Data-Over-Cable Service Interface Specifications
DCA - MHAv2

Remote PHY Specification

CM-SP-R-PHY-I01-150615

ISSUED

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number	CM-SP-R-PHY-I01-150615			
Document Title	Remote PHY Specification			
Revision History	I01 - Released 06/15/2015			
Date:	June 15, 2015			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document designed to guide discussion and generate feedback, and may include several alternative solutions for consideration.
Draft	A document in Specification format considered largely complete, but lacking review by Members and Technology Suppliers. Drafts are susceptible to substantial change during the review process.
Issued	A generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is available for Certification testing. Issued Specifications are subject to the Engineering Change (EC) Process.
Closed	A static document, reviewed, tested, validated, and closed to further ECs.

Trademarks

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

1 SCOPE

1.1 Introduction and Purpose

Modular Headend Architecture version 2 (MHAv2)/Remote PHY technology allows a CMTS to support an IP-based digital HFC plant. In an IP-based digital HFC plant, the fiber portion utilizes a baseband network transmission technology such as Ethernet, EPON (Ethernet over Passive Optical Networks), GPON (Gigabit Passive Optical Network), or any Layer 2 technology that would support a fiber-based Layer 1. MHAv2 uses a Layer 3 pseudowire between a CCAP-Core and a series of Remote PHY devices. One of the common locations for a Remote PHY device at an optical node device that is located at the junction of the fiber and coax plants.

1.2 MHAv2 Interface Documents

A list of the documents in the MHAv2 family of specifications is provided below. For updates, refer to http://www.cablelabs.com/specs/specification-search/.

Designation	Title
CM-SP-R-PHY	Remote PHY Specification
CM-SP-R-DEPI	Remote Downstream External PHY Interface Specification
CM-SP-R-UEPI	Remote Upstream External PHY Interface Specification
CM-SP-GCP	Generic Control Plane Specification
CM-SP-R-DTI	Remote DOCSIS Timing Interface Specification
CM-SP-R-OOB	Remote Out-of-Band Specification
CM-SP-R-OSSI	Remote PHY OSS Interface Specification

NOTE: MHAv2 does not explicitly use any of the original Modular Headend Architecture specifications.

1.3 Requirements and Conventions

In this specification, the following convention applies any time a bit field is displayed in a figure. The bit field should be interpreted by reading the figure from left to right, then from top to bottom, with the MSB being the first bit to read and the LSB being the last bit to read.

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

At the time of publication, the editions indicated were valid. All references are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific. For a nonspecific reference, the latest version applies.

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

[CANN]	CableLabs' Assigned Names and Numbers, CL-SP-CANN-I13-150515, May 15, 2015, Cable Television Laboratories, Inc.
[CCAP-OSSI v3.1]	DOCSIS 3.1 CCAP OSSI Specification, CM-SP-CCAP-OSSIv3.1-I04-150611, June 11, 2015, Cable Television Laboratories, Inc.
[CM-OSSI v3.1]	DOCSIS 3.1 Cable Modem OSSI Specification, CM-SP-CM-OSSIv3.1-I04-150611. June 11, 2015, Cable Television Laboratories, Inc.
[DEPI]	Downstream External PHY Interface Specification, CM-SP-DEPI-I08-100611, June 11, 2010, Cable Television Laboratories, Inc.
[DRFI]	DOCSIS Downstream Radio Frequency Interface, CM-SP-DRFI-I14-131120, November 20, 2013, Cable Television Laboratories, Inc.
[FIPS 140-2]	Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, May 2001.
[FIPS 180-4]	Federal Information Processing Standards Publication (FIPS PUB) 180-4, Secure Hash Standard, May 2014.
[GCP]	Generic Control Plane Specification, CM-SP-GCP-I01-150615, June 15, 2015, Cable Television Laboratories, Inc
[IANA-PORTS]	IANA, Port Numbers, June 2004.
[IEEE 802.1ae]	IEEE Std 802.1ae-2006, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security, August 2006.
[IEEE 802.1q]	IEEE Std 802.1q-2003, Virtual Bridged Local Area Networks, May 2003.
[IEEE 802.1x]	IEEE Std 802.1x-2010, IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, February 2010.
[IEEE 802.3]	IEEE Std 802.3™-2002, Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, March 2002.
[IEEE 1588]	IEEE Std 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, July 2008.
[ISO 13818-1]	ISO/IEC 13818-1:2013, Information Technology - Generic Coding of Moving Pictures and Associated Audio Information. Part 1: System, May 23, 2013.
[ITU-T J.83]	ITU-T Recommendation J.83 (4/97), Digital multi-programme systems for television sound and data services for cable distribution.
[MULPI v3.0]	DOCSIS MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-I27-150528, March 5, 2015, Cable Television Laboratories, Inc.
[MULPI v3.1]	DOCSIS MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.1-I06-150611, June 11, 2015, Cable Television Laboratories, Inc.
[PHY v3.0]	DOCSIS 3.0 Physical Layer Specification, CM-SP-PHYv3.0-I26-150305, March 5, 2015, Cable Television Laboratories, Inc.

