a PHB

NOTE: A management construct that puts together policy and PHB. The HL service determines any traffic conditioning for the BA, and defines the queue management and scheduling parameters needed to realize the service.

HLS PDU queue: queue in which Layer 3 protocol data units are held, pending transmission under the control of a specific Higher Layer Service

hub: combines a Feeder and Gateway, together with the NCC and NMC

hybrid transparent satellite network: network implemented partly as a transparent star satellite network and partly as a mesh overlay transparent satellite network

interactive network: set of RCSTs, Gateways, and NCC managed by a Satellite Network Operator (SNO)

IP Flow: sequence of IP packets from an IP source to an IP destination

NOTE: An RCST routes a flow considering the network-layer attributes, including: IP source and destination address, protocol type, DSCP.

IP MicroFlow: single instance of an application-to-application flow of packets which is identified by source address, destination address, protocol_id, and source port, destination port (where applicable)

LAN interface: interface presented by the RCST to an attached network, for example using the Ethernet standard

layer 1 mesh overlay system: satellite interactive network that supplements the unidirectional satellite link from a TDM feeder to RCSTs and the unidirectional satellite link from RCSTs to an MF-TDMA gateway with two-way satellite links between the RCSTs

NOTE: In such systems, the NCC is connected to the RCST via the feeder and gateway.

layer 1 regenerative and re-multiplexing system: satellite interactive network that relies on an on-board regenerative processor to demodulate upcoming MF-TDMA data from terminals and generate a TDM downlink signal with this data

NOTE: Such system looks like an RCS second generation system from the layer 1 RCSTs perspective.

Link Stream (LS): sequence of lower layer Payload-adapted PDUs holding the sequence of HLPDUs of the associated SA

lower layers: set of RCS network functions that are defined in the lower layer specification [1]

Lower Layer Service (LLS): control plane entity that maps to any mix of RA services and DA services, serving one or several HL services

NOTE: The LL service may be any combination of DA services and RA services.

M and C: Management and Control

management interface: interface of an RCST that is used for monitoring and management by the satellite service operator

NOTE: The interface is mapped to a layer 2 lable in the management SVN.

management plane: part of the layered RCS network architecture that provides the management of system elements, along with configuration of elements, monitoring of performance and the communications to maintain the network and to perform peraitonal functions

mesh connection: unidirectional or bidirectional connection over one mesh link or two oppositely directed mesh links connecting a pair of RCSTs, or a unidirectional connection over one mesh link connecting one RCST to a set of RCSTs

mesh link: link from an RCST to another RCST or a set of RCSTs that does not rely upon the signal being relayed by the Gateway

multicast: communication capability, which denotes unidirectional distribution from a single source access point to one or more destinations (a set of RCSTs and/or the Gateway)

Multiprotocol Label Switching (MPLS): transmission mechanism defined in IETF RFC 3031 [i.75]

NOTE: It operates between the link and network layers of the OSI model to unify the data transport service for circuit-based networks and packet based. It is also used to implement QoS and VPN features for packet switching over IP.

Network Control Centre (NCC): provides control and monitoring functions

NOTE: It generates control and timing signals for the operation of the Satellite Interactive Network to be transmitted by one or several Feeder Stations (DVB-RCS2-S).

Network Management Centre (NMC): responsible for NCC, RCST, Gateways and OBP management functions

NOTE: Management messages from the NMC are forwarded to the NCC, which transmits them to the RCSTs if required (DVB-RCS2-S).

northbound interface: interface to the OSS that provides high-level network management and configuration functions

On-Board Processor (OBP): router or switch or multiplexer in the sky; it can decouple the uplink and downlink air interface formats (modulation, coding, framing, etc.)

Operator Virtual Network (OVN): network built using the Interactive Network to support a service managed by an SNO (Satellite Network Operator)

Per Hop Behaviour (PHB): HLS entity identified by a PHB_ID associated with a HLS service that defines the queuing, policing, and scheduling parameters as a set of policies, needed to realize a specific QoS Class defined by DiffServ architecture (IETF RFC 2475 [i.31]) and to process one specific hop (IETF RFC 3086 [i.34])

PHB group: set of one or more PHBs that can only be meaningfully specified and implemented simultaneously, due to a common constraint applying to all PHBs in the set, to provide a service building block that allows a set of related forwarding behaviours to be specified together

NOTE: A single PHB is a special case of a PHB group. Common constraints can be queue servicing or queue management policy (IETF RFC 3260 [i.36]).

Quality of Service (QoS): network ability to provide service differentiation/guarantees and thus influence the perceived quality of communications with regard to a number of parameters (including delay, jitter, packet loss) experienced by packets in a Behaviour Aggregate when transferred by the interactive network

Random Access service (RA service): control plane entity that is defined for each RA allocation channel (RAAC) and that regulates RCST behaviour while forwarding data traffic on the corresponding RAAC and provides the allowance to load a specific RA allocation Channel (RAAC)

NOTE: The RA service corresponds to the utilization of a specific RAAC.

Request Class (RC): layer 2 entity in the control plane that identifies both a specific connectivity and a specific traffic aggregate and acts as a reference to the resource model for one or a set of link streams identifying the resources allocation policy and connectivity associated with the flow that generated the RC

NOTE: If a different connectivity is required (e.g. in a mesh case), the RCST specifies a different RC. The RC identifies both a specific connectivity and a specific traffic aggregate. Each RC can support any mix of Capacity Categories [1], this mapping is provided by the LL service configuration. The behaviour of an RC is not defined by the set of capacity categories but by the relation to HL services that map to the LL services and RC.

Return Channel via Satellite Terminal (**RCST):** terminal that combines the lower-layer specifications between [1] and the present document

Return Link (RL): Stream from the RCST to the NCC or Gateway

Return Link Encapsulation (RLE): encapsulation format defined in the Lower Layers Specification for use with burst-mode waveforms

NOTE: This has a similar higher-layer interface to GSE.

Satellite Virtual Network (SVN): logical subdivision of the network infrastructure. Traffic in one SVN is handled independently of traffic in other SVNs

NOTE: One SVN is reserved for management of all RCSTs in an Interactive Network. One of more SVNs may be combined to form a VRF Group.

Service Aggregate (SA): logical combination or multiplex of HLPDUs of one or more Behaviour Aggregates that use the same Lower Layer service and are associated to a Link Stream (LS)

star connection: connection where traffic is sent to or from a Gateway

NOTE: The Gateway and an RCST are next hop neighbours at IP network level.

SVN-MAC: 3 byte label that uniquely identifies a layer 2 endpoint within the Interactive network

NOTE: Each RCST is dynamically allocated one SVN-MAC for management, and at least one SVN-MAC for user plane traffic.

Traffic Class (TC): description of flows that are assigned to the same BA define by a traffic filter in terms of a DSCP or other characteristics that may distinguish a subset of HL PDUs in a larger aggregate and identifies the traffic that receives the same treatment within the satellite Interactive Network

traffic conditioning: control functions that can be applied to a Behavior Aggregate, application flow, or other operationally useful subset of traffic, e.g. routing updates (IETF RFC 2475 [i.31])

NOTE: This may include metering, policing, shaping, and packet marking. Traffic conditioning is used to enforce agreements between domains and to condition traffic to receive a differentiated service within a domain by marking packets with the appropriate DCSP and by monitoring and altering the temporal characteristics of the aggregate where necessary.

traffic stream: administratively significant set of one or more microflows which traverse a path segment

NOTE: A traffic stream may consist of the set of active microflows which are selected by a particular classifier.

unicast: communication capability, which denotes unidirectional distribution from a single source access point to a single specified destination access point (RCST or Gateway)

user plane: communications that carry user information in the RSC network architecture to provide the transfer of user data, along with associated controls (e.g. flow control, recovery from errors, etc.)

Virtual LAN (VLAN): term specified by IEEE 802.1Q [i.62] that defines a method of differentiating and separating traffic on a LAN by tagging the Ethernet frames

Virtual Routing/Forwarding (VRF) group: collection of one or more SVNs that share a common addressing space with an independent set of forwarding and routing tables that allow independent use of addresses in the private range in different VRFs

NOTE: A NAT gateway is required to communicate between VRF Groups that use overlapping network address spaces.

3.2 Symbols

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

Eb/N0	Ratio between the energy per information bit and single sided noise power spectral density
Es/N0	Ratio between the energy per transmitted symbol and single sided noise power spectral density
f0	Carrier frequency
fN	Nyquist frequency
NR,max	Number of replicas in a frame
Nrand	12-bit random number used as a random seed value during CRDSA frame decoding
Nslots	Number of the slots in the frame
Rs	Symbol rate corresponding to the bilateral Nyquist bandwidth of the modulated signal

3.3 Abbreviations

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

AAAA	Authentication Authorization Accounting Auditing
AAL	ATM Adaptation Layer
AC	Allocation Channel
ACM	Adaptive Coding and Modulation
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AF	Assured Forwarding PHB
AQM	Active Queue Management
AR	Address Resolution
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
BA	Behavior Aggregate
BE	Best Effort service class
BER	Bit Error Ratio
BGP	Border Gateway Protocol
BoD	Bandwidth-on-Demand
BPSK	Binary Phase Shift Keying
BRX	Burst in Reception
BSM	Broadband Satellite Multimedia
BUC	Block Up Converter
BW	BandWidth
C2P	Connection Control Protocol
CA	Connectivity Aggregate
CAC	Connection Admission Control
CBR	Constant Bit Rate
CC	Capacity Class
CCM	Constant Coding and Modulation
CD	Critical Data
CIR	Carrier to Interference Ratio
CL	Controlled Load service class
CLI	Command Line Interface
CMF	Control and Monitoring Functions
CMI	Control and Management Interface

CNR	Carrier Noise Ratio
CR	Capacity Request
CRA	Constant Rate Assignment
CRC	Cyclic Redundancy Check
CRDSA	Contention Resolution Diversity Slotted Aloha
CSC	Common Signalling Channel
CW	Continuous Wave
DA	Dedicated Assignment
DA-AC	Dedicated Access Allocation Channel
DAMA	Demand Assignment Multiple Access
DC	Direct Current
DCCP	Datagram Congestion Control Protocol
DCP	Dynamic Connectivity Protocol
DF	Don't Fragment flag
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DNS	Domain Name Service
DR	Designated Router
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DVB	Digital Video Broadcasting
DVB-S2	Digital Video Broadcasting - Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications
DVB-S2X	Digital Video Broadcasting - Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications: S2-Extensions
DVB-S2(X)	DVB-S2 / DVB-S2X
EE	Excellent Effort service class
EF	Expedited Forwarding PHB
EIRP	Equivalent Isotropic Radiated Power
eTOM	enhanced Telecommunication Operations Map
FCA	Fault, Configuration, Accounting
FCAPS	Fault, Configuration, Accounting, Performance, Security management
FEC	Forwarding Equivalence Class
FIFO	First In First Out
FL	Forward Link
FLSS	Forward Link SubSystem
FPDU	Frame PDU
FTP	File Transfer Protocol
GS	Generic Stream
GSE	Generic Stream Encapsulation
GW	GateWay
GW-RCST	GateWay RCST
HL	Higher Layer
HLPDU	Higher Layer PDU
HLS	Higher Layers (Satellite)
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDU	InDoor Unit
IETF	Internet Engineering Task Force
IFL	Inter-Facility Link
IF-MIB	Interfaces MIB
IGMP	Internet Group Management Protocol
IN	Interactive Network
INID	Interactive Network ID
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
IP-MIB	IP MIB
IPSEC	IP Security
ISI	Input Stream Identifier

IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
JT	Jitter Tolerant
KB	Kilo Bytes
L1	Physical Layer
L2	Link Layer
L3	Network layer
LANS	Local Area Networks
LDP	Label Distribution Protocol
LER	Label Edge Router
LL	Lower Layer
LLQ	Low Latency Queuing
LLS	Lower Layer Service
LNB	Low Noise Block
LQC	Link QOS Class
LS	Link Stream
LSP	Label Switched Paths
LSR	Label Switched Router
MAC	Medium Access Control
MAC24	A 24 bit MAC address
MAC48	A 48 bit MAC address
MBGP	Multi-protocol Border Gateway Protocol
MCRP	Multi-Channel Routing Protocol
MF-TDMA	Multi Frequency-Time Division Multiple Access
MIB	Management Information Base
MIB-II	Management Information Based version II
MLD	Multicast Listener Discovery
MMT	Multicast PID Mapping Table
MMT2	Multicast label Mapping Table
MPE	Multi-Protocol Encapsulation
MPEG	Moving Picture Experts Group
MPLS	Multi-Protocol Label Switching
MRIB	Multicast RIB
MSDP	Multicast Source Discovery Protocol (of ASM)
MTU	Maximum Transmission Unit
NA	Not-Accessible
NAPT	Network Address Port Translator
NAT	Network Address Translation
NBMA	Non-Broadcast Multiple Access
NC	Network Control service class
NCC	Network Control Centre
NCC/GW	Network Control Center/GateWay
NCC_ID	Network Control Center IDentifier
NCR	Network Clock Reference
ND	Neighbour Discovery
NIT	Network Information Table
NLID	Network Layer Information Descriptor
NMC	Network Management Centre
OAM	Operations And Management
OBP	On Board Processor
ODU	OutDoor Unit
OID	Object IDentifier
ONID	Original Network ID
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operations Support System
OUI	Organizationally Unique Identifier
OVN	Operator Virtual Network
PCP	Priority Code Point
PDP	Policy Decision Point (of DS)
PDR	Peak Data Rate
PDU	Protocol Data Unit

PEP	Policy Enforcement Point (of DS)
PEP	Protocol Enhancing Proxy (Agent)
PHB	Per Hop Behavior
PHY	Physical Link
PID	Program IDentifier
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast - Sparse Mode
PMTUD	Path MTU Discovery
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RA	Random Access
RA-AC	Random Access Allocation Channel
RBDC	Rate-Based Dynamic Capacity
RC	Request Class
RCS	Return Channel via Satellite
RCS-MAC	RCS Medium Access Control address
RCST	Return Channel via Satellite Terminal
RED	Random Early Detection
RFC	Request For Comments (IETF)
RIB	Routing Information Base
RIP	Routing Information Protocol
RL	Return Link
UL	UpLink
RLE	Return Link Encapsulation
RLSS	Return Link SubSystem
RMT	RCS Map Table
RO	Read-Only
RPLS	Return Path Link Subsystem
RRM	Radio Resource Management
RSPEC	Resource SPECification
RSVP	Resource reSerVation Protocol
RT	Real Time
RTN	ReTurN
RTP	Real-time Transfer Protocol
RW	Read-Write
SA	Service Aggregate
SAMI	Subscriber Account Management Interface
SAMIS	Subscriber Account Management Interface System
SAP	Service Access Point
SCADA	Supervisory Control And Data Acquisition
SCPC	Single Carrier Per Channel
SCTP	Stream Control Transport Protocol
SD	Satellite Dependent
SDDP	Software and Data Distribution Protocol
SDR	Sustainable Data Rate
SDU	Service Data Unit
SI	Satellite Independent/Service Information
SIP	Session Initiation Protocol
SI-SAP	Satellite Independent SAP
SLA	Service Level Agreement
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SNO	Satellite Network Operator
SO	Satellite Operator
SP	Service Provider
SVN	Satellite Virtual Network
SVNMAC	Satellite Virtual Newtork MAC
SVN-MAC	SVN Medium Access Control label
SVNO	Satellite Virtual Network Operator
SW	SoftWare

SWDL	SoftWare DownLoad
SYNC	SYNChronization burst
TBTP	Time Burst Time Plan
TC	Traffic Class
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TFTP	Trivial File Transfer Protocol
TID	Transfer IDentifiers
TIM-b	Terminal Information Message broadcast
TIM-u	Terminal Information Message unicast
TMN	Telecommunications Management Network
TRF	TRaFfic burst
TS	Transport Stream
TS-GW	Transparent Gateway
TSPEC	Traffic SPECification
TTL	Time To Live
TX	Transmission
TXID	Transmission IDentifier
UDP	User Datagram Protocol
ULE	Unidirectional Lightweight Encapsulation
USM	User-based Security Model
VBDC	Volume-Based Dynamic Capacity
VCM	Variable Code Modulation
VI	VIdeo service class
VLAN	Virtual LAN
VO	VOice service class
VoIP	Voice over IP
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WRQ	Write ReQuest
XML	eXtensible Markup Language

4 Reference System Architecture

4.0 Introduction

DVB-RCS2 is the standard conceived to provide a standardized broadband interactivity connection as an extension of the Digital Video Broadcasting Satellite systems. It defines the MAC and physical layer protocols of the air interface used between the satellite operator hub and the interactive user terminal. It embraces the DVB-S and the DVB-S2(X) standards implemented in the commercial broadcasting environment, exploiting economics of scale.

To support interoperability, the DVB-RCS2 specification describes Higher layers components adapted to satellite interactive systems. These components are parts of control and management planes and rely mainly on DVB and IETF standards or are derived from them.

A typical DVB-RCS2 Interactive Network will utilize a satellite with multi or single beam coverage. In most networks, the satellite carrying the forward link signal will also support the return link. The forward link carries signalling from the NCC and user traffic to RCSTs. The signalling from the Network Control Centre (NCC) to RCSTs that is required to operate the return link system is called "Forward Link Signalling". A Network Management Centre (NMC) provides overall management of the system elements and manages the Service Level Agreement (SLA) assigned to each RCST.

The NCC is the central entity that supports control signalling via the Lower Layer Signalling (L2S) and the NMC is a central entity that support management signalling via IPv4.

4.1 System Roles

The system roles are defined by the DVB-RCS2 system specification [i.1]. This clause provides an informative description of roles and stakeholder/actors and their interaction/relationship in the context of the DVB-RCS2 high-level system architecture. This description is provided to help understanding of the framework of DVB-RCS2 management and control operations.

A role is defined by a logical grouping of responsibilities, with the intention of providing a generic framework for related functional entities with appropriate granularity, in order to allow role mapping to one or more real-life (physical) element(s) or entity(ies). A single role can be a real-life actor or multiple roles can be combined in one business actor. A role may have business responsibilities and/or technical responsibilities.

The system roles considered in a DVB-RCS2 system are defined in the system specification [i.1] and are illustrated by the model shown in the next figure 4.1. These definitions are included for convenience in the present document, as an introduction to HLS addressing concepts.

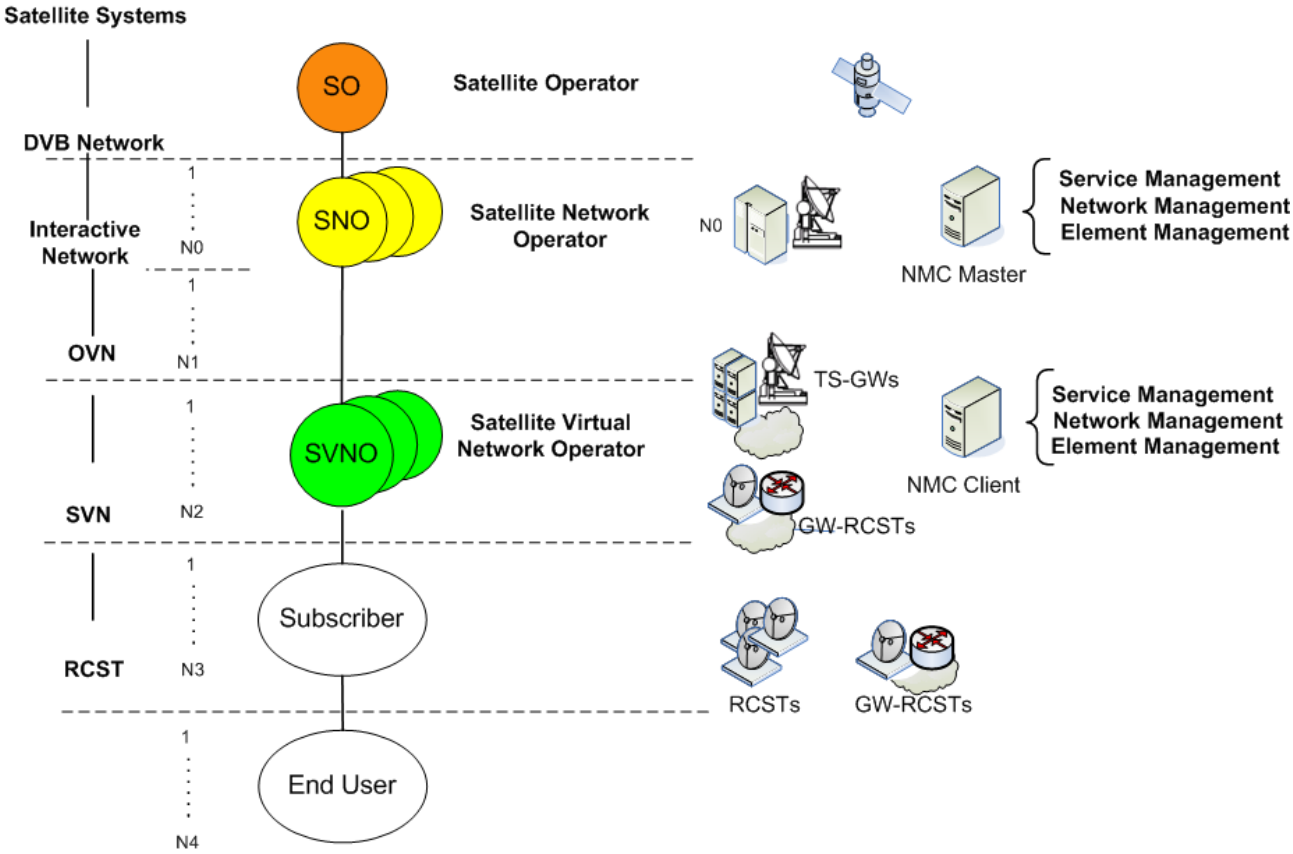


Figure 4.1: DVB-RCS2 actors and roles

- **The Satellite Operator** (SO) provides the satellite space segment and the satellite ground facility, consisting primarily of the Satellite Operating Centre. It owns and is responsible for maintaining, managing, deploying and operating the satellite and for all regulatory matters related to this operation. It sells capacity at transponder level to one or several SNOs.

NOTE 1: In a regenerative satellite system, the SO exchanges OBP configuration and status data with the SNO.

- **Satellite Network Operators (SNO)** are assigned one or more satellite transponders that they use to provide transmission and connectivity resources via the satellite system. The SNO operates in a DVB network, identified by an ONID. Each SNO controls its own capacity, owns at least one Hub/NCC and the NMC, and configures the time/frequency plan. Each IN is managed by the SNO (one DVB-RCS2 system). In the transparent architecture, the SNO controls the transparent gateway. The SNO may divide the interactive network into one or more **Operator Virtual Networks (OVN).** SNOs distribute their own physical and logical resources among OVNs. An OVN allows a defined subset of the RCSTs to form an RCS network that is independently controlled and managed by a Satellite Virtual Network Operator (SVNO). SVNOs are also called Service Providers, or SPs. Each SVNO will manage one or several OVNs. Some examples of SPs are an ISP, Telco or VPN SP. System physical resources are distributed among OVNs. The OVN is the base of the contract between the SNO and the SVNO.

NOTE 2: For the mesh regenerative systems, there is a master SNO, controlling the Network Operation Centre (for OBP configuration), and secondary SNOs. The master SNO does not necessary use a single NCC/NMC.

- **Satellite Virtual Network Operators (SVNO)**, are assigned one or more Operator Virtual Networks (OVN).Each OVN is given some physical (e.g. peak and guaranteed kbps or frequency bandwidth, depending on the system definition) and logical (e.g. one Group_ID, a set of SVN numbers) resources. An active RCST can only be a member of one OVN. This is assigned at logon to the RCS Network. Each OVN is assigned a pool of SVN numbers from which it can allocate SVN-MAC addresses. The SVN concept is used to logically divide the addressing space controlled by the operator. SVNOs sell connectivity services to their subscribers. In a regenerative architecture, a SVNO may also manage one or several GWs.

- A subscriber is connected to the network via an RCST, with the service provided by one SVNO. Although an RCST may belong to only one OVN, it may participate in several SVNs, associated to the same SVNO.

- End-users are the physical person(s) or entity (e.g. application) that use(s) the subscribed satellite services. They use the RCSTs or hosts connected to the RCST LAN interface.

The RCST determines the ONID and INID from the Forward Link acquisition. They are indirectly determined by the start-up Forward Link and the population_Id, configured in advance in the RCST. The RCST understands the combination of {ONID, INID} as the SNO domain.

NOTE 3: A combination of {ONID, INID} identifies the network as an administrative entity to the RCST and thus implicitly, the SNO domain.

The NMC may exist as two principally types in a network, one used by the SNO and one used by the SVNO. The SVNO may have a back end connection to the SNO NMC.

One single terminal may be managed concurrently by one SNO and one SVNO. This applies to the consumer linear, consumer CPM, corporate, SCADA linear, SCADA CPM, backhaul and Institutional. This terminal belongs to the end user that assumes its cost. This subscriber will have one service package with the SNO or SVNO.

A multi-dwelling Satellite Terminal comprises multiple subscribers at a single location that share the terminal to access satellite broadband services. These subscribers belong to different domains or organizations differentiated by IP addressing. The RCST does not belong to one specific end user but to the SVNO. The service packages available to the residents of the multi-dwelling terminal are generally the same as those offered to typical consumers.

4.2 Higher Layer functional modules

Each RCST belongs to one RCS Interactive Network. The RCS Interactive Network complies the organization of the ISO/OSI protocol stack with protocol layers grouped into three layers:

- Physical layer (L1), specified by the DVB-RCS2 Lower Layer Specification

- Link layer (L2), partially specified by the DVB-RCS2 Lower Layer Specification

- Network layer and above (L3+), the main focus of the present document.

The RCS Interactive Network is further organized in three planes:

- User-plane (U-plane)

- Control-plane (C-plane)
- Management-plane (M-plane)

RCS functional modules can be logically placed in one or more of the three protocol layers (PHY, L2, L3+), and in one of the planes (U-, C, M-plane) as represented in figure 4.2.

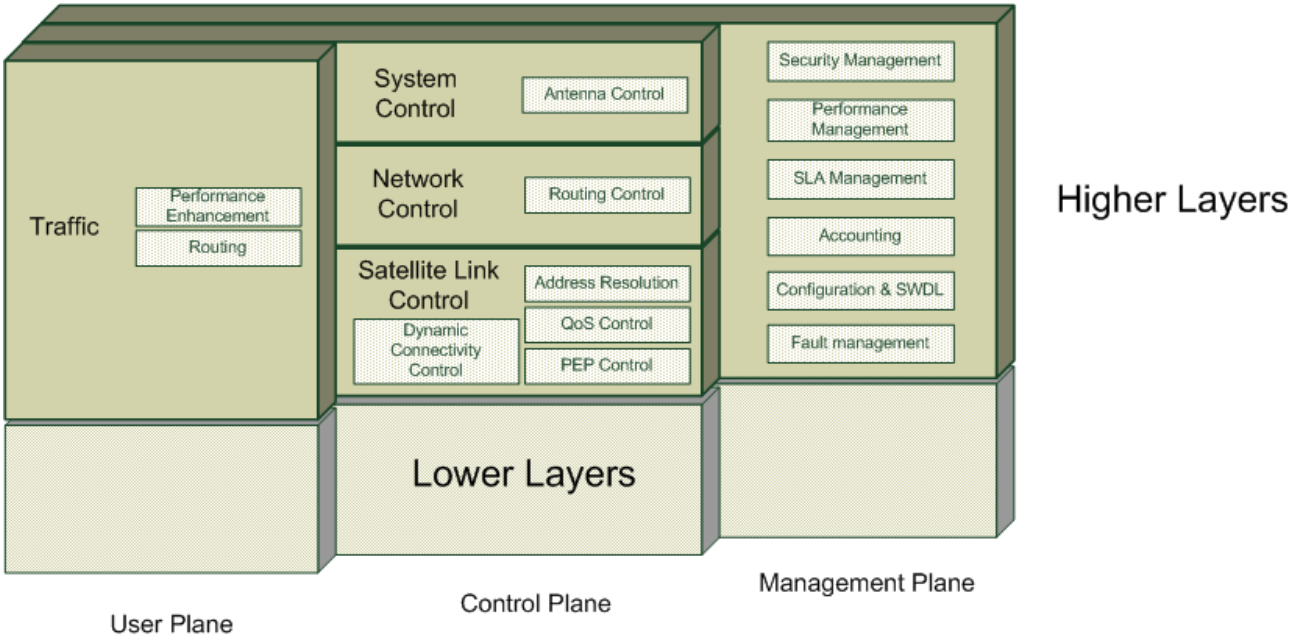


Figure 4.2: Higher layers functional modules

Figure 4.2 shows a simplified model that identifies the higher layer components and associates each with the corresponding plane. The present document defines link-layer functions relating to the operation of the network as a whole, other link layer functions are defined in [1] covering the full management plane. The main focus of the present document is the operation of protocols and networking functions at and above the network-layer.

All user plane functions of the interactive network for the present document, are performed in the DVB-RCS2 higher layers context.

4.3 Reference Architecture for Higher Layers

The RCST Higher Layers functional modules interface with:

- NCC Control and Monitoring Functions (CMF). This generates control and timing signals for the operation of the RCS Interactive Network. The signals are transmitted by one or several Feeders. The NCC is the central entity that supports signalling via the Lower Layer Signalling (L2S) as specified in [1].
- NMC management functions for Fault, Configuration, Accounting, Performance, Security (FCAPS) management. It transmits management signals using a Feeder.
- A set of one or more RCSTs that provide user traffic in star or mesh connectivity to end users.

The management functions performed in the NMC support the interface with an OSS for business management functions.

The DVB-RCS2 higher layers context covers the management and control functions that to be performed by an RCST at the higher layers, excluding the physical interfaces or transmission mechanisms covered in [1].

The reference architecture for the Higher Layers is represented in figure 4.3. The reference architecture is divided into three different planes. Each higher layer function can be mapped to one of these planes and in different elements as shown in the figure 4.3.

The RCST has two physical interfaces:

- Satellite interface
- LAN interface

An RCST satellite interface (layer 1) supports several Link Interfaces (layer 2), that again may have a User and control Interface (Layer 3) and an RCST Management and Control Interface (layer 3+).

The RCST is associated with their higher layer traffic interface types:

- Satellite User and Control Interface
- Satellite RCST Management and Control Interface
- LAN User and Control Interface
- LAN RCST Management and Control Interface

The Hub shares the satellite interface with the RCST, and has also another physical interface, Back-end interface, the latter with Higher Layer Traffic Interfaces:

- Back-end User and Control Interface
- Back-end Entity Management and Control Interface

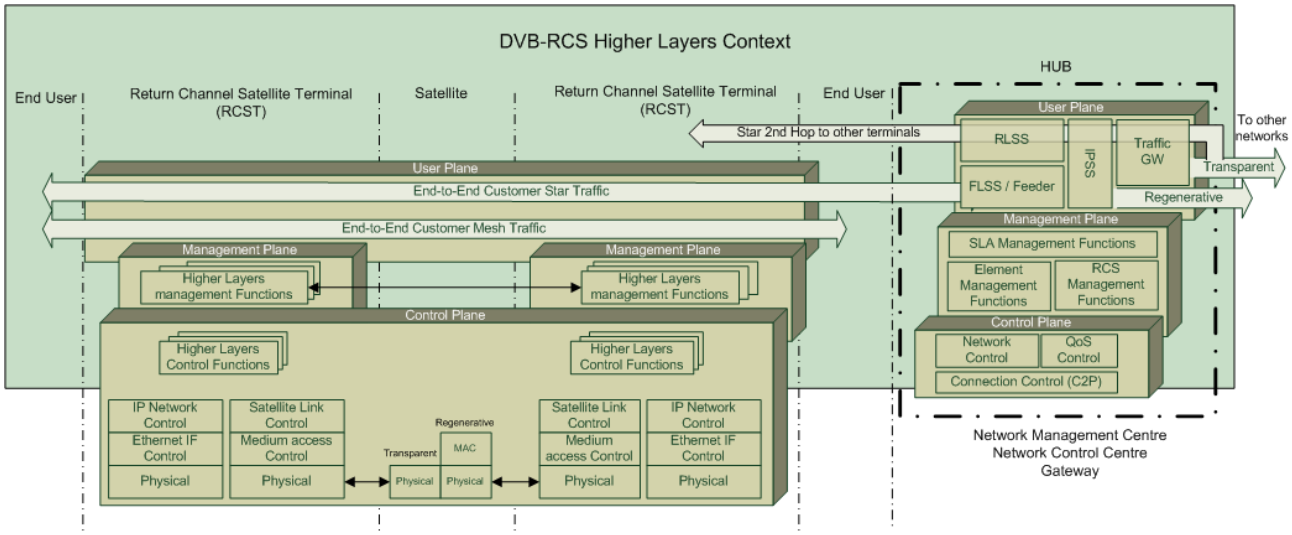


Figure 4.3: Elements functional architecture mapped in user, control and management planes

5 Operator Virtual Networks (OVN), SVNs and VRFs

This clause details administrative aspects of the RCST.

Each RCST shall be associated with a single OVN at logon. The OVN function operates in the management plane. It allows partitioning of the RCS network into independent and isolated sub-networks, where each sub-network comprises a set of network elements sharing a certain pool of resources.

An OVN is composed by one or more Satellite Virtual Networks (SVNs). An OVN consists of a managed routed IP address space. Multiple SVNs may be used to divide an IP network into multiple subnetworks, resembling the use of VLANs for controlling the scope of broadcast packets and logical separation of the user traffic. In addition, an OVN may use SVNs to control IP addressing through the Virtual Router Forwarding (VRF) function. An SNO or SVNO that wishes to independently assign a private address to an SVN shall assign the SVN to a VRF group (i.e. this allows an SNO or SVNO to re-use the same private IP address range as used in other SVNs).

The RCST shall comply to the OVN addressing plan and routing information provided by the SNO or the SVNO.

A Virtual Routing Forwarding (VRF) Group has the following properties:

- When IP routing is used, the set of IP addresses shall be coordinated within all SVNs that comprise a VRF group: each IP address shall uniquely identify a single IP interface. Address re-use (overlapping) is allowed for an address in the private IP address range (IETF RFC 1918 [8]) or an IPv6 Unique Local Address, providing that the reuse is in a different VRF group.
- When MAC bridging is used, each VRF Group consists of a unique set of bridged layer 2 addresses.
- A VRF Group is normally assigned to one OVN. An OVN that supports multiple VRFs, allows an independent addressing plan in each VRF Group.

A multi-dwelling terminal shall support several SVNs, each one of them may correspond to a different Internet Service Provider. All these SVNs are controlled by the same SVNO and belong to the same OVN.

The complete addressing plan of each OVN includes:

- The set of SVN to be used and, assignment of each SVN to a VRF Group.
- The list of network addresses on the LAN Interface of each RCST assigned to an OVN.
- The default Gateway for each RCST (if any) and the list of Gateways that the RCST may access by following a certain criteria (e.g. traffic congestion, multicast capabilities, etc.)

The VRF of an RCST connects with the link interfaces (Layer 2) that supports user traffic.

6 Satellite Virtual Network (SVN) addressing

6.0 Introduction

This clause provides an overview of the SVN addressing resolution required in the context of the HLS, in other words, the binding between the addresses used at layer 2 and the network layer interfaces, such as IP Multicast and Satellite Virtual Networks (SVNs).

6.1 SVN-MAC identifier

An RCST is uniquely identified within one SVN at layer 2 by a 3 byte SVN-MAC label. The SVN-MAC label equals the RCS-MAC of 24 bit length used in [1]. The value of the SVN mask indicates the number of bits in the SVN-MAC (from the most significant) that is interpreted as the SVN number, as shown in figure 6.1.

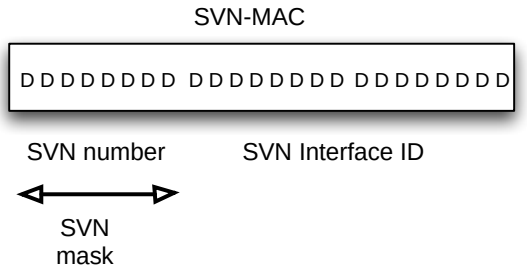


Figure 6.1: Relationship of SVN-MAC, SVN_mask, SVN number and SVN Interface ID

The SVN-MAC label is used for identification of the layer 2 destination in packets transmitted using the RCS Interactive Network.

6.2 IP unicast address resolution to SVN-MAC

6.2.0 Introduction

A PDU sent using the return link in the star or mesh topology may carry an indication of the SVN, or suppress this and imply the SVN at the receiving Gateway. When the label is suppressed, the Gateway may utilize the TBTP2 to derive the RCST source address and knowledge that the traffic is directed to the gateway. The LLS can associate traffic with an SVN and provide transmission with neither a L2 source nor a destination address.

6.2.1 IPv4 address resolution for M and C SVN-MAC

The RCST shall be assigned one SVN-MAC label for management and control, as configured by the SNO during logon (see clause 8). SVN number zero is reserved for the SNO management and control in the OVN to which the RCST belongs. All RCSTs are therefore a member of the zero SVN.

PDUs received by an RCST with the assigned management SVN-MAC label shall be passed for host-processing by the RCST and passed to the control and management function within the higher layers.

A Gateway is able to identify M and C messages by the IPv4 address of the RCST, and therefore the SVN-MAC label needs not be sent on the return link, only the SVN number, since the LLS provides functions to identify the SVN.

The SNO-NMC connects via a management interface (SVN zero) that does not support a User and Control interface.

NOTE: Certain implementations may require the SVN-MAC label sent in the return link to easily identify the RCST for M and C.

6.2.2 Network address resolution to user traffic SVN-MAC

The RCST shall support at least one traffic interface, with a non-zero SVN. An SVNO may configure additional traffic interfaces by assigning additional SVN-MAC labels to an RCST that support this, also with a non-zero SVN. Each RCST traffic interface shall be identified by a SVN-MAC label, unique within the SNO forwarding link traffic multiplex. The SVN-MAC and SVN mask allows an RCST to identify the corresponding SVN number.

The SVNO-NMC connect via a management interface (SVN) that may support User and Control Interface.

NOTE 1: The SNO domain may use one or more multiplex streams. Each multiplex stream specification then indicates a forward link traffic multiplex for the RCS map service as specified in [1].

The RCST shall support SVNO management signalling using any assigned traffic SVN.

Within the OVN an RCST shall be assigned one or more IPv4 address corresponding to the configured SVN-MAC labels. The IPv4 address shall be unique within a VRF Group. In addition, the RCST shall allow the SVN-MAC interface to be assigned an IPv6 address and may support other network addresses.

NOTE 2: An RCST that is assigned multiple SVN-MAC labels corresponding to multiple traffic SVNs will normally also be assigned a separate IP address for each SVN-MAC (e.g. an IPv4 or IPv6 address). These addresses may be presented on separate physical LAN interfaces or separate VLAN sub-interfaces providing connectivity to multiple routed networks.

NOTE 3: The LLS includes mechanisms for SVN identification that allow it to suppress transmission of the SVN-MAC on a return link.

6.2.3 Multicast address resolution to a multicast SVN-MAC

The RCST shall support IP multicast addresses mapping to a SVN-MAC label using a mapping defined per SVN or via an explicit mapping indicated in the MMT2 signalling [1]. A multicast group shall be available to receivers in different SVNs using the shared address space as indicated in MMT2. The layer 2 mapping from an IP group destination address to a L2 SVN-MAC is specified in the LL [1]. This shall be performed using one of the two methods below:

- An implicit mapping based on a hash of the layer 3 network address to one of a range of SVN-MAC multicast labels.

This mapping is independent for each SVN. The SNO therefore defines the size of the mask for each SVN. It is important that multicast network addresses used in SVNs that belong to different VRF Groups may be identical but correspond to different multicast groups and need to be handled separately. This direct mapping is simple, but a restricted range of SVN-MAC addresses increases the risk of aliasing in which more than one independent layer 3 multicast group is mapped to the same layer 2 address. This mapping may be restricted to either IPv4 or IPv6. When both IPv4 and IPv6 are supported, the two sets of addresses may be mapped to the same block of SVN addresses. However this can also result in overlap between IPv4 and IPv6 multicast. This overlap between address ranges does not currently exist when utilizing Ethernet and could have unwanted side-effects and the operator is therefore provided with flexibility to separate the two address spaces by utilizing one bit in the SVN-MAC to indicate whether the mapping is for IPv4 and IPv6.

- An explicit mapping indicated in the MMT2 as defined in [1].