[PHY v3.1]	DOCSIS 3.1 Physical Layer Specification, CM-SP-PHYv3.1-I06-150611, June 11, 2015, Cable Television Laboratories, Inc.
[SECv3.0]	DOCSIS 3.0 Security Specification, CM-SP-SECv3.0-I15-130808, August 8, 2013, Cable Television Laboratories, Inc.
[SECv3.1]	DOCSIS 3.1 Security Specification, CM-SP-SECv3.1-I03-150611, June 11, 2015, Cable Television Laboratories, Inc.
[PKCS#7]	RSA Laboratories, PKCS #7: Cryptographic Message Syntax Standard, An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993.
[R-DEPI]	Remote Downstream External PHY Interface Specification, CM-SP-R-DEPI-I01-150615, June 15, 2015, Cable Television Laboratories, Inc.
[R-DTI]	Remote DOCSIS Timing Interface Specification, CM-SP-R-DTI-I01-150615, June 15, 2015, Cable Television Laboratories, Inc.
[R-OOB]	Remote Out-of-Band Specification, CM-SP-R-OOB-I01-150615, June 15, 2015, Cable Television Laboratories, Inc.
[R-OSSI]	Remote PHY OSS Interface Specification, CM-SP-R-OSSI-D02-150408, April 8, 2015, Cable Television Laboratories, Inc.
[R-UEPI]	Remote Upstream External PHY Interface Specification, CM-SP-R-UEPI-I01-150615, June 15, 2015, Cable Television Laboratories, Inc.
[RFC 768]	IETF RFC 768, User Datagram Protocol, August 1980.
[RFC 791]	IETF RFC 791, Internet Protocol-DARPA, September 1981.
[RFC 868]	IETF RFC 768, Time Protocol, May 1983.
[RFC 1191]	IETF RFC 1191, MTU Path Discovery, November 1990.
[RFC 1350]	IETF RFC 1350, The TFTP Protocol (Revision 2), July 1992.
[RFC 1945]	IETF RFC 1945, Hypertext Transfer Protocol -- HTTP/1.0, May 1996.
[RFC 1981]	IETF RFC 1981, Path MTU Discovery for IP version 6, August 1996.
[RFC 2131]	IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.
[RFC 2348]	IETF RFC 2348, TFTP Blocksize Option, May 1998.
[RFC 2597]	IETF RFC 2597, Assured Forwarding PHB Group, June 1999.
[RFC 2616]	IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, June 1999.
[RFC 2983]	IETF RFC 2983, Differentiated Services and Tunnels, October 2000.
[RFC 3246]	IETF RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior), March 2002.
[RFC 3260]	IETF RFC 3260, New Terminology and Clarifications for Diffserv, April 2002.
[RFC 3308]	IETF RFC 3308, Layer Two Tunneling Protocol (L2TP) Differentiated Services Extension, November 2002.
[RFC 3748]	IETF RFC 3748, Extensible Authentication Protocol (EAP)
[RFC 3931]	IETF RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3), March 2005.
[RFC 4131]	IETF RFC 4131, Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus, September 2005.
[RFC 4307]	IETF RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), December 2005.
[RFC 5216]	IETF RFC 5216, IEAP-TLS Authentication Protocol, March 2008.
[RFC 5247]	IETF RFC 5247, EAP Key Management Framework, August 2008.
[RFC 5280]	IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[RFC 6960]	IETF RFC 6960, I.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 2013.
[RFC 7296]	IETF RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2), October 2014.
[RSA 1]	RSA Laboratories, PKCS #1: RSA Encryption Standard. Version 1.5, RSA Security, Inc., Bedford, MA, November 1993.
[RSA 3]	RSA Laboratories, PKCS #3: Diffie-Hellman Key Agreement Standard, Version 1.4, RSA Security, Inc., Bedford, MA, November 1993.
[Vendor ID]	Refers to RFC 3232 "Assigned Number" by the IETF, Jan 2002. This spec refers to the IANA web page which is http://www.iana.org/assignments/enterprise-numbers.
[X.509]	ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks, March 2000.

2.2 Informative References

This document uses the following informative references:

[IANA-L2TP]	IANA, Layer Two Tunneling Protocol (L2TP) Parameters.
[ISO 8802-2]	ISO/IEC 8802-2: 1994 (IEEE Std 802.2: 1994) - Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2: Logical link control.
[RFC 3140]	IETF RFC 3140, Per Hop Behavior Identification Codes, June 2001.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Federal Information Processing Standards: 100 Bureau Drive, Mail Stop 3200, Gaithersburg, MD 20899-3200. Phone +1-301-975-4054; Fax +1-301-926-8091. http://csrc.nist.gov/publications/fips/.
- The Institute of Electrical and Electronics Engineers, Inc., Internet: http://standards.ieee.org
- International Organization for Standardization (ISO), Tel.: +41 22 749 02 22, Fax: +41 22 749 01 55, www.standardsinfo.net
- Internet Assigned Numbers Authority, IANA, Internet: http://www.iana.org
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001. http://www.ietf.org.
- ITU Recommendations: Place des Nations, CH-1211, Geneva 20, Switzerland. Phone +41-22-730-51-11; Fax +41-22-733-7256. http://www.itu.int.
- Public Key Cryptography Standards: RSA Security Inc. 174 Middlesex Turnpike, Bedford, MA 01730. Phone +1-781-515-5000; Fax 781-515-5010. http://www.rsasecurity.com/rsalabs/.
- SCTE, Society of Cable Telecommunications Engineers, 140 Philips Road, Exton, PA 19341-1318, Phone+1-800-542-5040; Fax+1-610-363-5898. http://www.scte.org/default.aspx/.

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Bonded Channels	A logical channel comprising multiple individual channels.
Cable Modem (CM)	A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.
CCAP-Core	A CCAP device that uses MHAv2 protocols to interconnect to an RPD.
Converged Interconnect Network	The network (generally gigabit Ethernet) that connects a CCAP-Core to an RPD.
Customer Premises Equipment (CPE)	Equipment at the end user's premises; may be provided by the service provider.
Data Rate	Throughput, data transmitted in units of time usually in bits per second (bps).
Decibels (dB)	Ratio of two power levels expressed mathematically as $dB = 10\log_{10}(P_{OUT}/P_{IN})$.
Decibel-Millivolt (dBmV)	Unit of RF power expressed in decibels relative to 1 millivolt, where $dBmV = 20\log^{10}$(value in mV/1 mV).
Downstream (DS)	• Transmissions from CMTS to CM. This includes transmission from the CCAP-Core to the EQAM, as well as the RF transmissions from the EQAM to the CM • RF spectrum used to transmit signals from a cable operator's headend or hub site to subscriber locations.
Dynamic Host Configuration Protocol (DHCP)	A network protocol enabling a server to automatically assign an IP address to a network element.
Edge QAM Modulator (EQAM)	A headend or hub device that receives packets of digital video or data. It re-packetizes the video or data into an MPEG transport stream and digitally modulates the digital transport stream onto a downstream RF carrier using quadrature amplitude modulation (QAM).
Flow	A stream of packets in DEPI used to transport data of a certain priority from the CCAP-Core to a particular QAM channel of the EQAM. In PSP operation, there can exist several flows per QAM channel.
Gbps	Gigabits per second
Gigahertz (GHz)	A unit of frequency; 1,000,000,000 or 10^9 Hz
GigE (GE)	Gigabit Ethernet (1 Gbps)
Hertz (Hz)	A unit of frequency; formerly cycles per second
Hybrid Fiber/Coax (HFC) System	A broadband bidirectional shared-media transmission system using optical fiber trunks between the headend and the fiber nodes, and coaxial cable distribution from the fiber nodes to the customer locations.
Institute of Electrical and Electronic Engineers (IEEE)	A voluntary organization which, among other things, sponsors standards committees and is accredited by the American National Standards Institute (ANSI).
Internet Engineering Task Force (IETF)	A body responsible for, among other things, developing standards used in the Internet.
Internet Protocol (IP)	An Internet network-layer protocol
kilohertz (kHz)	Unit of frequency; 1,000 or 10^3 Hz; formerly kilocycles per second
L2SS	Layer 2 Specific Sublayer. DEPI is an L2SS of L2TPv3.