The MMT2 structure allows an RCST to differentiate aliasing for different network protocol address ranges e.g. so high rate streams e.g. this could allow a specific flow to be explicitly mapped to a layer 2 label. The simplest MMT contains one record per SVN that indicates the SVN-MAC range (i.e. mask size) that is to be used for mapping multicast traffic. This usage resembles the use with the direct mapping and would be functionally identical when the mask is configured to have the same length. The MMT2 may be used to support a network group that is accessible from more than one SVN and is mapped to a common SVN-MAC. In this particular case the SVN-MAC does not reside within the SVN for which the content will be received. The SNO is responsible for such system-wide co-ordination of the use of SVN-MACs. The MMT2 may also be used to support non-IP multicast services.

In addition, the RCST may use this third method:

- A mapping directly to a unicast SVN-MAC label assigned to an RCST.

In this case the RCST will unconditionally receive the multicast stream, and will perform any required filtering at the layer 3 interface, based on the contents of its IGMP/MLD group membership or PIM-SM forwarding state. This method shall be exclusive and shall not be used when a multicast-mapped address is used. The group address shall not be announced in the MMT2 for the SVN to which the SVN-MAC belongs. This rule is to prevent the packet being replicated and duplicate copies received by the same layer 3 interface.

These methods are specified for the IPv4, IPv6 and MAC address families, and may be used with any format. The choice of appropriate method depends on the goals of SVNO and SNO and shall be given at RCST logon following clause 9.

7 Network Layer Functions

7.0 Introduction

The RCST network layer functions may comprise:

- **Methods to exchange L2 LAN information** - i.e. how LAN information is exchanged between an RCST and a Gateway to enable L2 packet forwarding.
- **Methods to exchange L3 routing information** - i.e. how dynamic routing information is exchanged between an RCST and a Gateway to enable IP packet forwarding.
- **Interface between the network layer to the satellite lower layer** - i.e. how to map network layer services to satellite lower layer services, such as QoS.

RCST support for bridging is an implementation dependent feature.

7.1 Network Interfaces and Forwarding

An RCST shall support the following forwarding modes:

- Layer 3 IPv4 user traffic packets forwarding
- Layer 3 IPv6 user traffic packets forwarding

- Dual stack IPv4/IPv6 forwarding

An RCST may support forwarding of the following types of PDUs:

- Layer 3 VLAN tag IP routing
- Layer 2 Ethernet Frames - when working in Bridge Mode: VLAN bridging or Ethernet bridging
- Layer 3 non-IP packets: MPLS bridging or X.25 bridging

The optional support is implementation dependent.

The RCST unicast IP packet forwarding function towards the LAN or satellite interface follows the procedure for typical packet processing outlined in figure 7.1.

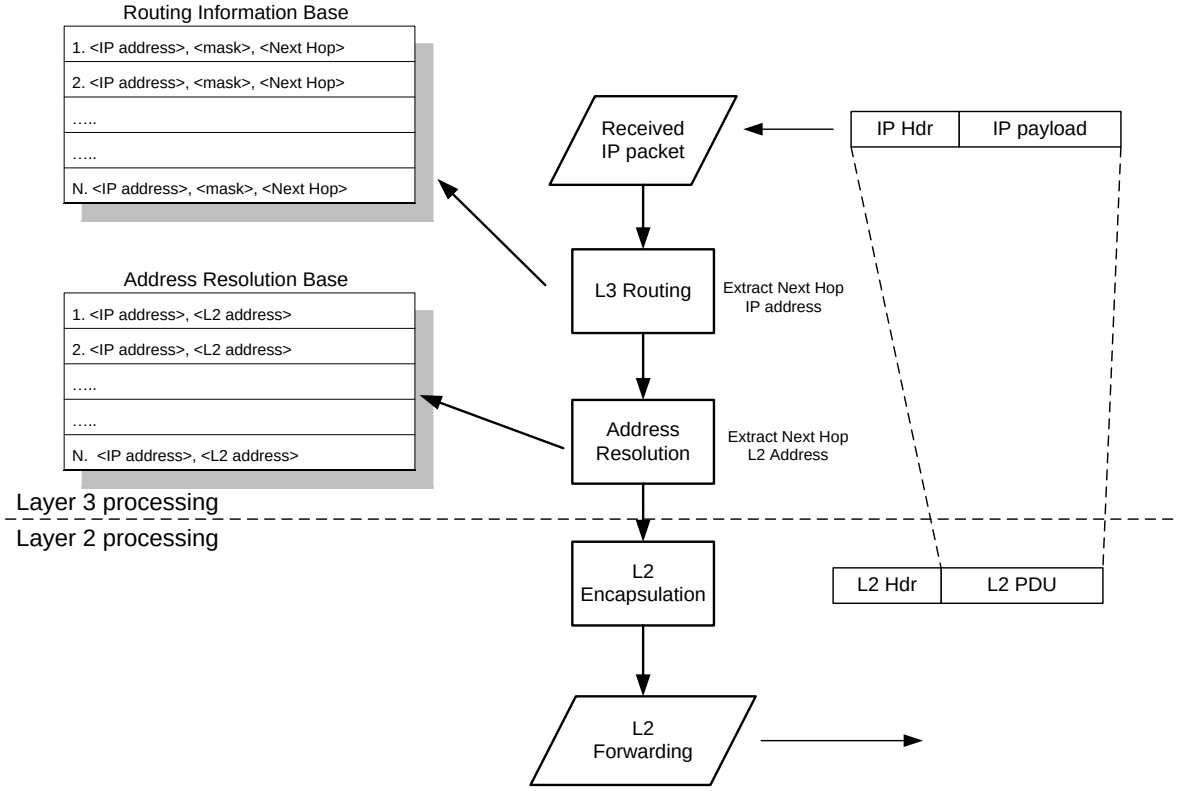


Figure 7.1: RCST Unicast IP packet forwarding

RCST IP packet forwarding comprises 5 main functions:

- **Routing Function (layer 3)**
  This function handles the generation and maintenance of a Routing Information Base, RIB. When the RIB is built, the information is used to select the appropriate next hop IP address corresponding to the IP destination address in the header of each processed packet, by performing a lookup of the destination address to find the best match entry. Support for dynamic routing is optional in an RCST, when supported, this function is responsible for detecting neighbouring routers and their reach ability to remote networks, and importing appropriate information to the RIB.

- **Address Resolution Function (layer 3)**
  This function receives the next hop IP address and looks this up in the Address Resolution (AR) database to determine the L2 next hop. It then queues the packet for the (sub) interface on which it will be sent.

- **QoS (layer 2/3)**
  This function manages the queue of packets awaiting transmission from L3 to a L2 next hop. It determines which packets are scheduled for transmission at L2. The function is described in clause 7.4.

- **Encapsulation Function (layer 2)**
  This function processes a queued IP packet, encapsulating this for transmission. In the encapsulation header this function sets the destination SVN-MAC (or a compressed form of this) to the destination address determined by the AR function. This method is specified in the Lower Layer Specification.

- **L2 Forwarding Function (layer 2)**
  This function is responsible for all L2 operations resulting in transmission of the encapsulated packet over the egress interface towards the L2 next hop.

  Forwarding for IPv4 on the satellite interface is required for core protocols, such as SNMP access by a SVNO to a SVN interface, PEP negotiation, Routing, etc. This support is required to support any network layer forwarding on the LAN Interface, even if IPv4 services are not supported on the LAN Interface.

7.2 IPv4/IPv6 Interface to the link layer

7.2.0 Introduction

The RCST IP processing function shall support:

- IPv4 only (IETF RFC 1812 [6]).
- Dual stack IPv4 and IPv6 (hybrid IPv4/IPv6) (IETF RFC 1812 [6], IETF RFC 6204, [i.13], IETF RFC 4241 [14] and IETF RFC 6434 [i.10]).
- IPv6 -only IETF RFC 6204 [i.13] and IETF RFC 6434 [i.10] except for SNO/SVNO management done over IPv4 (IETF RFC 1812 [6]). In this case IPv4 is still required for the IP management interface.
- A Maximum Transmission Unit (MTU) of at least 1 500 bytes for each SVN interface, a larger value may be negotiated by the lower layers for each SVN [1].

7.2.1 IPv4 Interface to the Link Layer

The RCST IP processing function shall comply with the IPv4 interface to the lower layers. IPv4 (IETF RFC 791[i.14]), (IETF RFC 792 [i.15]) defines the IPv4 network-layer, this is the default network service provided by the present document. The requirements for hosts and routers using IPv4 are defined in IETF RFC 1122 [i.16] and the router requirements are defined in IETF RFC 1812 [6].

IPv4 packets received on the RCST LAN interface shall be forwarded according to the RCST IPv4 routing table (held in the RIB). Packets may also be redirected to an internal agent (e.g. PEP, intercepting proxy, etc.) for processing prior to transmission. Packets for transmission over the air interface are forwarded to the QoS module for transmission on the satellite interface. An RCST shall decrement the TTL field of packets that it forwards (IETF RFC 1812 [6]) and shall not modify the DF field of an IPv4 packet that it forwards (IETF RFC 791[i.14]).

IPv4 addresses are represented in the Domain Name System (DNS) using A records. The RCST shall support DNS as defined in IETF RFC 1034 [i.64] and IETF RFC 1035 [i.65]. The RCST shall also be able to perform DNS queries for these records.

The RCST IPv4 interface configuration shall be managed as given in clause 8.

7.2.2 IPv6 Interface to the Link Layer

The RCST IP processing function shall comply with the IPv6 interface to the lower layers. The base specification for IPv6 is defined in IETF RFC 2460 [i.28]. The RCST shall support the node requirements defined in IETF RFC 4294 [20] and superseded by ID.draft-ietf-6man-node-req-bis [i.10]. The RCST shall support ICMPv6 (IETF RFC 4443 [i.45]), DHCP (IETF RFC 3315 [i.37]), Stateless Address Auto configuration (IETF RFC 2462 [9]) and Neighbour Discovery (IETF RFC 4861 [16]). If the RCST supports a MTU greater than 1 500 Bytes on both the LAN and satellite interfaces, then Path MTU discovery shall be supported according to IETF RFC 1981 [18].

IPv6 packets received on the LAN interface [i.29] of an RCST shall be forwarded according to the RCST IPv6 routing table (held in the RIB). Packets may also be redirected to an internal agent (e.g. PEP, intercepting proxy, etc.) for processing prior to transmission. Packets for transmission over the air interface are forwarded to the QoS module for transmission over the satellite. An RCST shall decrement the IPv6 Hop Count Field of packets that it forwards.

The RCST shall manage IPv6 addresses (IETF RFC 3513 [i.87]). IPv6 addresses are represented in the DNS using AAAA records. The use is defined in IETF RFC 1886 [7]. The RCST shall support DNS as defined in IETF RFC 3596 [i.89] according to the best practice recommended in IETF RFC 3901 [13]. The RCST shall also be able to perform DNS queries for these records.

The RCST IPv6 interface configuration shall be managed as given in clause 8.

7.2.3 Network Address Translation (NAT/NAPT) (optional)

This clause defines optional support for NAT/NAPT for IPv4. It does not specify the use of an NAT/NAPT for IPv6 by an RCST.

An RCST that supports the NAT/NAPT function, shall use the methods defined in IETF RFC 2663 [i.32], IETF RFC 4787 [i.50] for IPv4 for the following types: static, dynamic, port forwarding.

This RCST shall provide support for the NAT Behavioural Requirements for ICMP as defined by (IETF RFC 5508 [i.56]). It shall provide Multicast support for NAT as defined in IETF RFC 5135 [i.51]. It shall provide NAT/NAPT functions compatible with DNS Proxy functions as defined in IETF RFC 5625 [i.58].

If the RCST provides transport-specific NAT/NAPT functions, it shall provide these as defined for TCP (IETF RFC 5382 [i.54]), UDP (IETF RFC 4787 [i.50]), DCCP (IETF RFC 5597 [i.57]) and SCTP (Draft-ietf-behave-sctpnat-06 [i.11]).

The RCST NAT/NAPT configuration shall be configured and managed as given in clause 8.

7.3 RCST Routing function

7.3.0 Introduction

The RCST routing function shall enable the forwarding of both unicast and multicast traffic using the routing information stored in the routing table of the appropriate RCST Routing Information Base (RIB). The RCST shall allow the RIB to be populated with static routes via M and C functions and optionally using a dynamic routing protocol.

7.3.1 Overview of Routing

7.3.1.0 Introduction

In a star or mesh topology, the default route will normally be the IP address of the Gateway within the IP network associated with an RCST. The RCST will be configured with the IP network addresses corresponding to active LAN interfaces, which will be added to the RIB. The RIB can additionally import routes to other networks reachable via its LAN interface(s).

The RCST static RIB is consulted whenever an IP packet is received by the RCST on one of its ingress interfaces, to derive the next hop IP destination address corresponding to the IP destination address in forwarded IP packet. This in turn is used to identify the egress interface (L2 next hop). The static RIB is used to construct an IP forwarding table to improve performance of the routing process.

In a star topology, the routing process at an RCST is simple, however, the Gateway (GW) needs to be configured with routes for the set of IP networks that are reachable via each RCST. For example, in figure 7.2 this requires the GW to not only forward packets to RCST addressed to network 1, but also packets addressed to the network connected via the router attached to network 1.

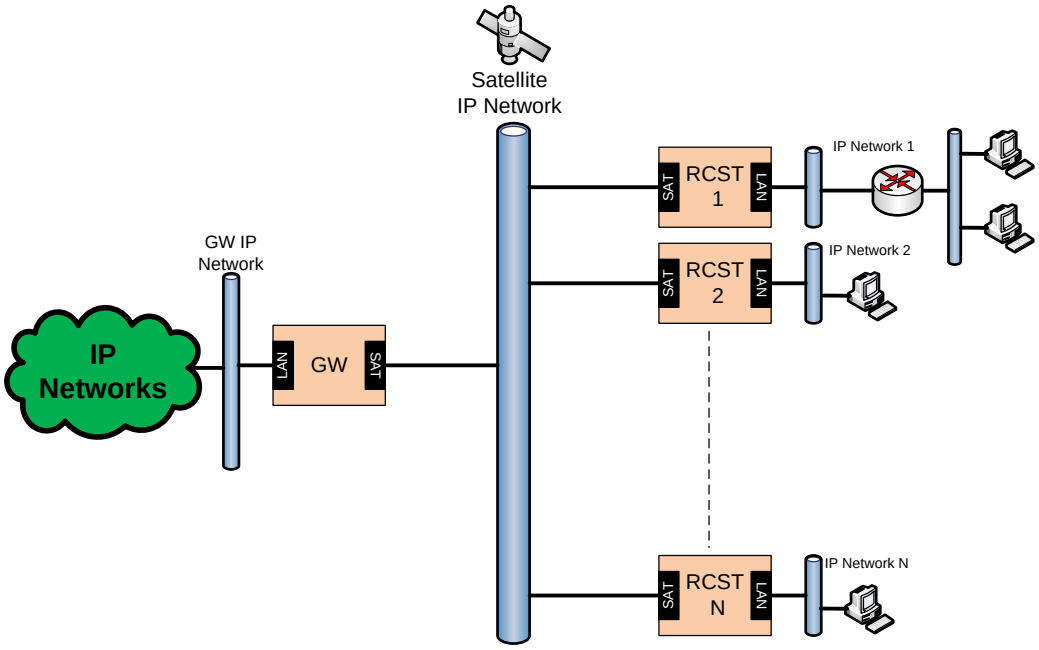


Figure 7.2: Example routing topology for a GW connecting N RCSTs

7.3.1.1 Overview of Dynamic Routing (optional)

An RCST can optionally support dynamic routing as specified in clauses 7.3.6 and 7.3.10. This function is required for some system profiles and may apply to star and mesh topologies.

Dynamic routing assists in managing the routing entries in the RIB for networks indirectly connected via an RCST. The dynamic routing protocol or dynamic connectivity at L2 that may be used to import routing information to the RIB from a neighbouring router or to export routing information from the RIB to other neighbouring routers. This allows the path metrics to be recalculated when there is a change in the topology of the connected network, providing resilience to network link and/or router failure.

Figure 7.3 shows a set of routed networks connected to RCST 1. Dynamic routing allows changes in the topology of the attached networks to impact the forwarding of packets by an RCST and allows an RCST to propagate changes in the routing information to the Gateway Router, where it may change the routing within the satellite network (e.g. when a router attached to an RCST advertises reach ability to a network that was formally reached via a different RCST).

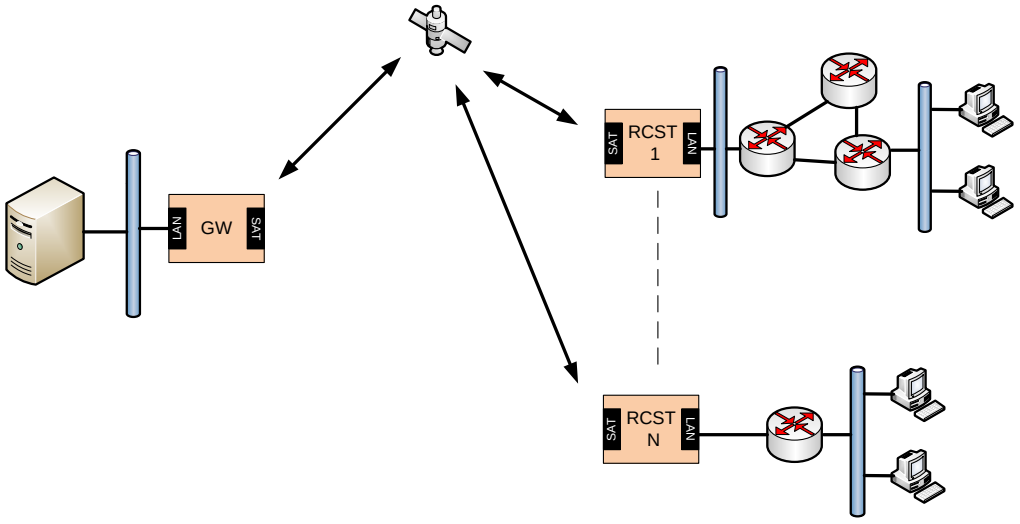


Figure 7.3: Multiple networks connected to an RCST

7.3.2 Routing

An RCST shall forward IP packets via the following IP traffic interfaces:

- **Satellite Interface -** One or more user traffic interfaces that connect the RCST to the satellite.
- **Management Interface -** A single IPv4 host interface used for RCST management and control.
- **LAN Interface -** One or more user traffic interfaces that connect the RCST to the LAN.

An RCST shall allow IPv4 and/or IPv6 to be configured for both the satellite and LAN user traffic interfaces.

The Gateway usually provides direct communication to all satellite IP networks. The RCST routing function shall be managed by the SNO and/or SVNO using the management interface, as defined in clause 8. The NMC is attached to the management network that provides connectivity to the management interface via the satellite.

7.3.3 VRF Groups

An RCST shall use a set of SVNs (i.e. related SVN-MAC addresses) that define one routable address domain for the higher layer processing. It shall maintain one routable address domain for each active address family (i.e. a RIB containing IPv4, IPv6, and the layer 2 forwarding table). To allow an RCST to support multiple routable address domains, an RCST may identify more than one Virtual Routing/Forwarding (VRF) group. Each VRF group shall define a routable address domain.

- An RCST that supports only one VRF group uses consistent IP addresses for all interfaces, including the management interface. The address reach ability information is stored in one single RIB. This is the default case.
- An RCST that supports more than one VRF group shall associate each VRF group with one RIB, a derived IP forwarding table (if used), and a set of interfaces that use the forwarding table. When dynamic routing is enabled for a VRF group, the RCST shall also provide one set of rules and one routing protocol instance for each VRF group (and possibly for each address family within a VRF group).

An RCST VRF group is identified as a combination of:

- A set of IP addresses with one routable address domain.
- One or more SVN-MAC (usually one).
- The OVN to which the VRF group belongs.

The RCST shall assign each SVN number to only one VRF group. All protocol data units exchanged within a VRF group shall be unambiguously addressed by the higher layer address carried by the PDUs (e.g. IPv4 or IPv6 addresses). Within a VRF group, all IP addresses shall be unique at Layer 3 and all bridged MAC addresses shall be unique at Layer 2. This function resembles provider-provisioned Layer 3 Virtual Private Networks (IETF RFC 4026 [i.42]). That is, within a VRF group, the set of SVNs may together use the full private addresses range, (plus any set of public IP addresses).

The RCST addressing plan information may include:

- The set of SVN to be used and assignment of each SVN to a VRF group (or the default VRF group).
- The list of network IPv4/IPv6 addresses per virtual LAN Interface.
- The IPv4 address of the RCST satellite interface for M and C signalling.
- The default route (e.g. gateway) for each RCST.

NOTE 1: An SVNO that wishes to independently assign a private IP address to an SVN may assign the SVN to a VRF group. For example, this allows an operator to re-use the same private IP address range in other parts of the Interactive Network.

NOTE 2: An RCST may support more than one IP network per SVN (e.g. in the case of dual stack IPv4 and IPv6 support).

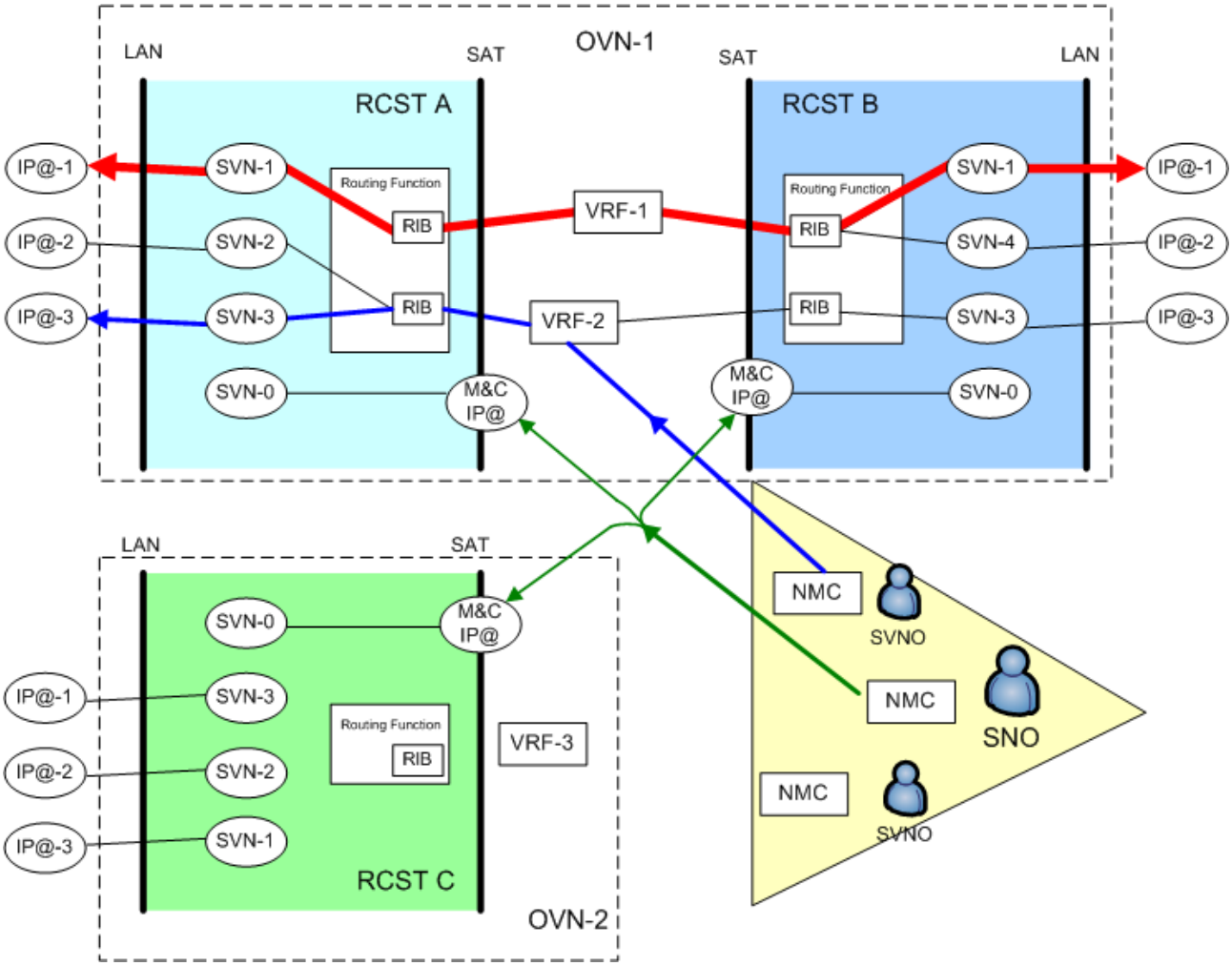


Figure 7.4: OVN, SVNs and VRFs domains

A bridged network can also utilize a VRF group, to ensure independent use of the MAC address space. This also supports situations where an operator wishes to allow the same MAC address to appear more than once within an interactive network.

The following examples illustrate the SVNO usage of VRF groups and multiple SVNs:

- An SVNO may use a single VRF group with one address space. Multiple SVNs may be used to segregate end user network traffic. This SVNO may allocate unique network addresses to each SVN-MAC that it supports. This addressing architecture could, for example, correspond to the assignment of globally routable IP addresses, or a single use of the private address space within the satellite interactive network.

- An SVNO may use multiple VRF groups. The SVNO is only required to allocate a network address that is unique within a VRF group. This addressing architecture allows the SVNO to assign customer networks to separate SVNs, each in a separate VRF group. In this case, the entire private address may be made available to each customer network. Routing between these address spaces would require NAT or NAPT to translate addresses between the VRF groups and also to/from the globally routed public Internet.

7.3.4 VLAN Support (optional)

7.3.4.0 Introduction

The RCST may support Virtual LANS (VLANs) on the LAN interface to isolate the traffic belonging to one logical L2 network from a different logical L2 network.

When a LAN interface supports interpretation of an IEEE 802.1D [i.63] tag at the LAN ingress interface, the VLAN ID field in the tag shall denote the VLAN assigned to the frame. Untagged frames may be supported by an interface that also supports 802.1D format frames. These untagged frames shall be associated with a default VLAN ID. An RCST shall interpret a VLAN at the IP level as a subnetwork, with traffic from different VLANs being forwarded by an IP router via different subnet interfaces.

An RCST may be configured so that traffic received from the satellite interface may be transmitted on a LAN (sub) egress interface with a correspondingly configured VLAN tag.

In this mode IP routing is agnostic to the value of the VLAN tag (if any) associated with a LAN interface and the tag value is removed prior to transmission over the satellite interface. Therefore there is no implicit coordination of the VLAN-IDs used at the ingress and egress LAN interfaces.

7.3.4.1 VLAN tagged IP routing (optional)

An RCST may optionally support a mode that forwards an IP packet with an associated L2 IEEE 802.1D [i.63] tag, both from and to an RCST that operates as an IP router.

This mode permits a satellite network router to forward frames at the network layer (e.g. IPv4 or IPv6 routing) and simultaneously preserve the Ethernet Tag Control Identifier Field in 802.1D format across the satellite network, extracted from the MAC-layer header of each IP packet received on the ingress LAN interface. The Tag Control Identifier includes the L2 VLAN ID and Priority Code Point, PCP. This allows the received tag value to be re-inserted at the egress LAN interface when the packet leaves the satellite network.

When the routing function forwards an IP packet over the satellite interface in this mode, the Ethernet Tag Control Identifier Field shall be forwarded by including a tag extension header placed directly before the IP network header. The presence of this extension header is indicated by the Protocol Type value 0x8100. In this mode, the extension header is not preceded by the 6 byte MAC addresses on the satellite interface as it is on the LAN Interface. This encapsulation format can be used with GSE and with the Return Link encapsulation. The Return Link encapsulation may alternatively use a compressed type value (LLS) (0x0F or 0x31). The latter value indicates omission of the Protocol Type field from the 802.1D format, requiring the receiver to synthesize it before submission to the egress LAN (e.g. based on the version field carried in the first byte of the IP header).

An RCST in this mode shall also support forwarding of untagged IP packets by the IP router (i.e. an IP packet received at the LAN ingress without IEEE 802.1D [i.63] tag). These packets shall be forwarded without a tag extension header, using the routing method described in clause 7.3.5.

An RCST shall not forward IP packets with a L2 broadcast address using this mode. IP packets sent with a L2 broadcast address (e.g. DHCP Request messages) are processed by the local router, as are packets directed to the IP address of a router interface (e.g. ICMP, routing), as in clause 7.3.5.

This option does not forward the content of Ethernet frames that do not directly encapsulate IP packets, i.e. Frames with a Protocol Type value of 0x8100, but with other content than IP.

An RCST that is configured to assign values to a VLAN tag on transmission using the LAN interface shall perform this mapping for all traffic, including any packets forwarded with this tag extension header. When the IEEE 802.1D [i.63] tag assignment is configured, the RCST shall set the transmitted Ethernet Tag Control Identifier Field based on the router/interface configuration (e.g. by mapping the DSCP). This overrides then an Ethernet Tag Control Identifier Field transported over the satellite interface (this tag could have been dropped at the satellite network ingress).

NOTE: When an RCST uses this mode, VLAN IDs will be transported to the gateway from the ingress LAN. Correct operation will rely upon consistent handling of the VLAN IDs associated with packets from multiple RCSTs. This has implications on the configuration of network protocols at the gateway, such as OSPF, and this may require use of traffic separation techniques such as use of VRF groups, VLAN tags, or provider backbone bridges at the gateway.

7.3.5 IPv4 Static Unicast Route Configuration

The RCST IP routing function shall be able to receive IPv4 static routing information from the SNO or the SVNO for each active SVN through the satellite interface. This information is used to populate the static RIB.

An RCST shall support use of administratively managed static routing based on a static RIB.

The IPv4 static routing information comprises a set of route entries. Each route entry shall include the following fields specified in the IP forwarding table MIB as given in IETF RFC 4292 [i.43]. This information is a part of the RCST configuration for the VRF group associated with one or more SVNs and shall be managed as defined in clause 8.

7.3.6 IPv4 Dynamic Routing Configuration (Optional)

7.3.6.0 Introduction

The RCST may optionally support a dynamic IPv4 routing protocol either by routing interactions though a satellite or LAN interface.

When dynamic routing is supported and enabled, the received routing information is used along with configuration information to populate the RCST RIB with IPv4 information. If this function is not enabled, the RCST shall discard all IP packets that carry routing protocol messages.

An RCST that provides the dynamic routing function for IPv4 on the LAN interface shall support OSPF (IETF RFC 2328 [i.22]). It may also be configured to support other routing protocols such as RIPv2 (IETF RFC 2453 [i.27]), IS-IS (IETF RFC 1142 [i.17]).

The RCST OSPF function shall start as soon as there is IP connectivity via a user traffic interface across the SVN network. In star transparent scenarios, the RCST OSPF configuration shall indicate that the Gateway is the OSPF Designated Router (DR) for the satellite IP network. In mesh scenarios, the RCST OSPF configuration shall indicate the GW-RCST that acts as DR for the satellite IP network.

NOTE: The DR filters this routing information according to its assigned addressing plan (that is, it should only import routes that are consistent with the addressing using within the SVN/OVN assigned to the RCST within a single VRF group).

The RCST may support dynamic routing through the satellite interface. The satellite interface dynamic routing may be implemented using OSPF, and for RCSTs supporting dynamic connectivity at L2 alternatively by using the routing part of DCP.

The RCST may support dynamic virtual IP routing, maintaining a set of completely isolated routing entities, one for each supported VRF group.

7.3.6.1 OSPF procedures through satellite interface

The RCST OSPF configuration may indicate that the GW is the OSPF Designated Router (DR) for the satellite SVN. The OSPF function shall start as soon as the RCST/GW is logged in the interactive network.

RCST configuration related to dynamic routing and OSPF may be superseded by instructions provided in the NLID descriptor.

The SVNO shall remotely update the OSPF configuration of an RCST interface by procedures relying on L3 IP connectivity.

The RCSTs and the GW shall use methods from standard OSPF running in broadcast mode for transmitting OSPF packets,

Upon RCST logon, the RCST may send Hello and Database Description OSPF packets to its DR.

The RCST may implement an updated OSPF Hello procedure, in which the Hello interval shall be of 30 min as maximum.

The RCST may cache the last received Hello packet.

7.3.6.2 OSPF procedures specific for mesh

This clause applies for those mesh systems using OSPF for dynamic routing.

In systems implementing dynamic connectivity, the OSPF function of the RCST shall propagate the OSPF Link State Advertisements towards the RCST-GW. The RCST-GW shall send the multicast OSPF Link State Update flooding packets towards the RCSTs attached to it.

In case that the communication with the RCST-GW fails, the RCST shall update its adjacency as if the RCST had failed to receive a Hello packet.

Mesh systems supporting dynamic connectivity shall use DCP protocol as the means to obtain the Layer 2 packet destination address in a traffic Link.

7.3.7 IPv4 Multicast

The RCST shall support the use of IPv4 multicast forwarding of traffic (IETF RFC 1112 [17]) from the satellite interface to the LAN interface(s). It shall also support IPv4 multicast forwarding of traffic from the LAN interface to the satellite interface(s), transported to the GW. This includes Administratively Scoped Multicast (IETF RFC 2365 [i.26]) and Source-Specific Multicast (IETF RFC 4607 [i.48] and IETF RFC 4608 [i.49]).

In IPv4, the Internet Group Management Protocol (IGMP) is used to discover multicast listeners (hosts that wish to receive multicast packets destined for specific multicast addresses) on directly attached links, include the RCST LAN interfaces.

The RCST IPv4 multicast functions:

- shall support satellite IPv4 multicast forwarding (multicast reception), being enabled/disabled by configuration (see clause 8);
- shall support static multicast configuration, as describes in clause 8;
- shall support IGMPv2 (IETF RFC 2236 [i.21]) on each LAN interface;
- may also support IGMPv3 (IETF RFC 3376 [i.38]) or IGMPv3 Lite (IETF RFC 5790 [i.102]) on each LAN interface;
- shall support IPv4 multicast transmission enable/disable by configuration (see clause 8);
- may optionally support IPv4 multicast routing using PIM-SM (IETF RFC 4601[i.47]) on a LAN interface configured by management (see clause 8);
- an RCST that supports dynamic multicast management may also support a dynamic multicast routing protocol on the LAN interface. In this case, the RCST shall support Protocol Independent Multicast (PIM) in the sparse mode (IETF RFC 4601 [i.47]) as the multicast routing protocol and shall provide methods to manage a Multicast RIB (MRIB).

7.3.8 IPv6 static unicast route configuration

The RCST IP routing function shall be able to receive IPv6 static routing information from the SNO or the SVNO for each active SVN through the satellite interface. This information is used to populate the RIB with IPv6 information.

The IPv4 static routing information comprises a set of route entries. Each route entry shall include the fields specified in the IP forwarding table MIB as given in IETF RFC 4292 [i.43]. This information is a part of the RCST configuration for the VRF group associated with one or more SVNs and shall be managed as defined in clause 8.

7.3.9 Dynamic IPv4 Multicast across satellite (Optional)

The RCST may optionally support dynamic IPv4 multicast membership across the satellite interface, this requires that RCST supports either an IGMP-Proxy Agent (IETF RFC 4605 [15]) plus the adaptations required for the satellite environment as detailed in [5] or supports PIM-SM (IETF RFC 4601 [i.47]).

7.3.10 IPv6 Dynamic Routing Configuration (Optional)

The RCST may optionally support a dynamic IPv6 routing protocol either by routing interactions though a satellite or LAN interface.

When dynamic routing is supported and enabled, the received routing information is used along with configuration information to populate the RCST RIB with IPv6 information. If this function is not enabled, the RCST shall discard all IP packets that carry routing protocol messages.

An RCST that provides the dynamic routing function for IPv6 on the LAN interface shall support OSPF (IETF RFC 5340 [i.53]).

Clause 7.3.6 provides information about the use of OSPF on the satellite interface.

7.3.11 IPv6 Multicast

The RCST shall support the use of IPv6 multicast forwarding of traffic from the satellite interface to the LAN interface(s). It shall also support IPv6 multicast forwarding of traffic from the LAN interface to the satellite interface(s), transported to the GW.

In IPv6 Multicast Listener Discovery (MLD, MLDv2 (IETF RFC 3810 [i.41]), or MLDv2 lite (IETF RFC 5790 [i.102]) protocol for IPv6 is used to discover multicast listeners (hosts that wish to receive multicast packets destined for specific multicast addresses) on directly attached links, include the RCST LAN interfaces.

The RCST IPv6 multicast functions:

- shall support satellite IPv6 multicast forwarding for the institutional RCST profile [i.1], and shall support static multicast configuration for each active SVN. For the rest of RCST profiles, IPv6 multicast forwarding in the return channel is optional;
- shall support static multicast configuration, (see clause 8);
- shall support MLDv2 (IETF RFC 3810 [i.41]) or MLDv2 Lite (IETF RFC 5790 [i.102]) on each LAN interface;
- shall support IPv6 multicast transmission enable/disable by configuration, (see clause 8);
- may optionally support IPv6 multicast routing using PIM-SM (IETF RFC 4601 [i.47]) on a LAN interface configured by management, (see clause 8);
- an RCST that supports dynamic multicast management may also support a dynamic multicast routing protocol on the LAN interface. In this case, the RCST shall support Protocol Independent Multicast (PIM) in the sparse mode (IETF RFC 4601 [i.47]) as the multicast routing protocol and shall provide methods to manage a Multicast RIB (MRIB).

The RCST IPv6 multicast routing configuration shall be configured and managed as given in clause 8.

7.3.12 Dynamic IPv6 Multicast across satellite (Optional)

The RCST may optionally support dynamic IPv6 multicast membership across the satellite interface, this requires that RCST supports either an MLD-Proxy Agent (IETF RFC 4605 [15]) or supports PIM-SM (IETF RFC 4601 [i.47]).

7.3.13 MPLS

7.3.13.0 Introduction

Multi Protocol Label Switching (MPLS) is defined in IETF RFC 3031 [i.75] and IETF RFC 4364 [i.100]. It operates at the boundary between L2 and L3, providing unidirectional connections known as Label Switched Paths (LSP). MPLS encapsulates IP and other traffic by adding an encapsulation header that includes an MPLS label. The use of the labels is controlled by one of the available techniques: LDP (IETF RFC 5036 [i.101]), RSVP (IETF RFC 2205 [i.20]), or BGP-4 (IETF RFC 4271 [i.98]). The MPLS labels have only local significance at a specific interface. The set of IP packets that are forwarded over a given LSP belongs to the same Forwarding Equivalence Class (FEC), and should receive the same treatment by the network.

7.3.13.1 MPLS support in the RCST (Optional)

An RCST may optionally support IP-based transport of MPLS packets (IETF RFC 4023 [i.95]) across the Operator Virtual Network. This transports MPLS signalling and data flows across the satellite interactive network. An RCST that supports this mode shall transparently forward IP packets with an IPv4 Protocol Number field or the IPv6 Next Header field set to 137. It shall assign MPLS packets with a specific FEC to a single HLS PHB group and HL service (IETF RFC 3270 [i.76]). It may similarly forward IP packets that use the Generic Routing Encapsulation (IETF RFC 2784 [i.74]) with a type of 0x8847 or 0x8848. In this mode, the RCST does not interact with the MPLS control plane.

An RCST connected to an MPLS network may also operate as a LSR (Label Switched Router) connected via the LAN interface to a standard LSR or LER. This requires MPLS signalling to be intercepted and processed by the RCST. It also requires an RCST to switch frames from/to the LAN Interface with a type of 0x8847 or 0x8848 (IETF RFC 3031 [i.75]). These frames may be sent on the satellite interface using the standard type value or the compressed type of 0x13 or 0x14, corresponding respectively to 0x8847 and 0x8848. An RCST that supports this function may implement M and C functions that enhance measurement and control for the MPLS traffic (IETF RFC 2702 [i.73]), allowing each LSP to be mapped to an appropriate HL service.

The RCST MPLS configuration shall be configured and managed as described in clause 8.

7.4 Quality of Service

7.4.0 Introduction

The RCST shall support QoS mechanisms both at layer 2 and at layer 3. This clause describes the RCST QoS model in terms of QoS definitions and the RCST QoS cardinality model. The RCST QoS requirements will be composed by:

- QoS elements definitions
- RCST HL QoS model mapping to LL (cardinality diagram)
- RCST QoS classification functions

An RCST shall support traffic differentiation according to DiffServ (IETF RFC 2474 [i.30], IETF RFC 2475 [i.31], IETF RFC 3086 [i.34] and IETF RFC 3260 [i.36]) for differentiation of the traffic transmitted towards the satellite.

A host originating a flow may not provide explicit QoS signalling, but may use a session-layer protocol to co-ordinate the communication. A signalling proxy at the RCST may snoop these session layer control messages to infer a QoS requirement. The QoS is instead inferred from session characteristics such as the choice of codec (e.g. snooping SIP signalling for a VoIP call to determine the encoding rate chosen by an application or interception of a multimedia request using HTTP). Intercepting proxies are described in clause 9.