L2TP Access Concentrator (LAC)	If an L2TP Control Connection Endpoint (LCCE) is being used to cross-connect an L2TP session directly to a data link, we refer to it as an L2TP Access Concentrator (LAC). An LCCE may act as both an L2TP Network Server (LNS) for some sessions and an LAC for others, so these terms must only be used within the context of a given set of sessions unless the LCCE is, in fact, single purpose for a given topology.
L2TP Attribute Value Pair (AVP)	The L2TP variable-length concatenation of a unique Attribute (represented by an integer), a length field, and a Value containing the actual value identified by the attribute.
L2TP Control Connection	An L2TP control connection is a reliable control channel that is used to establish, maintain, and release individual L2TP sessions, as well as the control connection itself.
L2TP Control Connection Endpoint (LCCE)	An L2TP node that exists at either end of an L2TP control connection. May also be referred to as an LAC or LNS, depending on whether tunneled frames are processed at the data link (LAC) or network layer (LNS).
L2TP Control Connection ID	The Control Connection ID field contains the identifier for the control connection, a 32-bit value. The Assigned Control Connection ID AVP, Attribute Type 61, contains the ID being assigned to this control connection by the sender. The Control Connection ID specified in the AVP must be included in the Control Connection ID field of all control packets sent to the peer for the lifetime of the control connection. Because a Control Connection ID value of 0 is used in this special manner, the zero value must not be sent as an Assigned Control Connection ID value.
L2TP Control Message	An L2TP message used by the control connection.
L2TP Data Message	Message used by the data channel.
L2TP Endpoint	A node that acts as one side of an L2TP tunnel.
L2TP Network Server (LNS)	If a given L2TP session is terminated at the L2TP node and the encapsulated network layer (L3) packet processed on a virtual interface, we refer to this L2TP node as an L2TP Network Server (LNS). A given LCCE may act as both an LNS for some sessions and an LAC for others, so these terms must only be used within the context of a given set of sessions unless the LCCE is in fact single purpose for a given topology.
L2TP Pseudowire (PW)	An emulated circuit as it traverses a packet-switched network. There is one Pseudowire per L2TP Session.
L2TP Pseudowire Type	The payload type being carried within an L2TP session. Examples include PPP, Ethernet, and Frame Relay.
L2TP Session	An L2TP session is the entity that is created between two LCCEs in order to exchange parameters for and maintain an emulated L2 connection. Multiple sessions may be associated with a single Control Connection.
L2TP Session ID	A 32-bit field containing a non-zero identifier for a session. L2TP sessions are named by identifiers that have local significance only. That is, the same logical session will be given different Session IDs by each end of the control connection for the life of the session. When the L2TP control connection is used for session establishment, session IDs are selected and exchanged as Local Session ID AVPs during the creation of a session. The Session ID alone provides the necessary context for all further packet processing, including the presence, size, and value of the Cookie, the type of L2-Specific Sublayer, and the type of payload being tunneled.
MAC Domain	A grouping of Layer 2 devices that can communicate with each other without using bridging or routing. In DOCSIS, it is the group of CMs that are using upstream and downstream channels linked together through a MAC forwarding entity.
Maximum Transmission Unit (MTU)	Maximum size of the Layer 3 payload of a Layer 2 frame.
Mbps	Megabits per second

Media Access Control (MAC)	Used to refer to the Layer 2 element of the system which would include DOCSIS framing and signaling.
Megahertz (MHz)	A unit of frequency; 1,000,000 or 10^6 Hz
Modulation Error Ratio (MER)	The ratio of average signal constellation power to average constellation error power – that is, digital complex baseband signal-to-noise ratio – expressed in decibels.
Microsecond (µs)	10^{-6} second
Millisecond (ms)	10^{-3} second
Modulation Error Ratio (MER)	The ratio of the average symbol power to average error power.
Multiple System Operator (MSO)	A corporate entity that owns and/or operates more than one cable system.
Nanosecond (ns)	10^{-9} second
Packet Identifier (PID)	PID (system): A unique integer value used to identify elementary streams of a program in a single or multi-program Transport Stream as described in section 2.4.3 of ITU-T Rec. H.222.0 [ISO 13818-1]
Physical Media Dependent (PMD) Sublayer	A sublayer of the Physical layer which is concerned with transmitting bits or groups of bits over particular types of transmission link between open systems and which entails electrical, mechanical, and handshaking procedures.
Pilot tones	Required in the HFC network to ensure that amplifiers in the network are operating correctly. Amplifiers use these tones to adjust gain and keep signals at the appropriate output level.
Precision Time Protocol	A protocol used to synchronize clocks throughout a network.
Program Clock Reference (PCR)	A timestamp in the Video Transport Stream from which decoder timing is derived.
Pseudowire	An IP tunnel between two points in an IP network.
QAM channel (QAM ch)	Analog RF channel that uses quadrature amplitude modulation (QAM) to convey information
Quadrature Amplitude Modulation (QAM)	A modulation technique in which an analog signal's amplitude and phase vary to convey information, such as digital data.
Radio Frequency (RF)	In cable television systems, this refers to electromagnetic signals in the range 5–1000 MHz.
Radio Frequency Interface	Term encompassing the downstream and the upstream radio frequency interfaces.
Request For Comments (RFC)	A technical policy document of the IETF; these documents can be accessed on the World Wide Web at http://www.rfc-editor.org/.
Request-Grant Delay Time	The time from when a CM requests bandwidth, using an uncontended bandwidth request (REQ), to when it receives a MAP message with the granted transmit opportunity in it.
Remote-PHY Device	The Remote-PHY Device (RPD) is a device in the network which implements the Remote-PHY specification to provide conversion from digital Ethernet transport to analog RF transport.
Session	An L2TP data plane connection from the CCAP-Core to the QAM channel. There must be one session per QAM Channel. There is one DEPI pseudowire type per session. There may be one MPT flow or one or more PSP flows per session. Multiple sessions may be bound to a single control connection.
StopCCN	L2TPv3 Stop-Control-Connection-Notification message
Trivial File Transfer Protocol (TFTP)	A file transfer protocol. Generally used for automated transfer of configuration or boot files between machines

Upconverter	A device used to change the frequency range of an analog signal, usually converting from a local oscillator frequency to an RF transmission frequency.
Upstream (US)	• Transmissions from CM to CMTS. This includes transmission from the EQAM to CCAP-Core as well as the RF transmissions from the CM to the EQAM. • RF spectrum used to transmit signals from a subscriber location to a cable operator's headend or hub site.
Upstream Channel Descriptor (UCD)	The MAC Management Message used to communicate the characteristics of the upstream physical layer to the cable modems.
Video on Demand (VoD) System	System that enables individuals to select and watch video content over a network through an interactive television system.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

ACK	L2TPv3 Explicit Acknowledgement message
ADC	Analog-to-Digital Converter
AF	Assured Forwarding
AGC	Automatic Gain Control
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
AVP	L2TPv3 Attribute Value Pair
BPI	Baseline Privacy Interface
CA	Certificate Authority
CAK	Connectivity Association Key
CCAP™	Converged Cable Access Platform
CDN	L2TPv3 Call-Disconnect-Notify message
CIN	Converged Interconnect Network
CLI	Command Line Interface
CM	Cable Modem
CMCI	Cable Modem to Customer Premises Equipment Interface
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
CRC16	CRC of length 16
CRL	Certificate Revocation List
CSMA	Carrier Sense Multiple Access
CVC	Code Verification Certificate
CVS	Code Verification Signature
CW	Continuous Wave
DAC	Digital-to-Analog Converter
dB	Decibels
dBmV	Decibel-Millivolt
DCA	Distributed CCAP Architecture
DEPI	Downstream External PHY Interface
DER	Distinguished Encoding Rules
DF	Don’t Fragment (bit)
DHCP	Dynamic Host Configuration Protocol
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DOCSIS	Data-Over-Cable Service Interface Specifications
DOCSIS-MPT (D-MPT)	DOCSIS MPT Mode
DPI	SCTE-35/Digital Program Insertion

DRFI	Downstream Radio Frequency Interface
DS	Downstream
DSA	Dynamic Service Flow Add
DSCP	Differentiated Services Code Point
DSC	Dynamic Service Flow Change
DSD	Dynamic Service Flow Delete
DTA	Digital Television Adapter
DTI	DOCSIS Timing Interface
DTS	DOCSIS Timestamp, 32-bit
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EBIF	Enhanced TV Binary Interchange Format
EF	Expedited Forwarding
EQAM	Edge QAM
ERM	Edge Resource Manager
ERMI	Edge Resource Manager Interface
ETSI	European Telecommunications Standards Institute
FDM	Frequency Division Multiplex
FQDN	Fully Qualified Domain Name
Gbps	Gigabits per second
GCP	Generic Control Plane
GE	Gigabit Ethernet (Gig E)）
GHz	Gigahertz
HDLC	High-Level Data Link Control
HELLO	L2TPv3 Hello message
HFC	Hybrid Fiber/Coax
HMAC	Hash-based Message Authentication Code
Hz	Hertz
I-CCAP	Integrated CCAP
ICCN	L2TPv3 Incoming-Call-Connected message
ICMP	Internet Control Message Protocol
I-CMTS	Integrated CMTS
ICRP	L2TPv3 Incoming-Call-Reply message
ICRQ	L2TPv3 Incoming-Call-Request message
ID	Identifier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

ISO	International Standards Organization
ITU	International Telecommunications Union
ITU-T	Telecommunication Standardization Sector of the International Telecommunication Union
kbps	Kilobits per second
kHz	Kilohertz
L2SS	Layer 2 Specific Sublayer
L2TP	Layer 2 Transport Protocol
L2TPv3	Layer 2 Transport Protocol version 3
L3	Layer 3
LAC	L2TP Access Concentrator
LCCE	L2TP Control Connection Endpoint
LNS	L2TP Network Server
LSB	Least Significant Bit
MAC	Media Access Control
MAP	Upstream Bandwidth Allocation Map (referred to only as MAP)
Mbps	Megabits per second
MCM	Multi-channel MPEG
M-CMTS	Modular Cable Modem Termination System
MER	Modulation Error Ratio
MHA	Modular Headend Architecture
MHz	Megahertz
MIB	Management Information Base
MKA	MACsec Key Agreement (protocol)
M/N	Relationship of integer numbers M,N that represents the ratio of the downstream symbol clock rate to the DOCSIS master clock rate
MPEG	Moving Picture Experts Group
MPEG-TS	Moving Picture Experts Group Transport Stream
MPT	MPEG-TS mode of R-DEPI
MPTS	Multi Program Transport Stream
ms	Millisecond
MSB	Most Significant Bit
MSK	Master Secret Key
MSO	Multiple System Operator
MSB	Most Significant Bit
MTU	Maximum Transmission Unit
NAD	Network Access Device
NDF	Narrowband Digital Forward
NDR	Narrowband Digital Return
ns	Nanosecond
NSI	Network Side Interface
ONU	Optical Network Unit
OCSP	Online Certificate Status Protocol