7.4.1 RCST Higher Layer QoS Model

7.4.1.0 Introduction

The RCST QoS function applies to all the user traffic in the same connectivity aggregate that shall be transmitted sharing a common transmission channel. The mapping of user traffic to a connectivity aggregate is responsibility of the forwarding and routing functions for the RCST.

Figure 7.5 illustrates relations between PDU aggregates and lower layer specific streams as these can be observed externally. The essential control entities are also shown.

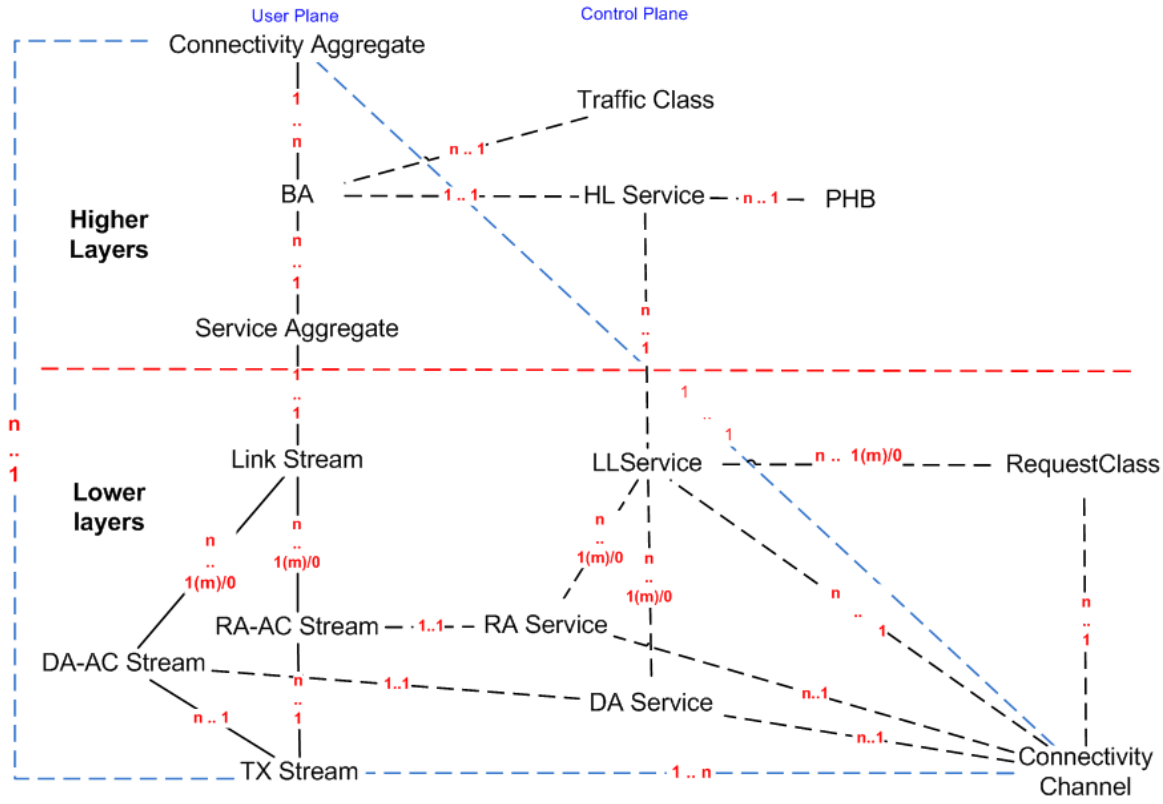


Figure 7.5: RCST QoS Control and Traffic model

Explanatory notes:

An RCST IP forwarding and routing function decide if a packet is destined for the satellite interface and therefore will seek to determine the next hop for this packet. This determines the Connectivity Aggregate (CA).

Each next hop may constitute a separate connectivity, or several next hops may share common L1 connectivity (e.g. through a shared carrier), depending on the configured topology.

A Traffic Class (TC) association is determined for each packet. The combination of the TC association and the CA association determines the Behaviour Aggregate (BA) to which a HLPDU belongs. This associates the TC with an HL Service.

NOTE 1: Aggregates are collection of packets.

The HL service maps a BA to a Lower Layer Service, and the traffic associated with a BA forms all or part of a single SA.

The HL Service determines any traffic conditioning specified for a BA, the characteristics of queuing at the HLS, and the corresponding Service Aggregate (SA) and LL Service to respectively be used for transmission and resource request. It also relates also the BA to a Per Hop Behaviour [i.34]. The PHB characterizes the BA and may be used by network operators to build consistent behaviours within a DS domain.

A Lower Layer Service (LL Service) is configured by the Lower Layer Signalling (L2S) system maps to the default Connectivity Channel (CC). All components of an LL Service set up by the L2S map to this connectivity by default.

All satellite resources map to the default Connectivity Channel unless the implementation is specifically designed and configured to differentiate the mapping of resources to connectivity.

A BA is provided with one LL Service, and may utilize any DA Service and RA Service that is permitted to be used by the LL service, but cannot use another LL Service.

The Service Aggregate (SA) is the sequence of Higher Layer PDUs (HLPDU) sent via a Link Stream (LS). The SA sequence is a multiplex of HLPDUs of the different BAs that map to the same SA.

The Link Stream (LS) is the sequence of Payload-adapted PDUs (PPDUs) hold the sequence of HLPDUs for the associated SA and may be associated to a logical flow of RLE/GSE traffic packets from the RCST or NCC/GW into the satellite network. All packets from one Link Stream have the same level of Precedence/Priority for layer 2 scheduling. The PPDUs in an LS may be multiplexed with PPDUs that belong to another LS. PPDUs are individually sized to fit within the available unoccupied Frame PDU (FPDU) payload.

The Link Stream (LS) may map to any combination of RA-AC Streams and DA-AC Streams as allowed by the associated LL service.

The SA sequence is a multiplex of HLPDUs of the different BAs that map to the same SA.

The aggregation to SA and LS for BAs that share an LL Service is implementation dependent. This freedom applies generally to BAs that share the set of DA Services and RA Services.

NOTE 2: Ordering is the key service that needs to be known when mapping PHBs (i.e. all flows within a PHB group should preserve packet order).

An LL Service allows use of either one or more DA Services or one or more RA services, or a combination of such service types.

An LL service may support two types of channels, depending on the capacity assignment:

- Dedicated Assignment (DA), the allocation channel is allocated via DAMA and dedicated capacity categories.
- Random Access (RA) assignment, the allocation channel is accessed via Random Access.

On the air interface, capacity is allocated to an Allocation Channel. The NCC may use one or more allocation channels to assign capacity to an RCST. An Allocation Channel represents a portion of the return link capacity that is assigned to one or more Streams.

NOTE 3: Signalling channels to the NCC are identified by the allowed content type of the channel.

Implementations may use Allocation Channels (AC) to indicate specific connectivity or for QoS differentiation:

- The mapping of an RC to an Allocation Channel is indirectly defined by the mapping between the nominal Dedicated Access Allocation Channel (DA-AC) and the nominal RC in the LL service.
- When allocation channels are used for differentiating connectivity, they may correspond to RL/UL physical partitions associated with different destination downlinks.

Each RA service is implemented on a dedicated RA allocation channel with an RCST specific and some generic load control. As seen from an RCST there is a 1 to 1 relation between an RA service and RA allocation channel.

A BA maps to an RA-AC if the allowed LL Service includes the corresponding RA service.

Each DA service is implemented on a dedicated DA-AC allocation channel given as part of the RCST QoS configuration. As seen from an RCST there is a 1 to 1 relation between an DA service and DA allocation channel.

A BA maps to an DA-AC if the allowed LL Service includes the corresponding DA service.

The Higher Layers interact with a Request Class via the concept of the LL Service.

When an RCST makes a capacity request it includes a reference to RC in the request sent to the NCC. The corresponding allocations made by the NCC in the TBTP2 are assigned to a specific DA-AC identified by an Assignment_ID.

An LL Service that allows use of a nominal DA Service is assumed to provide access to a nominal Request Class (RC). A nominal RC is not relevant if the DA service is solely FCA based.

An implementation shall be capable of forwarding BA traffic by requesting with the nominal RC, and feed the BA traffic to the nominal DA-AC. It may be assumed that requesting with the nominal RC will make the NCC provision the nominal DA-AC with resources. Traffic for a DA Service appears as FPDUs in a DA-AC Stream.

The DA service is established by the resource provisioning of the associated DA-AC, as controlled by the NCC.

An implementation may issue resource requests associated to other RCs than the nominal RC if allowed to do so by the LL Service associated to the BA with the corresponding traffic.

An implementation may forward BA traffic by other DA Services than the nominal if allowed in the LL Service configuration. Traffic may also be forwarded by other RA Services than the nominal if allowed in the LL Service configuration.

The RA Service is defined by the resources provided to the associated Random Access Allocation Channel (RA-AC) as controlled by the NCC, the RA Load Control parameters associated with this RA-AC and the current loading of the RA-AC by the RCST. Traffic for an RA Service appears as FPDUs in an RA-AC Stream.

An RCST shall assume that a nominal DA Service will/may be provisioned by the NCC as specified for the nominal RC associated the DA Service by an LL Service. The DA Service specification can then be inferred from the configuration of this RC.

An RCST is assumed capable of utilizing resources assigned by the NCC to a DA-AC in excess of the expectations inferred from capacity requests and indicated constant rate assignment.

An RCST supporting RA is assumed capable of utilizing resources dynamically and statically allocated to an RA-AC.

The DA-AC Streams and RA-AC Streams aggregate to a TX Stream that holds the whole SA, including all CAs, BAs and SAs.

The L2S Stream is not shown in the diagram. It relates to the DA-AC Stream, the RA-AC Stream and directly to the TX Stream. All lower layer control plane entities except the CC relate to the L2S Stream, as the CC is implicit from the L2S perspective.

This model applies to star transparent, mesh transparent overlay and mesh regenerative scenarios.

An RCST may support multiple connectivity channels, but in the star transparent scenario the set of receivers is limited to only one (the RCST and the gateway).

In case of mesh systems, the RCST will support dynamic creation of multiple connectivity channels. The NCC may assign a mesh link to a connectivity channel or assign multiple mesh destinations to a single connectivity channel dynamically thanks to L2 signalling based on DCP.

7.4.1.1 QoS Model for regenerative mesh (optional)

Interactive networks in meshed regenerative systems are built over Connectivity Channels (CC). In case of mesh, the terminal will support several CCs dynamically assigned by the NCC. Each CC represents a direct link between one RCST and one or more destination RCSTs.

The RCST QoS function for regenerative mesh, applies to all the user traffic in the same or different Connectivity Aggregates (CA), that are transmitted in one or more mesh transmission channels. The mapping of user traffic to a connectivity aggregate is responsibility of the forwarding and roting functions for the RCST. The mapping between the CA and the Connectivity Channels (CC) is indicated by the NCC thanks to DCP.

At least one CA is needed per destination or a CA could aggregate multiple destinations (when physical resources can be reused for different destinations). For each CA, it may be necessary a separate set of HL queues with their HL Services.

In a mesh system, the traffic packets in the different CAs are classified in BAs according to HL Services. Each BA will trigger a separate mesh link, and therefore, each CA may originate several connections. Traffic belonging to different mesh links may concur in the same SA queue (if they have the same Service and may use same resources, common Assignment ID).

At the routing stage, the RCST will aggregate several CAs per transmission stream. A CA may include multiple L2 destinations (in one or several destination RCSTs), each one corresponding to one link stream (LS). Therefore, the streams are related to (RCST) destinations in a mesh network. In a mesh regenerative system, a CC groups all the CAs directed to the same destination beam.

In mesh regenerative scenarios, the transmission streams associated with the different mesh links may not always be aggregated in the same connectivity channel, in contrast with the star transparent case. Concretely, this happens when the destination beam of two streams is not the same (except in the L2-L3 satellite switching case). There will be several connectivity channels according to different beam destinations.

In mesh systems, a different Assignment ID could be used for each mesh link or destination beam.

7.4.2 RCST QoS Classification Functions

7.4.2.0 Introduction

The RCST QoS classification function shall identify a microflow or an aggregate of microflows (traffic stream).

RCST QoS configuration shall be supported by:

- assignment of traffic to an HL Service (and hence associated with a PHB): a set of traffic filters linked to one HL service class;
- management of each HLS PDU Queue by the associated HL Service;
- separation of resource demand into the LL service (and hence the corresponding Request Class);
- assignment of traffic from a HLS PDU Queue to the corresponding LL service to meet the goals set by the HL Service.

The combination of connectivity and TC defines the mapping of traffic to an HL Service. A TC may be used in more than one connectivity, it may be related to the satellite interface. Each TC shall be mapped to one HL Service.

A BA is a collection of HLS PDUs sharing transmission policies. A BA may hold multiple link destinations when the Connectivity Channel supports this. Multiple BAs may share the same LL Service.

Table 7.1 lists the RCST QoS configuration items that shall be required in the RCST to ensure to correct QoS behaviour in the control and user plane.

Table 7.1: RCST Classification Functions

QoS configuration Item	RCST QoS function
TC mapping to BA	Definition of Traffic Classes based on a set of parameters defining filter masks/criteria and mapping of a TC into a BA and HL service as defined in the IP classification table.
HL Service mapping table	Configuration of HLS Service policies such as queuing, shaping, dropping and mapping to a PHB.

The QoS behaviour of the RCST shall be defined by QoS configuration tables in the control plane. These tables are defined as the RCST QoS configuration as specified in clause 8.

In addition, the RCST QoS data is completed with LL services information that is provided at logon and shall be saved in the MIB only for supervision, not for configuration, as specified in clause 8.

The RCST shall support HLS PDU queues monitoring related to BA and HL services.

7.4.2.1 IP Classification Table

The IP Classification Table defines the traffic classification used in RCST for transmission on a satellite interface. It is configured in each RCST by management or a local interface (e.g. CLI or web interface) as defined in clause 8. The exact format of IP Classification Table is as provided in clause 8.

The classification of packets can be based on filter criteria/masks, including primarily layer 3 (IPv4 or IPv6) parameters (IETF RFC 4594 [i.46]), but also be based on some layer 2 parameters. Each PDU is classified and associated to a Traffic Class (TC). If no filter mask is matched the packet shall be discarded.

A TC may be implemented as a set of one or more traffic filter records. Each record matches a set of header fields in the packet/PDU. A simple traffic filter could match only the DSCP, whereas a more complex multi-field classifier classifies packets based on the contents of a pre-selected set of header fields. The TC for IP MicroFlows shall include at least the DSCP, anyhow the recommended minimum TC may include a combination of the IP source addresses, the IP destination addresses, the DSCP, the protocol type and the source and destination port values.

IP MicroFlows are classified according to the first filter matched in the IP Classification Table. This assigns the traffic to a specific HLS service. The selected HLS service may also assign implementation-dependent methods including metering, connection control and admission control.

The description of the IPClassEntry parameters of the IP classification table is described in table 7.2.

Table 7.2: IP Classification table parameters

Classification Parameter	Description
IPClassIndex	Index of the Traffic Classification Table. Used to identify a packet type or flow type
IPClassDscpLow	Specifies the low value of a range of DSCP values to which a packet is compared. A value of 0 is used to inactivate
IPClassDscpHigh	Specifies the high value of a range of DSCP values to which a packet is compared. A value of 63 is used to inactivate
IPClassDscpMarkValue	Specifies the DSCP value used to mark (remark) a packet. Possible DSCP mark values are (0,63). A value of 64 indicates no DSCP marking
IPClassIPProtocol	Specifies the IP protocol to which a packet is compared (e.g. TCP, UDP, etc.)
IPClassIPSrcAddressType	Specifies the type of Internet source address type (IPv4 or IPv6)
IPClassIPSrcAddress	Specifies the Internet source address to which a packet is compared
IPClassIPSrcAddressPrefixLength	Specifies the number of bits of the Internet source address prefix
IPClassIPDstAddressType	Specified the Internet destination address type (IPv4 or IPv6)
IPClassIPDstAddress	Specifies the Internet destination address to which a packet is compared
IPClassIPDstAddressPrefixLength	Specifies the number of bits in the Internet destination address prefix
IPClassSrcPortLow	Specifies the low range of the source port number to which a packet is compared
IPClassSrcPortHigh	Specifies the high range of the source port number to which a packet is compared
IPClassDstPortLow	Specifies the low range of the destination port number to which a packet is compared
IPClassDstPortHigh	Specifies the high range of the destination port number to which a packet is compared
IPClassVlanPri	Specifies the VLAN User Priority to which a packet is compared
IPClassHLSAssociation	Associates the filter entry to a specific HL service (by reference to a HL service index)
IPClassAction	Specifies if the packets mapped to this entry (flow type) can be transmitted to the satellite interface or should be discarded ("0": Permit; "1": Deny). The parameter can be related to a firewall function, used to avoid undesired incoming traffic

The IP Classification table maps a set of traffic filters to the associated HLS service to be used by a traffic class.

The IP Classification table shall be kept in the RCST MIB as specified in clause 8.

7.4.2.2 HLS Service Mapping Table

The HLS Service Mapping table records the mapping of a HLS service to a Service Aggregate and LL Service. It also links the HL Service to the associated PHB.

The set of PHBs supported by an RCST are managed by the SVNO. Each PHB is identified by a PHB_ID.

The associated parameters per HL service are summarized in table 7.3.

The HLS mapping table shall be kept in the RCST MIB as specified in clause 8.

Table 7.3: HL service mapping table parameters

HL Service Parameter	Description
HLServiceIndex	Index value of the HL service
LLServiceAssociation	Associates the HL service to a specific LL service (by reference to a LL service index)
diffPolicyPHBindex	Associates the HL service to a specific DiffServ Policy PHB high-level "network wide" policy definitions (by a reference to a DiffServ Policy PHB index)
diffPolicyPHBname	PHB name associated to the PHB index
Priority	Nominal priority of the PDUs in the HL service aggregate
MinRate	Minimum level of resources available to the HL service aggregate
MaxRate	Maximum level of resources available to the HL service aggregate
MaxIngressBurst	Maximum burst of traffic that the HL service will take
MinIngressBurst	Minimum burst of traffic that the HL service will take
MaxEgressBurst	Maximum burst of traffic that the HL service will issue in excess of maximum long term rate
MaxDelay	Nominal maximum transit delay for a PDU of the HL service aggregate
SchedulingType	Packet ordering policy and packet drop policy - FIFO - LLQ - WFQ - WRED - Other
L3IfNumber	Link to layer 3 interface
MaxLatency	Minimum time to hold on to a PDU in the HL service aggregate before it may be discarded
LinkRetransmissionAllowed	Packet re-transmission allowed/not allowed

7.4.3 Dynamic Connectivity (optional)

Dynamic connectivity is a mechanism defined as the capability to establish, modify, or release links between RCSTs and gateways based upon events occurring on traffic/control or management level.

Dynamic connectivity is implicitly associated to Connectivity Channels. A certain Connectivity Channel shall be linked from one origin RCST or origin gateway to one or several RCST destinations or gateway destination.

Some mesh satellite interactive networks that exceed the reference model star transparent shall be built implementing dynamic connectivity in the form of:

- dynamically controlled connectivity via direct mesh link between RCSTs, through satellite on board conversion from MF-TDMA to one or more TDM carriers;

- dynamically controlled connectivity via direct mesh links between RCSTs equipped with an MF-TDMA receiver, through the MF-TDMA over a transparent satellite.

Dynamic lower layer connectivity is mandatory in mesh networks, while dynamic connectivity at higher layers may be applied for access control to any network scenario.

Dynamic connectivity shall be handled by a Dynamic Connectivity Protocol (DCP), as described in annex D.

The RCST shall trigger a connection request message upon reception of an IP packet in one of its LAN interface that cannot be mapped to an existing mesh link or a permanent link that does not require link establishment signalling. A packet can be forwarded to an active connection only when it is addressed to the same destination RCST and its associated QoS service matches that of the existing connection.

The RCST shall send a connection release request message for those active links not cursing traffic in any direction after a timeout that may be set via DCP messages or by RCST management.

The basic dynamic connectivity functions supported by a mesh RCST shall include:

- Connection establishment and release messages.
- RCST initiated, bidirectional connections.
- RCST initiated unidirectional multicast connections.

The RCST shall identify the Assignment ID associated with a mesh connection or CC in the TBTP2 by means of the information retrieved from the Logon Response Descriptor or from a DCP exchange.

The RCST shall maintain a table for its active mesh links, including at least the following information:

- Source and destination MAC24 address labels of the interfaces involved in the mesh link.
- IP addresses (IPv4 and IPv6) of the RCSTs (source and destination) LAN interfaces involved in the mesh link.
- HL service or QoS profile parameters used for the mesh link.
- Assignment_IDs of both RCST transmitters.

The message from the NCC establishes a user plane L2 interface for the peer and possibly also a management plane L2 interface for the peer, and correspondingly indicates at least one IP address that can be used to map IP traffic both of the interfaces.

Apart from traffic connections (mesh links), a signalling connection shall be established in the logon phase of the RCST, to be used for management and control messages issued from the RCST towards the NCC.

Mesh connectivity can be implemented without on board conversion using MF-TDMA receiver in the destination transparent mesh RCST, or through satellite OBP that coverts MF-TDMA to TDM carriers (regenerative mesh).

The lower layer logon request to the NCC indicates if the RCST supports DCP over L2, over IP or both, and if it supports transparent mesh networking and if it supports regenerative mesh networking.

7.5 Network Control Functions

7.5.0 Introduction

This clause describes network-layer control functions. These control functions are processed within the network layer of an RCST.

7.5.1 Internet Control Message Protocol (ICMP)

The RCST shall support ICMP on each IPv4 interface as defined in IETF RFC 792 [i.15] or on each IPv6 interface as defined in IETF RFC 4443 [i.45].

The RCST shall respond to an ICMP-Echo request received via the satellite interface to any of its configured IP Interfaces when sent using the SVN-MAC label for the IP Interface.

An RCST shall respond to an ICMP-Echo request received via the satellite interface to the broadcast subnet address of IP network for which it is configured, when this is received using the SVN-MAC identifier corresponding to the IP Interface.

An RCST shall not respond to an ICMP-Echo request sent to the management IP address via a LAN Interface (unless this VRF Group is explicitly made available on a dedicated LAN interface).

An RCST should respond to an ICMP-Echo request sent to any assigned traffic IP address via any LAN Interface.

An RCST shall not respond to any ICMP-Echo request sent with an IP multicast destination address.

7.5.2 Neighbour Discovery (ND)

An RCST that supports IPv6 shall support ND as a configurable option on each active LAN interface. Use of ND on the satellite air interface is not specified in the present document.

7.5.3 Dynamic Host Configuration

The Dynamic Host Configuration Protocol (DHCP) is defined in IETF RFC 2131 [i.19]. The DHCP automates network-parameter assignment to network devices connected to a LAN interface from one or more DHCP servers. DHCP makes it easy to add new network devices to a network.

An RCST may support DHCP as a configurable option on each LAN interface. This may be a DHCP client interface.

An RCST may support a DHCP server that provides dynamic, automatic or static leases of addresses using an active LAN interface. An RCST that provides an IPv4 DHCP server may support DHCP-Relay as a configurable option on each active LAN interface.

The extensions of DHCP for IPv6 (DHCPv6 [i.37]) are specified in IETF RFC 3315 [i.37]. An RCST that supports IPv6 shall support DHCPv6 as a configurable option on each active LAN interface. This may be a client interface, or may be a server providing dynamic, automatic or static leases of addresses.

An RCST that supports an IPv6 DHCP server may support DHCP-Relay as a configurable option on an active LAN interface.

7.6 Extensions for Adapting the PDU

7.6.0 Introduction

As introduced in the System specification [i.1], the RCST shall support a forward link using the Generic Stream Encapsulation (GSE) [2] protocol exclusively, including for transport of signalling, except for the migration scenarios already stated in the System specification [i.1]. The RCST shall also comply to GSE additional extensions defined in IETF RFC 4326 [i.44] and IETF RFC 5163 [i.52]. The RCST Return Link shall support MF-TDMA link using the Return Link Encapsulation (RLE) [1].

An RCST may receive a GSE PDU that includes one or more extensions headers that are added by a remote HLS module to a PDU payload.

The PDU queued in the HLS PDU Queue may include one or more extensions headers that are added by an HLS module to a PDU payload. These extensions headers are identified at the HLS level by a 16 bit identifier encoded according to [2], and formatted as defined in section 5 of IETF RFC 4326 [i.44]. These extension headers are communicated along with the PDU payload to the remote HLS entity at the Gateway, NCC, or RCST. These headers shall be processed according to the reception rules for GSE.

Extension headers correspond to one of two types:

- An Optional Extension Header has a pre-defined length that is encoded in the extension field. An Optional Extension Header does not modify the format or encoding of the enclosed PDU (i.e. it can only add a tag or additional information to a PDU). If the header codepoint is not recognized at the receiver, the optional information is silently discarded, and the remainder of the PDU is processed (including any remaining extension headers). Sender modules that introduce optional headers may also include a probing mechanism to ensure that the remote endpoint is able to process the header they provide.

- Each Mandatory Extension Header has a length that is not necessarily communicated in the extension field. No limit is placed on the maximum length of a Mandatory Extension Header. A Mandatory Extension Header can modify the format or encoding of the enclosed PDU (e.g. to perform encryption and/or compression). The term "mandatory" refers to the receiver processing action, and not to the required support for the option. If the header codepoint is not recognized at the receiver, the PDU is silently discarded. Sender modules that introduce mandatory headers are advised to include a probing mechanism to ensure that the remote endpoint is able to process the header they provide.

Using this method, several PDU extension headers can be chained in series. The sender at the RCS lower layers may also add extension headers that enhance the physical layer (such as headers to support packet FEC). These extension headers are also removed after processing by the corresponding lower layer receiver, before an encapsulated PDU is passed to the higher layers. IETF RFC 5163 [i.52] provides guidance on the ordering of extension headers when multiple extension headers are used.

Reception of an encapsulated PDU with an unknown protocol feature shall result in discard of the enclosed PDU.

7.6.1 Header Compression

Operation of header compression is not specified in the current version of the present document.

7.6.2 Bulk Compression

While bulk compression is intended to be transparent, that is the output data stream is meant to be identical to the input data stream, there are also loosely compression methods that rely on transcoding to modify the data. This approach generally requires knowledge and is described further in the clause on transcoding.

Operation of bulk compression is not specified in the current version of the present document.

8 Management signalling

8.0 Introduction

This clause and subclauses are in the present document provided as a recommendation for guiding in aligning implementations of M and C, aiming at a future evolution towards normative status.

The following recommendations are intended to be partly superseded and partly supplemented by an implementation dependent RCST MIB ASN.1 specification compatible with RCS2 MIB and an implementation dependent RCST configuration file specification. The combination of the present document and these specifications, assumed provided for an implementation, are intended to be the basis for bilateral interoperability in the management plane over the satellite interface.

8.1 Management reference architecture

8.1.0 Introduction

This clause describes the network management functionality associated with DVB-RCS2 network. The purpose is to establish the basic framework for RCS network to be seen as part of the TMN model of telecom network management to help the operators to configure and manage the RCS network in an easy way. For this reason, the main management interfaces, management protocols, information and syntax needs to be identified.

Three elements are identified in the RCS network for provisioning of the management functionalities in DVB-RCS:

- The Operation Support Systems (OSS): it includes the management functions that enable a Provider to monitor, control, analyse and manage systems, resources and services. It provides high level support and control interface to lower level management data from network elements. The OSS should provide the development of a flexible service integration framework, which eases the introduction of new Technologies and reduces the cost base.

- The Network Management Centre (NMC) of the OVN.
- The Network Elements (RCST, Gateways, NCC, OBP).

The OSS is located in the in the Telco or Service Provider premises. In both cases, the OSS shall obtain the management information of the RCS network through the OSS-NMC interface.

The OVN management functionality shall assure the interoperability among OVN elements from different vendors, and the seamless integration with other networks, Service Providers and OSS (see figure 8.1).

The NMC performs all management functions, namely system configuration, fault management, system performances management and accounting data retrieval (FCAPS functions). The NMC and NCC could either be directly connected through a LAN interface, or via IP connection over terrestrial backhaul networks.

The NCC is in charge of control activities, i.e. session control (terminal log-on and RCST synchronization maintenance), resources control (RRM and SLA enforcement) based on DAMA rules, and DVB-S2(X)/DVB-RCS2 tables control (i.e. NCC to RCST signalling and vice-versa).

The NCC is composed by a NCC core server, responsible of the Network Control Function and optimally by a Mediation Device, which is the front-end of the NCC from the management point of view. The NCC may be fully redundant based on a hot redundancy scheme: in case the nominal NCC fails, control is automatically switched over the second redundant NCC. Both NCCs should have a synchronized connection with the NMC with no loss of data in case of switchover.

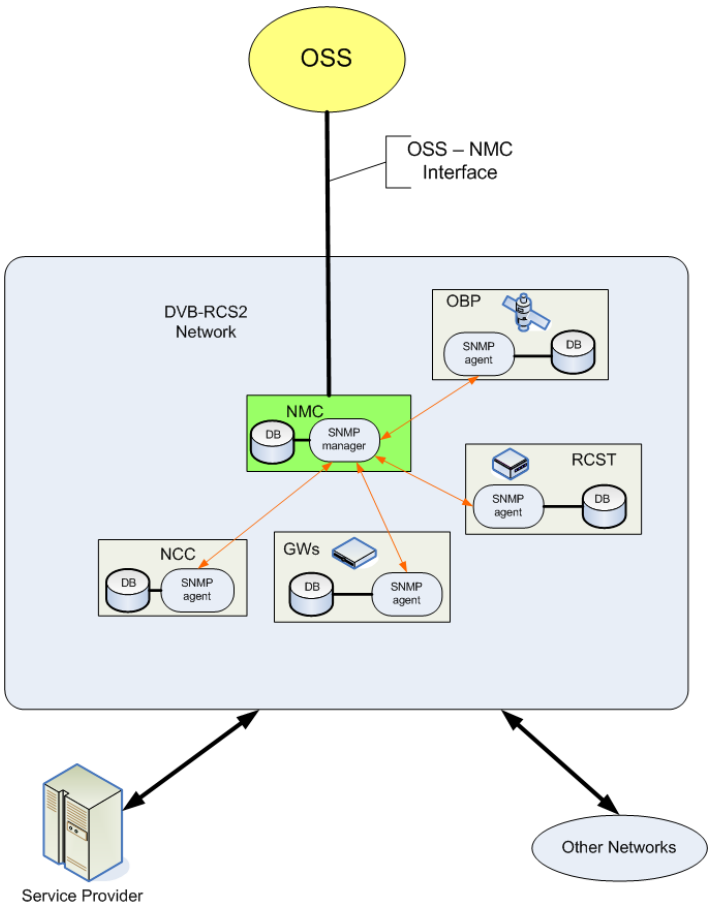


Figure 8.1: Management Reference Architecture

The management functionality of the OVN is divided in two environments:

- Internal management: covers the SNO and SVNO management functions towards the OVN and SVNs thanks to the NMC. The central manager is the NMC, which manages the following interactive satellite Network Elements (NEs):
  - RCSTs or satellite terminal.

- Gateways that provide IP access to external networks.
- NCC responsible of the control signalling and monitoring functions in real time over the Satellite Interactive Network to be transmitted by one or several Feeder Stations (DVB-RCS2-S).
- NMC network devices.
- OBP (On Board Processor) in mesh regenerative networks.

- OSS-NMC management (external): it compounds the NMC functionalities required to establish external management relationships with external management systems to the interactive satellite network. This relationship can be established by the SNO or SVNO.

The basic functionality of the NMC includes the manager of the elements of the network (RCST, GW, NCC). These functions shall support a SNMPv2c/SNMPv3 protocol and MIB data base (in the communication between NMC and network elements - Internal interface). The NMC is the SNMP manager and the RCST, NCC or Gateway are the SNMP agents. The NMC is extended to include Service and Network related management functions to provide an interface for an external OSS.

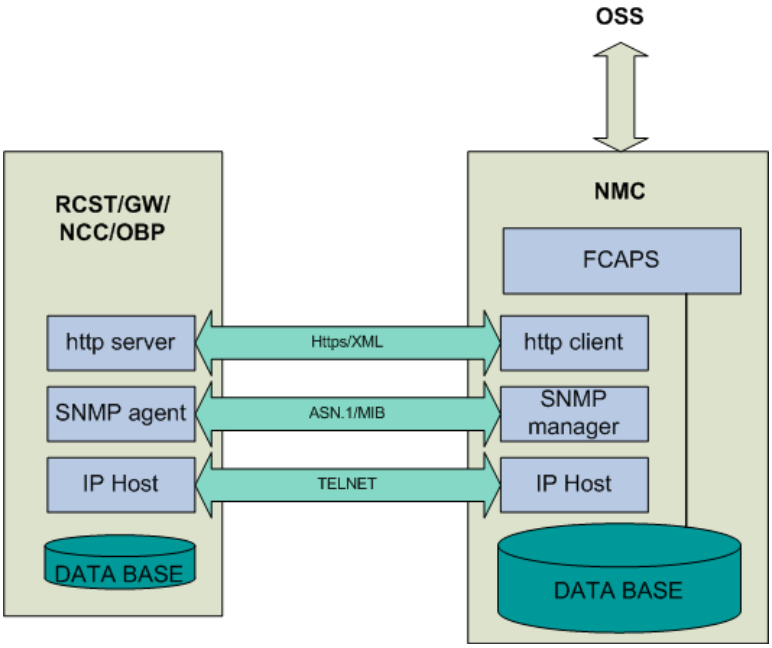


Figure 8.2: RCST - NMC management interactions

The NMC is the central entity that supports management signalling via IPv4.

In a multi SVNO environment, two types of NMC are considered:

- Primary NMC: this manages all the network elements of an interactive network. It is associated to the Satellite Network Operator (SNO).
- Secondary NMC: it is an instance of primary NMC associated to the Satellite Virtual Network Operator (SVNO). It can only manage the network elements associated to the SVNs of the SVNO using the IPv4 address allocated to the SVN interface.

The SVNO NMC or secondary NMC has a back-end connection to the SNO NMC or primary NMC. This connection could be provided via IP over terrestrial backhaul networks.

The NMC primary may support multiple SVNOs connections, allowing them to monitor their RCSTs and to down-load accounting data per SVN. A cold redundant equipment may be implemented in case of failure of the NMC primary. A common data base or synchronized data bases should be shared between the two NMCs in cold redundancy.

The NMC management functions specified follow the TMN framework of five-logical layers model:

- Business management.

- Service management.
- Network management.
- Element management.
- Network elements.

The NMC is specified in terms of the Service, Network and Element management layers. Business management is out of the scope for the present document. The Network element layer consists of the individual network elements, the RCSTs and gateways. The specification of the RCS network management aligns with the layers of the TMN models characterized by the FCAPS functions. They are characterized in the following clauses.

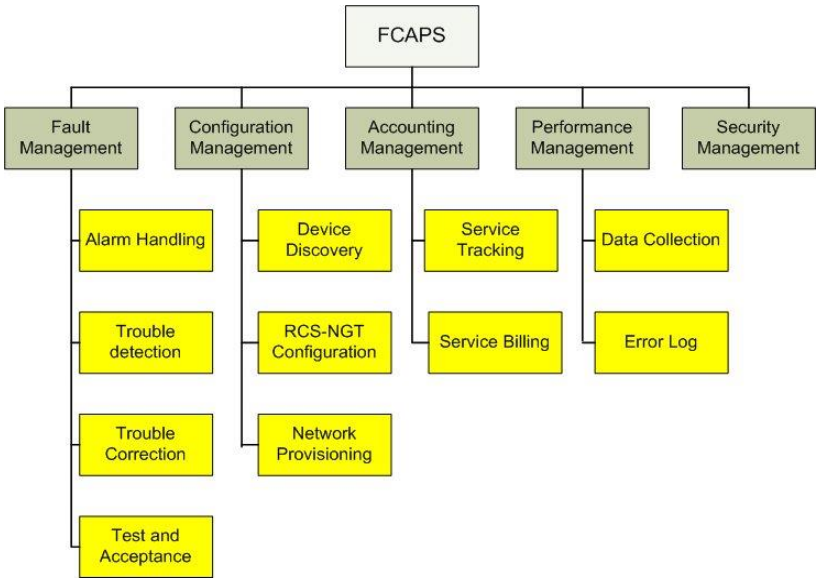


Figure 8.3: DVB-RCS2 FCAPS

One single terminal may be managed concurrently by one SNO and one SVNO. This applies to all RCST profiles.

In case of consumer, corporate, SCADA, backhaul and institutional the terminal belongs to the end user that assumes its cost. This subscriber will have one service package with the SNO or SVNO.

The multi-dwelling Satellite Terminal may comprise multiple subscribers at a single location that share the terminal to access satellite broadband services. None of these subscribers can afford the cost of the terminal. The terminal belongs to the SNO or SVNO. These subscribers have one different service package with the SNO or SVNO. The service packages available to the residents of the multi-dwelling terminal are generally similar to those offered to consumers. The SNO or SVNO should ensure each subscriber domain or organization differentiation based on VSNs.

A multi-dwelling terminal should support several SVNs, each one of them may correspond to a different subscriber. All these SVNs are controlled and managed by the same SVNO and belong to the same OVN. The SVNO and SNO should have the capability to assign each multi-dwelling RCST's SVN to a different subscriber and service package.

8.1.1 FCAPS

8.1.1.0 Introduction

This clause defines the functional areas of network management in terms of FCAPS (Fault, Configuration, Accounting, Performance and Security) as applied to the management of an RCS2 network.

8.1.1.1 Fault management

Fault management seeks to identify, isolate, correct and record system faults. Fault identification relies on the ability to monitor and detect problems, such as error-detection events. RCS2 relies on SNMP notifications to deliver critical events that cause service interruption and need immediate response. Examples of these events are interface state up/down, and thresholds events when the total number of RCSTs in a fault condition exceeds a configured threshold.

8.1.1.2 Configuration management

Configuration management modifies the system configuration variables and collects configuration information for supervision. Configuration management is primarily concerned with network control via modifying operating parameters on network elements such as the RCST. Configuration parameters include both physical resources (e.g. interfaces) and logical objects (e.g. QoS parameters).

8.1.1.3 Accounting management

Accounting management includes collection of usage data and permits billing the customer based on the use of network resources. The NMC is the network element responsible for providing the usage statistics to support billing based on the RCST accounting data. Billing is out of the scope of the present document.

8.1.1.4 Performance management

Performance management includes collecting statistics of parameters such as frames lost at the MAC layer and number of codeword errors at the Physical layer.

SNMP polling is the mechanism used for collection mechanism for collection of RCST performance management statistics.

8.1.2 OSS – NMC interface

The OSS - NMC interface supports a comprehensive view of the network towards the SNO or external operators offering cost-effective management of the OVN.

The OSS - NMC interface provides the standard based management functions required in the NMC to interface with an OSS for efficient operation, administration, management and provisioning (OAMP and P) for day-to-day maintenance. The OSS - NMC interface allows the NMC FCAPS functionality integration with the OSS using an adaptation layer. These management functions should follow the interaction of processes defined by the eTOM.

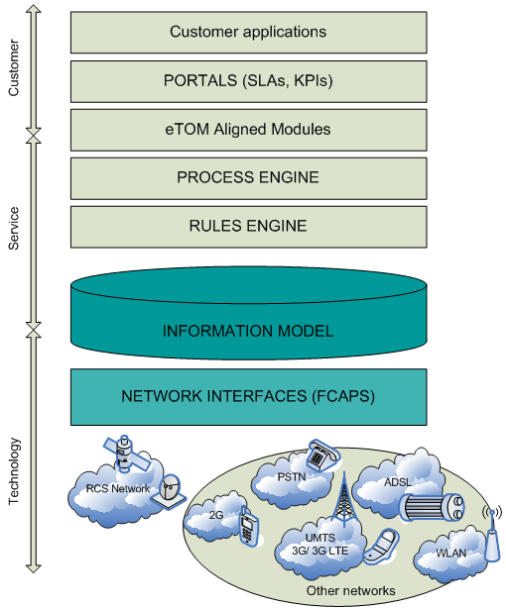


Figure 8.4: OSS-NMC management Interface

The NMC may use distributed SNMP-based management, offering a feature-rich management framework. The OSS-NMC interface may provide a database that stores the information with the status and service provisioning of the OVN. The information may be accessible via XML messaging of via MIB object model (IETF RFC 1155 [i.66]) and SNMPv3 (IETF RFC 2570 [i.71], IETF RFC 2575 [i.72] and IETF RFC 3416 [i.82]). Optionally, vendor specific solutions may be implemented.