OSSI	Operations System Support Interface
PAE	Port Access Entity
PAT	Program Association Table
PCR	Program Clock Reference
PHB	Per Hop Behavior
PHB-ID	Per Hop Behavior Identifier
PHS	Payload Header Suppression
PHY	Physical Layer
PID	Packet Identifier
PKI	Public Key Infrastructure
PMD	Physical Media Dependent Sublayer
PMT	Program Map Table
PMTUD	Path MTU Discovery
PNM	Proactive Network Maintenance
PPP	Point-to-Point Protocol
PSI	Program Specific Information
PSIP	Program and System Information Protocol
PSP	Packet Streaming Protocol
PTP	Precision Time Protocol
PW	Pseudowire
QAM	Quadrature Amplitude Modulation
RDC	Regional Data Center
R-DEPI	Remote Downstream External PHY Interface
RF	Radio Frequency
RFI	Radio Frequency Interface
RFC	Request For Comments
RPD	Remote-PHY Device
RSA	Rivest-Shamir-Adleman (cryptosystem)
R-UEPI	Remote Upstream External PHY Interface
SCCRN	L2TPv3 Start-Control-Connection-Connected message
SCCRP	L2TPv3 Start-Control-Connection-Reply message
SCCRQ	L2TPv3 Start-Control-Connection-Request message
S-CDMA	Synchronous Code Division Multiple Access
SGID	Service Group Identifier
SLI	L2TPv3 Set Link Info message
SPTS	Single Program Transport Stream
SSD	Secure Software Download
StopCCN	L2TPv3 Stop-Control-Connection-Notification message
TCP	Transmission control protocol
TFTP	Trivial File Transfer Protocol
TSID	MPEG2 Transport Stream Identifier

UCD	Upstream Channel Descriptor
UDP	User Datagram Protocol
US	Upstream
UTC	Coordinated Universal Time
VoD	Video On Demand
VoIP	Voice over IP

5 TECHNICAL OVERVIEW

5.1 Introduction

In a Remote PHY Architecture, the classic integrated CCAP (I-CCAP) is separated into two distinct components. The first component is the CCAP-Core and the second component is the Remote PHY Device (RPD).

The CCAP-Core contains both a CMTS Core for DOCSIS and an EQAM Core for Video. The CMTS Core contains the DOCSIS MAC and the upper layer DOCSIS protocols. This includes all signaling functions, downstream and upstream bandwidth scheduling, and DOCSIS framing. The DOCSIS functionality of the CMTS Core is defined by [MULPI v3.0]. The EQAM Core contains all the video processing functions that an EQAM provides today.

The Remote PHY Device is a physical layer converter whose functions are:

- To convert downstream DOCSIS, MPEG video and OOB signals received from a CCAP-Core over a digital medium such as Ethernet or PON to analog for transmission over RF or linear optics.
- To convert upstream DOCSIS, and OOB signals received from an analog medium such as RF or linear optics to digital for transmission over Ethernet or PON to a CCAP-Core.

The RPD platform contains mainly PHY related circuitry, such as downstream QAM modulators, upstream QAM demodulators, together with pseudowire logic to connect to the CCAP-Core.

It provides a subset of the following external interfaces:

CIN Facing:

- One or more 10G or 1G Ethernet or PON ports

Access Network Facing:

- One or more 10G or 1G Ethernet or PON ports
    - Additional RPDs may be daisy-chained through these ports
- One or more RF ports providing connectivity to the access network
    - RF ports may be unidirectional (for use with an external combiner) or bi-directional (internal combiner)
    - RF port output may be RF over coaxial cable or over analog optics

An example reference implementation based on Ethernet is shown in Figure 1.

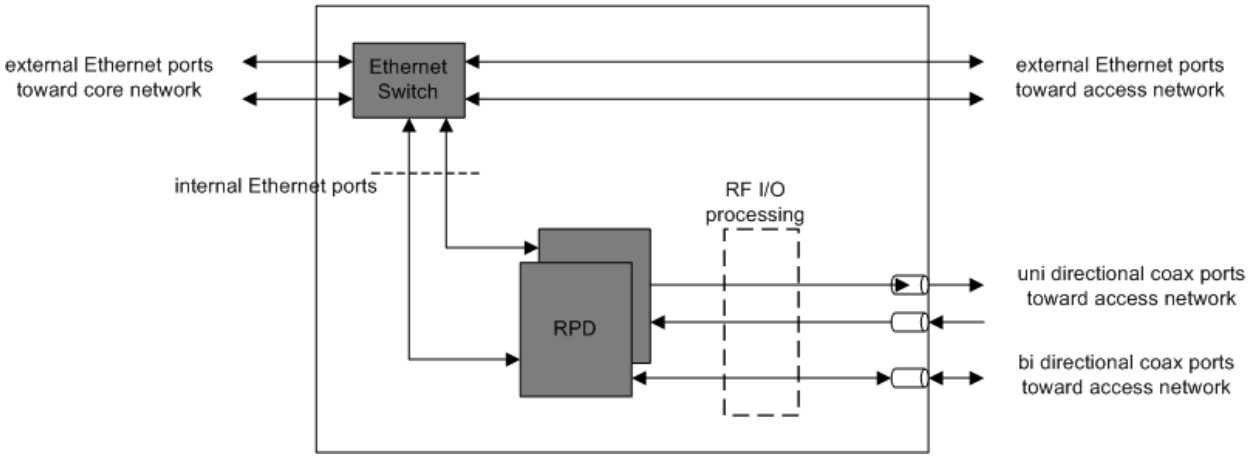

Figure 1 - Logical View of RPD Internals

The DOCSIS functionality of the Remote PHY Device is defined by[PHY v3.1], [MULPI v3.1], [DRFI], and [PHY v3.0].

Together, the CCAP-Core and the RPD are the functional equivalent of an I-CCAP (Integrated CCAP), just with different packaging. The MHAv2 specifications describe how the CCAP-Core and the RPD interface with each other.

Note that MHAv2 functionality and signaling and DOCSIS functionality and signaling are completely separate. The DOCSIS functionality and signaling remain the same for both I-CMTS and Remote PHY solutions. MHAv2 focuses on a simple deconstruction of the CMTS that moves the CCAP PHY elements into an external RPD device while keeping the DOCSIS CMTS-to-CM signaling untouched.