The external OSS should access for the OVN management information related with service provisioning and SLA, fault, performance and accounting functions.

The OSS - NMC service provisioning application should keep:

- Network inventory management (full list of the network elements present).
- Service configuration and SLA data per OVN subscriber.
- Status of the OVN elements based on the set of supported IETF MIB-II tables.

The OSS - NMC fault management application should keep:

- Network events/faults detection from all the OVN elements.
- Alarm data to a trouble ticket.
- Alarm data to an SLA application.

Faults are sent from the NMC to the OSS as SNMP notifications (traps).

The OSS - NMC accounting management should include collection of usage data based on a subscriber's use of network resources for billing.

The OSS - NMC performance management should include collection of parameters of performance monitoring data from the multiple vendors equipment across OVN. The data and statistics can be made available through collection of XML files via FTP or via NMC SNMP polling of the network elements and creation of a summary file per element per collection interval.

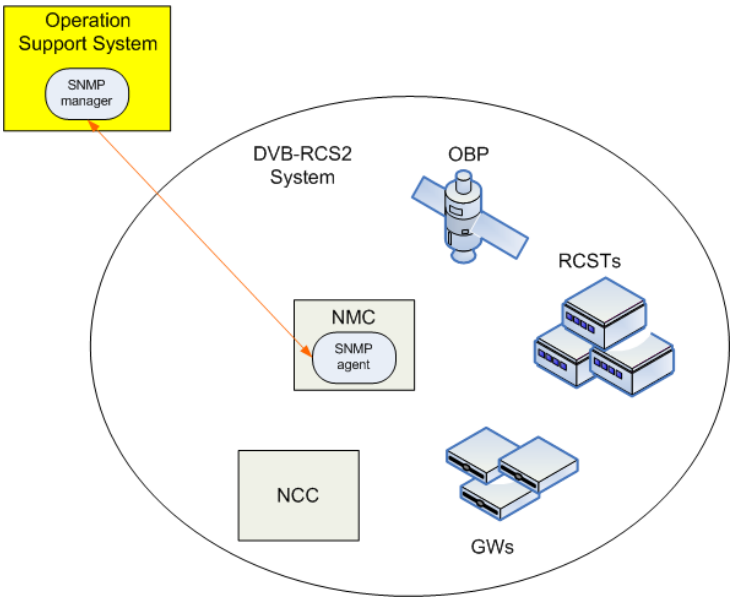


Figure 8.5: OSS-NMC management architecture

8.1.3 Subscriber accounting management interface

The specification of a Subscriber Account Management Interface (SAMI) enables prospective vendors to address the operational requirements of subscribers account management in a uniform and consistent manner. This enables operator and other interested parties to define, design, and develop Operations and Business Support Systems necessary for the commercial deployment of different class of services of DVB-RCS2, with accompanying usage-based billing of services for each individual subscriber.

Subscriber account management interface refers to the following business processes and terms:

- Class of Service Provisioning Processes, which are involved in the automatic and dynamic provisioning and enforcement of subscribed class of policy-based Service Level Agreements (SLAs).
- Usage-Based Billing Processes, which are involved in the processing of bills based on services rendered to and consumed by paying subscribers. The present document focuses primarily on bandwidth-centric usage-based billing scenarios.

SAMIS uses the business model defined by IPDR streaming protocol (IPDR/SP Protocol Specification, version 2.1 [i.12]) for the reliable and resource efficient transmission of accounting data. The IPDR Streaming Protocol enables efficient and reliable delivery of any data, mainly Data Records from Service Elements to any systems, such as mediation systems and BSS/OSS.

The IPDR approach is based on an object oriented modelling approach well known in the industry for capturing requirements and analysing the data in a protocol independent representation. This approach defines requirements with use cases to describe the interactions between the operations support systems and the network element. The management information is represented in terms of objects along with their attributes and the interactions between these encapsulated objects (or also referred to as entities in some representations).

An RCS2 SAMIS IPDR record should be constructed from a number of attributes that describe the IPDR itself, the RCST that is serving the subscriber, and the QoS attributes and counters.

8.2 Management Protocol Stack

The basic management functionality consists of gathering of information about the state of electronic equipment from a remote location and the ability to control (read and write) this state remotely. It implies the use of a management protocol for the data exchange and use a unified set of tools with a common interface to help analysing and predicting problems so that remedial actions can be taken in a pro-active way.

The baseline Network Management protocol is SNMPv2c for consumer and SCADA profiles and SNMPv3 (IETF RFC 2570 [i.71]), (IETF RFC 2575 [i.72] and IETF RFC 3416 [i.82]) for the other profiles.

The following means should be available for M and C of an RCST based on standard protocols:

- For RCST configuration, XML (XML11) format may be used (see clause 8.4).
- Optionally, other management protocols can complement SNMP. These protocols are:
  - SysLog (IETF RFC 5424 [i.55]) (e.g. for trouble correction, performance monitoring, trouble detection).
  - Existing proprietary techniques including command-line-interface (CLI) or HTTP PUT/POST/GET messages.

The following means are considered for M and C of an RCST based on standard protocols:

a) SNMP access via the NLID in L2S (custom tunnelling)

b) DHCP Option transmitted via L2S

c) SNMP access via UDP/IPv4

d) Configuration via XML file transferred by FTP/TCP/IPv4

e) M and C access via web browser and HTTP/TCP/IPv4

And the following may be available:

f) M and C access via web browser and HTTP/TCP/IPv6

g) ASCII instructions entered via the NLID in L2S (custom tunnelling)

The RCST Management protocol stack is illustrated by figures 8.6, 8.7 and 8.8.

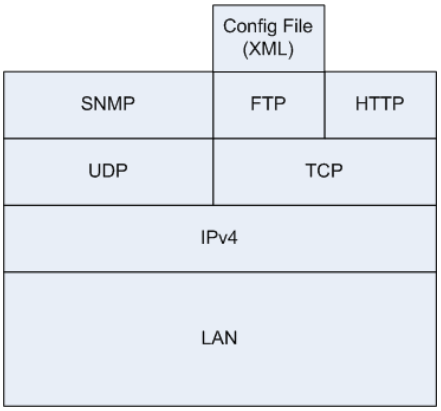


Figure 8.6: Protocol Stack for RCST management from the LAN interface

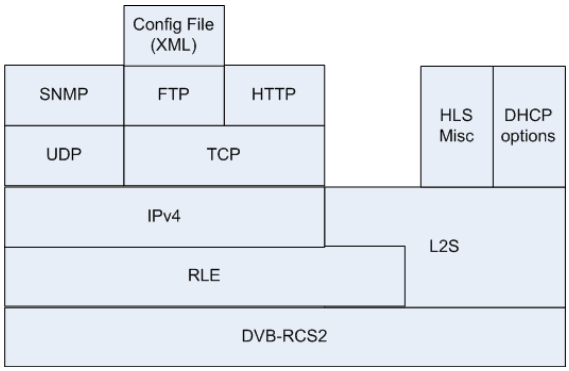
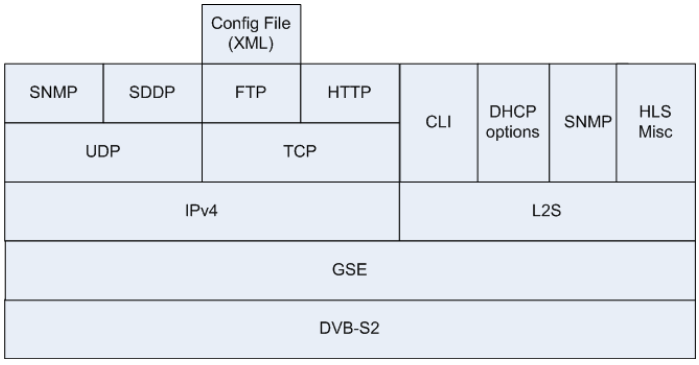


Figure 8.7: Protocol Stack for RCST satellite interface management (return link)



NOTE: HLS misc includes:
- HL capabilities indication
- Status flags for management
- automated pointing alignment signals
- SW version management

Figure 8.8: Protocol Stack for RCST remote management (forward link)

The IETF SNMP related RFCs are listed in table 8.1.

Table 8.1: SNMP IETF RFCs

IETF RFC 3410 [i.77]	Introduction and applicability statements for Internet Standard Management Framework
IETF RFC 3411 [i.39]	An architecture for describing Simple Network Management Protocol (SNMP)
IETF RFC 3412 [i.78]	Simple Network Management Protocol (SNMP) Applications
IETF RFC 3416 [i.82]	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
IETF RFC 3414 [i.80]	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
IETF RFC 3417 [i.83]	Transport Mappings for the Simple Network Management Protocol (SNMP)
IETF RFC 1157 [i.67]	A Simple Network Management Protocol
IETF RFC 3418 [i.84]	Management Information Base for the Simple Network Management Protocol (SNMP)
IETF RFC 3419 [i.85]	Textual Conventions for Transport Addresses
IETF RFC 3584 [i.88]	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
IETF RFC 3826 [i.92]	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
IETF RFC 1901 [i.69]	Introduction to Community-based SNMPv2 (Informational)

For support of SIMv2, table 8.1 lists the IETF SNMP-related RFCs which could be supported.

8.3 RCST Management Interfaces

Access to M and C functions may be discriminated according to interfaces, allowing to differentiate SNO, SVNO and user access to M and C.

The RCST M and C may be supported over the different interfaces as follows.

Table 8.2: Management protocols usage

	SNO/NCC	**SNO/NMC using RCST IPv4@ of SVN-0**	**SVNO/NMC using RCST IPv4@ of SVN-n (n>0)**	**LAN side manager using RCST IPv4@ from LAN interface**
Custom L2S as specified in LLS	According to LLS	Not required	Not required	Not required
NCC- flags/L2S	According to LLS	Not required	Not required	Not required
HL-Capability/L2S	Sent during logon with SVNO/NMC data	Sent to the RCST through the NCC during logon	Not required	Not required
HL-Initialize/L2S	Sent during logon with SNO/NMC data	Sent to the RCST through the NCC during logon	Not required	Not required
SNMP/NLID/L2S	Sent during logon with SNO/NMC data	Sent to the RCST through the NCC during logon	Sent to the RCST through the NCC	Not required
DHCP/L2S	Sent during logon with SVNO/NMC data	Not required	Sent to the RCST through the NCC with DHCP options per SVN-n	Not required
CLID/L2S	Implementation dependent	Implementation dependent	Not required	Not required
SNMP/UDP/IPv4	Not required	Allowed, mainly for supervision	Allowed, mainly for supervision	Only allowed for RCST installer
FTP/TCP/IPv4	Not required	Only for configuration/log file upload/download	Only for configuration/log file upload/download	Only allowed for RCST installer
HTTP/TCP/IPv4	Not required	Allowed	Allowed	Allowed with different access policies
SDDP/UDP/IPv4	Not required	Allowed for RCST SW download	Not required	Not required
SNMP/UDPIPv6	-	-	-	Only allowed for RCST installer

Support of M and C via SNMP/NLID/L2S may be required for bootstrap and other communication required supported when the IPv4 stack is not operational.

Only the SNO has access to this interface, via the NCC.

8.4 RCST configuration file management

The XML (XML11) format may be used for RCST configuration. It is recognized that an XML representation may be generated using Recommendation ITU-T X.693 [3].

NOTE: XML RCS configuration file requires the specification of object naming. As a first step ASCII representation will be used.

The following requirements apply for RCST configuration file management:

The RCST may, according to configuration, download over IPv4 using FTP a given configuration instruction file from a given location, as specified by the SNO/NMC via SNMP, and alternatively and optionally also as specified by other administrative means.

The RCST may be designed to accept a configuration instruction file that is not larger than 100 KB, and may accept a larger configuration instruction file.

The RCST may be able to store a minimum of one configuration instruction file for later to be taken into use, and may be able to store several.

The RCST assumes one of the stored configuration instruction files to hold the next configuration. Which configuration instruction file is considered next is implementation dependent.

The RCST takes the next configuration instruction file into use as instructed by the SNO/NMC. The RCST keeps its current configuration if there is no next configuration instruction file available.

The RCST may be able to process and effectuate configuration instructions provided by the NMC in a configuration file built from ASCII characters that are valid for configuration of the specific RCST.

The RCST may consider a configuration instruction file to be valid if all but the 4 last bytes hold ASCII characters of the valid range, and the last 4 bytes holds a valid CRC32 of the rest of the file content.

The RCST may accept a clear text CRC32 unless the RCST is administratively configured to only accept a de-scrambled CRC32.

The RCST may support implementation dependent de-scrambling of the configuration instruction file CRC32.

A claimed implementation of a standardized configurable object is expected to comply with the characteristics as specified for the standard object.

The RCST is expected to accept a file with a set of managed object configuration instructions that is consistent with the part of the current configuration of the RCST that is not being updated by the configuration instructions.

The RCST is expected to be capable of separating object configuration instructions that uses the delimitation rules that apply for the RCST implementation.

The RCST may silently discard a configuration instruction for a non-standard object.

The RCST may silently discard a configuration instruction exceeding the minimum configuration range for a standard object.

The RCST may silently discard a set of configuration instructions that is inconsistent with other configuration of the RCST that is not updated by the same configuration instruction file.

The RCST may accept configuration instruction for a standard managed object from a file also containing configuration instructions for non standard managed objects as long as all configuration instructions are delimited according to the rules that apply for the RCST.

The RCST may support at least Read-Only SNMP access to the current value of the standardized managed objects.

The RCST may provide a configuration file version number or a checksum if this is requested.

The version indicator of the configuration file is a Display String (IETF RFC 1213 [i.68]). The file version will be contained in the file and its calculation is vendor specific. The following data objects may be used in the configuration update procedure:

- IP address of the TFTP/FTP server and path where the configuration file is located.
- Command to start the configuration download.
- Parameter to store the version of the downloaded configuration file.
- Command to activate the new configuration file.
- Parameter to store the version of the active configuration file.

The RCST configuration file parameters follow the same syntax as the parameters configured in the RCST MIB.

The configuration file remote download proceeds as follows:

1) Configuration update process may start anytime once the RCST has acquired the forward link and has performed a first log on.
2) The SNO will configure the FTP server IP address in the RCST.
3) The SNO will send a command for starting the download of the configuration file.
4) The RCST uses FTP and the above information to download the configuration file. Once downloaded, it validates the configuration file and checks the file version. Upon a successful validation and check, the RCST may update the parameter storing the last 'downloaded' configuration with the version of the file that was just downloaded.
5) The SNO will execute a command to activate the new configuration file at the desired time of activation (immediately following the download command or at a later time). In some RCST implementation, it may be required for the RCST to reboot in order to take into account the new configuration file (vendor specific). When the configuration file is activated, the RCST may update the object indicating the active configuration version of the activated configuration.

Full or delta configuration of common elements defined by the present document may be supported.

If there is a change done to the RCST configuration in advance of the activation of the file, this may be superseded by the newly activated Configuration File.

8.5 RCST Software Delivery Download Management

8.5.0 Introduction

When the RCST boots, it will first verify that the installed SW image is appropriate and will only then join the OVN (see the definition of the protocol for software upgrade in annex C).

The transition between software download and joining the OVN is vendor specific (a vendor may choose to perform a re-boot to achieve this).

8.5.1 RCST Software Delivery Download parameters

The basic parameters to perform the RCST software update are:

- Minimum SW version to operate in the System. This information is obtained from TIM-b through the Lowest Software Version descriptor. Lowest Software versions to operate in the interactive system are classified according to vendor OUI.
- Current software version executing at the terminal. The version is indicated to the NCC in the Logon burst (see [1]).
- Alternate software version (not the default for execution) stored in the RCST.

- Reboot command parameter. This variable may be used to force an RCST to reboot:

  1) idle

  2) normal = normal reboot (from current software load)

  3) alternate = reboot from alternate load (swap to alternate load before reboot)

- The IP information for downloading a software version that is being broadcasted/multicasted. This consists of the multicast IPv4 address and the UDP port that can be used to perform the Software download.

- A flag parameter to indicate to the RCST whether or not to ignore or not the SW version notified in TIM-b.

The RCST software update parameters may be kept in the RCST MIB and accessed by the SNO.

8.5.2 RCST Software Delivery Download procedure

The IP information to perform the SW download is taken from the Lowest Software Version descriptor that can be included in both TIM-b and TIM-u tables. Once RCST has acquired the forward channel, the RCST decodes this descriptor when included in the TIM-b, to execute a Software Upgrade procedure if the SW version of the RCST is lower that the indicated lowest software version broadcasted/multicasted, unless it has been configured to ignore broadcasted/multicasted Software updates.

The RCST does not need to download a new Software in case the lowest SW version indicated or a later version is already available.

At any moment, the SNO may force a Software change procedure on the RCST, using the Lowest Software Version descriptor included in the TIM-u. This applies for an upgrade or a downgrade, upon SNO discretion. In this case, the RCST may interrupt an ongoing software download operation.

The RCST may calculate an implementation dependent checksum of the downloaded Software image.

The software version field of the Logon burst is of size 8-bits, this cannot therefore be used to represent the exact software version. The value assigned in the CSC for a given software image is a vendor-specific. Vendors may publish a mapping table that relates the value reported in the CSC burst to the actual software version. The NCC should use the MAC address (in the CSC) to differentiate the reported software version for a specific vendor. In this way it may discriminate between two reported values from different vendors.

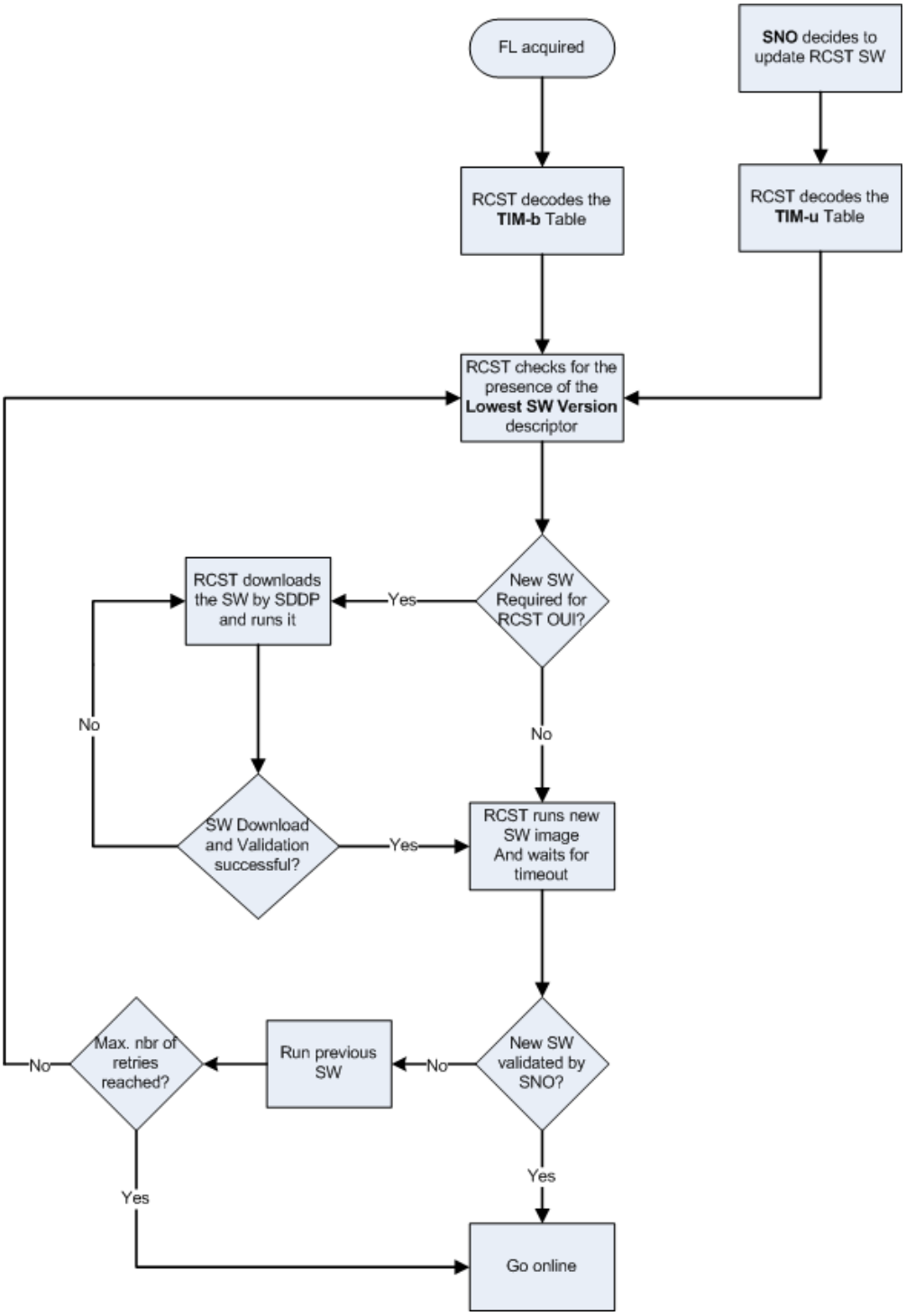


Figure 8.9: RCST SW check and download

8.6 RCST Managed Objects

8.6.0 Introduction

The management information is a collection of managed objects residing in the different network elements and entities of DVB-RCS2 system.

Each RCST may support a MIB (Management Information Base) in line with the present document. The RCST MIB is the collection of managed objects residing in a virtual information store, and collections of related objects are defined in MIB modules.

The RCST MIB is written using ASN.1 and follows SMIv2 (IETF RFC 1155 [i.66]).

Each managed object is expected to be specified with:

- the function applicable for the managed object
- impact of the managed object with respect to the applicable function
- parameter value type
- minimum value range for configuration
- default value
- persistence of configured value across reboot
- persistence of configured value across change of SNO domain
- persistence of configured value across an ordered reset to system faults (if this is applicable)
- mandatory or optional support over SNMP for interfacing a standard SNMP/IP based manager
- mandatory or optional support via ASCII based configuration instructions provided on file via FTP
- differences between SVNO and SNO management
- mandatory or optional support via HTTP for interfacing a standard web browser

The managed objects for support of RCST management are identified in the following clauses. Several sources are used to collect existing managed objects:

- MIB objects from IETF RFC 5728 [i.59] located under the iso.org.dod.internet.mgnt.mib-2 branch. IANA has assigned transmission number 239.
- MIB objects from MIB-II, sysObjectID from the system group of the mib-2 is used to provide an OID pointer to the vendor-specific RCS2 MIB.
- Additional MIB modules which includes RCS2 vendor specific management information.

The configuration of managed objects in the RCST may be supported either by SNMPv2c/SNMPv3 protocol and by configuration file. For most objects the latter is applicable.

The RCST may use the following tables to provide the desired SNMP Access:

- snmpCommunityTable (IETF RFC 3584 [i.88]) for SNMP community configuration;
- snmpTargetAddrTable (IETF RFC 3413 [i.79]);
- vacmAccessTable (IETF RFC 3415 [i.81]): view access table configuration.

The RCST may implement the MIB requirements in accordance to the present document regardless of the status of the object in the referenced source (e.g. deprecated or optional).

If not required by the present document, additional objects are optional.

The SNMP messages supported by the RCST are given in table 8.3.

Table 8.3: SNMP messages

Messages	Interface
get-request [MIB variable]	forward
get-next-request [MIB variable]	forward
get-response [MIB variable,value]	return
set-request[ack flag]	forward
trap[MIB variable value, value]	return

The RCST responds with the appropriate error/exception condition, such as noSuchObject for SNMPv2c, when an attempt to access the non existent additional MIB object is made.

An RCST may as minimum implement MIB functional groups indicated Essential (E), and may also implement other (O) functional groups indicated.

Table 8.4: RCST MIB functional groups

Functional Group	MIB Module	Description	E/O	Source/Reference
System		MIB-2 System group is mandatory for any kind of device	E	IETF RFC 1213 [i.68] IETF RFC 3418 [i.84] See note 1
Interfaces	IF-MIB	MIB-2 The network interfaces of the RCST	E	IETF RFC 1213 [i.68] IETF RFC 2863 [11]
IP	IP-MIB	Internet Protocol forwarding and routing information	E	IETF RFC 1213 [i.68] IETF RFC 4292 [i.43] IETF RFC 4293 [i.99]
ICMP	ICMP-MIB	MIB-2 ICMP	E	IETF RFC 1213 [i.68]
TCP	TCP-MIB	Transmission Control Protocol MIB Module	O	IETF RFC 1213 [i.68] IETF RFC 4022 [i.94]
UDP	UDP-MIB	User Datagram Protocol MIB Module	O	IETF RFC 1213 [i.68] IETF RFC 4113 [i.96]
SNMP	SNMPv2-MIB	SNMPv2 MIB Module	E	IETF RFC 1213 [i.68] IETF RFC 3418 [i.84]
IGMP	IGMP-STD-MIB	Internet Group Management Protocol MIB Module	O	IETF RFC 2933 [12]
Ethernet	EtherLike-MIB	Ethernet Interface MIB module	O	IETF RFC 3635 [i.91]
System configuration	RCS2-MIB	Sytem parameters, functional flags	E	IETF RFC 5728 [i.59]
Network Configuration	RCS2-MIB	SVN MAC, multicast	E	IETF RFC 5728 [i.59]
L3VRF configuration	RCS2-MIB	VRF configuration	E	RCS2 See note 2
Installation	RCS2-MIB	RCS2 installation parameters, antenna alignment	E	IETF RFC 5728 [i.59]
Control	RCS2-MIB	Device control	E	IETF RFC 5728 [i.59]
State	RCS2-MIB	Device status	E	IETF RFC 5728 [i.59]
Statistics	RCS2-MIB	For packets transmission, reception, BW allocated,	E	RCS2
QoSConfiguration	RCS2-MIB	for the satellite interface	E	RCS2
FlinkConfiguration	RCS2-MIB	part of satellite layer 1	E	IETF RFC 5728 [i.59]
RlinkConfiguration	RCS2-MIB	part of satellite layer 1	E	IETF RFC 5728 [i.59]
IPv4 DHCP	DHCP-MIB	IPv4 DHCP options	O	IETF RFC 2132 [i.70]
IPv6 DHCP	DHCP-MIB	IPv6 DHCP options	O	IETF RFC 3633 [i.90]
VLAN	RCS2-MIB	VLAN mode	O	IETF RFC 4188 [i.97]
DCP Agent Configuration	RCS2-MIB	For mesh	O	RCS2
PEP Types	RCS2-MIB	For PEP types configuration	O	RCS2
NAT/NAPT	NAT, NAPT MIB	NAT and NAPT variants	O	IETF RFC 4008 [i.93] IETF RFC 3489 [i.86]
NOTE 1: The MIB-2 groups are the basic unit of conformance. The MIB-2 groups lists are applicable to RCS2 implementation, then the RCST is expected to implement all objects in a functional group. NOTE 2: RCS2 identifies the new MIB elements introduced for RCS2.				

The SNMP object type syntax is provided in table 8.5.

Table 8.5: RCST MIB SNMP objects syntax

SNMP Object Type	Description
Integer32	Represents integer-valued information -2^31 and 2^31 inclusive in big Indian order from SNMPv2-SMI.
INTEGER	Used to represent integer-valued information as named-number enumeration. In this case, only those named-numbers so enumerated may be present as a value.
OCTET STRING	A string of 0 or more 8-bit bytes. Each byte has a value between 0 and 255. In the BER encoding used for this data type, a count of the number of bytes in the string precedes the string. These strings are not null-terminated strings.
DisplayString	A textual description of the entity. Printable ASCII characters.
PhysAddress	OCTET STRING specifying a media or physical address.
MacAddress	Represents an 802 MAC address represented in the 'canonical' order defined by IEEE 802-2001 [i.61], OCTET STRING (SIZE(6)).
Counter32	A non-negative integer whose value increases monotonically from 0 to 2^32 - 1, and then wraps back to 0 from SNMPv2-SMI.
Counter64	A non-negative integer whose value increases monotonically from 0 to 2^64 - 1, and then wraps back to 0.
Gauge32	A non-negative integer between 0 and 2^32 - 1, whose value can increase or decrease, but latches at its maximum value. That is, if the value increments to 2^32 - 1, it stays there until reset from SNMPv2-SMI.
Gauge64	A non-negative integer between 0 and 2^64 - 1, whose value can increase or decrease, but latches at its maximum value. That is, if the value increments to 2^64 - 1, it stays there until reset.
Unsigned32	Unsigned32 specifies a value whose range includes only non-negative integers (0 to 4294967295), as given in SNMPv2-SMI.
RowStatus	Type textual convention, mainly used to declare dynamic tables, to manage the creation and deletion of conceptual rows, used as the value of the SYNTAX clause for the status column of a conceptual row (IETF RFC 2579 [i.103]). The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active(1). A row can be created either by createAndGo and automatically change to active state or createAndWait to add more parameters before becoming active.
TimeTicks	Non-negative integer which represents the time, modulo 2^32 (4 294 967 296 decimal), in hundredths of a second between two epochs, from SNMPv2-SMI.
TimeStamp	Textual convention based on the TimeTicks type. With a TimeStamp, the first reference epoch is defined as the time when sysUpTime (MIB-II system SNMP object) was zero, and the second reference epoch is defined as the current value of sysUpTime from SNMPv2-TC.
SEQUENCE	Similar to a programming structure with entries.
Sequence Of	An array with elements with one type.
InetAddress	Denotes a generic Internet address, either IPv4 or IPv6 address as an OCTET STRING (SIZE (0..255)) as defined in (IETF RFC 2465 [10]).
InetAddressType	Type of Internet address, unknown(0), IPv4(1), IPv6(2), dns(16) as defined in IETF RFC 2465 [10].
InetAddressPrefixLength	This data type is used to model InetAddress prefixes. This is a binary string of up to 16 octets in network byte-order (IETF RFC 2465 [10]).
InetPortNumber	Port number as defined in IETF RFC 2465 [10].
Textual conventions	Textual conventions for RCST indications of DVBRCS2 capabilities, including profiles, options and optional features from SNMPv2-TC. The mapping to the profiles is to be understood as described here: (0) refers to the most significant bit. A value of 1 indicates that the respective option is supported.
DSCP	Differentiated Service Code Point from DIFFSERV-DSCP-TC.

The access rights to a particular SNMP object are defined cross-checking both the maximum level of access of that SNMP object and the access rights granted to the entity according to its community name.

Table 8.6: RCST MIB Objects MAX-ACCESS values

MAX-ACCESS Value	SNMPv2 Protocol Operation	
	READ-ONLY	READ-WRITE
Read-Only (RO)	Available for get and trap operations	
Read-Write (RW)	For get and trap operations	Available for get, set, and trap operations
Read-Create (RC)	Available for get and trap operations	Available for get, set, create, and trap operations
Accessible-for-notify	Available for trap operations	
Not-Accessible (NA)	Unavailable	

The following clauses provide details for the managed objects. An RCST may implement the managed objects as specified in these clauses.

The RCST may support a minimum of 10 available SNMP table rows, unless otherwise specified to the RFC. The RCST minimum number of available SNMP table rows mean rows (per table) that are available to support device configuration.

8.6.1 System group

The system group follows the definition provided in IETF RFC 1213 [i.68] and IETF RFC 3418 [i.84].

The RCST may implement the System Group (IETF RFC 3418 [i.84]) possibly with exceptions, as specified in the System MIB module listed in this clause.

Table 8.7: RCST System Group

Functional Group	System						
Element	Parameter	Type	Unit	Range	Default	Description	Source
sysDescr	DisplayString	RO	-	-	-	Textual description of the entity in ASCII characters	IETF RFC 1213 [i.68]
sysObjectID	Object ID	RO	-	-	-	Vendor's authoritative identification	IETF RFC 1213 [i.68]
sysUpTime	TimeTicks	RO	Hundreds of seconds	-	-	Time since the network management was re-initialized (time since logon)	IETF RFC 1213 [i.68]
sysContact	DisplayString	RW	-	-	-	Contact person for this managed RCST	IETF RFC 1213 [i.68]
sysLocation	DisplayString	RW	-	-	-	GPS position of the RCST ODU expressed as longitude, latitude and altitude. The string has 31 characters in the following format <xx.xxx>, <a>, <yyy.yyy>, <b>, <zzzz.z>, M, where x,y and z represent digits, a=N or S, b= E or W	IETF RFC 1213 [i.68]
sysServices	INTEGER	RO	-	(0..127)	-	Value that indicates the set of services that this entity primarily offers	IETF RFC 1213 [i.68]

8.6.2 Interfaces group

The interfaces group follows the definition provided in IETF RFC 2863 [11]. This clause documents only the differences or particularities from the requirements specified in the interfaces MIB module.

The ifType label values for DVB-RCS2 may be assigned by IANA. The ifTypes associated with an RCST interface in RCS2 are:

- dvbRcs2downstream: corresponds to the forward link on an RCS2 system. It is based on DVB-S2(X) standard [4] and [21]. Only transparent systems are considered by the present MIB module.

- dvbRcs2MAClayer: represents the complete air interface of an RCST. This interface support star and mesh networks and is bi-directional. Only star networks are considered by the present MIB module.
- dvbRcs2upstream: represents the physical link for the return of an RCS2 transparent system of the uplink of an RCS2 regenerative system. It is based on the specification provided in [1].

One or several Ethernet interfaces are used on the LAN side of the RCST.

An instance of ifEntry is expected for each dvbRcs2downstream (normally one) and dvbRcs2MAClayer interface (normally one).

The ifStackTable (IETF RFC 2863 [11]) identifies the relationships among sub-interfaces. The dvbRcs2MAClayer interface is layered on top of the downstream and upstream interfaces.

The RCST may discard any traffic over an interface whose ifAdminStatus is "down" (traffic includes data and management traffic where applicable).

Table 8.8: RCST Interfaces Group

Functional Group	interfaces						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
ifNumber	INTEGER	RO	-	0..32	3	Number of network interfaces present in the RCST, minimum 3. In case of VLAN, the virtual interface has to be accounted for.	IETF RFC 1213 [i.68]
ifTable	SEQUENCE ifEntry	-	-	-	-	Interfaces table contains information on the entity's interfaces.	IETF RFC 1213 [i.68]
ifEntry	ifEntry SEQUENCE OF{ ifIndex, ifDescr ifType ifMtu ifSpeed ifPhysAddress ifAdminStatus ifOperStatus ifLastChange ifInOctets ifInUcastPkts ifInNUcastPkts ifInDiscards ifInErrors ifInUnknownProtos ifOutOctets ifOutUcastPkts ifOutNUcastPkts ifOutDiscards ifOutErrors ifOutQLen ifSpecific }	-	-	-	-	Each downstream or upstream interface is one ifEntry. Each dvbRcs2MACLayer interface may be attached to a different VRF.	IETF RFC 1213 [i.68]
ifIndex	INTEGER	RO	-	1..32	-	ifTable index used to link the LAN interface to its assigned MAC24 address, by means of the VRF group table.	IETF RFC 1213 [i.68]
ifType	INTEGER	RO				IANA value of dvbRcs2 interface See note.	IETF RFC 1213 [i.68]

Functional Group	interfaces						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
ifSpeed	GAUGE	RO	Bits/s			Speed in bits/s of this interface. This is the symbol rate multiplied with the number of bits per symbol.	IETF RFC 1213 [i.68]
ifHighSpeed	INTEGER	RO	Bits/s				IETF RFC 1213 [i.68]
ifPhysAddress	OCTET STRING	RO	-	-	-	MAC24 (L2 address) associated to the interface.	IETF RFC 1213 [i.68]
ifAdminStatus	INTEGER	RO	-	-	-	Administrative status of the interface.	IETF RFC 1213 [i.68]
ifOperStatus	INTEGER	RO	-	-	-	Current operational status of the interface 'down' = notReady; 'dormant' = configFileComplete 'up' = operational	IETF RFC 1213 [i.68]
ifMTU	INTEGER	RO	bytes		1 500	Size of the largest frame that can be sent on this interface, specified in octets. The value includes the length of the MAC header.	IETF RFC 1213 [i.68]
ifInOctets	Counter	RO	Octets		0	The total number of octets received on this interface including the L2 header.	IETF RFC 1213 [i.68]
ifInUcastPkts	Counter	RO	Packets		0	Number of unicast packets received on this interface. Including IP data packets and L2S packets.	IETF RFC 1213 [i.68]
ifInNUcastPkts	Counter	RO	Packets		0	Number of multicast or broadcast packets received on this interface. Including IP data packets and L2S packets.	IETF RFC 1213 [i.68]
ifInDiscards	Counter	RO	Packets		0	Total number of received packets that have been discarded on this interface. Including IP data packets and L2S packets.	IETF RFC 1213 [i.68]
ifInErrors	Counter	RO	Packets		0	Number of inbound packets that contained error preventing them from being deliverables to higher layers. Possible reasons L2 errors.	IETF RFC 1213 [i.68]
ifInUnknownProtos	Counter	RO	Packets		0	Number of frames with unknown packet type.	IETF RFC 1213 [i.68]
ifOutOctets	Counter	RO	Octets		0	Returns the number of octets transmitted on this interface, including the length of L2 header.	IETF RFC 1213 [i.68]

Functional Group	interfaces						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
ifOutUcastPkts	Counter	RO	Packets		0	Returns the number of packets transmitted on this interface. Including IP data packets and L2S packets.	IETF RFC 1213 [i.68]
ifOutNUcastPkts	Counter	RO	Packets		0	Returns the number of multicast/broadcast of octets transmitted on this interface including IP data packets and L2 packets.	IETF RFC 1213 [i.68]
ifOutDiscards	Counter	RO	Packets		0	Total number of outbound packets which were discarded, possible reasons are buffer shortage, or not enough transmission resources.	IETF RFC 1213 [i.68]
ifOutErrors	Counter	RO	Packets		0	Number of packets that could not be transmitted due to errors.	IETF RFC 1213 [i.68]
NOTE: For support of multiple MAC24 addresses, including the management MAC24, the virtual interfaces correspond to ifType = dvbRcsMAClayer.							

8.6.3 ip group

The RCST requirements for IETF RFC 4293 [i.99] are defined in this clause.

The RCST may implement the ipv4GeneralGroup.

The RCST may implement ipv6GeneralGroup.

The RCST may implement the ipv4InterfaceTable.

The RCST may populate the ipv4InterfaceTable with each Ethernet interface with an assigned IPv4 address. The RCST may record other interfaces in the ipv4InterfaceTable which have assigned IPv4 addresses.

The RCST may populate the ipv6InterfaceTable with each Ethernet interface with an assigned IPv6 address. The RCST may record other interfaces in the ipv6InterfaceTable which have assigned IPv6 addresses.

The RCST may implement the ipSystemStatsTable.

The RCST may implement the ipIfStatsTable.

The RCST may implement the ipAddressPrefixTable.

The RCST may implement the ipAddressTable.

The RCST may implement the ipNetToPhysicalTable.

The RCST may implement the ipDefaultRouterTable.

If the RCST has been configured for a default route, the RCST is assumed to populate the default router in the ipDefaultRouterTable.

The RCST may populate the ipDefaultRouterTable with an IPv4 and/or IPv6 statically configured default router or a default router learned through a dynamic update mechanism such as a routing protocol update or IPv6 router advertisement message.

The RCST IP forwarding table follows the format given by IETF RFC 4293 [i.99] that describes the managed objects related to the forwarding of Internet Protocol (IP) packets in an IP version independent manner. This clause documents only the differences or particularities from the requirements specified in the interfaces MIB module.

The RCST ip forwarding information is composed by the inetCidrRoute branch that hangs from the ipForward MIB group from the ip(24) of mib-2.

Each VRF group will count with its own inetCidrRouteTable set of entries identified by the ifIndex, the interface identifier. The RCST network MIB group is assumed to contain the list of VRFs that apply to a particular RCST (see clause 8.6.13) and the association with the SVN number.

Each entry in the inetCidrRouteTable will have as index the following MIB objects:

- inetCidrRouteDestType
- inetCidrRouteDest
- inetCidrRoutePfxLeng
- inetCidrRoutePolicy
- inetCidrRouteNextHoType
- inetCidrRouteNextHop

These objects may be provided for the creation of a new route entry in the table and are considered "not accessible". Any modification will require a route deletion and a new route creation.

This is dynamic SNMP table, independently if the IP routes are created thanks to statically (i.e. during initial installation) or dynamically (i.e. thanks to OSPF dynamic routing protocol).

The information of the default Gateway for the RCST (if any) and the list of Gateways that the RCST may access by following a certain criteria (e.g. traffic congestion, multicast capabilities) may be included in the ipInetCidrRouteTable, the metric objects could be used for this purpose.