5.2 System Diagram

Figure 2 shows an abstracted view of a cable operator's network. Note that there are more aggregation points beyond a headend such as a super headend or a regional data center (RDC). For the scope of this specification, the focus will be on the headend aggregation point.

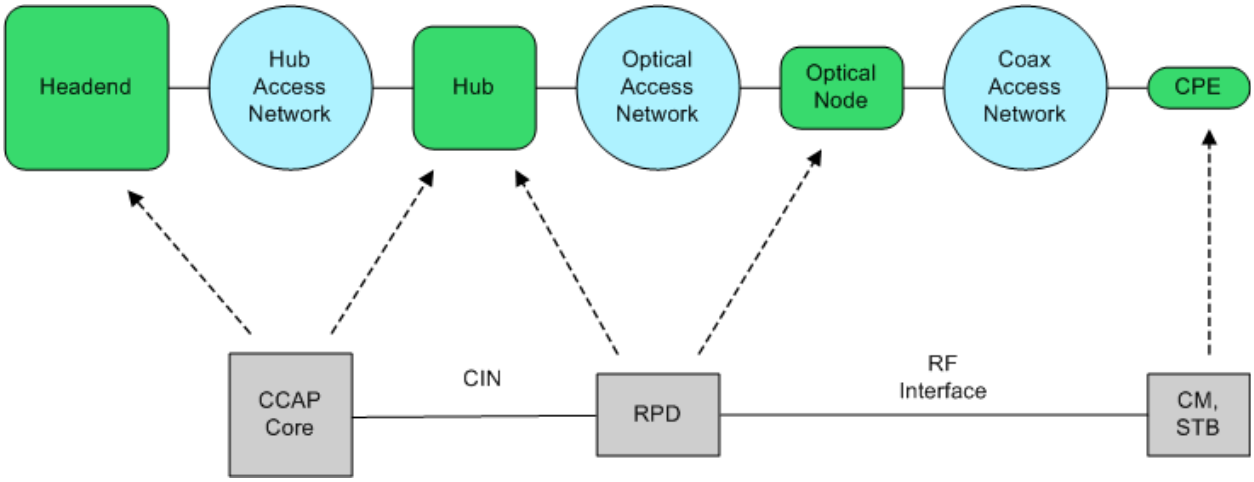

Figure 2 - Remote PHY System Diagram

The items in green are physical locations. The headend is where the majority of the equipment that does not require direct connectivity to the access network resides. Video channel line-ups are often created in the headend. The headend aggregates a number of hubs, with the hub containing equipment that requires direct connectivity to the HFC plant. One example of equipment in the hub is the I-CCAP. The hub aggregates a number of optical nodes. The optical nodes are located in the field and convert between a long point-to-point optical run and a local coax network. The optical node aggregates traffic from a number of subscriber endpoints such as DOCSIS CMs and Video STBs.

5.2.1 Hub Access Network

The hub access network is the network that connects the headend and the hub. The hub access network can be either a switched Layer 2 network or a routed Layer 3 network. It typically is a multi-hop network, which means there can be multiple switches and/or routers between equipment in the headend and the hub.

5.2.2 Optical Access Network

The optical access network is located between the hub and the optical node. The access network has a forward path and a reverse path.

5.2.2.1 Using Linear Optics

The classic HFC plant uses linear optics where the RF spectrum from the coax is modulated onto an optical wavelength. The only type of signal that can traverse this type of network is an RF modulated signal such as a QAM or an OFDM signal.

5.2.2.2 Using Digital Optics Only

A variation of the classic HFC plant uses digital optics in the return path. The RF spectrum is digitized and sampled at the optical node, sent to the headend, and then reconstructed into an analog signal. From the viewpoint of this specification, this will be considered as a subset of a linear optics HFC plant since its operation is transparent to the transmission path which is still a modulated signal such as QAM or OFDMA.

5.2.2.3 Using Digital Optics with IP

A new HFC plant architecture is available that can use any fiber compatible baseband networking technology, such as Ethernet, EPON, or GPON, to drive the fiber portion of the HFC plant. The coax portion of the HFC plant remains the same. With digital optics based upon IP networking, the optical access network could be directly connected from the CCAP-Core to the optical node. Since the hub is aggregating many optical nodes, the access network may have one or more network elements in it, where the network elements could be a Layer 2 switch or a Layer 3 router. Note that this model includes network elements that may be physically located at the hub but are connected between the CCAP-Core and the optical node.

One of the goals of MHAv2 is to accommodate this new digital IP-based HFC plant architecture while maintaining the minimum impact on the CCAP definition and operation. In this manner, I-CCAP and Remote PHY implementations may be used as needed for different HFC plant architectures while maintaining a common CCAP feature set and software loads.

5.2.3 Coax Access Network

The coax portion of the network is an FDM (frequency division multiplex) plant that carries RF modulated signals. It has an upper frequency bound and a frequency range that is split between the upstream and downstream spectrums.

5.2.4 Location of the Remote PHY Device

For an optical access network based on linear optics, the RPD is located at the hub. For an optical access network based on digital optics, the RPD is located at the optical node.

5.2.5 Location of the CCAP-Core

The previous version of I-CCAP is located at the hub where the RF ports can have direct connectivity to the access network. Since the CCAP-Core does not have RF ports, this restriction is removed. The CCAP-Core can be located at the hub or headend (or at another location beyond the headend, like the regional data center).

The network between the CCAP-Core and the RPD is known as the Converged Interconnect Network (CIN). The CIN encompasses either or both the hub access network and the optical access network. The CIN can contain both Layer 2 switches and Layer 3 routers.

5.3 System Architecture

5.3.1 System Components

The reference architecture for a Modular CMTS system is shown in Figure 3. Architectures for video and OOB are similar. This architecture contains both physical and logical components. This section briefly introduces each device and interface.