Table 8.9: RCST IP Forwarding Group

Functional Group	Ip forwarding						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
inetCirdRouteNumber	Gauge32	RO	-	-	-	The number of current netCidrRouteTable entries that are not invalid.	IETF RFC 4292 [i.43]
inetCidrRouteDiscards	Gauge32	RO	-	-	-	Number of valid route entries discarded from the inetCisdrRouteTable. Entries that do not appear in the table.	IETF RFC 4292 [i.43]
inetCidrRouteTable	SEQUENCE	NA	-	-	-	The RCST's IP Routing Table.	IETF RFC 4292 [i.43]
inetCidrRouteEntry	SEQUENCE OF	NA	-	-	-	A particular route to a particular destination, under certain policy.	IETF RFC 4292 [i.43]
inetCidrRouteDestType	InetAdressType	NA	-	-	-	The type of inetCidrRouteDest address, as defined in IETF RFC 4001 [i.104].	IETF RFC 4292 [i.43]
inetCidrRouteDest	InetAddress	NA	-	-	-	Destination IP address of this route following IETF RFC 4292 [i.43]	IETF RFC 4292 [i.43]
inetCidrRoutePfxLen	InetAddressPrefixLength	NA	-	-	-	Number of leading one bits that form the mask following IETF RFC 4292 [i.43].	IETF RFC 4292 [i.43]
inetCidrRoutePolicy	OBJECT IDENTIFIER	NA	-	-	00	Additional index that may delineate between different entries. Not used by default for RCS2 RCST.	IETF RFC 4292 [i.43]
inetCidrRouteNextHopType	InetAddressType	NA	-	-	-	Address type of the next hop.	IETF RFC 4292 [i.43]

Functional Group	Ip forwarding						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
inetCirdRouteNextHop	InetAddress	NA	-	-	-	Next hop IP address	IETF RFC 4292 [i.43]
inetCidrRouteIfIndex	InterfaceIndexOrZero	RC	-	-	-	The ifIndex value that identifies the local interface through which the next hop of this route should be reached. Value 0 represents no interface specified.	IETF RFC 4292 [i.43]
inetCidrRoutetype	INTEGER	RC	-	-	-	Type of route following IETF RFC 4292 [i.43].	IETF RFC 4292 [i.43]
inetCidrRouteProto	IANAipRouteProtocol	RO	-	-	-	The routing mechanism via which this route was learned, only applies for dynamic routing and OSPF protocol (13) Open Short Path First.	IETF RFC 4292 [i.43]
inetCidrRouteAge	Gauge32	RO	Seconds	-	-	Number of seconds since the route was last updated.	IETF RFC 4292 [i.43]
inetCidrRouteNextHopAS	InetAutonomousSystemNumber	RC	-	-	0	Autonomous System number of the next hop. Default value zero, unknown or not relevant.	IETF RFC 4292 [i.43]
inetCidrRouteMetric1	Integer32	RC	-	-	-1	Primary metric for this route. The semantics of the metric are determined by OSPF. When not used, default value is -1.	IETF RFC 4292 [i.43]
inetCidrRouteMetric2	Integer32	RC	-	-	-1	Alternative routing metric. Default not used, -1.	IETF RFC 4292 [i.43]
inetCidrRouteMetric3	Integer32	RC	-	-	-1	Alternative routing metric. Default not used, -1.	IETF RFC 4292 [i.43]
inetCidrRouteMetric4	Integer32	RC	-	-	-1	Alternative routing metric. Default not used, -1.	IETF RFC 4292 [i.43]
inetCidrRouteMetric5	Integer32	RC	-	-	-1	Alternative routing metric. Default not used, -1.	IETF RFC 4292 [i.43]
inetCidrRouteStatus	RowStatus	RC	-	-	-	The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	IETF RFC 4292 [i.43]

8.6.4 Ethernet Interface MIB group

The RCST may implement (IETF RFC 3635 [i.91]) for each of its Ethernet interfaces.

8.6.5 icmp MIB group

The RCST may implement icmpStatsTable from IETF RFC 4293 [i.99].

The RCST may implement icmpMsgStatsTable from IETF RFC 4293 [i.99].

8.6.6 udp MIB group

The RCST may implement UDP-MIB (IETF RFC 4113 [i.96]).

8.6.7 tcp MIB group

The RCST may implement TCP-MIB group (IETF RFC 4022 [i.94]).

8.6.8 snmp MIB group

The RCST may implement the SNMP group from IETF RFC 3418 [i.84]. This group provides SNMP protocol statistics and protocol error counters.

The snmpCommunityTable is defined in the "SNMP Community MIB Module" section of IETF RFC 3584 [i.88].

The snmpTargetAddrTable is defined in the "Definitions" section of IETF RFC 3413 [i.79].

The RCST may create one row in snmpTargetAddrTable for each SNMPv2c Transport Address Access.

SNMP access is controlled and specified by the MIB objects in IETF RFC 3315 [i.37] through IETF RFC 3415 [i.81], and IETF RFC 3584 [i.88]. The RCST may have several interfaces. If SNMP access filters are applied to RCST IfIndex 1, the RCST may apply the same filters to the "Additional LAN interfaces".

8.6.9 dhcp MIB group

The RCST DHCP options configuration for IPv4 may follow (IETF RFC 2132 [i.70]).

The RCST DHCP options configuration for IPv6 may follow (IETF RFC 3633 [i.90]).

The RCST DHCP LAN interface server for IPv4 may be disabled in the RCST by default. When enabled, it may be possible to configure the IPv4 address of the RCST LAN interface, IPv4 mask, and a range of IPv4 addresses allocable for the DHCP service.

The RCST DHCP LAN interface server for IPv6 may be disabled by default.

8.6.10 igmp MIB group

The RCST may implement IETF RFC 2933 [12] when supporting IGMPv2 for dynamic multicast group management.

8.6.11 System configuration group

System configuration group gathers some basic information that would allow anyone to trace the history "the life" of the RCST, as well as to get a complete description of its constitution on the component point of view, including the options/features support statement. Many of the parameters will be defined at installation.

The RCST system configuration MIB group includes the following modules:

- dvbRcs2SystemProfileMap represents the RCS2 profiles supported.
- dvbRcs2SystemOptionalMap represents the RCS2 options supported. They represent important functionality, with impact on interoperability, and their support is advertised with the RCST logon.
- dvbRcs2SystemFeatureMap represents the RCS2 optional features. These represent minimum features, not necessary for interoperability.

Table 8.10: RCST System RCS2 Group

Functional Group	DvbRcs2SystemConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2SystemProfileMap	Textual convention	RW		Consumer-Linear(0), SOHO (1), Multi-dwelling (2), Corporate (3), SCADA-Linear(4), Backhaul (5), Institutional (6), Consumer-CPM(7), SCADA-CPM(8).		Indicates RCST profile definition. Until version 1.2.1 of the present document, Consumer-Linear was consumer and SCADA-Linear was SCADA	RCS2
dvbRcs2SystemOptionMap	Textual convention	RW		16QAMrtn (0), 32APSKfwd (1), waveformFlex (2), contentionSync(3), nomarclFec (4), multiTs (5), qsTs (6), VLAN (7), enhMulticas t(8).		Enumerates the RCST options for RCS2	RCS2
dvbRcs2SystemFeaturesMap	Textual convention	RO		qpsk_8psk_cpmRtn (0), refWaveforrms (1), customWaveforms (2), waveformBound (3), waveformToTimeslot (4), eirpPowerCtrol (5), constantPowerCtrl (6), fwdLinkDvbs2 (7), fwdLinkSingleGS (8), fwdLinkTSPacketStream (9), fwdLinkMultipleStreams (10), gseBBFrameCRC32 (11), damaTraffic (12), unsolicitedDATraffic (13), slottedAlohaLogon (14), recombinedDAMA (15), raReplicas (16), inbandSignalling (17), signallingDAtimeslots (18), dhcpLAN (19), ipv4ipv6Support (20), DynamicMulticast (21), diffservQoS (22), mplsSupport (23), motorControl (24), sddp (25), pepNegotiationProtocol (26), authenticatedLogon (27), dynamicRouting (28), mesh (29), SCPC (30), space3 (31), Mobile (32), QPSK_8PSKSupport(33), CPMSupport(34), DVBS2XACM(35), NCRv2(36).		Optional compatibility features and minor options mapping. The terminal informs the Hub which are the supported features. The Hub in return will set up the option flags required for a particular session	RCS2

Functional Group	DvbRcs2SystemConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2LowerLayerCapabvilities	Textual convention	RO		multipleGS1 (0), multipleGS2 (1), reserved1 (2), fullRangeFLMODCOD (3), fullRangeRLMODCOD (4), fastCarrierSwitching (5), carrierSwitchingClass1 (6), carrierSwitchingClass2 (7), EsN0powerCtrl (8), constantPowerSpectrumDensity (9), slottedAlohaTraffic (10), crdsaTrafficSupport (11), reserved2 (12), reserved3 (13), reserved4 (14), customCCCPMwaveform (15), service1 (16), service2 (17), service3 (18), service4 (19), nbrofL2ifs (20), nbrofL2ifs (21), nbrofL2ifs (22), nbrofL2ifs (23), SWversion1 (24), SWversion2 (25), SWversion3 (26), SWversion4 (27), SWversion5 (28), SWversion6 (29), SWversion7 (30), SWversion8 (31), return_cc_support (32), Reserved (4) (33), Reserved (5) (34), Reserved (6) (36), Dcp_ip_support (37), Dcp_l2_support (38), regenerative_mesh_support (39), transparent_mesh_support (40).		Lower layer capabilities following table 8.5 from [1]	RCS2
dvbRcs2SystemCapabilities	Textual convention	RO		freqhoppingRange1 (0), freqhoppingRange2 (1), mfTdma (2), rcstClass1 (3), rcstClass2 (4), dynamicConnectivity (5), mobile (6), transec (7).		RCST capabilities to be informed to the NCC during logon	RCS2
dvbRcs2HigherLayerCapabilities	Textual convention	RO		ipv4ipv6Support (0), multicastFwd (1), enhMulticast (2) dynamicMulticast (3), diffservQoS (4), mplsSupport (5), snmpv2c (6), Snmpv3 (7), dynamicConnectivity (8), transecHooksSupport (9), dynamicRouting (10), ospfSupport (11), firewall (12), multiSVNO (13), VLAN (14), dhcpLAN (15), motorControl (16), sddp (17), pepNegotiationProtocol (18), authenticatedLogon (19), mesh (20), reserved (21),		Higher layer capabilities	RCS2

Functional Group	DvbRcs2SystemConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
				reserved (22), reserved (23).			
dvbRcs2PointingAlignmentSupport	Unsigned32	RO		0 – Reserved 1 – Nominal CW EIRP in the pointing direction 2-127 Reserved 128-255 User defined		8 bit field that indicates the support of pointing alignment probing	RCS2
dvbRcs2SystemNetworkTopologySupport	Textual convention	RO		starTransparent (0), meshRegenerative (1), meshTrasnparent (2), hybrid (3)		Network topology as described in [i.1]	RCS2
dvbRcs2SystemNetworkEncapsulationModeTx	INTEGER	RO		ATM (1), MPEG (2), RLE (3), GSE (4).		Encapsulation mode for transmission	RCS2
dvbRcs2SystemNetworkEncapsulationModeRx	INTEGER	RO		ATM (1), MPEG (2), RLE (3), GSE (4).		Encapsulation mode for reception	RCS2
dvbRcs2SystemOduAntennaSize	INTEGER32	RW	cm	-		Diameter of the antenna	IETF RFC 5728 [i.59]
dvbRcs2SystemOduSspa	INTEGER32	RW	0.1W	-		Power level of the Solid State Power Amplifier	IETF RFC 5728 [i.59]
dvbRcs2SystemOduGain	INTEGER32	RW	0.1dBi	-		Antenna peak gain of the ODU	IETF RFC 5728 [i.59]
dvbRcs2SystemOduTxType	SnmpAdminString	RW		-		Type of transmitter installed in the ODU	IETF RFC 5728 [i.59]
dvbRcs2SystemOduRxType	SnmpAdminString	RW		-		Type of LNB installed in the ODU, with information such as vendor type, output type	IETF RFC 5728 [i.59]
dvbRcs2SystemOduRxBand	INTEGER	RW		High-band (0), Low Band (1)		LNB high band/Low band selector. High band corresponds to the emission of an 18-26 khz tone with 0,4-0,8 Vpp in the Rx IFL cable	IETF RFC 5728 [i.59]

Functional Group	DvbRcs2SystemConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2SystemOduRxLO	INTEGER32	RW		-		LNB High Band/Low Band selector. High Band corresponds to the emission of an 18-26 kHz tone with 0,4-0,8 Vpp in the Rx IFL cable: (0) - High Band (1) - Low Band"	IETF RFC 5728 [i.59]
dvbRcs2SystemOduTxLO	INTEGER32	RW		-	-	Frequency of Block Up-Converter Local Oscillator (in 100 Hz)	IETF RFC 5728 [i.59]
dvbRcs2SystemPopulationID	INTEGER	RW		-	-	Population ID, required during installation.	IETF RFC 5728 [i.59]
carrierFrequencyChange	INTEGER	RO		(1) Class1, (2) Class2, (3) Class 3, (4) Class 4	-	RCST carrier frequency hopping class	RCS2

8.6.12 Network Config group

This group contains all the MIB objects related to addressing and network parameters for the RCS2 RCST.

The minimum set of network config group parameters is intended to cover the RCST addressing plan the RCST VRF groups configuration.

The RCST addressing plan is composed of:

- The set of SVN to be used and, assignment of each SVN to a VRF Group included in the vrfGroupTable.
- The list of network IPv4/IPv6 addresses per virtual LAN Interface: information provided using the ifTable for interfaces definition and the ipInetCidrRouteTable.
- The IPv4 address of the RCST satellite interface for M and C signalling included in this group.

Table 8.11: RCST Network RCS2 Group

Functional Group	dvbRcs2NetworkConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2OamInetAddressType	InetAddressType	RW	-	-	-	Type of internet address of dvbRcs2NetworkOaminetAddress. As specified, the type should be IPv4 (1).	RCS2
dvbRcs2NetworkOamInetAddress	InetAddress	RW	-	-	-	Terminal IP address for management.	IETF RFC 5728 [i.59]
dvbRcs2NetworkOamInetAddressPrefixLength	InetAddressPrefixLength	RW	-	-	-	Prefix length of the terminal management IP address. If the prefix is unknown or does not apply, the value is zero.	IETF RFC 5728 [i.59]

dvbRcs2NetworkOamInetAddressAssign	INTEGER (0) oamInetAddressStatic, (1) oamInetAddressDynamic	RW	-	-	-	Identifies wether the OAM IP address is statically or dynamically assigned.	IETF RFC 5728 [i.59]
svnMacMgmt	OCTET STRING	RW	-	-	-	RCST MAC24 address used for M & C, given at logon. Saved in the MIB object for supervision.	RCS2
svnMacMgmtMask	OCTET STRING	RW	-	-	-	SVN mask used for M and C given at logon. Saved in the MIB for supervision.	RCS2
NetworkConfigTable	SEQUENCE OF NetworkConfig ENTRY	NA				RCST LAN interface addresses configuration. See note.	RCS2
NetworkConfigEntry	SEQUENCE OF { NetworkConfigIndex, NetworkConfigLANInetAddressIfIndex, NetworkConfigLANInetAddressType, NetworkConfifLANInetAddressPrefixLength, NetworkConfigAirInterfaceDefaultGatewayInetAddresstype, NetworkConfigAirInterfaceDefaultGatewayInetAddress, NetworkAirInterfaceDefaultGatewayInetAddressPrefixLength, NetworkPrimaryDnsServerInetAddressType, NetworkPrimaryDnsServerInetAddress, NetworkPrimaryDnsServerInetAddressPrefixLength, NetworkSecondaryDnsServerInetAddressType, NetworkSecondaryDnsServerInetAddress, NetworkSecondaryDnsServerInetAddressPrefixLength}	NA					
NetworkConfigIndex	INTEGER	NA				Table index.	
NetworkConfigLANInetAddressIfIndex	INTEGER	RC				ifIndex from the interfaces group.	
NetworkConfigLANInetAddressType	InetAddressType	RC	-	-	-	Type of Internet address on the LAN interface. If there is no address, the value is unknown (0).	RCS2
NetworkConfigLANInetAddress	InetAddress	RC	-	-	-	Internet address of the LAN interface associated to the IfIndex.	RCS2
NetworkConfigLANInetAddressPrefixLength	InetAddressPrefixLength	RC	-	-	-	Prefix length of the LAN IP address associated to the IfIndex.	RCS2

NetworkConfigAirInterfaceDefaultGatewayInetAddresstype	InetAddressType	RC	-	-	-	Default gateway IP address type.	RCS2
NetworkConfigAirinterfaceDefaultGatewayInetAddress	InetAddress	RC	-	-	-	IP address of the default gateway associated to the IfIndex.	RCS2
NetworkConfigAirInterfaceDefaultGatewayInetAddressPrefixLength	InetAddressPrefixLength	RC	-	-	-	Prefix length of the default gateway IP address.	RCS2
NetworkConfigPrimaryDnsServerInetAddressType	InetAddressType	RC	-	-	-	Type of IP address for dns server.	RCS2
NetworkConfigPrimaryDnsServerInetAddress	InetAddress	RC	-	-	-	DNS server IP address in the NCC.	RCS2
NetworkConfigPrimaryDnsServerInetAdrressPrefixLength	InetAddressPrefixLength	RC	-	-	-	Prefix length for the DNS server in the NCC.	v
NetworkConfigSecondaryDnsServerInetAddressType	InetAddressType	RC	-	-	-	Type of IP address for the secondary DNS server in the NCC.	v
NetworkConfigSecondaryDnsServerInetAddress	InetAddress	RC	-	-	-	IP address of the secondary DNS server in the NCC.	v
NetworkConfigSecondaryDnsServerInetAddressPrefixLength	InetAddressPrefixLength	RC	-	-	-	Prefix length of the secondary DNS server in the NCC.	RCS2
NetworkConfigRowStatus	Row Status	RC	-	-	-	The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1). A row can be created either by createAndGo and automatically change to active state or createAndWait to add more parameters before becoming active.	RCS2
dvbRcs2NetworkNmcMgtInetAddress	InetAddressType	RW	-	-	-	Type of address of the management server in the NMC.	IETF RFC 5728 [i.59]
dvbRcs2NetworkNmcMgtInetAddress	InetAddress	RW	-	-	-	NMC IP address.	IETF RFC 5728 [i.59]
dvbRcs2NetworkNmcMgtinetAddressPrefixLength	InetAddressPrefixLength	RW	-	-	-	NMC IP address prefix length.	IETF RFC 5728 [i.59]
dvbRcs2NetworkConfigFileDownloadUrl	Uri (SIZE(0..65535))	RW	-	-	-	Fullpath name for the configuration file download.	IETF RFC 5728 [i.59]
dvbRcs2NetworkInstallLogFileDownlaodUrl	Uri (SIZE(0..65535))	RW	-	-	-	Full path name of the installation log file to download.	IETF RFC 5728 [i.59]
dvbRcs2NetworkConfigFileUploadUrl	Uri (SIZE(0..65535))	RW	-	-	-	Fullpath name for the configuration file upload.	IETF RFC 5728 [i.59]

dvbRcs2NetworklogFileUploadUrl	Uri (SIZE(0..65535))	RW	-	-	-	Full path name for the event log file.	IETF RFC 5728 [i.59]
dvbRcs2NetworkInstallLogFileUploadUrl	Uri (SIZE(0..65535))	RW	-	-	-	Full path name for the installation log file.	IETF RFC 5728 [i.59]
NOTE: One different LAN interface could be identified per subscriber for a Multi-dwelling terminal.							

8.6.13 L3VirtualRoutingForwardingConfig group

These set of parameters determine L3 virtual routing forwarding configuration of the RCST.

RCST configuration related to dynamic routing and OSPF can be superseded by instructions provided in the NLID descriptor.

The SVNO may remotely update the OSPF configuration of an RCST interface by procedures relying on L3 IP connectivity.

Option *ospfSupport* in *dvbRcs2SystemOptionMap* MIB group shall be set for configuring RCST OSPF support.

The OSPF function automatically creates entries in the *inetCidrRouteTable* of the *ip* RCST MIB group. The routes for different SVNs are identified by parameter *inetCidrRouteIfIndex*, which identifies the interface to which the route applies.

The *L3VirtualRoutingForwardingConfig* group allows configuring OSPF settings per VRF group in the RCST. For meshed networks, *vrfOSPFRouting* parameter should be always enabled, and *vrfOSPFrouterAddress* should include the DR address (either statically or dynamically configured). Static configuration allows reducing signalling load to elect the DR.

Table 8.12: RCST VRF RCS2 Group

Functional Group	dvbRcs2 L3VirtualRoutingForwardingConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
vrfGroupTable	SEQUENCE OF vrfGroupEntry	NA	-		-	VRF group table that contains the IP routing forwarding information of the RCST per interface.	RCS2
vrfGroupEntry	SEQUENCE { vrfGroupIndex, vrfGroupSVNnumber, vrfSVNMAClabel, vrfGroupIfInterface, vrfGroupSVNMask, vrfSVNmtu, vrfGroupIfInterface, vrfOSPFrouting, vrfOSPFrouterAddressType, vrfOSPFrouterAddress, vrfOSPFrouterPrefix, vrfOSPFbackupRouterAddressType, vrfOSPFbackupRouterAddress, vrfOSPFbackupRouterAddressPrefix, vrfMulticastMappingMethod vrfMulticastFwd vrfMulticastRtn vrfIgmpVersion vrfIgmpQuerierLAN vrfIgmpProxy vrfIgmpQuerierSAT	NA	-		-	VRF group table entry, each entry will identify a particular SVN association to one VRF group, and the corresponding interface ifIndex.	RCS2

Functional Group	dvbRcs2 L3VirtualRoutingForwardingConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
	vrfIgmpForward vrfPimSM vrfMldQuerierLAN vrfMldProxy vrfMldQuerierSAT vrfMldForward vrfGroupStatusRow}						
vrfGroupIndex	INTEGER	NA	-		-	VRF group table index or VRF group identified.	RCS2
vrfGroupSVNnumber	INTEGER	RC	-		-	SVN number associated to this VRF group.	RCS2
vrfGroupSVNMAClabel	OCTET STRING	RC	-		-	SVNMAC label identifier attached to this VRF group.	RCS2
vrfGroupSVNMask	OCTET STRING	RC	-		-	The corresponding SVN mask attached to this VRF group.	RCS2
vrfSVNmtu	Unsigned32	RC				The MTU that applies to all traffic SVNs.	RCS2
vrfGroupIfInterface	INTEGER	RC	-		-	ifIndex from the interfaces group linked to this VRF group. Each Each entry in the ipInetCidrRouteTable is linked to a different interface.	RCS2
vrfOSPFRouting	INTEGER	RC		Static (1), Dynamic (2)		Routing option: static or dynamic.	RCS2
vrfOSPFrouterAddressType	InetAddressType	RC	-	-	-	In case of dynamic routing, this is the type of address of the OSPF module in the NCC/Gateway Router.	RCS2
vrfOSPFrouterAddress	InetAddress	RC	-	-	-	In case of dynamic routing, this is the address of the OSPF module in the NCC/Gateway Router.	RCS2
vrfOSPFrouterPrefix	InetAddressPrefix	RC	-	-	-	In case of dynamic routing, this is the prefix of address of the OSPF module in the NCC/Gateway Router.	RCS2
vrfOSPFbackupRouterAddressType	InetAddressType	RC	-	-	-	Backup OSPF DR address type.	RCS2
vrfOSPFbackupRouterAddress	InetAddress	RC	-	-	-	Backup OSPF DR address.	RCS2
vrfOSPFbackupRouterPrefix	InetAddressPrefix	RC	-	-	-	Backup OSPF DR address prefix.	RCS2
vrfMulticastMappingMethod	INTEGER	RC		Mode1 (1), mode2 (2), mode3 (3)	Mode1 (1)	Configuration of the multicast mapping method in the terminal as described in clause 6.2.3. See note.	RCS2
vrfMulticastFwd	boolean	RC		Disable(0), enable (1)	Enable (1)	Enable/disable multicast reception.	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2 L3VirtualRoutingForwardingConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
vrfMulticastRtn	boolean	RC		Disable (0), enable (1)	Enable (1)	Enable/disable multicast transmission When enabled, the RCST can forward multicast traffic towards the satellite interface.	IETF RFC 5728 [i.59]
vrfIgmpVersion	INTEGER	RC		(2) version 2, (3) version 3	(2) version 2	IGMP v2 is mandatory if dynamic multicast is implemented.	RCS2
vrfIgmpQuerierLAN	boolean	RC		Disable (0), enable (1)	Disable (0)	Enable/disable igmp querier towards RCST LAN Static or dynamic multicast towards the LAN.	RCS2
vrfIgmpProxy	boolean	RC		Disable (0), enable (1)	Disable (0)	Enable/disable igmp proxy towards the satellite interface For sending IGMP queries to the satellite interface.	RCS2
vrfIgmpQuerierSAT	boolean	RC		Disable (0), enable (1)	Disable (0)	Enable/disable igmp querier towards the satellite interface Flag activated, the RCST can dynamically manage multicast groups with listeners behind other RCSTs belonging to the same SVN.	RCS2
vrfIgmpForward	boolean	RC		Disable (0), enable (1)	Disable (0)	Enable/disable IGMP forwarding (no treatment to IGMP messages) When enable assumes IGMP querier and proxy are disabled. This is used when customer needs to use a separate multicast router.	RCS2
vrfPimSM	boolean	RC		Disable (0), enable (1)	Disable (0)	When enabled, the RCST will intercept multicast PIM messages over the satellite interface.	RCS2
vrfMldQuerierLAN	boolean	RC		Disable (0), enable (1)	Disable (0)	Implies multicast reception enabled fro IPv6.	RCS2
vrfMldProxy	boolean	RC		Disable (0), enable (1)	Disable (0)	Required for dynamic multicast using MLD for IPv6.	RCS2
vrfMldQuerierSAT	boolean	RC		Disable (0), enable (1)	Disable (0)	For sending general and group queries to the satellite interface.	RCS2

Functional Group	dvbRcs2 L3VirtualRoutingForwardingConfig						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
vrfMldForward	boolean	RC		Disable(0), enable(1)	Disable (0)	Transparent forwarding of MLD messages to/from the satellite interface.	RCS2
vrfGroupStatusRow	Row Status	RC	-	-	-	The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active(1). A row can be created either by createAndGo and automatically change to active state or createAndWait to add more parameters before becoming active.	RCS2
NOTE: The 3 modes for multicast mapping are: Mode1) Implicit mapping hash layer 3 network address to one of a range of SVN-MAC multicast labels. Mode2) Explicit mapping given by MMT2. Mode3) Mapping directly to a unicast SVN-MAC label assigned to an RCST.							

8.6.14 Installation group

These set of parameters determine the installation parameters for the RCST initial antenna alignment.

Table 8.13: RCST Installation RCS2 Group

Functional Group	dvbRcs2Installation						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2InstallAntennaAlignmentState	INTEGER (1) antennaAlignmentStart, (2) antennaAlignmentdeny, (3) antennaAlignmentContinue, (4) antennaAlignmentStop, (5) antennaAlignmentSuccess, (6) antennaAlignmentFail	RW				Indicates state of the antenna alignment.	IETF RFC 5728 [i.59]
CwFrequency	Unsigned32	RW	X 100 Hz			Frequency of the transmitted continous wave.	IETF RFC 5728 [i.59]
CwMaxDuration	Unsigned32	RW	seconds			Time after which the CW carrier should be put down.	IETF RFC 5728 [i.59]
CwPower	Integer32	RW	x 0,1 dBm			IDU tx power level when the IDU is configured to send CW.	IETF RFC 5728 [i.59]
CoPolReading	Unsigned32	RW	x 0,1 dB			Co-polarization measured value during installation.	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2Installation						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
XPolReading	Unsigned32	RW	x 0,1 dB			Cross-polarization measured value during installation.	IETF RFC 5728 [i.59]
CoPolTarget	Unsigned32	RW	x 0,1 dB			Co-polarization target value during installation.	IETF RFC 5728 [i.59]
XPolTarget	Unsigned32	RW	x 0,1 dB			Cross-polarization target value during installation.	IETF RFC 5728 [i.59]
StandByDuration	Unsigned32	RW	x 0,1 dB			Time to wait in stand-by mode.	IETF RFC 5728 [i.59]
TargetEsN0	Unsigned32(0..315)	RW	x 0,1 dB			This value describes the wanted Es/N0 value that enables operation of the return link with the required link with the required error performance.	IETF RFC 5728 [i.59]
MaxFwdAlignThrExeDuration	Unsigned32	RW	seconds			The duration of the time interval during which fwd alignment accuracy should be achieved.	RCS2
MaxFail	Counter	RO	nbr			Max nbr of alignment failures.	RCS2
posDelayCorrection	Unsigned32	RW	NCR ticks			Additional initial delay correction for the RCST, in NCR ticks. The system will delay transmission of the CSC burst by this number of ticks.	RCS2

Functional Group	dvbRcs2Installation						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
posSearchN	Unsigned32	RW				Maximum attempts of timing position search for the start time of logon burst during logon. If N is this value then (2N+1) attempts will be done along with T(Burst_start_offset), which ranges as -NT.....0T.....+NT.	RCS2
PointingAlignment Support	INTEGER 0 – Nominal CW EIRP in the pointing direction 1 – Supported pointing alignment methods - (1) Burst probe, and CW probe by fixed non-configurable EIRP - (2) Burst probe, and CW probe by configurable EIRP	RW				Flag used to inform the NCC the kind of alignment procedure supported by the RCST. The type of alignment is selected during the alignment process.	RCS2

8.6.15 Control group

This MIB group contains objects a network manager can use to invoke actions and tests supported by the RCST agent and to retrieve the action/test results.

Table 8.14: RCST Installation RCS2 Group

Functional Group	dvbRcs2Control						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2CtrlReboot	INTEGER	RW		Idle (1), normal (2), alternate (3)		Variable that forces RCST to reboot: (1) idle, (2) normal reboot (from current SW load), (3) reboot from alternate load.	IETF RFC 5728 [i.59]
dvbRcs2CtrlRCSTTxDisable	INTEGER	RW		Idle (1), disable (2)		This variable forces the RCST to stop transmission.	IETF RFC 5728 [i.59]
dvbRcs2CtrlUserTrafficDisable	INTEGER	RW		Idle (1), disable (2)		Variable to disable user traffic (only RCST management signalling traffic can be transmitted).	IETF RFC 5728 [i.59]
dvbRcs2CtrlCwEnable	INTEGER	RW		Off (1), on (2)		Variable to force RCST start transmission of CW.	IETF RFC 5728 [i.59]
dvbRcs2CtrlOduTxReferenceEnable	INTEGER	RW		Off (1), on (2)		Enables activation and deactivation of the 10 MHz reference clock in the Tx IFL cable.	IETF RFC 5728 [i.59]
dvbRcs2CtrlOduTxDCEnable	INTEGER	RW		Off (1), on (2)		Enables activation and deactivation of DC in the Tx IFL.	IETF RFC 5728 [i.59]
dvbRcs2CtrlOduRxDCEnable	INTEGER	RW		Off (1), on (2)		Enables activation and deactivation of DC in the Rx IFL.	IETF RFC 5728 [i.59]
dvbRcs2CtrlDownloadFileCommand	INTEGER	RW		Idle (1), config (2), installationLog (3)		Variable that initiates an RCST configuration file download process.	IETF RFC 5728 [i.59]
dvbRcs2CtrlUploadFileCommand	INTEGER	RW		Idle (1), config (2), eventAlarm (3), installationLog (4)		Variable that initiates an RCST configuration file upload process.	IETF RFC 5728 [i.59]
dvbRcs2CtrlActivateConfigFileCommand	INTEGER	RW		Idle (1), activate (2)		Variable that triggers the RCST to use the configuration file and updates its parameters accordingly.	IETF RFC 5728 [i.59]
dvbRcs2CtrlRcstLogonCommand	INTEGER	RW		Idle (1), logon (2)		Variable that initiates RCST logon.	IETF RFC 5728 [i.59]
dvbRcs2CtrlLogoffCommand	INTEGER	RW		Idle (1), logoff (2)		Variable that initiates RCST logoff.	IETF RFC 5728 [i.59]

8.6.16 State group

This MIB group describes the fault state, software versions, configuration file versions and rest of status parameters of the RCST.

Table 8.15: RCST State RCS2 Group

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2RCSTMode	INTEGER	RW		(0) Installation (1) Operational		Identifies the current status mode of the RCST and allows the RCST to return to the installation mode when needed.	IETF RFC 5728 [i.59]
dvbRcs2RCSTFaultStatus	INTEGER	RO		(0) No Fault, (1) fault		Provides the fault status of the terminal.	IETF RFC 5728 [i.59]
dvbRcs2FwdLinkStatus	INTEGER	RO		(0) notAcquired, (1) acquired		Provides the status of the RCST forward link.	IETF RFC 5728 [i.59]
dvbRcs2RtnLinkStatus	INTEGER	RO		(0) loggedOff, (1) loggedOn		Provides the status of the RCST return link.	IETF RFC 5728 [i.59]
dvbRcs2DvbState	INTEGER	RO		configComplete (1), nitWait (2), pat1Wait (3), pmt1Wait (4), rmtWait (5), pat2Wait (6), pmt2Wait (7), dvbRcsWait (8), loggingOn (9), coarseSync (10), fineSync (11), active (12), hold (13), loggedOff (14)		The current state of the IDU.	RCS2
dvbRcs2logUpdated	INTEGER	RO		(0) noUpdate, (1) logFileUpdated		Indicates the existence of an updated event log file: no update (0), event log file updated (1). The RCST should remove the "Event file updated" indication as the log file is fetched by the NCC.	IETF RFC 5728 [i.59]
dvbRcs2RCSTCurrentSoftwareVersion,	snmpAdminString	RO				Current RCST Sw version.	IETF RFC 5728 [i.59]
dvbRcs2RCSTAlternateSoftwareVersion,	snmpAdminString	RO				Alternate (backup/new) RCST software version.	IETF RFC 5728 [i.59]
dvbRcs2RCSTActivatedConfigFileVersion,	snmpAdminString	RO				Version of the most recently activated configuration file.	IETF RFC 5728 [i.59]
dvbRcs2RCSTDownloadedConfigFileVersion	snmpAdminString	RO				Version of the most recently downloaded configuration.	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2FwdStatusTable	SEQUENCE OF dvbRcs2Fwd StatusEntry	NA				Table that describes the current status of the Forward Link interfaces.	IETF RFC 5728 [i.59]
dvbRcs2FwdStatusEntry	SEQUENCE {dvbRcs2Fwd StatusIndex, dvbRcs2Fwd StatusIfRefer ence, dvbRcs2Fwd StatusONetId , dvbRcs2Fwd StatusNetId, dvbRcs2Fwd StatusNetNa me, dvbRcs2Fwd StatusFormat , dvbRcs2Fwd StatusFreque ncy, dvbRcs2Fwd StatusPolar , dvbRcs2Fwd StatusInnerF ec, dvbRcs2Fwd StatusSymbol Rate, dvbRcs2Fwd StatusRolloff , dvbRcs2Fwd StatusModula tion , dvbRcs2Fwd StatusFecFra me, dvbRcs2Fwd StatusPilot , dvbRcs2Fwd StatusBer, dvbRcs2Fwd StatusCnr, dvbRcs2Fwd StatusRxPow er}	NA				An entry in the forward lnk status table. Each entry is associated with a physical interface.	IETF RFC 5728 [i.59]
dvbRcs2FwdStatusIndex	Unsigned32 (1..8)	NA				Index of the forward link table.	IETF RFC 5728 [i.59]
dvbRcs2FwdStatusIfReference	Unsigned32 (1..8)	RO				Cross reference to the interface table.	IETF RFC 5728 [i.59]
dvbRcs2FwdStatusONetId	Unsigned32	RO				Reflects the last ONID given during logon RCS2 (from the RCS tables).	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcsFwdStatusNetId	Unsigned32	RO				Interactive network ID of the forward link (from the RCS table).	IETF RFC 5728 [i.59]
dvbRcsFwdStatusNetName	SnmpAdminString	RO				The name of the interactive network of the forward link (from the RCS Map Table).	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcsFwdStatusFormat	INTEGER	RO		dvbs (0), dvbs2ccm (1), dvbs2acm (2), dvbs2xacm (3)		Specifies the transmission format applied on the forward link. Supported values are (from RCS Map Table): 0: DVB-S 1: DVB-S2 using CCM 2: DVB-S2 using VCM or ACM 3: DVB-S2X using ACM".	IETF RFC 5728 [i.59]
dvbRcsFwdStatusFrequency	Unsigned32	RO	100 Hz			An estimate of the frequency of the forward link. Its value is given in multiples of 100 kHz.	IETF RFC 5728 [i.59]
dvbRcsFwdStatusPolar	INTEGER			(0) linear-horizontal (1) linear-vertical (2) circular-left (3) circular-right		2-bit field giving the polarization of the forward link Supported values are (from RCS Map Table): 00: linear and horizontal 01: linear and vertical 10: circular left 11: circular right.	IETF RFC 5728 [i.59]
dvbRcsFwdStatusInnerFec	INTEGER			unknown (-1), fecRate12 (0), fecRate23 (1), fecRate34 (2), fecRate56 (3), fecRate78 (4), fecRate89 (5), fecRate35 (6), fecRate45 (7), fecRate910 (8), fecRate25 (9), fecRate13 (10), fecRate14 (11), noInnerCode(12)		Specifies the inner Forward Error Correction used on the forward link for transmission to the RCST. The RCST will report a value that has been used for transmission to the RCST within the most recent 60 seconds. If this is not relevant, the RCST will report 'unknown'. For DVB-S2X the terminal may report 'unknown'.	
dvbRcsFwdStatusSymbolRate	Unsigned32	RO	100 symbols/s			An estimate of the symbol rate of the forward link. Its value is given in multiples of 100 symbols/s.	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcsFwdStatusRolloff	INTEGER	RO		(0) not defined, (1) 10 %, (2) 20 %, (3) 25 %, (4) 35 %, (5) 5%, (6) 15%		An estimate of the roll-off applied on the forward link. Supported values are: 0: undefined 1: 0.10 2: 0.20 3: 0.25 4: 0.35 5: 0.05 6: 0.15	RCS2
dvbRcsFwdStatusModulation	INTEGER	RO		unknown (0), mBPSK (1), mQPSK (2), m8PSK (3), m16APSK (4), m32APSK (5), m64APSK (6), m128APSK (7), m256APSK (8)		Indicates the modulation on the forward link used for transmission to the RCST. Supported values are: 0: unknown 1: BPSK 2: QPSK 3: 8PSK 4: 16APSK 5: 32APSK 6: 64APSK 7: 128APSK 8: 256APSK The RCST will report a value that has been used for transmission to the RCST within the most recent 60 seconds. If this is not relevant, the RCST will report 'unknown'.	IETF RFC 5728 [i.59]
dvbRcsFwdStatusFecFrame	INTEGER	RO		unknown (0), shortframe (1), longframe (2), midframe (3)		Indicates the frame length used on the forward link for transmission to the RCST. Supported values are: 0: Unknown 1: Short frame 2: Normal frame 3: Mid frame The RCST will report a value that has been used for transmission to the RCST within the most recent 60 seconds. If this is not relevant, the RCST will report 'unknown'.	IETF RFC 5728 [i.59]
dvbRcsFwdStatusPilot	INTEGER	RO		unknown (0), pilotNotused (1), pilotUsed (2)		Indicates whether pilots are used on the forward link for transmission to the RCST. Supported values are: 0: Unknown	

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
						1: Pilots are not used 2: Pilots are used The RCST will report a value that has been used for transmission to the RCST within the most recent 60 seconds. If this is not relevant, the RCST will report 'unknown'.	
dvbRcsFwdStatusBer	Integer32	RO	Exponent of 10			Provides the RCST BER on the Forward Link in log10 units.	IETF RFC 5728 [i.59]
dvbRcsFwdStatusCnr	Integer32	RO	0,1 dB			Provides the RCST CNR on the Forward Link in 0,1 dB units.	IETF RFC 5728 [i.59]
dvbRcsFwdStatusRxPower	Integer32	RO	0,1 dBm			Provides the RCST power level of the Forward Link as received by the IDU, in 0,1 dBm units.	IETF RFC 5728 [i.59]
dvbRcs2RtnStatusEbN0	Integer32	RO	0,1 dB			The EbN0 value reported for the return link, referenced to the regular SYNC burst transmission, in 0,1 dB.	IETF RFC 5728 [i.59]
dvbRcs2RtnStatusSFDuration	Unsigned32	RO	0,1 ms			The duration of the currently applied return link superframe structure, in tenths of milliseconds.	IETF RFC 5728 [i.59]
dvbRcs2RtnStatusTxPower	Unsigned32	RO	0,1 dB			Transmission IDU Tx power during last logon.	IETF RFC 5728 [i.59]
dvbRcs2AlignmentStatus	INTEGER (0) not confirmed aligned, (1) confirmed aligned	RO				RCST flag that reflects the alignment status given by the NCC during logon.	RCS2
dvbRcs2SubscriptionStatus	INTEGER (0) NotConfirmedSubscription (1) ConfirmedSubscription					Flag to reflect the RCST subscription status given by the NCC at logon.	RCS2

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2ComissionedStatus	INTEGER (0) Not confirmed commissioned (1) confirmed user associated to the RCST (2) higher layer M and C address is assigned (3) NCC indicates the commissioning is completed	RO				RCST commissioned status. The flag can be raise by loading a new configuration file. At a change of NIT or RMT, the RCST changes this flag to "Not confirmed commissioned".	RCS2
typeOfLogon	INTEGER	RO		Basic (0), LargeTiming (1)		Two variants of logon procedure exist, the basic procedure and a procedure extension called Logon at Large Timing.	RCS2
NetworkingStatus	Unsigned32	RO					RCS2
RCSTidentifier	Unsigned32	RO				RCST identifier given at logon Reset every logon session.	RCS2
lowerLayerCapabilities	Textual convention	RO		MultipleGSsupport (0), MultipleGSsupport (1), reserved (2), fullRangeFLmodcod (3), fullrangeRLmodcod (4), carrierSwitchClass (5), EsN0powerCtrl (6), ctepowerSpectrum Density (7), slottedAlohaTraffic (8), crdsaTraffic (9), stream (10), reserved (11), reserved (12), reserved (13), reserved (14), reserved (15), reserved (16)		RCST lower layer capabilities.	RCS2
statusSatelliteID	Unsigned32	RO				Reflects the last valid value of SatelliteID at logon.	RCS2
statusPopulationID	Unsigned32	RO				Reflects the last valid value for PopulationID at logon.	RCS2

Functional Group	dvbRcs2State						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
StatusNCC_ID	Unsigned32	RO				Reflects the last valid value for NCC_ID at logon.	RCS2
transmissionContextIndication	INTEGER (0) TDMA_DA (1) TDMA_slottedAloha (2) TDMA_CRDSA (3) TDMA_RAtype3 (4) TDMA_RAtype4 (5) TDM (6) Other	RO				RCST transmission context identification.	RCS2

8.6.17 Statistics group

Statistics are provided in the interfaces group per SVN interface or per IPv4/IPv6 interface.