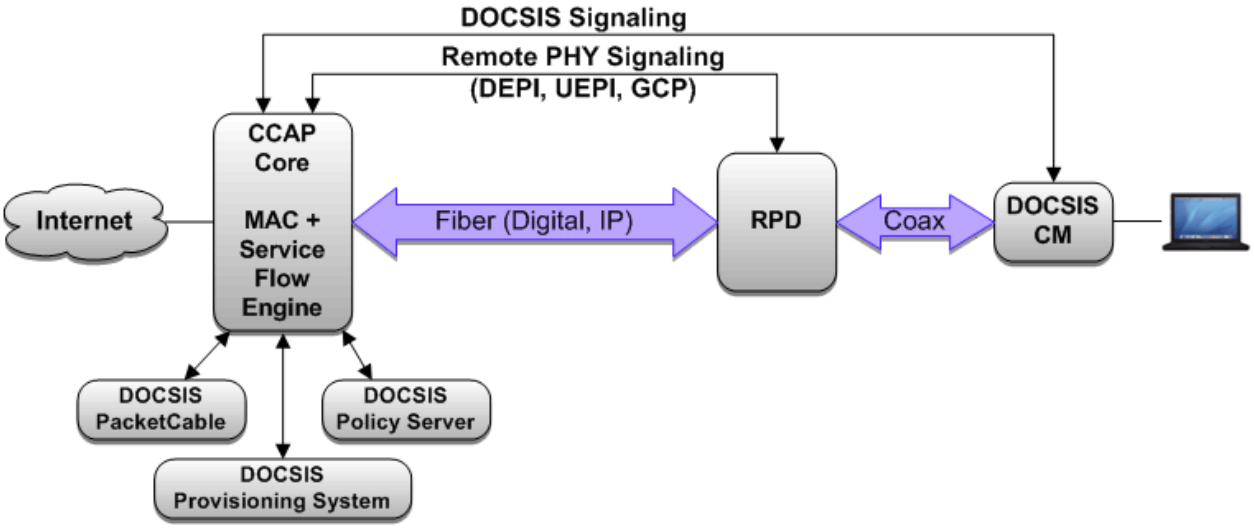

Figure 3 - MHAv2 Reference Architecture for DOCSIS Signaling and Provisioning

The **RPD** is a component that has network interface on one side and an RF interface on the other side. The RPD provides Layer 1 PHY conversion, Layer 2 MAC conversion, and Layer 3 pseudowire support. The RPD RF output may be RF combined with other overlay services such as analog or digital video services.

The **CCAP-Core** contains everything a traditional CMTS does, except for functions performed in the RPD. The CCAP-Core contains the downstream MAC, the upstream MAC, and all the initialization and operational DOCSIS-related software.

Note that the original MHAv1 architecture had the downstream PHY external and the upstream PHY internal. MHAv1 was used to interface to an EQAM (Edge QAM) device that was co-located at the headend with the CMTS Core. Thus, the main difference between MHAv1 and MHAv2 is the location of the upstream PHY and the role of the solution in the marketplace. From a technical standpoint, the solutions are very similar.

Due to the physical separation of the downstream PHY and the upstream PHY in MHAv1, a DOCSIS Timing Interface (DTI) Server was needed to provide a common frequency of 10.24 MHz and a DOCSIS timestamp between the two MHAv1 elements. In MHAv2, the same DTI server is not required since the downstream and upstream PHYs are co-located in the RPD. A different timing solution referred to as R-DTI is used to provide timing services for functions such as DOCSIS scheduling.

R-DEPI, the Remote Downstream External PHY Interface, is the downstream interface between the CCAP-Core and the RPD. More specifically, it is an IP pseudowire between the MAC and PHY in an MHAv2 system that contains both a data path for DOCSIS frames, video packets, and OOB packets, as well as a control path for setting up, maintaining, and tearing down sessions. MHAv1 used the MPT (MPEG-TS) encapsulation. MHAv2 retains the original MPT encapsulation for backward compatibility but also added a new MPEG encapsulation called MCM (Multi-channel MPEG). MHAv2 also requires the PSP (Packet Streaming Protocol) mode for expansion of new services like DOCSIS 3.1.

R-UEPI, the Remote Upstream External PHY Interface, is the upstream interface between the RPD and the CCAP-Core. Like R-DEPI, it is an IP pseudowire between the PHY and MAC in an MHAv2 system that contains both a data path for DOCSIS frames, and a control path for setting up, maintaining, and tearing down sessions.

NSI, or the Network Side Interface, is unchanged, and is the physical interface the CMTS uses to connect to the backbone network. Today, this is typically 10 Gbps Ethernet.

CMCI, or Cable Modem to Customer Premise Equipment Interface, is also unchanged, and is typically Ethernet, USB, or WiFi. Within this document, CMCI is referred to as RPD.

5.4 Remote PHY Device Architecture

Figure 4 shows the architecture for an RPD.

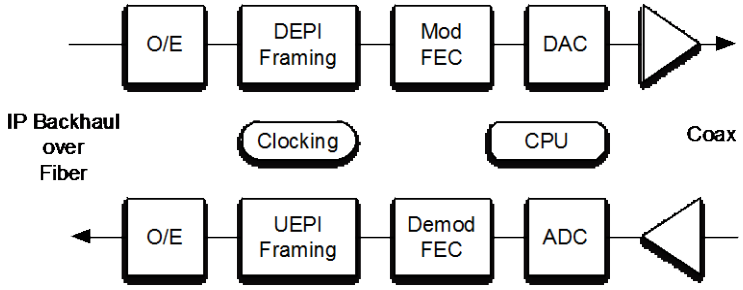

Figure 4 - Remote PHY Device Block Diagram

Packet traffic arrives from the CCAP-Core on the downstream receiver. The DEPI framing is terminated; the payload is extracted, framed, modulated, and transmitted out the cable interface. In the upstream, the signal is received from the coax, digitized, demodulated, and the DOCSIS frames are extracted from the FEC payload. The DOCSIS frames are then placed into the UEPI encapsulation and transmitted out the upstream transmitter to the CCAP-Core. A clocking circuit interfaces to R-DTI and manages clocking and timing accuracy for the RPD. There is a local CPU that manages the DEPI and GCP control planes and provides an interface into network management.

Figure 4 is meant to be explanatory and is not meant to be all-inclusive. Specific implementations may differ.