Other statistics could be provided per HLS queue, in terms of packets sent/received, and per multicast session.

RCST statistics may include:

- number of logons
- last time of a logon session
- number of SYNC without response
- number of CMT2 losses
- number of TBTP2 losses
- number of schedule failures

The counters are assumed reset after an RCST reboot but kept after logoff/logon sessions.

Table 8.16: RCST Statistics RCS2 Group

Functional Group	dvbRcs2RcstStatistics						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
nbrLogons	Counter32	RO			0	Counter of logon sessions since last reboot.	RCS2
lastTimeLogonSession	Seconds	RO			0	Time elapsed since last successful logon	RCS2
nbrSYNCnotanswered	Counter32	RO			0	Counter of SYNC sent with no answer from NCC.	RCS2
nbrCMT2losses	Counter32	RO			0	Counter of CMT2 losses, after waiting maxresponse time for a CMT2.	RCS2
nbrSchedulerFailures	Counter32	RO			0	Counter of Scheduler failures since last reboot.	RCS2
nbrRtnLinkFailures	Counter32	RO			0	Counter of rtn link failures since last reboot.	RCS2
nbrNCCReceiveFailures	Counter32	RO			0	Counter of NCC reception errors since last reboot.	RCS2
nbrLinkFailureRecovery	Counter32	RO			0	Counter of Link Failure recoveries since last reboot.	RCS2

8.6.18 QoS configuration group

This group contains objects to configure the Quality of Service (QoS) of the RCST.

The QoS configuration may include the following tables:

- IP Classification table
- HLS mapping table
- LLS configuration table (for supervision only, saves the information given at logon)

Table 8.17 is a sketched list of managed objects that would be required for managing RCST QoS configuration. Well-known queuing terms are here used to indicate the packet ordering policy and the packet drop policy applied for the flow.

The actual implementation of an attempted QoS configuration could be possible to read back via SNMP/IP, and could depend on the actual support in the specific device.

The RCST keeps its MAC service configuration in the MIB after reboot or logon, as long it connects to the same NCC/NMC. Change in any of the parameters in the NIT given by the Network_ID or in RMT given by the NCC_ID.

Table 8.17: RCST QoS RCS2 Group

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
IPClassTable	SEQUENCE OF IPClassEntry	NA	-	-	-	Traffic Classification table for IP traffic.	RCS2
IPClassEntry	SEQUENCE { IPClassIndex, IpClassDscpLow, Ip IPClassDscpHigh, IPClassDscpMarkValue, IPClassIPProtocol, IPClassSrcInetAddressType, IPClassIPSrcInetAddress, IPClassSrcInetAddr, essPrefixLength, IPClassDstInetAddressType, IPClassIPDstInetAddress, IPClassIPDstInetAddressPrefixLength, IPClassSrcPortLow, IPClassSrcPortHigh, IPClassDstPortLow, IPClassDstPortHigh, IPClassVlanUserPri, IPClassVLANID, IPClassHLSAssociation, IPClassAction, IPClassOutOctets, IPClassOutPkts, IPClassRowStatus}	NA	-	-	-	IP traffic classification entry.	RCS2
IPClassIndex	Unsigned32	NA	-	-	-	Index automatically incremented one by one.	RCS2
IPClassDscpLow	Dscp	RC	-	-	-	Low value of a range of DiffServ code points.	RCS2
IPClassDscpHigh	Dscp	RC	-	-	-	High value of a range of DiffServ code points.	RCS2
IPClassDscpMarkValue	DscpOrAny	RC	-	-	-	DiffServ code point value used to mask the packet; -1 indicates no DSCP marking.	RCS2
IPClassIPProtocol	Unsigned32	RC	-	-	-	IP protocol to which a packet is compared. A value of 255 means match all.	RCS2
IPClassSrcInetAddressType	InetAddressType	RC	-	-	-	Type of Internet address of IpClassIpSrcInetAddress	RCS2
IPClassIPSrcInetAddress	InetAddress	RC	-	-	-	IP source address to which a packet is compared.	RCS2
IPClassSrcInetAddressPrefixLength	InetAddressPrefixLength	RC	-	-	-	Prefix length of the IP source that will be matched for this traffic class.	RCS2
IPClassDstInetAddressType	InetAddressType	RC	-	-	-	Type of Internet address of IpClassIpDstInetAddress	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
IPClassIPDstInetAddress	InetAddress	RC	-	-	-	IP destination address to which a packet is compared.	RCS2
IPClassIPDstInetAddressPrefixLength	InetAddressPrefixLength	RC	-	-	-	Prefix length of the IP destination that will be matched for this traffic class.	RCS2
IPClassSrcPortLow	InetPortNumber	RC	-	-	-	Low range of source port to which a packet is compared.	RCS2
IPClassSrcPortHigh	InetPortNumber	RC	-	-	-	High range of source port to which a packet is compared.	RCS2
IPClassDstPortLow	InetPortNumber	RC	-	-	-	Low range of destination port to which a packet is compared.	RCS2
IPClassDstPortHigh	InetPortNumber	RC	-	-	-	High range of destination port to which a packet is compared.	RCS2
IPClassVlanUserPri	Integer32 (-1..7)	RC	-	-	-	VLAN user priority to which a packet is compared. A value of -1 indicates that the selectivity is inactive. 16-bit Tag that contains a 3-bit Priority field and a 12-bit VLAN number.	RCS2
IPClassVLANID	Integer32	RC	-	-	-	VLAN identifier (12bits) from the 802.1D/Q tag header.	RCS2
IPClassHLSAssociation	Unsigned32	RC	-	-	-	Associate the filter entry to a specific HL service.	RCS2
IPClassAction	INTEGER	RC	-	-	-	Forward the packet (1), or act a firewall when set to (-1).	RCS2
IPClassOutOctets	Counter32	RO	-	-	-	Statistics of packets octets that matched this IP traffic class since last logon.	RCS2
IPClassOutPkts	Counter32	RO	-	-	-	Statistics of packets that matched this IP traffic class since last logon.	RCS2
IPClassRowStatus	RowStatus	RC	-	-	-	The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	RCS2
HLServiceTable	SEQUENCE OF HLServiceEntry	NA	-	-	-	HLServices table.	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
HLServiceEntry	SEQUENCE{ HLServiceIndex HLserviceLLService Association HLservicediffPolicyPHBindex HLservicePHBname HLservicePriority HLserviceMinRate HLserviceMaxRate HLserviceMaxIngressBurst HlserviceMinIngressBurst HLserviceMaxEgressBurst HLserviceMaxDelay HLserviceQueueType HLserviceL3IfNumber MaxLatency LinkRetransmissionAllowed HLServiceRowStatus}	NA	-	-	-	Table entry for HL service table.	RCS2
HLServiceIndex	Unsigned32	NA	-	-	-	Table index.	RCS2
HLserviceLLService Association	Unsigned32	RC	-	-	-	This object is an association of the HLservice to a LL service.	RCS2
HLservicediffPolicyPHBindex	Unsigned32	RC	-	-	-	Identification of the PerHopBehaviour (PHB). If follows the unsigned 16-bit binary encoding as specified in IETF RFC 3140 [19]. The value 0 designates the Default PHB.	RCS2
HLservicePHBname	SNMPAdminString	RC	-	-	-	The name of the PHB.	
HLservicePriority	Unsigned32	RC				HL service priority level.	RCS2
HLserviceMinRate	Unsigned32	RC	kbps			HL service minimum rate, minimum level of resources available to the HL services aggregate, in kilo bits per second.	RCS2
HLserviceMaxRate	Unsigned32	RC	kbps			HL service maximum rate, maximum level of resources available to the HL services aggregate in kilo bits per second.	RCS2
HLserviceMaxIngressBurst	Unsigned32	RC	Bytes			HL service Max Ingress burst, maximum burst of traffic that the HL services will take.	RCS2
HLlserviceMinIngressBurst	Unsigned32	RC	Bytes			HL service Min Ingress burst, minimum burst of traffic that the HL services will take.	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
HLserviceMaxEgressBurst	Unsigned32	RC	Bytes			HL service Max Egress Burst, maximum burst of traffic that the HL services will issue in excess of maximum long term rate.	RCS2
HLserviceMaxDelay	Unsigned32	RC	Seconds			Maximum Delay for this HL service, nominal maximum transit delay for a PDU of the HL service aggregate.	RCS2
HLserviceQueueType	INTEGER	RC		FIFO (0), LLQ (1), WFQ (2) WRED (3), Other (4)		Queue scheduling typedrop strategy associated to the HLService: FIFO is Tail Drop LLQ is Head Drop WFQ is based on the CIR per HL service as the minimum weight parameter Other is a vendor specific strategy.	RCS2
HLserviceL3IfNumber	Unsigned32	RC				Interface ID associated to the HL service (interface identifier from the interfaces group).	RCS2
MaxLatency	Unsigned32	RC	-	-	-	Minimum time to hold on to a PDU in the HL services aggregate before it may be discarded.	RCS2
LinkRetransmissionAllowed	Unsigned32	RC	-	-	-	Packet re-transmission allowed/not allowed.	RCS2
HLServiceRowStatus	RowStatus	RC	-	-	-	The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	RCS2
LLserviceTable	SEQUENCE OF LLserviceEntry	NA	-	-	-	LowerLayer services table that saves the information provided by the LL service descriptor for supervision only.	RCS2

LLserviceEntry	SEQUENCE {
	LLserviceIndex
	LLserviceRCIndex
	LLserviceDAACIndex
	LLserviceCS_RAACmap
	LLserviceRCIndex
	LLserviceRAACIndex
	LLserviceCD_RCmap
	LLserviceCS_DAACmap
	LLserviceRowStatus
	}
		NA	-	-	-	Entry of LL service Table.	RCS2

LLserviceIndex	Unsigned32	NA	-	-	-	Index of LL service Table.	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
LLserviceRCIndex	Unsigned32	RC	-	-	-	A 4 bit field indicating the nominal request class for the associated Link Service.	RCS2
LLserviceDAACIndex	Unsigned32	RC	-	-	-	A 4 bit field indicating the nominal dedicated access allocation channel associated with the Link Stream. The Assignment ID associated to the request class has an offset to the Assignment ID Base equal to the nominal_da_ac_index.	RCS2
LLserviceCS_RAACmap	Unsigned32	RC	-	-	-	16 bit field indicating the allowance to conditionally map resource demand for the associated Link Stream into capacity requests for other RCs, with bit 0 referring to rc_index=0, bit 1 referring to rc_index=1 and so on.	RCS2
LLserviceRCIndex	Unsigned32	RC	-	-	-	A 16 bit field indicating the allowance to conditionally map traffic from the Link Stream into the different dedicated assignment allocation channels, indicated by a flag for each DA-AC, with bit 0 referring to da_ac_index=0, bit 1 referring to da_ac_index=1 and so on.	RCS2
LLserviceRAACIndex	Unsigned32	RC	-	-	-	A 4 bit field indicating the nominal random access allocation channel associated with the Link Lower layer Service. The corresponding Assignment ID equals the highest Assignment ID value in the system minus ra_ac_index.	RCS2
LLserviceCD_RCmap	Unsigned32	RC	-	-	-	An 8 bit field indicating the allowance to conditionally map Link Stream traffic into the different random access allocation channels, indicated by a flag for each RA-AC, with bit 0 referring to ra_ac_index=0, bit 1 referring to ra_ac_index=1 and so on.	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
LLserviceCS_DAAC map	Unsigned32	RC	-	-	-	A 16 bit field indicating the allowance to conditionally map traffic from the Link Stream into the different dedicated assignment allocation channels, indicated by a flag for each DA-AC, with bit 0 referring to da_ac_index=0, bit 1 referring to da_ac_index=1 and so on.	RCS2
LLserviceRowStatus	Unsigned32	RC	-	-	-	An 8 bit field indicating the allowance to conditionally map Link Stream traffic into the different random access allocation channels, indicated by a flag for each RA-AC, with bit 0 referring to ra_ac_index=0, bit 1 referring to ra_ac_index=1 and so on.	RCS2
RCTable	SEQUENCE OF RCEntry	NA	-	-	-	RC Table configuration table.	RCS2
RCEntry	SEQUENCE { RCindex LLserviceIndex RCcontantAssignment RCvolume_allowed RCrbdc_allowed RCmax_service_rate RCmin_service_rate RCconstant_service_rate RCmax_backlog RCrowStatus }	NA	-	-	-	RC Entry associated to an specific LL service ID.	RCS2
RCindex	Unsigned32	NA	-	-	-	The RCST by default maps its default request class to rc_index 0.	RCS2
RCcontantAssignment	INTEGER	RC		Non-solicited (0), Solicited (1)		Flag to indicate if constant non-solicited assignment is provided for the RC.	RCS2
RCvolume_allowed	INTEGER	RC		NotAllowed (0), Allowed (1)		Flag to indicate if A/VBDC requests are allowed for the rc_index.	RCS2
RCrbdc_allowed	INTEGER	RC	kbps	NotAllowed (0), Allowed (1)		Flag to indicate if RBDC requests are allowed for the rc_index in kilo bits per second.	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
RCmax_service_rate	Unsigned32	RC	kbps			Field that indicates the maximum service rate for the rc_index. The maximum allowed RBDC equals this level substracted by the CRA in kilo bits per second.	RCS2
RCmin_service_rate	Unsigned32	RC	kbps			Field that indicates the minimum rate that can be expected assigned when actively requesting any dynamic capacity for the rc_index.	RCS2
RCconstant_service_rate	Unsigned32	RC	kbps			16-bit field indicating the admitted CRA level associated with the request class in kilo bits per second.	RCS2
RCmax_backlog	Unsigned32	RC	kbps			8-bit field indicating the max volume request backlog that the NCC will accept to hold for the rc_index in kilo bits per second.	RCS2
RCrowStatus	RowStatus	RC				The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	RCS2
RAACTable	SEQUENCE OF RAAC Entry	RC				Table that contains the Random Access allocation channels configuration.	RCS2
RAACEntry	SEQUENCE { RAACTable RAACEntry RAACIndex RAACmaxUniquePayloadBlock RAACmaxConsecutiveBlock RAACminIdleBlock RAACdefaults_field_size RAAC_raLoad_control RAACrowStatus}	RC				Entry for Random Access Table.	RCS2
RAACIndex	Unsigned32	RC				Index for Random Access Table.	RCS2
RAACmaxUniquePayloadBlock	Unsigned32	RC				8-bit field that indicates the max number of unique payloads that the RCST is permitted to send in an RA block.	RCS2
RAACmaxConsecutiveBlock	Unsigned32	RC				8-bit field that indicates the max number of consecutive RA blocks that the RCST is permitted to access for sending unique payloads.	RCS2

Functional Group	dvbRcs2QoSConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
RAACminIdleBlock	Unsigned32	RC				8-bit field that indicates the min nbr of RA bloacks that the RCST ignores for a given ra_ac index after having accessed a max allowed nbr of consecutive RA blocks.	RCS2
RAACdefaults_field_size	Unsigned32	RC				8-bit field indicating the method dependent size of the defaults_for_ra_load_control field that contains the default values for the dynamic load control parameers.	RCS2
RAAC_raLoad_control	Unsigned32	RC				A defauts_field_size byte field that contains the default values for the load control method for the random access allocation channel.	RCS2
RAACrowStatus	RowStatus	RC				The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	RCS2
NOTE: HL services links with LL services, each entry can be associated to only one MAC24 interface, or applying to all L2 interfaces when parameter IfNumber is left empty.							

8.6.19 Flink configuration group

Table 8.18 contains the list of the fowardlink attachment points (e.g. different for installation and operation).

Table 8.18: RCST Flink configuration RCS2 Group

Functional Group	dvbRcs2FwdConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2FwdStartTable	Sequence of FwdStartEntry	NA				The Table described the forward link parameters used for the start up with the NCC.	IETF RFC 5728 [i.59]
dvbRcs2FwdStartEntry	SEQUENCE { dvbRcs2FwdStartIndex, dvbRcs2FwdStartPopID, dvbRcs2FwdStartFrequency, dvbRcs2FwdStartPolar , dvbRcs2FwdStartFormat, dvbRcs2FwdStartRolloff, dvbRcs2FwdStartSymbolRate , dvbRcs2FwdStartInnerFec, dvbRcs2FwdStartRowStatus	NA					IETF RFC 5728 [i.59]

Functional Group	dvbRcs2FwdConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
dvbRcs2FwdStartIndex	Unsigned32 (1..8)	NA				Index of the Forward Link StartConfig table.	IETF RFC 5728 [i.59]
dvbRcs2FwdStartPopId	Integer32	RC				Population identifier associated with the start-up Forwardlink: -1: any (auto) 0-65535: specific StartPopId If 'any' is set, the RCST will assume membership of any announced population ID and will commence with logon in accordance with this assumption.	IETF RFC 5728 [i.59]
dvbRcs2FwdStartFrequency	Unsigned32	RC	x100 kHz			Frequency of the start transponder carrying a Network Information Table to which any RCST triggers to acquire forward link. Its value is given in multiples of 100 kHz.	IETF RFC 5728 [i.59]
dvbRcs2FwdStartPolar	INTEGER	RC		linearHorizontal (0), linearVertical (1), circularLeft (2), circularRight (3)		2-bit field giving the polarization of the start transponder carrying a network Information Table to which any RCST shall trigger to acquire forward link: 00: linear and horizontal 01: linear and vertical 10: circular left 11: circular right	IETF RFC 5728 [i.59]
dvbRcs2FwdStartFormat	INTEGER	RC		auto (-1), dvbs (0), dvbs2ccm (1), dvbs2acm (2) dvbs2xacm (3)		Specifies the transmission format standard applied for the startup stream. The start transport stream carries a Network Information Table that the RCST uses for acquiring the forward link signalling. Supported values are: -1: unspecified (automatic format acquisition is assumed) 0: DVB-S (support of this value is mandatory if DVB-S support is claimed) 1: DVB-S2 with CCM (support of this value is mandatory if DVB-S2 CCM support is claimed) 2: DVB-S2 with VCM or ACM (support of this value is mandatory if DVB-S2 ACM support is claimed) 3: DVB-S2X with ACM (support of this value is mandatory if DVB-S2X ACM support is claimed) This allows the RCST to discriminate between CCM and VCM/ACM when selecting the forward link. The support of automatic format selection is optional.	IETF RFC 5728 [i.59]

Functional Group	dvbRcs2FwdConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
						One or several of the other format selections should be supported, according to the claimed SatLabs profile support.	
dvbRcs2FwdStartRollOff	INTEGER	RC		autoRolloff (0), rolloff010, (1) rolloff020 (2), rolloff025 (3), rolloff035 (4) rolloff005 (5) rolloff015 (6)		Specifies the receive filter roll-off applied on the start transponder. The start transponder carries a Network Information Table that the RCST uses for acquiring the forward link signalling.Supported values are: 0: any (auto) 1: 0.10 2: 0.20 3: 0.25 4: 0.35 5: 0.05 6: 0.15	IETF RFC 5728 [i.59]
dvbRcs2FwdStartSymbolRate	Unsigned32	RC	x100 symbols/s			Specifies the symbol rate on the start transponder carrying a Network Information Table to which any RCST triggers to acquire forward link. Its value shall be given in multiples of 100 symbols/s.	IETF RFC 5728 [i.59]
dvbRcs2FwdStartInnerFec	INTEGER	RC		autoFec (-1), fecRate12 (0), fecRate23 (1), fecRate34 (2), fecRate56 (3), fecRate78 (4), fecRate89 (5), fecRate35 (6), fecRate45 (7), fecRate910 (8), fecRate25 (9), fecRate13 (10), fecRate14 (11), noInnerCode (12)		Specifies the inner Forward Error Correction used on the start transponder carrying a Network Information Table to which any RCST triggers to acquire forward link. Supported values are: autoFec (-1), fecRate1/2 (0), fecRate2/3 (1), fecRate3/4 (2), fecRate5/6 (3), fecRate7/8 (4), fecRate8/9 (5), fecRate3/5 (6), fecRate4/5 (7), fecRate9/10 (8), fecRate2/5 (9), fecRate1/3 (10), fecRate1/4 (11), noInnerCode (12) The support of autoFec is mandatory if DVB-s2X ACM support is claimed and otherwise the support of autoFec is optional.	IETF RFC 5728 [i.59]
dvbRcs2FwdStartRowStatus	RowStatus	RC				The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	IETF RFC 5728 [i.59]

8.6.20 Rlink configuration group

Table 8.19 contains the list of the return link attachment points (e.g. different for installation and operation).

Table 8.19: RCST Rlink configuration RCS2 Group

Functional Group	dvbRcs2RtnConfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
RtnConfigMaxEirp	Integer32	RW	x0,1 dBm			Max Equivalent Isotropic Radiated Power (EIRP) of the RCST, given in resolution of 0,1 dBm and applied when the IDU can, itself, set the necessary IDU TX output level, e.g. when using a BUC that has a power level detector and that provides sufficient feedback to the IDU.	
RtnConfigDefIfLevel	Integer32	RW	x0,1 dBm			IDU TX output level applied in case the dvbRcsRtnConfigMaxEirp cannot be used. The resolution is 0,1 dBm and the accuracy is ± 1 dBm.	

8.6.21 VLAN configuration group

VLAN MIB is configurable on a per-interface basis and depends in several parts on the IF-MIB (IETF RFC 2863 [11]).

The RCST may support the following MIB table entries to control the use of the VLAN-Tagged IP Routing mode:

- A management parameter that describes whether an RCST is capable of supporting this mode as part of the System configuration MIB dvbRcs2SystemOptionMap.
- A management parameter that allows the NCC to control the use of this mode by an RCST for a specific LAN interface.

VLAN configuration requires an extra table for VLAN mapping to SVNs as described in HLS guidelines [i.5].

8.6.22 NAT/NAPT configuration group

NAT MIB is configurable on a per-interface basis and depends in several parts on the IF-MIB (IETF RFC 2863 [11]).

NAT MIB is defined in IETF RFC 4008 [i.93] and NAPT variants in IETF RFC 3489 [i.86].

The RCST may implement the natInterfaceTable MIB module from IETF RFC 4008 [i.93] to configure interface specific realm type and the NAT services enabled for the interface. natInterfaceTable is indexed by ifIndex and also includes interface specific NAT statistics.

The RCST may implement natAddrMapTable MIB module from IETF RFC 4008 [i.93] to configure address maps on a per-interface basis.

The RCST may implement two Bind tables, natAddrBindTable and natAddrPortBindTable from IETF RFC 4008 [i.93], defined to hold the bind entries. Entries are derived from the address map table and are not configurable.

The RCST may implement the natSessionTable defined to hold NAT session entries.

The RCST NAT/NAPT function may be configurable per enabled interface, including the following parameters:

- NAT enable/disable flag. By default NAT may be disabled.

- Global and Local addresses.
- Static NAPT UDP/TCP port translation range.
- Dynamic NAPT UDP/TCP port translation range.

8.6.23 PEP negotiation configuration

The PEP negotiation group compiles all the necessary information to perform PEP negotiation between the RCST and the NCC.

Table 8.20: RCST PEP negotiation RCS2 Group

Functional Group	dvbRcs2RCSTPepNegotiation						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
hlsAgentmulticastInetAddresstype	InetAdressType	RW	-	-	-	Multicast IPv4 address type to be used by the HLS negotiation agent.	RCS2
hlsAgentMulticastInetAddress	InetAddress	RW	-	-	-	Multicast IPv4 address to be used by the HLS negotiation agent.	RCS2
hlsAgentMulticastInetAddressPrefixLength	InetAddressPrefixLength	RW	-	-	-	Multicast IPv4 address prefix length to be used by the HLS negotiation agent.	RCS2
hlsnegotiationAgentudpPort	InetPortNumber	RW	-	-	-	UDP port to be used by the HLS negotiation agent.	RCS2
pepTypePerIfTable	SEQUENCE OF pepTypeIdEntry	NA	-	-	-	RCST PEP configuration per Interface.	RCS2
pepTypeIfEntry	SEQUENCE { pepTypeIfIndex , pepType, pepTypefInterfaceID, pepTypenonStandardPEPmechanism, pepTypeIfVendorID, pepTypeIfProductID, pepRypeStandardsID, pepCapability, pepTypeIfTCP, pepTypeIfHTTP , pepTypeRowStatus}	NA	-	-	-	PEP table entry.	RCS2
pepTypeIfIndex	Unsigned32	NA	-	-	-	Index for PEP configuration per interface.	RCS2
pepTypefInterfaceID	Interface	RC	-	-	-	Interface ID from the interfaces group.	RCS2
pepTypenonStandardPEPmechanism	BOOLEAN	RC	-	-	-	Flag to disable non standard PEP mechanisms for SVN-MAC.	RCS2
pepTypeIfVendorID	OCTET STRING	RC	-	-	-	PEP Vendor ID.	RCS2
pepTypeIfProductID	OCTET STRING	RC	-	-	-	PEP Product ID.	RCS2
pepTypeStandardsID	OCTET STRING	RC	-	-	-	PEP Standard ID.	RCS2
pepCapability	OCTET STRING	RC	-	-	-	PEP Control capability bitmap field as specified in table 7.3.	RCS2

Functional Group	dvbRcs2RCSTPepNegotiation						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
pepTypeIfTCP	INTEGER	RC		Disabled (0), Enabled (1)		TCP PEP status enabled/disabled.	RCS2
pepTypeIfHTTP	INTEGER	RC		Disabled (0), Enabled (1)		HTTP PEP status enabled/disabled.	RCS2
pepTypeRowStatus	RowStatus	RC	-	-	-	The row status, used according to row creation and removal conventions. A row entry cannot be modified when the status is marked as active (1).	RCS2

8.6.24 SDDP configuration

The SDDP configuration group comprises information related to download of software to the RCST by SDDP.

Table 8.21: RCST SDDP RCS2 Group

Functional Group	dvbRcs2SDDPconfiguration						
Element	**Parameter**	**Type**	**Unit**	**Range**	**Default**	**Description**	**Source**
Blksize	Unsigned32	RO	Bytes			Set the DATA block size to another value than the default of 512 bytes.	RCS2
Tsize	Unsigned32	RO	Bytes			Indicates the total transfer size.	RCS2
manufID	Unsigned32	RO	24 bit as decimal value			Indicates the OUI.	RCS2
SwVersion	Unsigned32	RW				Current SW version in the SW distribution carousel, respective to the manufID and vendor specific parameters.	RCS2
MinSwVersion	Unsigned32	RW				Indicates the minimum SW version required for log-on, with respect to manufID and vendor specific parameters.	RCS2
Method	Unsigned32	RW				Indicates if the SW update method is different from the default "immediate". It can also be "pending", i.e. awaiting the next RCST restart.	RCS2
Timeout	Unsigned32	RW	seconds			Indicates the timeout when waiting for the next DATA packet, default value is given in the initial configuration (sec).	RCS2
MgroupType	InetAddressType	RW					RCS2
MgroupAddress	InetAddress	RW				Set a redirection multicast group address respective to the manufID and vendor specific parameters.	RCS2
MgroupPrefixLength	InetAddressPrefixLength	RW					RCS2
Port	InetPort	RW				Sets a redirection UDP port respective to the manufID and vendor specific parameters.	RCS2
Layer2	Unsigned32	RW	Bytes			Indicate the redirection layer 2 address for a specific download.	RCS2

8.7 RCST Commissioning and initialization

8.7.0 Introduction

This clause provides a description of the initial RCST commissioning and configuration for a successful logon in the OVN.

The RCST commissioning and configuration is done during installation by RCST configuration file and is completed during logon thanks to the information provided in the TIM unicast message. Earlier local/remote configuration of the terminal is superseded by the information contained in the Logon Response Descriptor, Lower Layer Service Descriptor, Higher Layer Descriptor or the MIB objects in the Network Layer Information Descriptor (NLID).

The format of the Higher Layer descriptor is provided in [1].

The complete set of RCST parameters seeks to be sufficient to ensure correctly operation in the RCS2 interactive satellite system.

The RCST commissioning and configuration covers the following steps:

1) Verify RCST commissioned flag. If not OK initiate the RCST initial settings.

2) RCST initial settings made by the installer or through a configuration file.

3) RCST Software check and update. The correct version is identified through Forward Link signalling.

4) RCST MAC-level logon (as defined in [1]). The RCST acquires the corresponding set of descriptors.

5) RCST configuration update. A final adjustment of the RCST configuration can be made in this phase thanks to the latest RCST logon information. The System configuration MIB may reflect the options and final system configuration of the RCST after logon.

After these steps, the RCST will reach the operational state and will be ready to transmit traffic. Figure 8.10 shows a sequence diagram with the different states and performed actions. Subsequent updates of software and configuration are assumed possible once the RCST is in operational state using the management IP interface.

If the commissioned-ok flag is not set, the RCST may block network forwarding of user traffic to/from the LAN interface. This allows further IP configuration. The RCST completes the configuration by enabling traffic forwarding when the commissioned-ok flag is set (e.g. by loading a new configuration or direct action to raise the flag).

The RCST logon procedure logon may be conditioned by the commissioning state of the RCST. The commissioning state of the RCST is assumed notified to the NMC and to the NMC through the logon flags as specified in [1].

The RCST MIB-II system, interfaces, ip, RCS2 system, RCS2 network, RCS2 QoS, RCS2 VRF parameters are assumed to be configured before the RCST can start working at the MAC level.

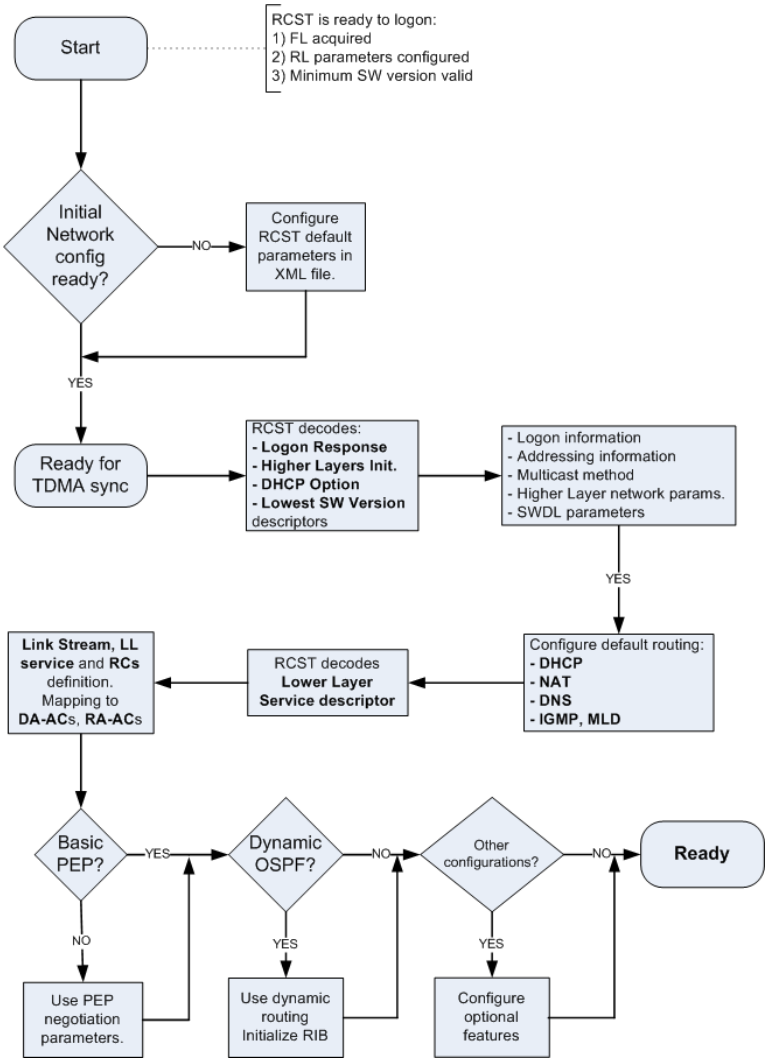


Figure 8.10: RCST commissioning and logon procedure

The following clause enumerates a list of parameters necessary for RCST initial commissioning.

8.7.1 RCST Management Signalling Configuration parameters

The RCST management signalling information may include:

- RCST IPv4 address for M and C
- RCST SVN-MAC of the management interface
- SVN mask bits of the assigned management SVN-MAC
- IPv4 address and subnet of the Management interface of the NMC
- SNMP read/write community strings (char string) for the SNO and SVNO

The RCST needs to indicate it has a valid M and C IP address associated or its management entity or not at logon.

The RCST needs to keep its M and C address across reboots and re-logons as long as it connects to the same NCC/NMC.

The management SVN is indicated by the NCC in the MAC Logon response.

After successful logon, the RCST is assumed able to receive remote configuration commands using the SNMP protocol, or any tunnelling protocol specified in [1].

SNMP configuration is given also by MIB parameters in SNMP group (see clause 8.8).

8.7.2 RCST HLS Configuration parameters

The RCST HLS parameters are configurable both locally by the RCST installer and remotely by management via configuration file.

The RCST systems parameters may be configured providing the following parameters:

- RCST System group (see clause 8.6.1)
- RCST System configuration group (see clause 8.6.10)

The RCST completes its SVN interfaces configuration according to the parameter values provided during logon. The logon information provided in Logon Response and the Higher Layer Initialization and the DHCP Option descriptors, whose format is specified in [1] supersede the configuration provided by local or remote configuration file.

The RCST addressing and networking information may be configured by providing the following parameters:

- RCST interfaces group (see clause 8.6.2)
- RCST IP group (see clause 8.6.3)
- RCST RCS2 network group (see clause 8.6.12), including the DNS proxy enabled for IPv4/IPv6 using IPv4IPv6 transport per interface
- RCST RCS2 VRF configuration (see clause 8.6.13)
- RCST VLAN configuration (see clause 8.6.21)
- RCST NAT/NAPT configuration (see clause 8.6.22)

The set of networking and routing options in the RCST may be initialize during logon thanks to the DHCP Option descriptor in TIM-u message, specifically per each of the LAN interfaces corresponding to the traffic SVNs supported by the RCST.

Once the RCST has decoded the Lower Layer Service descriptor, it is needed to perform the mapping between the HLS and LL parameters related to QoS (LL services). For that purpose, a minimum configuration with the default setting for the following parameters may be provided through an RCST configuration file. This information may be superseded using a TIMu NLID descriptor during logon.

The RCST QoS configuration may include:

- Default entry in the IP classification table. The RCST may include one entry in this table, matching all the IP traffic. This entry is linked to the default HLService.
- HLS mapping table. At least one entry with the default policy is provided in the default RCST configuration.
- LL service parameters provided during logon.

The MIB objects needed to configure these parameters are listed in clause 8.6.

The use of non-standard PEP by a SVN is enabled in the lower layer signalling. PEP negotiation is also configured by the lower layers per SVN using the Higher Layer Initialization descriptor, notified in the logon TIM-u following the PEP negotiation protocol parameters in clause 8.6.23.

The configuration may be controlled following login using the HLS agent negotiation messages (see clause 9.2.1) transport over UDP/IP.

PEP negotiation protocol configuration is supported via the RCST MIB as described in clause 8.6.23. PEP may be enabled/disabled per RCST interface.

8.8 RCST MIB access management Roles

M and C could be supported by the different roles interfaces as follows, indicated as Essential (E) or Other (O):

Table 8.22: RCST MIB access management roles

Functional Group	Description	SNO						SVNO				User	
		SNMP/ NLID		SNMP/IP		ASCII File/FTP		SNMP/IP		ASCII File/FTP		HTTP/IP	
		O/E	Access	O/E	Access	O/E	Access	O/E	Access	O/E	Access	O/E	Access
SystemConfig	RCS2 System config	E	WO	E	RW	E	WO	E	RO	E	RW	O	RO
NetworkConfig	RCS2 Network config	E	WO	E	RW	E	WO	E	RO	E	RW	O	RO
Installation	RCS2 installation	-	-	E	RW	E	WO	E	RW	E	RW	O	RO
Control	RCS2 control commands	E	WO	E	RW	E	WO	E	RW	E	RW	O	RO
State	RCS2 state	-	-	E	RO	-	-	E	RO	-	-	O	RO
Statistics	RCS2 statistics	-	-	E	RO	-	-	E	RO	-	-	O	RO
QoSConfiguration	for the satellite interface	-	-	E	RO	E	WO	E	RO	E	WO	O	RO
FlinkConfiguration	part of satellite LL	-	-	E	RO	E	WO	E	RO	E	WO	O	RO
RlinkConfiguration	part of satellite LL	-	-	E	RO	E	WO	E	RO	E	WO	O	RO
VRFConfig	VRF	-	-	O	RO	O	WO	E	RO	E	WO	O	RO
VLAN	VLAN	-	-	O	RO	O	WO	E	RO	E	WO	O	RO
DCP Agent Configuration	For mesh	-	-	O	RO	O	WO	E	RO	E	WO	O	RO
PEP Negotiation	PEP	-	-	O	RO	E	WO	E	RO	-	-	O	RO
System	System MIB-II	-	-	E	RW	E	WO	E	RO	E	WO	O	RO
Interfaces	Interfaces MIB-II	-	-	E	RW	E	WO	E	RO	E	WO	O	RO
IP	IP MIB-II	-	-	E	RW	E	WO	E	RO	E	RW	O	RO
ICMP	ICMP MIB-II	-	-	E	RW	E	WO	E	RO	E	RW	O	RO
TCP	TCP parameters	-	-	O	RO	O	WO	O	RO	E	RW	O	RO
UDP	UDP parameters	-	-	O	RO	O	WO	O	RO	E	RW	O	RO
SNMP	SNMP parameters	O	WO	E	RW	E	WO	E	RO	E	RW	O	RO
IGMP	IGMP MIB-II	O	WO	E	RW	E	WO	O	RO	E	RW	O	RO
Ethernet	Ethernet MIB-II	-	-	O	RO	O	WO	O	RO	O	WO	O	RO
NAT/NAPT	NAT/NAPT MIB-II	-	-	E	RW	E	WO	E	RO	E	RW	O	RO
IPv4 DHCP	DHCP options	-	-	E	RW	E	WO	E	RO	E	RW	O	RO
IPv6 DHCP	DHCP options	-	-	E	RW	E	WO	E	RO	E	RW	O	RO

9 Intercepting traffic

9.0 Introduction

This clause describes a set of agents that provide deep packet inspection to allow cross-layer optimization of higher layer functions.

Interception of packets is associated with a specific SVN-MAC over which the traffic will be sent/received.

9.1 Agent Architecture

In the present document, an agent is defined as an entity that intercepts specific control traffic flows, redirecting these to an HLS module.

Figure 9.1 illustrates this ingress/egress processing by the higher-layer system, focussing on network-layer processing following reception of a packet by the LAN interface. The diagram is intended to be informative and does not mandate any particular internal structure of an RCST. Solid lines represent the flow of PDUs and other data through the system, whereas dashed lines are used to denote control relationships. Simple functions or objects are represented by boxes, selector mechanisms by hexagons, and complex objects by pentagons.

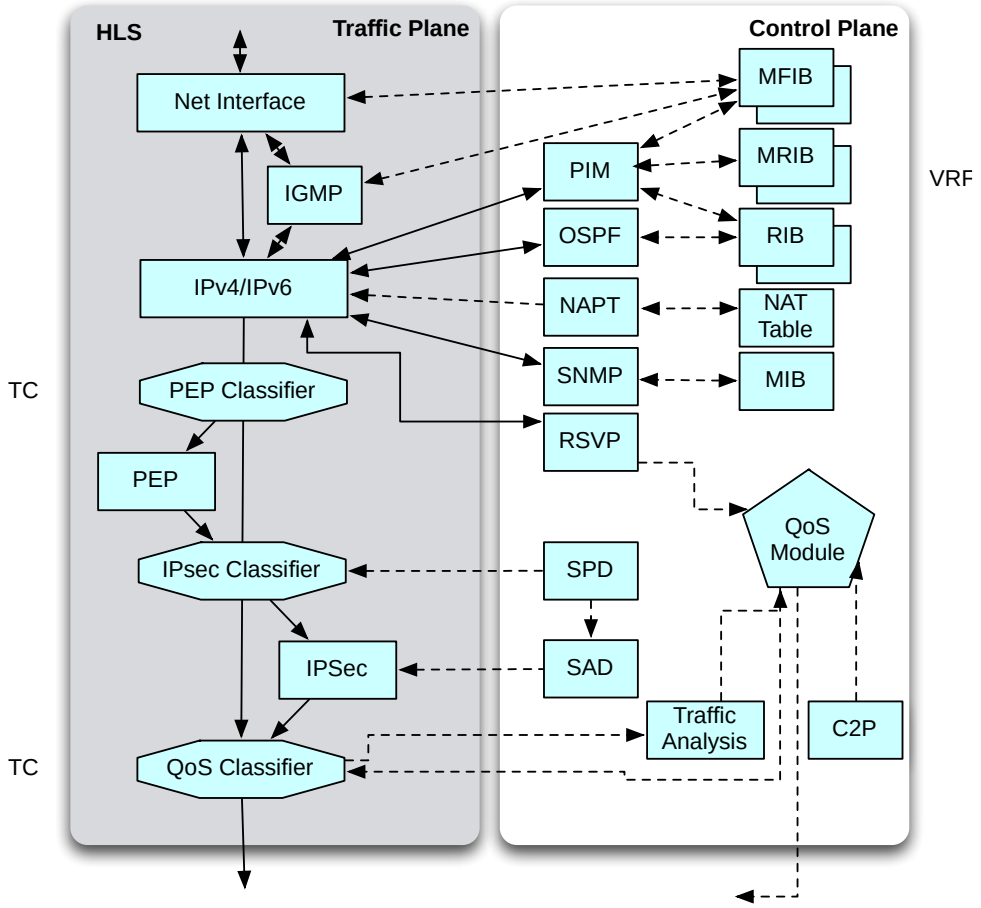


Figure 9.1: RCST network layer functions illustrating an example of placement of PEP and IPsec

9.2 HLS Agent Control Protocol

9.2.0 Introduction

This clause describes a protocol to configure and control the agents in an RCST.

The RCST shall support the HLS agent control protocol. This protocol is used over the IPv4 address provisioned for a satellite interface and bound to a SVN-MAC label for management signalling. Functions of the protocol include selecting operational parameters and enabling/disabling specific agents.

Each RCST Agent control message shall contain a one byte field in the first byte of each message. This indicates the type of message. A message with a type value of zero shall be used to indicate an error message. A message with an unknown type shall be silently discarded. Receivers shall not generate an error message for an unknown message type (these values are reserved for future versions of the specification).

Messages exchanged using an SVN shall be used by the NCC to configure the operation of the RCST Agent modules for the corresponding Traffic SVN. Messages shall be exchanged using the management SVN.

The following message types are supported in the present version of the present document.

Table 9.1: Agent Control message formats

Message	Message ID	Vendor OUI and Product ID	Product Capability List	Configuration Block
Error	0			
PEP Advertise	1	N ≥ 1	N	
PEP Offer	2	M ≥ 1		
PEP Use	3	1		0 or 1
Reserved	>3			

A receiver shall silently ignore all reserved values.

The RCST shall support the current set of messages for TCP-PEP negotiation. Each offer contains N descriptors for the offered TCP-PEPs. Each response contains M descriptors for the supported TCP-PEPs, where M=<N. The NCC finally selects one TCP-PEP.

The RCST Agent negotiation messages shall be transported in the following way:

- The IPv4 multicast group destination address and UDP port number are received via a descriptor in the TIM-U.
- A PEP Advertise message is received on the forward link. This shall be directed to either the advertised IPv4 multicast address or unicast to the assigned RCST IPv4 address. The message is sent using the advertised UDP port.
- A PEP Offer message is sent with an IPv4 destination address that matches the IP source address of the PEP Advertise message and using the UDP destination port that was used in the PEP Offer message. The IP packet is sent with the IP source of the RCST and using the same SVN on which the PEP Offer was received.
- A PEP Use or PEP Error message is sent in response to a PEP Offer message. This has an IP source address that is identical to the IP destination address of the PEP Offer and a IPv4 destination address identical to the IP source address used for the PEP Offer. The UDP source port is identical to the UDP destination port of the PEP Offer message.

The above exchange is used to configure the PEP used for a specific SVN. An RCST that supports multiple SVNs shall repeat this negotiation for each SVN that is active.

Other uses of this protocol are currently reserved.

9.2.1 PEP Negotiation Protocol

9.2.1.0 Introduction

An RCST or/and NCC can provide a TCP-PEP and protocol acceleration support. The Satlabs systems recommendations (SatLabs System Recommendations [i.4]) define a TCP-PEP for use for with an RCS network. Advice on the use of TCP-PEPs is provided in IETF RFC 3135 [i.35] and IETF RFC 3449 [i.40]. IETF RFC 3135 [i.35] advises that operators and users should be able to control whether a TCP-PEP is used for a specific session.

The RCST shall support a mechanism by which an RCST selects the TCP-PEP Agent that it will use. When multiple versions of a specific TCP-PEP are available, this mechanism shall also be used to select the version that is used. When no TCP-PEP is available, this mechanism shall be used to indicate no TCP-PEP support to the NCC.

Each uniquely identifiable set of parameters is called a "PEP configuration". A vendor has the flexibility to create multiple "PEP configuration" entries for the same TCP-PEP module, if this introduces potential modes that can be recognized as a basis for negotiation.

An RCST shall allow none (null TCP-PEP), one or multiple versions of a TCP-PEP to simultaneously process traffic. The use of the null TCP-PEP does not modify the traffic.

When multiple TCP-PEP are supported by the RCST, one and only one PEP shall be configured per SVN-MAC. A Traffic Class may be used to segregate traffic between different active TCP-PEP modules.

The RCST shall comply with the PEP negotiation that comprises three stages:

1) In the first stage, the PEP negotiation starts with a message advertising a set of PEP configurations. This may be broadcast periodically (in the case of a NCC), or triggered by another event (e.g. Logon or setup a mesh connection).

2) In the second stage, the RCST selects the TCP-PEP it prefers to use from the offered set (if any). It then generates an offer message. The choice is based on local policy at the receiver and knowledge of the available PEP configurations. An RCST may (optionally) utilize the capability field to choose between equivalent offers. This identifies one or more candidate PEP configurations. This could be one of the following:

    - A single offered TCP-PEP configuration, which the RCST believes matches the initiator's offered set of PEP configurations.
    - An offer indicating multiple TCP-PEP configuration offerings, from which the initiator should choose one to use.
    - An error response that indicates that client wishes to abort the present negotiation.

3) The final stage is the selection of the PEP to be used for the SVN-MAC on which the offer was received. The initiator selects an identical or compatible PEP configuration. This selection should be made from the offered set, and the initiator then informs the RCST which TCP-PEP to use. An error message may be sent when the negotiation cannot be completed.

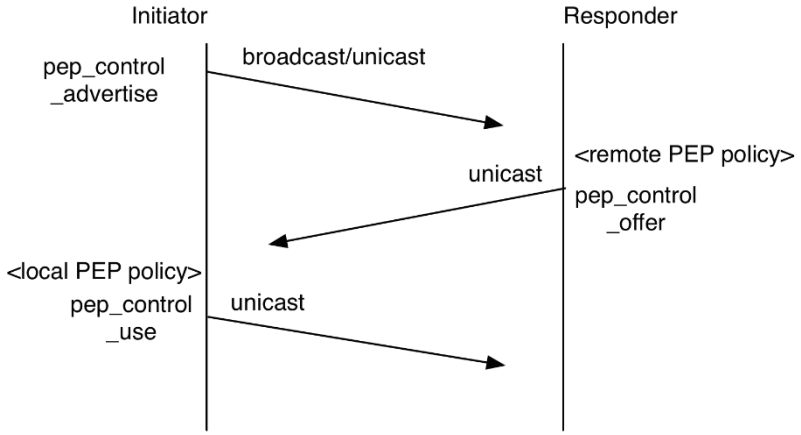


Figure 9.2: PEP Negotiation Exchange

Once activated, the relevant configuration of parameters can be successfully performed by a two-sided PEP, an optional configuration string may be used to assist in this initial configuration.

In case of mesh systems, the NCC/NMC is responsible for controlling the PEP negotiation between each RCST and its assigned GW-RCST in a similar way that done for star transparent topologies.

9.2.1.1 PEP Control Advertise Message

9.2.1.1.0 Introduction

A PEP Control Advertise Message is used to indicate the set of TCP-PEP configurations available at the initiating entity. Each PEP configuration is identified by the combination of a pep_vendor_id (encoded as a 24-bit OUI value), and a pep_standards_id. The pep_product_id is selected by the vendor to identify a particular implementation (software version and/or model number). The pep_standards_id field references a particular feature set (uniquely identifiable version of a PEP).

The RCST shall accept the PEP Control Advertise message sent in broadcast mode by the NCC. The broadcast message announces a system-wide capability applicable to all SVNs.

The RCST shall accept the PEP Control Advertise message sent in unicast to a peer RCST using a mesh connection.

The PEP-Capability field is used to carry an indication of the class of TCP-PEP mechanisms that are supported. This is intentionally not a detailed specification of specific mechanisms or specific values, and should only be used to help identify the most suitable client TCP-PEP configuration.

Table 9.2: PEP Control Advertise Message

Syntax	No. of bits (default value)	Mnemonic
pep_control_advertisement () {		
pep_control_type	8 (0x01)	uimsbf
number_of_records	8	uimsbf
for (i=0; i < number_of_records i++) {		
pep_vendor_id	24	uimsbf
pep_product_id	16	uimsbf
pep_standards_Id	16	uimsbf
pep_capability	48	uimsbf
}		
}		

The default PEP profile shall be zero. A non-zero value is used to indicate a fully-specified PEP configuration.

9.2.1.1.1 PEP capability parameters

Table 9.3 shows the PEP Control capability field. The default PEP profile shall be zero. A non-zero value is used to indicate a specified PEP configuration. A sender shall assign all reserved values to zero, and shall ignore any reserved values on reception.

Table 9.3: PEP Control capability field

Syntax	No. of bits	Mnemonic
pep_capability () {		
pep transparent_ipv4_supported	1	bslbf
pep_transparent_ipv6_supported	1	bslbf
pep_transparent_other_supported	1	bslbf
pep_ipv4_supported	1	bslbf
pep_ipv6_supported	1	bslbf
pep_other_supported	1	bslbf
reserved	1	bslbf
pep_ipv4_header_compression	1	bslbf
pep_ipv4_content_compression	1	bslbf
pep_ipv6_header_compression	1	bslbf
pep_ipv6_content_compression	1	bslbf
pep_net_content_compression	1	bslbf
pep_udp_header_compression	1	bslbf
pep_udp_content_compression	1	bslbf
pep_tcp_header_compression	1	bslbf
pep_tcp_content_compression	1	bslbf
pep_tcp_transparent_interception	1	bslbf
pep_tcp_transform	1	bslbf
pep_http_header_compression	1	bslbf
pep_http_transparent_interception	1	bslbf
pep_http_transform	1	bslbf
pep_http_content_transcode	1	bslbf
pep_https_transform	1	bslbf
pep_rtp_header_compression	1	bslbf
pep_rtp_content_compression	1	bslbf
pep_rtp_transparent_interception	1	bslbf
pep_rtp_transform	1	bslbf
pep_other_transform	1	bslbf
pep_other_custom	1	bslbf
reserved	3	bslbf
}		

The following one-sided capabilities can be used to enable/disable all PEP functions for a particular IP address family (i.e. methods that do not require a remote peer to transform the PDUs to a standard format). One-sided operation uses only a PEP at the advertising end, and no enhancement at the remote end. Remote sides may therefore reasonably expect that one-sided enhancements will be able to provide some form of acceleration.

pep_transparent_ipv4_supported: The PEP will intercept and process IPv4 packets using a method that can operate without a peer at the remote side. This includes the possibly also of interpreting transport and higher packets carried within IPv4 packets, as indicated by other flags. If this field is '0', the PEP will not perform any of the transparent functions listed in this section for IPv4 traffic.

pep_transparent_ipv6_supported: The PEP will intercept and process IPv6 packets using a method that can operate without a peer at the remote side. This includes the possibly also interpreting transport and higher packets carried within IPv6 packets, as indicated by other flags. If this field is '0', the PEP will not perform any of the transparent functions listed in this section for IPv6 traffic.

pep_transparent_other_supported: The PEP will intercept and process other (e.g. user-defined) packets packets using a method that can operate without a peer at the remote side. This includes the possibly also interpreting transport and higher packets carried within these packets, as indicated by other flags. If this field is '0', the PEP will not perform any of the transparent functions listed in this section for traffic that is neither IPv4 or IPv6.

pep_tcp_transparent_interception: The PEP will intercept TCP connections (e.g. split TCP) by preserving TCP compatibility with the receiver.

pep_http_transparent_interception: The PEP will intercept HTTP by preserving HTTP compatibility (e.g. pre-fetching) by preserving HTTP compatibility with the receiver.

pep_http_content_transcode: The PEP will perform HTTP content transcoding (e.g. image/voice codec transcoding to reduce the bandwidth required for transmission) and seek to preserve HTTP compatibility with the receiver.

pep_rtp_content transcode: The PEP will perform RTP content transcoding; (e.g. to reduce the bandwidth required for transmission) and seek to preserve RTP compatibility with the receiver.

pep_other_content_transcode: The PEP will perform another custom transcoding of content.

The following capability attributes resemble those defined for one-way operation, but require a corresponding PEP entity at the remote end. The specifics of the PEP method depend on the specific implementation as defined by the combination of (pep_vendor_id, pep_product_id, pep_standards) fields.

pep_ipv4_supported: The PEP will intercept and process IPv4 packets (including possibly also interpreting transport and higher packets carried within IPv4 packets, as indicated by other flags). If this field is '0', the PEP will not perform any 2-sided PEP functions listed below for IPv4 traffic.

pep_ipv6_supported: The PEP will intercept and process IPv6 packets (including possibly also interpreting transport and higher packets carried within IPv6 packets, as indicated by other flags). If this field is '0', the PEP will not perform any 2-sided PEP the functions listed below for IPv6 traffic.

pep_other_supported: The PEP will intercept and process other (e.g. user-defined) packets (including possibly also interpreting transport and higher packets carried within these user-defined packets, as indicated by other flags). If this field is '0', the PEP will not perform any 2-sided PEP functions listed below for these traffic that is not IP4 nor Ipv6.

pep_ipv4_content_compression: The PEP will perform lossless compression of IPv4 content.

pep_ipv6_content_compression: The PEP will perform lossless compression of IPv6 content.

pep_net_content_compression: The PEP will perform lossless compression of content carries in other network layer packets that do not use IPv4 or IPv6.

pep_udp_content_compression: The PEP will perform lossless compression of UDP content.

pep_tcp_content_compression: The PEP will perform lossless compression of TCP content.

pep_other_compression: The PEP will perform lossless compression of custom content.

pep_ipv4_header_compression: The PEP will perform IPv4 header compression and provision the remote peer to perform a corresponding appropriate inverse transform for decompression at the remote peer.

pep_ipv6_header_compression: The PEP will perform IPv6 header compression and provision the remote peer to perform a corresponding appropriate inverse transform for decompression at the remote peer.

pep_udp_header_compression: The PEP will perform compression of UDP/IP headers and provision the remote peer to perform a corresponding appropriate inverse transform for decompression at the remote peer.

pep_tcp_header_compression: The PEP will perform compression of TCP/IP headers and provision the remote peer to perform a corresponding appropriate inverse transform for HTTP packets.

pep_http_header_compression: The PEP will perform compression of HTTP headers and provision the remote peer to perform a corresponding appropriate inverse transform for decompression at the remote peer.

pep_rtp_header_compression: The PEP will perform compression of RTP/UDP/IP headers and provision the remote peer to perform a corresponding appropriate inverse transform for RTP packets.

pep_tcp_transform: The PEP will intercept TCP/IP connections (e.g. split TCP) and provision the remote peer to perform a corresponding appropriate inverse transform for TCP packets.

pep_http_transform: The PEP will intercept HTTP/TCP/IP and provision the remote peer to perform a corresponding appropriate inverse transform for HTTP packets.

pep_https_transform: The PEP will intercept HTTPS/TCP/IP and provision the remote peer to perform a corresponding appropriate inverse transform for secure HTTPS packets.

pep_rtp_transform: The PEP will intercept RTP and provision the remote peer to perform a corresponding appropriate inverse transform for RTP packets.

pep_other_transform: The PEP will intercept other (e.g. user-defined) packet types and provision the remote peer to perform a corresponding appropriate inverse transform for other protocols.

pep_other_custom: The PEP will perform other (e.g. user-defined) two-sided enhancements that do not match any of the above capabilities.

A sender shall assign all reserved values to zero, and shall ignore any reserved values on reception.

9.2.1.2 PEP Control Offer Message

An RCST shall respond to the advertisement with an offer that indicates the set of TCP-PEPs that it wishes to support. The RCST shall make this selection by matching the combination of Vendor OUI (24 bits) and the product ID against the corresponding values for the TCP-PEPs that it supports. The capability information is not present (the initiator should understand the capabilities/compatibility of each TCP-PEP).

The PEP Control Offer Message is a unicast message that is used to indicate the set of TCP-PEP configurations that are available at the remote entity. Each TCP-PEP is identified by the pep_vendor_id (encoded as a 24-bit OUI value), and a pep_product_id, selected by the vendor to identify a particular feature set (software version and/or uniquely identifiable version of a TCP-PEP). The message includes the standards_id and pep_capability fields of the advertisement message. The responder should only include TCP-PEP configurations in the list that are expected to be compatible with those that were offered. If there are no available TCP-PEPs, it shall return an error message to abort the use of a TCP-PEP.

An RCST may issue a PEP Control Offer Message at any time for any active SVN-MAC. The offer shall force renegotiation of the PEP to be used for the SVN-MAC.

Table 9.4: PEP Control Offer Message

Syntax	No. of bits (default value)	Mnemonic
pep_control_offer_response () {		
pep_control_type	8 (0x02)	uimsbf
number_of_records	8	uimsbf
for (i=0; i < number_of_records i++) {		
pep_vendor_id	24	uimsbf
pep_product_id	16	uimsbf
pep_standards_Id	16	uimsbf
pep_capability	32	uimsbf
}		

The pep_capability value has the same format as specified for an offer message. A sender shall assign all reserved values to zero, and should ignore unknown values on reception.

9.2.1.3 PEP Control Use Message

Transmission of a PEP control use message instructs the remote entity to use one of the offered PEPs for the SVN-MAC on which it is received. The message shall identify one of the offered set of TCP-PEPs and may optionally include a block of up to 256 bytes configuration data to be sent to the remote TCP-PEP. The contents of the configuration block shall be transported to the remote TCP-PEP without modification. Use of this data is vendor-specific.

A PEP Control Use Message may be sent at any time for any active SVN-MAC. The message shall assign the PEP to be used for the specified SVN-MAC.

Table 9.5: PEP Control Use Message

Syntax	No. of bits (default value)	Mnemonic
pep_control_use () {		
pep_control_type	8 (0x03)	uimsbf
pep_vendor_id	24	uimsbf
pep_product_id	16	uimsbf
pep_config_size	8	uimsbf
for (i=0; i < pep_config_size i++) {		
pep_configuration_block	8	uimsbf
}		
hls_tc	16	uimsbf
}		

Reception of a PEP Control Use message shall cause the receiving entity to use the instructed PEP for the SVN-MAC on which it is received. The PEP shall be bound to a traffic classifier ID when the hls_tc value is non-zero. Classifier IDs are configured at a remote RCST using the QoS module (e.g. this could be used to bind all traffic from a particular set of IP addresses to a PEP, or to use multiple classifiers to enable a sender to select which traffic is not processed by a specific PEP).

No response is required unless the entity cannot activate the required PEP configuration. In this latter case, the entity shall return an error code to report the problem. Reception of a request to use a PEP that was not in the set of offered PEPs shall result in returning an error message with an error code of "3".

The reply is sent as a UDP datagram sent to the source of the advertisement with the same port.

9.2.1.4 Agent Control Error Message

The Agent Control Error Message is a unicast message that indicates that requested action in a control message was not performed by a client. The message includes a one byte field indicating the requested_action that generated the error and a one byte error_code that uses one of the values specified in table 9.6.

Table 9.6: Agent Control Error Message

Syntax	No. of bits (default value)	Mnemonic
agent_control_error () {		
agent_control_type	8 (0x00)	uimsbf
requested_action	8 (0x00)	uimsbf
error_code	8	uimsbf
}		

The set of currently specified error codes is specified below.

Table 9.7: Agent Control Error Message

Error Codes	Value	Note
protocol_error	0	The Control message has an unknown syntax.
no_compatible_pep	1	There are no available PEP Entities that match those listed in an offer or use message.
temporary_error	2	The PEP Control message cannot be processed at this time, or has been disabled (this value indicates a soft error, and implementation should not cache this response and should try again later).
invalid_use	3	The PEP requested in a "use" message was not one of the offered set of PEPs.
unspecified_error	4-255	

NOTE: No error message is issued for an unknown control value, to allow for the possible introduction of other control messages in future releases of the present document.

9.3 Signalling and Control Agents

9.3.0 Introduction

This clause identifies a set of functions that may exist in the HLS to intercept signalling and provide control functions to the HLS. The present document only specifies a limited subset of this set of agents.

9.3.1 RSVP Proxy

RSVP is specified in IETF RFC 2205 [i.20]. IETF RFC 2750 [i.33] defines extensions for supporting generic policy based admRcs2ion control in RSVP. Operation of an RSVP proxy is not specified in the current version of the present document.

9.3.2 IGMP/MLD Proxy

Operation of an IGMP/MLD proxy is not specified in the current version of the present document.

9.3.3 RSVP-TE Proxy

Operation of a RSVP-TE proxy is not specified in the current version of the present document.

9.3.4 DNS Proxy

Relaying (proxy) of DNS is defined in IETF RFC 5625 [i.58] and may be used to support NAT usage. Operation of a DNS proxy is not specified in the current version of the present document.

10 Control Of Motorized Mount (Optional)

This clause specifies what is needed to control a motorized mount for steering an antenna.

In order to control the motorized mount, the modem shall support the elements of the DiSEqC standard as defined in the Eutelsat Reference Document "Bus Functional Description", version 4.2 available free of charge through the Eutelsat website (https://www.eutelsat.com/en/support/technical-support-teleports-resources-tools.html). In particular, the modem shall be able to support the elements described in the clause titled "Bus Hardware Specification", "Method of Data-Bit Signalling" and "Message Data Format".

Concerning the "Bus Hardware Specification", the modem shall support the recommended DC Supply current drain level of up to 500 mA.

Regarding the "Message Data Format", the following shall be supported:

- For the Framing Byte, the byte with Hex value E0 shall be supported ("Command from Master, No reply required, First transmission").
- For the Address Byte, the bytes with Hex values 31 and 32 (Azimuth Positioner and Elevation Positioner, respectively) shall be supported. If a third motorized axis is used for polarization control, the byte with Hex value 21 shall be supported.
- For the Command Byte, the bytes with Hex values 60, 6B, 6C, 6E shall be supported.

The antenna alignment procedure follows the steps shown in figure 10.1. In a first phase of the procedure, the RCST shall use the alignment thresholds to perform the alignment of the forward channel. The alignment threshold parameters to be used are: *MaxFwdAlignThrExcDuration*, *MaxFail*, described in table 10.1.

Once the requested accuracy of the forward channel alignment has been reached, the RCST shall start decoding the Forward Link signalling.

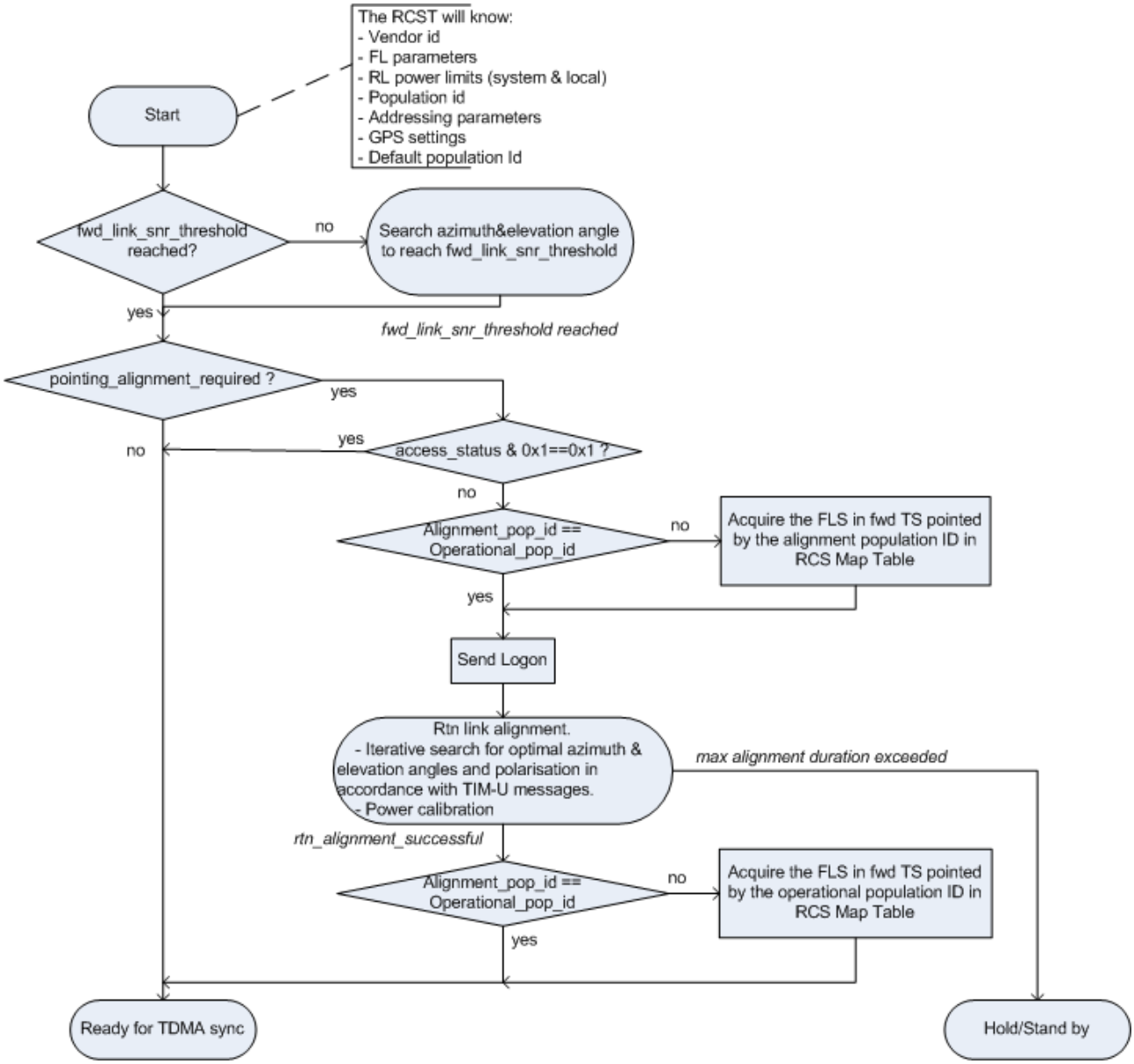


Figure 10.1: RCST antenna alignment and logon

Table 10.1: Alignment parameters in the initial configuration

Parameter	Description
MaxFwdAlignThrExcDuration	The duration of the time interval during which fwd alignment accuracy shall be achieved.
MaxFail	Maximum number of alignment failures. The corresponding counter is incremented every time the state machine re-visits the FwdAligment state.

Annex A (informative): RCST MIB

Annex intentionally left blank.

This informative annex will include the new RCST MIB following the MIB objects requirements in clause 8, in a revised version of the present document.

The RCST MIB recommended syntax is ASN.1.

Annex B (informative): RCST Configuration file

Annex intentionally left blank.

This informative annex will include the configuration file in XML format following the MIB definition, in a revised version of the present document.

Annex C (informative): Specification of the Software Download Delivery Protocol (SDDP)

C.1 Introduction

The present annex defines a unidirectional multicast protocol, from hub to terminals allowing to update the Software run by Terminals. This is denoted SDDP (Software and Data Download Protocol) and allows sending Software files in a data carousel fashion (the same file transmission being sent successively in loops) In particular:

- This annex defines how to locate the forward link stream containing SDDP in a network.
- This annex defines the signalling information used to locate SDDP.
- This annex defines the transmission of SDDP as a standardized IP multicast.
- SDDP is based on the OUI (Organization Unique Identifier) identifying a terminal manufacturer.
- This annex defines components that can be used to enhance the SDDP functionality in an upward-compatible way. This provides a standard mechanism for carrying additional information, e.g. update scheduling information, extensive selection and targeting information, action notification, filtering descriptors.

C.2 Scope

DVB-RCS2 terminal software is complex. To guarantee the functionality of a terminal, as well as increasing its functionality once deployed in the field, a software update service is required. The present annex specifies a mechanism for signalling a software update service and the means to carry the data for this software update service.

The SDDP protocol takes advantage of the IP capabilities present in a DVB-RCS2 terminal to keep the lower layer implementation simple and unchanged from the DVB-RCS2 specification (DVB-RCS2). It also takes advantage of the multicast capabilities of DVB-S and DVB-S2.

C.3 Overview of the Basic Protocol

A file transfer begins with a request send from the Hub to write a file (WRQ message) or an information (INFO message) indicating where the file is located. The transmission of the file content on the forward link then proceeds. The file is sent in fixed length blocks, specified by the block size parameter (see clause C.7), typically 512 bytes. Each data packet contains one block of data (DATA message). A data packet of less than the block size terminates the transfer.

Most errors cause termination of the transfer. Errors are caused by three types of events: not being able to satisfy the request (e.g. access violation), receiving a packet that cannot be explained by a delay in time or by duplication in the network (e.g. an incorrectly formed packet), and loss of access to a necessary resource (e.g. memory resources exhausted or access denied during a transfer).

SDDP recognizes only one error condition that does not cause termination, the source port of a received packet being incorrect.

This protocol is very restrictive, in order to simplify implementation. For example, the fixed length blocks makes allocation straightforward.

C.4 Relation to other Protocols

SDDP is based on the TFTP Protocol (Revision 2) elements specified in IETF RFC 1350 [i.18] modified to apply for the one-way file transfer associated with multicast. TFTP options as specified by IETF RFC 2347 [i.23], TFTP Blocksize Option (IETF RFC 2348 [i.24]) and TFTP Timeout Interval and Transfer Size Options (IETF RFC 2349 [i.25]) are also supported. In addition, application specific options are defined. The TFTP elements are amended with an optional information carousel that supports scaling and increased speed of commissioning.

The SDDP is implemented on top of the User Datagram Protocol (UDP). Since this Datagram service is implemented on IP, packets will have an IP header, a UDP header, and a SDDP header. Additionally, the packets will be encapsulated and sent using a DVB-RCS2 FL stream.

Figure C.1 shows the order of the contents of a packet encapsulated using an MPE/GSE header, IP header, UDP header, SDDP header and the payload of the SDDP packet. (This may or may not be data depending on the type of packet as specified in the SDDP header.) SDDP does not specify any values in the IP header. On the other hand, the source and destination port fields of the UDP header (its format is given in the appendix) are used by SDDP and the length field reflects the size of the SDDP packet. The Transfer IDentifiers (TID's) used by SDDP are passed to the UDP layer to be used as ports; therefore they should be between 0 and 65,535. The initialization of TID's is discussed in the clause on initial connection protocol.

The SDDP header consists of a 2B opcode field that indicates the type of packet (e.g. DATA, etc.) These opcodes and the formats of the various types of packets are discussed further in the clause on SDDP packets.

Figure C.1: Order of Headers when using a GSE Stream

C.5 Basic SDDP Packet Formats

SDDP supports three types of packets, all of which have been mentioned below.

Table C.0

Opcode	Operation
2	Write request (WRQ)
3	Data (DATA)
255	Information (INFO)

The SDDP header of a packet contains the opcode associated with that packet.

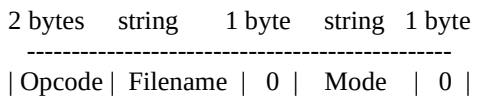


Figure C.2: WRQ packet

WRQ packets (opcode 2) have the format shown in figure C.2. The file name is a sequence of bytes in netascii terminated by a zero byte. The mode field contains the string "octet" (or any combination of upper and lower case, such as "OCTET", "Octet", etc.) in netascii. Octet mode is used to transfer a file that is in the 8-bit format of the indicated target type.

Figure C.3: DATA packet

Data is transferred in DATA packets depicted in figure C.3. DATA packets (opcode = 3) have a block number and a data field. The block numbers assigned to data packets begin with one and increase by one for each new block of data. This restriction allows the sender to use a single number to discriminate between new packets and duplicates. The data field is from zero to N bytes long. If it is exactly N bytes long, the block is not the last block of data. If it is from zero to (N-1) bytes long, it signals the end of the transfer. If the file ends with a final data segment of N bytes the transfer will be terminated by a block with a zero length data field. The default value of N is 512. Another block size can be indicated by the parameter "blksize".

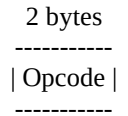


Figure C.4: INFO packet

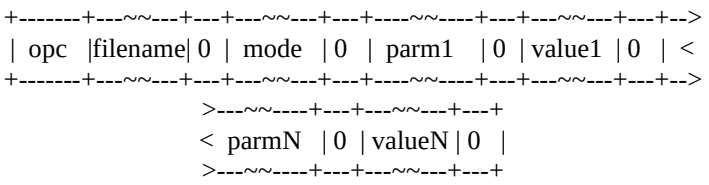
Control information may be transferred regularly in INFO packets depicted in figure C.4. INFO packets (with opcode = 255) typically carry additional parameters (see clause C.7). INFO packets may occur anywhere in the SDDP stream.

C.6 Parameter Transfer

The parameter transfer mechanism specified in the present document allows file transfer parameters to be conveyed prior to the transfer using a mechanism that is consistent with SDDP's Request Packet format.

SDDP parameters are appended to the Write Request and Information packets.

Parameters are appended to an SDDP Write Request packet as follows:



Opc	The opcode field contains a 2, for Write Requests (IETF RFC 1350 [i.18]).
Filename	The name of the file to be read or written (IETF RFC 1350 [i.18]). This is a NULL-terminated field.
Mode	The mode of the file transfer: "netascii", "octet", or "mail", as defined in IETF RFC 1350 [i.18]. This is a NULL-terminated field.
parm1	The name of the first parameter in case-insensitive ASCII (e.g. blksize). This is a NULL-terminated field.
value1	The value associated with the first parameter, in case-insensitive ASCII. This is a NULL-terminated field.
parmN, valueN	The final parameter/value pair. Each NULL-terminated field is specified in case-insensitive ASCII.

Figure C.5: SDDP parameters in WRQ packet

INFO messages have exactly the same layout as WRQ ones. The only difference is that they are assigned an opcode of 255 instead of 2. INFO messages are repeated at a higher rate than a WRQ. The WRQ is sent only once per loop of the data carousel, on the same redirected IP address and UDP port as the data, just before the file is sent. INFO messages may be sent at a higher rate and are sent on the default multicast group and port. The maximum length of INFO messages or WRQ is 512 bytes.

The parameter names and values are all NULL-terminated, in keeping with the original request format. If multiple parameters are to be specified, they are appended to each other. The order in which parameters are specified is not significant. The maximum size of a request packet is 512 octets.

C.7 Parameters

Table C.1: SDDP parameters

Parameter	Required functionality (O/M)	Presence of the parameter in message (O/M)	Occurrence	Function	Value
blksize	***M***	***O***	WRQ, INFO	Set the DATA block size to another value than the default of 512 bytes.	Decimal number of bytes
Tsize	***M***	***M***	WRQ, INFO	Indicates the total transfer size.	Decimal number of bytes
manufID	***M***	***M***	WRQ, INFO	Indicates the OUI.	24 bit OUI as decimal value
Vendor specific parameters	***O***	***O***	WRQ, INFO	Maximum of 10 vendor specific parameters. A server support that many parameters. An RCST implementation does not consider the server is able to handle more.	Manufacturer specific
ver	***M***	***O***	WRQ, INFO	Current SW version in the SW distribution carousel, respective to the manufID and vendor specific parameters.	Manufacturer specific
minver	***O***	***O***	WRQ, INFO	Indicates the minimum SW version required for log-on, with respect to manufID and vendor specific parameters.	Manufacturer specific
method	***O***	***O***	WRQ, INFO	Indicates if the SW update method is different from the default "immediate". It can also be "pending", i.e. awaiting the next RCST restart.	"immediate" "pending"
timeout	***O***	***O***	WRQ, INFO	Indicates the timeout when waiting for the next DATA packet, default value is given in the initial configuration (sec).	Decimal seconds
mgroup	***O***	***O***	INFO	Set a redirection multicast group address respective to the manufID and vendor specific parameters.	Dot separated decimal
port	***O***	***O***	INFO	Sets a redirection UDP port respective to the manufID and vendor specific parameters.	Decimal
layer2	***O***	***O***	INFO	Indicate the redirection layer 2 address for a specific download.	Decimal number of bytes

An M indicates parameters and functionality that should be supported. An O indicates parameters and functionality that may or should be supported. It some cases the lack of support of the latter type of functionality should be compensated through the capability of manual configuration at the RCST to allow the RCST to be entered into a system that utilizes all capabilities of the SDDP.

If a parameter occurs in an INFO message and the occurrence column states "WRQ, INFO" it should also be present in the WRQ message.

The SDDP server has to provide the mandatory parameters and may supply the other parameters as required for functionality and consistency.

C.8 Initial Connection Protocol

A transfer may be established by sending an INFO message on the default multicast group and UDP port. In this case the terminal will redirect to a new IP address and port and will start reading the file on this multicast address and UDP port. A WRQ should be sent on the redirected IP address and UDP port to signal the beginning of the file. The terminal implementation may either wait for this WRQ and obtain the data blocks of the file in order (starting from block number 1) or it may just pickup anywhere in the data carousel (not waiting for the WRQ) and it may download the file until all block numbers of that file have been received. There should be only one file per redirected IP address and port.

In the case that a new software is introduced for a certain terminal the server needs to first start the data carousel for this software and after that can start sending INFO messages. When the old software is withdrawn, the server should first stop sending the INFO messages and after that stop the data carousel.

A transfer may also be established by sending WRQ messages on the default multicast group and port, that the RCST keeps listening even after redirection. In this case the terminal will use the default multicast IP address and UDP port for obtaining the data stream.

If an INFO messages does not contain any redirection a write request is to be expected on the default multicast group and UDP port.

The default multicast group and UDP port are 239.192.0.1 and 49152 unless specified otherwise in the RCST configuration. The default port value is used as the default Transfer Identifier (TID) of TFTP.

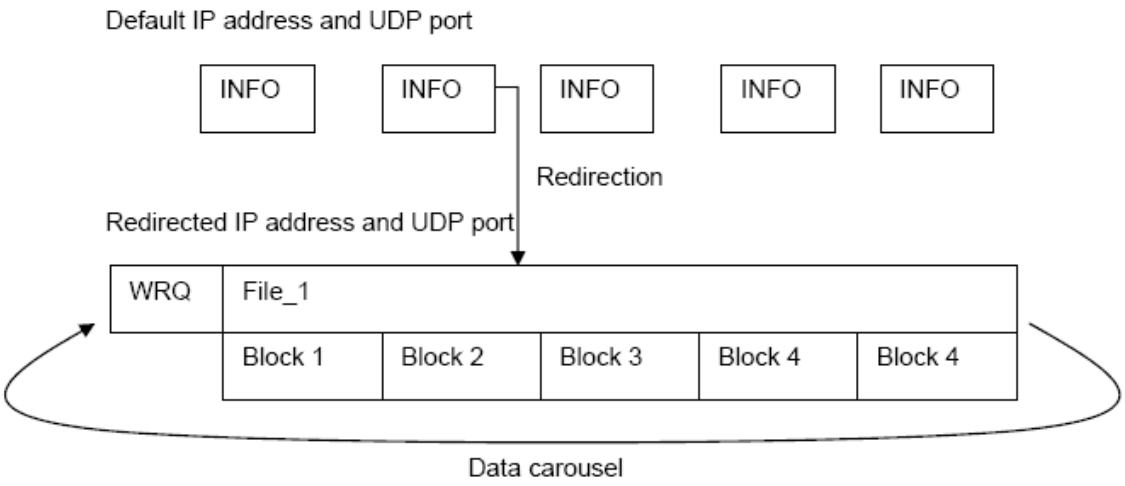


Figure C.6: SDDP redirection and carousel

C.9 Service Location

Once the IP/DVB service is identified, the RCST can map the multicast SVN-MAC label value used to identify the SDDP flow within a FL stream.

The SW update information channel can run alone on the default address (locally scoped, all systems) or can be multiplexed with a SW stream/carousel. SW streams can be separated into different multicast addresses that map to different IPv4 and hence different layer 2 address labels.

C.10 Signal Sequence and Timing

The RCST should be capable of receiving DATA packets at a pace of up to 50 kbps. This allows the RCST time to access the data storage. An RCST may have capability to support even higher rates. This is subject to manufacturer specification.

If the RCST has not received the next DATA packet within a given timeout (see timeout parameter in clause C.7) it has to terminate the file reception and it has to retune to the default multicast group and UDP port.

In the case that the RCST implementation waits for the WRQ before storing any data packets, the RCST is required to retune to the default multicast group and UDP port if such a request could not be received within 30 minutes.

An RCST that is not engaged in receiving DATA packets is required to be capable of decoding INFO packets and WRQ on its default multicast group and UDP port.

C.11 Flow Diagram for SDDP

The following procedure occurs every time the RCST initiates a logon procedure:

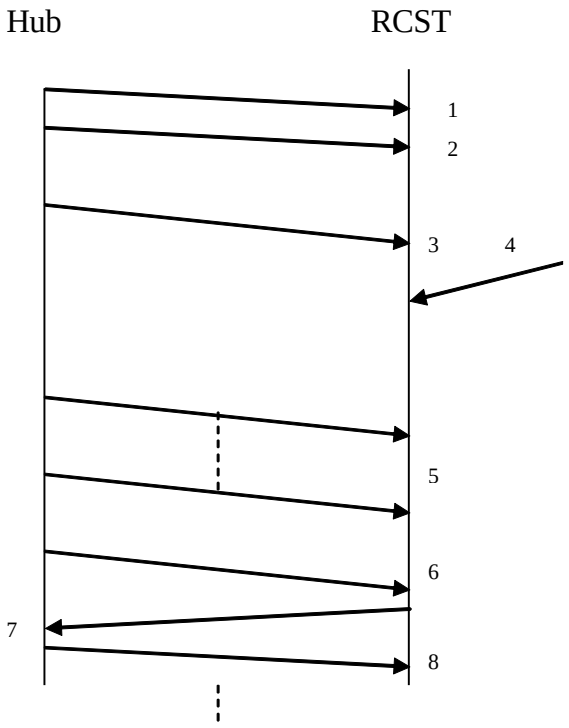


Figure C.7: SDDP flow diagram

1) An RCST in initialization mode tunes onto the FL.

2) It locates the appropriate L2 multicast SVN-MAC for SWDL.

3) It starts reception using the configured IPv4 multicast address and port (normally the default values) and decodes the stream. The stream may include manufacturer specific receiver redirection to another multicast address and port. It may also include additional vendor specific information.

4) The operator may directly set the multicast address and port to be used as entry point (can compensate for lack of redirection information).

5) The RCST sets the link-layer filter that allows it to receive IPv4 Multicast packets from a particular layer 2 SVN-MAC label., and the port where it expects to find SW update, and receives a file.

As SW update download is completed, the RCST replaces the alternate SW load with the new downloaded SW and updates the *dvbRcs2RCSTAlternateSoftwareVersion* MIB parameter (IETF RFC 5728 [i.59]).

6) In parallel the RCST will acquire the TBTP/TBTP2.

7) The RCST can send logon request in CSC slot.

8) The hub will respond with TIM-U.

Vendor specific configuration can prevent an RCST from logon until a given SW version has been downloaded. SW version can indeed be checked in the RCST capability field of the CSC burst (see DVB-RCS2). Otherwise the RCST logon will proceed in parallel with the SW download.

As an RCST continuously listens to the Forward Link Signalling, the SW download can be triggered at any time when multicast address and port are found.

C.12 Definition of multicast IP address

The SW information channel should be located on the default multicast address. Vendor specific redirection information should be located in this channel. Alternatively the target multicast address and port can be configured manually at the RCST.

The default multicast address should be under control by the network operator and should not be used for user traffic. It is within the local network control block address range. Note that if IGMP is in use on the FL general IGMP queries can also occur addressed to this address. These will not interfere with SDDP that uses UDP.

The hub should block user traffic on the multicast addresses assigned to SW update to avoid any possibility of conflict. It is e.g. possible to select custom SW update multicast addresses from the Organization Local Scope multicast addresses. Another possibility is to use non-conflicting addresses from the Local Network Control Block, but note that packets with these addresses will not be forwarded by IP routers.

Administratively Scoped IP Multicast (IETF RFC 2365 [i.26]) specifies:

239.192.0.0/14 is defined to be the IPv4 Organization Local Scope, and is the space from which an organization should allocate sub-ranges when defining scopes for private use.

C.13 Transfer Error Handling

The RCST should discard duplicate packets and should also detect missing packets through the consecutive block numbering. The SW acceptance process of the RCST should include vendor specific consistency control of the received data.

C.14 Vendor-Specific Methods

Additional vendor specific parameters may be included as required as in TFTP.

An RCST should ignore any unknown parameters.

C.15 Location of the Assigned Layer 2 Address

This clause specifies actions when operating in a transition mode. An RCST using a FL in the MPEG-TS mode will detect the PID on which it will listen for the SW update information stream in the following manner:

Before logon:

- directly on a layer with an address identified by MMT lookup.

After logon:

- through a direct address mapping to a multicast SVN-MAC label;
- through the Forward Interaction Path descriptor [1] received as logon response.

Annex D (normative): The Dynamic Connectivity Protocol (DCP)

D.0 Introduction

Dynamic Connectivity Protocol (DCP) is only considered normative for mesh profile.

Dynamic connectivity is supported for DVB-RCS2 under control of the Dynamic Connectivity Protocol (DCP) specified in this annex. Mesh RCS2 systems (transparent overlay and regenerative) shall support DCP for mesh link establishment and control.

DCP is a control protocol used between the NCC and the RCST, and also between RCSTs. The protocol is operative when IP connectivity with the NCC is achieved after lower layer RCST logon. DCP supports dynamic mapping of IP traffic and policies to L2, and supports to dynamically set up of one or several concurrent mesh links as required for this.

D.1 DCP Basics

The main function of the DCP protocol is to support dynamic connectivity. DCP is used as a dynamic link control protocol for regenerative Mesh DVB-RCS2 systems and transparent Mesh overlay DVB-RCS2 systems. Control messages may be exchanged over IPv4 protocol or directly over L2, between the NCC and the RCST, to achieve a dynamic Link. Control messages may also be exchanged directly between RCSTs over dynamic links. The RCST is informed of how to encapsulate DCP messages by the information in the Extension Protocol Descriptor specified in [1] in the Logon response.

DCP protocol stack is shown in figure D.1.

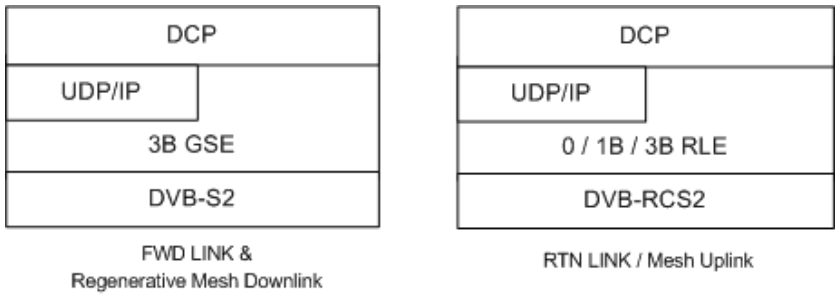


Figure D.1: DCP FWD/RTN protocol stacks

For L2 encapsulation mode, the NCC uses GSE over FWD link based using the SDU DCP protocol type given in table 5.1 "Some Recognized SDU protocol types" from ETSI EN 301 545-2 [1], and the RCST uses DCP compressed protocol type value over the RTN link following table 7.3 "Compressed protocol type values" from ETSI EN 301 545-2 [1].

In the case of transparent mesh overlay:

- 0B RLE applies if DCP is used in the default SVN for transparent mesh, on the RTN Link.
- 1B RLE applies if DCP is used in a non-default SVN for transparent mesh, on the RTN Link.
- 3B RLE applies if DCP is used on any Mesh Link, as currently depicted in the ETSI EN 301 545-2 [1].

In the case of regenerative mesh, not only the use of default SVN may impact on the RLE mode, but the different OBP switchin/routing types.

- 0B RLE applies if DCP is used in the default SVN for regenerative mesh and OBP physical layer or burst label switching mode, on the RTN Link.

- 1B RLE applies if DCP is used in a non-default SVN for regenerative mesh and OBP RLE packet or fragment switching mode, on the RTN Link.
- 3B RLE applies if DCP is used on any Mesh Link [1] and for regenerative mesh with OBP RLE packet or fragment or L3 packet switching/routing, as currently depicted in the LL guidelines [i.6].

The messages architecture stack is as shown in figures D.2 and D.3.

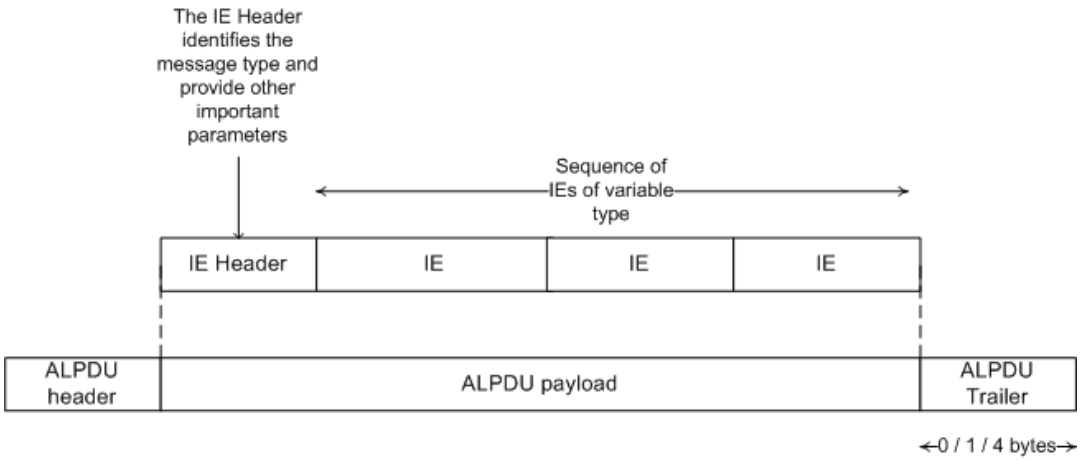


Figure D.2: DCP messages structure over L2

When DCP signalling is UDP/IPv4 based, standard logon procedures and the additional mesh_system_descriptor and extension_protocol_descriptor, are used. The messages architecture stack is as shown in figure D.2.

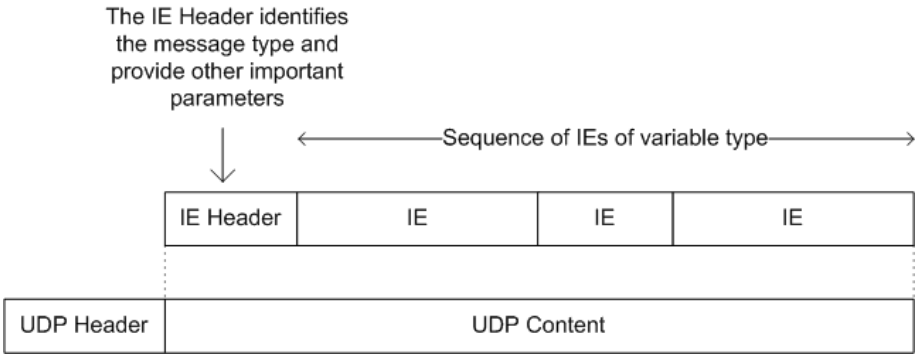


Figure D.3: DCP messages structure over UDP

Each message type is composed as a sequence of Information Elements and the first IE is a standard header present in each message type. The IE Header identifies the message type and provides other important parameters. The messages are transported using the UDP protocol.

The following IEs are defined for DCP.

Table D.1: Information Elements with reference to IE Type

IE type ID	Information Element Type (IE)	Comments
0x00	Common Message Header	Part of every message. Contains type uniquely identifying the message, address type and length for the entire message.
0x01	Status/Reason	Status/reason depending on the message type.
0x02	RCST Declaration	Information about RCST relevant for mesh as provided by the RCST itself at logon.
0x03	RCST Router declaration	Information about the LAN side IP subnets reachable via the specific RCST. Provided by the RCST itself at logon.
0x04	RCST Configuration	Mesh configuration parameters given to RCST at logon response.
0x05	DCP Address Space	Host addresses that shall be resolved by the Mesh Controller at the NCC.
0x06	Hub Link Address Space	Host addresses that shall be accessed via the hub link.
0x07	DCP System Parameter	System parameters as timeouts, etc.
0x08	Triggering datagram identifier	Information about the datagram initiating link service establishment as source and destination address, QoS class and assumed next hop.
0x09	Route Entries for link	Information about subnet that can be reached using a specific RCST.
0x0A	Assigned Link Identifier	Global link reference, request class and link service ID assigned to the link. Request class is local to RCST.
0x0B	Link Configuration	Configuration parameters such as type, duration, etc.
0x0C	RCST Uplink Transmission Profile	QoS Profile for the link service and Assignment ID for the transmitter.
0x0D	Uplink FPDU Identifier	TXID assigned to link service transmitter.
0x0E	Downlink FPDU Identifier	TXID assigned to link service receiver.
0x0F	Remote RCST Address	MAC24 addresses of the remote RCST.
0x10	Remote RCST identifiers	Group ID of the remote RCST, and the Assignment ID of the link service used by the remote RCST.
0x11	Checksum	CRC-32 in all messages, set as the last four bytes.
0x12	EsNo	8 bit indicating received Es/N0 from peer in keep-alive messages.
0x13	Control timers	Control timers for DCP logon, routes and links.
0x14-0x7F	Reserved	
0x80-0xFF	User defined	

D.2 DCP Messages

The minimum set of messages to implement a valid DCP is shown in the table D.2. The set of messages differs for the transparent mesh and regenerative mesh scenarios as indicated.

Table D.2: DCP Messages with reference to Message ID

ID	Signal /Message	MESH TRANSPARENT (M/O)	MESH REGENERATIVE (M/O)
0x00	Acknowledgement	M	M
0x01	DCP Logon Request	M	O
0x02	DCP Logon Response	M	O
0x03	Link Service Establishment Request by RCST	M	M
0x04	Link Service Establishment Response by NCC	M	M
0x03	Link Service Establishment Request by NCC	M	M
0x04	Link Service Establishment Response by RCST	M	M
0x05	Link Service Release Request	M	M
0x06	Link Service Release Response	M	M
0x07	Link Service Status Enquiry	M	O
0x08	Link Service Status Response	M	O
0x09	DCP Agent Management Request	M	O
0x0A	DCP Agent Management Response	M	O
0x0B	Link Service Keep-Alive	M	O
0x0C	Link Keep-Alive	M	O
0x0D-0x1F	Reserved		

D.3 Messages composition

Table D.3: DCP Messages composition and support in the two scenarios

ID	Signal/message	IE	Parameter Group	TRANSPARENT (M/O)	REGENERATIVE (M//O)
0x00	Acknowledgement			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x01	DCP Logon Request			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x02	RCST Declaration	M	M
		0x03	RCST Router Declaration	M	M
		0x11	Checksum	M	M
0x02	DCP Logon Response			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x04	RCST Configuration	M	M
		0x05	DCP Address Space	M	M
		0x06	Hub Link Address Space	M	M
		0x07	DCP System Parameters	M	M
		0x13	Control Timers	M	O
		0x11	Checksum	M	M
0x03	Link Service Establishment Request by RCST			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x08	Triggering Datagram Identifier	M	M

ID	Signal/message	IE	Parameter Group	TRANSPARENT (M/O)	REGENERATIVE (M//O)
		0x0C	RCST Uplink Transmission Profile	M	O
		0x11	Checksum	M	M
0x04	Link Service Establishment Response by NCC			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x09	Route Entries for Link	M	M
		0x0A	Assigned Link Identifiers	M	M
		0x0D	Uplink FPDU Identifier	M	M
		0x0E	Downlink FPDU Identifier	M	O
		0x0B	Link Configuration	M	M
		0x0C	RCST Uplink Transmission Profile	M	M
		0x0F	Remote RCST Address	M	M
		0x10	Remote RCST Identifiers	M	O
		0x11	Checksum	M	M
0x03	Link Service Establishment Request by NCC			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x09	Route Entries for Link	M	M
		0x0A	Assigned Link Identifiers	M	M
		0x0D	Uplink FPDU Identifier	M	O
		0x0E	Downlink FPDU Identifier	M	M
		0x0B	Link Configuration	M	O
		0x0C	RCST Uplink Transmission Profile	M	M
		0x0F	Remote RCST Address	M	M
		0x10	Remote RCST Identifiers	M	M
		0x11	Checksum	M	M
0x04	Link Service Establishment Response by RCST			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x0C	RCST Uplink Transmission Profile	M	O
		0x11	Checksum	M	M
0x05	Link Service Release Request			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x06	Link Service Release Response			M	M
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x07	Link Service Status Enquiry			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x08	Link Service Status Response			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x09	DCP Agent Management Request			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M

ID	Signal/message	IE	Parameter Group	TRANSPARENT (M/O)	REGENERATIVE (M//O)
0x0A	DCP Agent Management Response			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x0B	Link Service Keep-Alive			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x11	Checksum	M	M
0x0C	Link Keep-Alive			M	O
		0x00	Common Message Header	M	M
		0x01	Status/Reason	M	M
		0x12	EsNo	M	M
		0x11	Checksum	M	M

D.4 IEs composition

Table D.4: Common Message Header

Parameter Group	Parameter Name	Size (bits)	Value	
Common Message Header				
	IE Type	8	0x00	
	Message Type	5		See table D.24
	Address Type	3		See table D.9
	Message Length	16		Length of total message including all IEs
	IPv4 Address	32		From NCC: Source or remote RCST From RCST: Source
	Mesh Subnet ID	8		Layer 3 network
	SVN ID	16		Layer 2 network
	Link ID	16		SVN0 for generic M&C; User SVN for link specific
	Link Service ID	8		Indicates the QoS class

Table D.5: Message type

Parameter Group	Parameter Name	Size (bits)	Value	
Status/Reason				
	IE Type	8	0x01	
	Status/Reason	8		See table D.26

Table D.6: RCST Declaration

Parameter Group	Parameter Name	Size (bits)	Value	
RCST Declaration				
	IE Type	8	0x02	
	Hardware ID	48		
	DCP version	8		
	Mesh Capability Map	32		See table D.25
	Transmitter Power Class	8		
	BRX Fan-In	8		Number of concurrent bursts that may be decoded
	Max Concurrent Links	16		Number of concurrent dynamic links
	Reserved	40		

Table D.7: RCST Router Declaration

Parameter Group	Parameter Name			Size (bits)	Value
RCST Router declaration					
	IE Type			8	0x03
	Number of SVNs			8	
	SVN loop				
		SVN ID		16	
		Number of Subnets		8	
		Subnets loop			
			IPv4 Base Address	32	
			Subnet Mask	8	
			Metric	8	
	Reserved			112	

Table D.8: RCST Configuration

Parameter Group	Parameter Name		Size (bits)	Value	
RCST Configuration					
	IE Type		8	0x04	
	Primary default GW		32		
	Secondary default GW		32		
	Alternate secondary default GW		32		
	Number of LQC profiles		8		
	LQC Profiles Loop				
		LQC Index	8		QoS service
		CRA	16		
		RBDC max	16		
		RBDC min	16		
		VBDC max backlog	16		
		Reserved	16		
	Reserved		112		

Table D.9: DCP Address Space

Parameter Group	Parameter Name			Size (bits)	Value	
DCP Address Space						
	IE Type			8	0x05	
	Number of SVNs			8		
	SVN loop					
		SVN ID		16		
		Mesh Subnet ID		8		
		Mesh Subnet Name		128		16 characters
		Number of subnets		8		
		Subnets loop				
			Base Address	32		
			Subnet Mask	8		
			Metric	8		
			CBR LQC Map	8		Flags indicating applicability for QoS clases
			Route Duration Type	8		See table D.27
			Reserved	8		
	Reserved			16		

Table D.10: Hub Link Address Space

Parameter Group	Parameter Name			Size (bits)	Value	
Hub Link Address Space						
	IE Type			8	0x06	
	Number of SVNs			8		
	SVN loop					
		SVN ID		16		
		Number of subnets		8		
		Subnets loop				
			Base Address	32		
			Subnet Mask	8		
			Metric	8		
			CBR LQC Map	8		Flags indicating applicability for QoS clases
			Route Duration Type	8		See table D.27
			Reserved	8		
	Reserved			16		

Table D.11: DCP System Parameters

Parameter Group	Parameter Name	Size (bits)	Value	
DCP System Parameters				
	IE Type	8	0x07	
	DCP Multicast Address	32		
	DCP Multicast Port	16		
	Protocol Version	8		
	System Options	8		See table D.28
	Reserved	32		

Table D.12: Triggering Datagram Identifier

Parameter Group	Parameter Name	Size (bits)	Value	
Triggering datagram identifier				
	IE Type	8	0x08	
	Size of IE	8		extendable IE
	Soure address	32		
	Destination Address	32		
	Next hop address	32		
	Reserved	0		

Table D.13: Route Entries for Link

Parameter Group	Parameter Name		Size (bits)	Value	
Route Entries for link					
	IE Type		8	0x09	
	Next Hop Address		32		
	CBR LQC Map		8		Flags indicating applicability for QoS clases
	Route duration type		8		See table D.27
	Number of subnets		8		
	Subnets loop				
		Base Address	32		
		Subnet Mask	8		
		Metric	8		
		Reserved	8		
	Reserved		16		

Table D.14: Assigned Link Identifiers

Parameter Group	Parameter Name	Size (bits)	Value
Assigned Link Identifiers			
	IE Type	8	0x0A
	Global Link Reference	16	
	Request Class	16	
	Link QoS Class	8	
	Reserved	16	

Table D.15: Link Configuration

Parameter Group	Parameter Name	Size (bits)	Value	
Link Configuration				
	IE Type	8	0x0B	
	Link type	4		See table D.29
	Link duration type	4		See table D.30
	Link options	32		See table D.31
	Downlink interface type	16		IANA types; TDM-240, TDMA - 241; 0 indicates that the downlink is not in use
	Uplink interface type	16		IANA types; TDMA - 241; 0 indicates that the uplink is not in use
	Reserved	16		

Table D.16: RCST Uplink Transmission Profile

Parameter Group	Parameter Name	Size (bits)	Value	
RCST Uplink Transmission Profile				
	IE Type	8	0x0C	
	Constant Service Rate	16		
	Maximum Service Rate	16		
	Minimum Service Rate	16		
	VBDC maximum backlog	16		
	Assignment ID	16		Used to tag useful slots
	Reserved	16		

Table D.17: Uplink FPDU Identifier

Parameter Group	Parameter Name	Size (bits)	Value	
Uplink FPDU Identifier				
	IE Type	8	0x0D	
	Reserved	8		
	TXID	16		Used in the Payload label

Table D.18: Downlink FPDU Identifier

Parameter Group	Parameter Name	Size (bits)	Value	
Downlink FPDU Identifier				
	IE Type	8	0x0E	
	Reserved	8		
	TXID	16		Used in the Payload label

Table D.19: Remote RCST Address

Parameter Group	Parameter Name	Size (bits)	Value	
Remote RCST Address				
	IE Type	8	0x0F	
	M&C MAC24	24		M&C MAC address of the remote RCST
	User MAC24	24		User MAC address of the remote RCST

Table D.20: Remote RCST Identifiers

Parameter Group	Parameter Name	Size (bits)	Value	
Remote RCST identifiers				
	IE Type	8	0x10	
	Group ID	8		
	Assignment ID	24		
	RPLS	16		Physical Layer Segment monitored by the remote RCST
	Reserved	16		

Table D.21: Checksum

Parameter Group	Parameter Name	Size (bits)	Value	
Checksum				
	IE Type	8	0x11	
	Checksum	32		Calculated over complete message except the last 32 bits, using same method as for RLE

Table D.22: EsNo Message

Parameter Group	Parameter Name	Size (bits)	Value	
EsNo				
	IE Type	8	0x12	
	EsNo	8		As for CMT/CMD; normalized to lowest symbol-rate

Table D.23: Control Timers Message

Parameter Group	Parameter Name	Size (bits)	Value	
Control timers				
	IE Type	8	0x13	
	Short Link Duration	8		Minutes
	Long Link Duration	8		Minutes
	Short Link Idle Time	8		Seconds
	Long Link Idle Time	8		Seconds
	Short Route Duration	8		Minutes
	Long Route Duration	8		Minutes
	Control Request Timeout	8		Seconds
	Control Response Timeout	8		Seconds
	Other signal timeout	8		Seconds
	Short holdoff	8		Minutes. Applied when Mesh Controller rejects link establishment due to a temporary condition; duration of a temporary route blocking entry; flush buffer at blocking; give "destination unreachable" and drop packets
	Long holdoff	8		Minutes
	Reserved	32		

D.5 IE field coding details

Table D.24 indicates the interpretation of different values of specific fields of the IEs.

Table D.24: Addressing type

IE Fields	bits	Comments	Value
Addressing type	3		
		IPv4 user IP addressing	0x00
		IPv6 user IP addressing	0x01
		Ethernet user packet addressing	0x02
		Reserved	0x03-0x06
		User Defined	0x07

Table D.25: Mesh capability field coding

Mesh capability	Size(bits)	Capability	Bit
Mesh Capability	32	Mesh LQC index 0	0
		Mesh LQC index 1	1
		Mesh LQC index 2	2
		Mesh LQC index 3	3
		Mesh LQC index 4	4
		Mesh LQC index 5	5
		Mesh LQC index 6	6
		Mesh LQC index 7	7
		In-band link quality reporting	8
		Link Power control	9
		Reserved	10
		Non-volatile links and routes	11
		IP/UDP/RTP compression	12
		Reserved	13-24
		User Defined	25-31

Table D 26: Status/Reason

IE Fields	bits	Comments	Value
Status/Reason	8	Message with undefined status and reason	0x00
		Response to inconsistent message	0x01
		Logon reject: unauthorised logon	0x02
		Logon OK	0x03
		Logon OK, clear all links and routes	0x04
		Normal Logon Request	0x05
		Re-logon due to LAN subnets change	0x06
		Reserved	0x07-0x0A
		Unspecified Link Request	0x10
		Link request due to new traffic	0x11
		Previous attempt failed on timeout	0x12
		Link request due to link failure	0x13
		Permanent link	0x14
		Next hop rejected on previous request	0x15
		Link request due to new traffic (resend)	0x16
		Link request MCAST configuration update	0x17
		Reserved	0x18-0x2F
		Link establishment in progress	0x30
		Link complete	0x31
		Link establishment accept	0x32
		Link establishment accept with reduction of profile	0x33
		Reserved	0x34-0x3F

		Link rejected due to inconsistent message	0x40
		Link rejected with reroute to indicated next-hop	0x41
		Link rejected due to incorrect next hop	0x42
		Link rejected due to insufficient privileges	0x43
		Link rejected due to network congestion	0x44
		Link rejected due to temporary endpoint congestion	0x45
		Link rejected due to unreachable destination (temporary)	0x46
		Link rejected due to unreachable destination (permanent)	0x47
		Link reject due to lack of resources	0x48
		Link rejected without specific reason	0x49
		Reserved	0x4A-0x6F
		Release request due to timeout	0x70
		Release request due to idle link	0x71
		Release request without specific reason	0x72
		Release request due to system failure	0x73
		Release request due to link error	0x74
		Reserved	0x75-0x8F
		Release in progress	0x90
		Link ID not known	0x91
		Link released	0x92
		Clear all dynamic link and routes	0xA0
		Clear all session data and logon	0xA1
		Clear all session data and go to star-only state	0xA2
		Leave star-5 only state and logon to Mesh Controller	0xA3
		Clear the link with given ID and all routes to the next hop identified by the link ID	0xA4
		Reserved	0xA5-0xAF
		Keep-Alive	0xB0
		Reserved	0xB1-0xDF
		User Defined	0xE0-0xFF

Table D.27: Route duration type

IE Fields	bits	Comments	Value
Route duration type	8	Unlimited	0x00
		Short limit	0x01
		Long limit	0x02
		Tied to link	0x03
		Reserved	0x04-0x0E
		Permanent route for automatic reestablishment.	0x0F
		Reserved	0x10-0x7F
		User defined	0x80-0xFF

Table D.28: System options field coding

System options	Size(bits)	Option	Bit
System options enabling	8	Reserved	0
		Reserved	1
		Mesh link quality feedback	2
		Reserved	3-5
		User defined	6-7

Table D.29: Link type coding

Link Type	Size(bits)	Value/Code	
Link types	4	Bi-directional TDMA	0x00
		Downlink TDMA	0x01
		Uplink TDMA	0x02
		Downlink TDM, Uplink TDMA	0x03
		Downlink TDM	0x04
		Reserved	0x05-0x0D
		User Defined	0x0E-0x0F

Table D.30: Link duration coding

Link Duration	Size(bits)	Value/Code	
Link duration	4	No autonomous release	0x00
		Release after short idle	0x01
		Release after long idle	0x02
		Release after short duration	0x03
		Release after long duration	0x04
		Release after short duration or short idle, whatever occurs first	0x05
		Release after long duration or long idle, whatever occurs first	0x06
		Sustain for a short duration and then release after a short idle	0x07
		Sustain for a long duration and then release after a long idle	0x08
		Reserved	0x09-0x0D
		User Defined	0x0E
		Permanent link for automatic reestablishment (non-volatile)	0x0F

Table D.31: Link options coding

Link Options	Size(bits)	Option	Bit
Link options	32	Apply in-band link quality reporting	0
		Apply power control	1
		Reserved	2
		Use cRTP	3
		PEP-TCP allowed	4
		PEP-HTTP allowed	5
		Reserved	6-24
		User Defined	25-31

Annex E (normative):
Antenna Alignment message data formats

E.0 Introduction

Table E.1 shows all required Message Data Formats to control the motorized mount. The table includes the meaning, format and possible Data values for the Command Bytes.

Table E.1: Motorized Mount Command Bytes

Byte 1 Framing Byte	Byte 2 Address Byte	Byte 3 Command Byte	Byte 4 Data Byte	Byte 5 Data Byte
E0	31	60 Stop azimuth Positioned movement.	00 Example; E0 31 60 00 Stops the azimuth Positioner.	Not used
"	"	6B Drive motor to Reference Position (Reset position).	00 Example; E0 31 6B 00 Moves the azimuth Positioner to Reference Position (Reset position).	Not used
"	"	6C Goto x.x°, drive motor to x.x°. Store current motor position.	**WX,** where **W** = **D**; for **Anticlockwise** Rotation **W** = **E**; for **Clockwise** Rotation **XY** = hexadecimal value of **integer** part of the azimuth angle. **Z** = hexadecimal value of **decimal** part of the azimuth angle (see table in clause 7.3.X.1). Special command; E0 31 6C A0 00 - Stores the azimuth Positioner actual position. Example; E0 31 6C E0 03 Rotates the azimuth Positioner 0,2° clockwise from the current position.	**YZ,** See left
"	"	6E Goto x.x°. Drive motor to x.x° from Reference Position.	**WX,** where **W** = **D**; for **Anticlockwise** Rotation **W** = **E**; for **Clockwise** Rotation **XY** = hexadecimal value of **integer** part of the azimuth angle. **Z** = hexadecimal value of **decimal** part of the azimuth angle (see table in clause 7.3.X.1). Example; E0 31 6E E0 95 Rotates azimuth Positioner 9,3° clockwise from Reference Position.	**YZ,** See left
"	32	60 Stop elevation Positioner movement.	00 Example; E0 32 60 00 Stops the elevation Positioner.	Not used
"	"	6B Drive motor to Reference Position (Reset position).	00 Example; E0 32 6B 00 Moves the elevation Positioner to Reference Position (Reset position).	Not used

Byte 1 Framing Byte	Byte 2 Address Byte	Byte 3 Command Byte	Byte 4 Data Byte	Byte 5 Data Byte
"	"	6C Goto x.x°, drive motor to x.x°. Store current motor position.	**WX,** where **W** = **D**; for **Down** Rotation **W** = **E**; for **Up** Rotation **XY** = hexadecimal value of **integer** part of the elevation angle. **Z** = hexadecimal value of **decimal** part of the elevation angle (see table in clause 7.3.X.1). Special command; E0 32 6C A0 00 - stores the elevation Positioner actual position. Example; E0 32 6C E0 03 Moves up elevation Positioner 0,2° from the current position.	**YZ,** See left
"	"	6E Goto x.x° Drive motor to x.x° from Reference Position.	**WX,** where **W** = **D**; for **Down** Rotation **W** = **E**; for **Up** Rotation **XY** = hexadecimal value of **integer** part of the elevation angle. **Z** = hexadecimal value of **decimal** part of the elevation angle (see table in clause 7.3.X.1). Example; E0 32 6E E0 95 Moves elevation Positioner up 9,3° from the Reference Position.	**YZ,** See left
"	21	60	00 Stop skew Positioner movement	Not used
"	"	6B Drive motor to Reference Position (Reset position).	00 Example; E0 21 6B 00 Drive motor to Reference skew position (Reset position).	Not used
"	"	6C Goto x.x°, drive motor to x.x°. Store current motor position.	**WX,** where **W** = **D**; for **Anticlockwise** Rotation (looking from behind dish towards satellite) **W** = **E**; for **Clockwise** Rotation **XY** = hexadecimal value of **integer** part of the elevation angle. **Z** = hexadecimal value of **decimal** part of the elevation angle (see table in clause 7.3.X.1). Special command; E0 21 6C A0 00 - stores the skew Positioner actual position. Example; E0 21 6C E0 03 Moves skew Positioner 0,2° clockwise from the current position.	**YZ,** See left

Byte 1 Framing Byte	Byte 2 Address Byte	Byte 3 Command Byte	Byte 4 Data Byte	Byte 5 Data Byte
"	"	6E Goto x.x° Drive Motor to x.x° from Reference Position.	**WX,** where **W** = **D**; for **Anticlockwise** Rotation (looking from behind dish towards satellite) **W** = **E**; for **Clockwise** Rotation **XY** = hexadecimal value of **integer** part of the azimuth angle. **Z** = hexadecimal value of **decimal** part of the azimuth angle (see table in clause 7.3.X.1). Example; E0 21 6E E0 95 Rotates skew Positioner 9,3° clockwise from Reference Position.	**YZ,** See left

E.1 Hexadecimal value for the decimal part

Table E.2: Hexadecimal value

Decimal	Hex	Decimal	Hex
0,0°	0	0,5°	8
0,1°	2	0,6°	A
0,2°	3	0,7°	B
0,3°	5	0,8°	D
0,4°	6	0,9°	E

The hexadecimal value for the decimal part of the azimuth, elevation or skew angle (=Z) is in accordance with table E.2.

E.2 Stored position

The command to store the position of the azimuth Positioner is E0316CA000, for elevation Positioner it is E0326CA000 and for skew Positioner it is E0216CA000. At the moment of sending these commands the motorized mount stores internally the actual positions.

To move the Positioners into these stored positions the commands are E0316CD000 for azimuth Positioner, E0326CD000 for elevation Positioner and E0216CD000 for skew Positioner.

E.3 Reference position (reset position)

The motorized mount Reference Positions (Reset Positions) are fixed, factory set positions for the elevation, azimuth and skew Positioners.

The Azimuth Reference Position is the midpoint of the movement range of the azimuth axis. For a terminal pointed correctly it would correspond to pointing directly South/North (depending on installation being on Northern/Southern hemisphere).

The Elevation Reference Position is defined as the tangent line on the Earth surface of the place of installation. For a motorized mount perfectly on a vertical pole it would correspond to pointing directly towards the horizon.

The Skew Reference Position is the position when the skew is aligned with the vertical polarization being exactly normal to the horizon.

Annex F (informative): Bibliography

ETSI TS 102 292: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks".

ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB Systems".

ETSI EN 301 192: "Digital Video Broadcasting (DVB); DVB specification for data broadcasting".

ETSI TS 102 294: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; IP interworking via satellite; Multicast functional architecture".

ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Services and architectures".

ETSI TS 102 357: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Common Air interface specification; Satellite Independent Service Access Point SI-SAP".

IETF RFC 1633: "Integrated Services in the Internet Architecture: an Overview", Braden, R., Clark, D., and S. Shenker, June 1994.

IETF RFC 2210: "The Use of RSVP with IETF Integrated Services",Wroclawski, J., September 1997.

IETF RFC 2211: "Specification of the Controlled-Load Network Element Service",Wroclawski, J., September 1997.

IETF RFC 2212: "Specification of Guaranteed Quality of Service", Shenker, S., Partridge, C., and R. Guerin, September 1997.

IETF RFC 2578: "Structure of Management Information, Version 2 (SMIv2)", McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., STD 58, April 1999.

IETF RFC 2597: "Assured Forwarding PHB Group", Heinanen, J., Baker, F., WeRcs2, W., and J. Wroclawski, June 1999.

IETF RFC 2697: "A Single Rate Three Color Marker", Heinanen, J. and R. Guerin, September 1999.

IETF RFC 2858: "Multiprotocol Extensions for BGP-4", Bates, T., Rekhter, Y., Chandra, R., and D. Katz, June 2000.

IETF RFC 2996: "Format of the RSVP DCLASS Object", Bernet, Y., November 2000.

IETF RFC 3164: "The BSD Syslog Protocol", Lonvick, C., August 2001.

IETF RFC 3181: "Signaled Preemption Priority Policy Element", Herzog, S., October 2001.

IETF RFC 3246: "An Expedited Forwarding PHB (Per-Hop Behavior)", Davie, B., Charny, A., Bennet, J.C., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, March 2002.

IETF RFC 3247: "Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)", Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney, W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, March 2002.

IETF RFC 3261: "SIP: Session Initiation Protocol", Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E.,Schooler, June 2002.

IETF RFC 3290: "An Informal Management Model for Diffserv Routers", Bernet, Y., Blake, S., Grossman, D., and A. Smith, May 2002.

IETF RFC 3312: "Integration of Resource Management and Session Initiation Protocol (SIP)",Camarillo, G., Marshall, W., and J. Rosenberg, October 2002.

IETF RFC 4259: "A Framework for transmission of IP Datagrams over MPEG-2 Networks", Montpetit, M.-J., Fairhurst, G., Clausen, H., Collini-Nocker, B., and H. Linder, November 2005.

IETF RFC 4760: "Multiprotocol Extensions for BGP-4", Bates, T., Chandra, R., Katz, D., and Y. Rekhter, January 2007.

"Internet Assigned Numbers Authority", Internet Assigned Numbers Authority, June 2008.

NOTE: Available at http://www.iana.org.

History

Document history		
V1.1.1	May 2012	Publication
V1.2.1	April 2014	Publication
V1.3.1	February 2020	BlueBook update – Draft V1.3.1