5.5 Remote PHY Operation

Figure 5 shows the internal components of an RPD. The following subsections explain the behavior and functionality of these internal components.

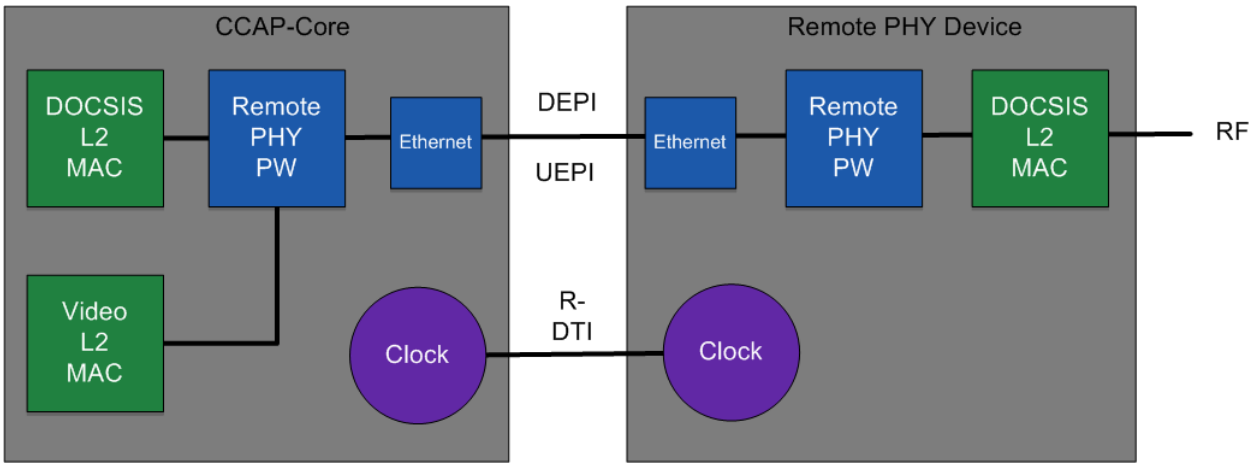

Figure 5 - R-PHY Internal Components

5.5.1 R-DEPI and R-UEPI

R-DEPI and R-UEPI are IP-based pseudowires that are inserted between the DOCSIS MAC in the CCAP-Core and the DOCSIS PHY in the RPD. R-UEPI is an extension to R-DEPI. R-UEPI uses the same control plane structure and a unique set of encapsulations in the upstream direction.

R-DEPI's job is to take either of the formatted DOCSIS frames, transport them through a Layer 2 or Layer 3 network, and deliver them to the RPD for transmission. R-UEPI's job is to take DOCSIS frames that have been received and

demodulated by the DOCSIS upstream PHY in the RPD and transport them to the CCAP-Core for processing. The RPD does not provide any upstream DOCSIS processing; with one minor exception, the RPD will extract the bandwidth request frames from the DOCSIS stream and send them in a separate pseudowire so that bandwidth request frames can be given a higher priority than data frames.

The base protocol that is used for the R-DEPI is the Layer 2 Tunneling Protocol version 3, or L2TPv3 for short, and is specified in document [RFC 3931]. L2TPv3 is an IETF protocol that is a generic protocol for creating a pseudowire, which is a mechanism to transparently transport a Layer 2 protocol over a Layer 3 network. Examples of protocols supported by L2TPv3 include ATM, HDLC, Ethernet, Frame Relay, PPP, etc.

Each data packet contains a 32-bit session ID. In the original MPT encapsulation, that session ID is associated with a single QAM Channel. The UDP header—as part of an L2TPv3 encapsulation—is not used in the MHA protocols. The L2TPv3 session ID directly follows the IP header. It is worth noting that the L2TPv3 session ID lands in the same part of a packet as a classic UDP DP/SP. This allows network equipment that classify based upon UDP headers, to be reused for L2TPv3 headers.

L2TPv3 permits creating a subheader whose definition is specific to the payload being carried. The control channel allows for signaling messages to be sent between the CCAP-Core and the RPD. Typical control messages will set up a "control connection" between the CCAP-Core and the RPD, and then set up multiple data sessions (one for each downstream and upstream QAM or OFDM channel). Each session can be marked with different Differentiated Services Code Points (DSCPs) and can support different encapsulation protocols.

There are two main pseudowire techniques defined by R-DEPI. Each main type supports a variety of subtypes. The first technique, known as MPT mode, transports multiple 188-byte MPEG-TS packets by placing them into the L2TPv3 payload with a unique subheader that contains a sequence number so packet drops can be detected. The encapsulation of DOCSIS frames into MPEG-TS packets is performed in the CCAP-Core. The second technique, known as the Packet Streaming Protocol (PSP), transports DOCSIS frames in the L2TPv3 payload. The DOCSIS frames are then encapsulated in MPEG-TS packets within the EQAM. PSP mode allows DOCSIS frames to be both concatenated, to increase network performance, and fragmented, in case the tunneled packets exceed the network MTU size. MPT mode is generally used for single carrier QAM systems such as DOCSIS 3.0 and video, while PSP mode is used for downstream OFDM channels and for the DOCSIS upstream.

5.5.2 Remote DTI

Remote DTI (see [R-DTI]) provides timing synchronization between CCAP-Cores and RPDs based on the IEEE 1588v2 standard [IEEE 1588]. The protocol supports the basic synchronization between the CCAP-Core and Remote PHY Device for DOCSIS/video/OOB services and the precision time synchronization for emerging services such as wireless backhaul.

5.6 Latency

One of the technical considerations of the MHAv2 architecture is its impact on the round-trip request-grant delay time. The request-grant delay time is the time from when a CM requests bandwidth, using an uncontended bandwidth request (REQ), to when it receives a MAP message with the granted transmit opportunity in it.

MHAv2 locates the upstream scheduler in the CMTS Core. To prevent the MAP from being slowed down by other traffic in the CIN, the DOCSIS traffic (or a subset containing the MAP messages) may be sent in an independent L2TPv3 flow that can have a unique DSCP. The value of the marked DSCP value should be consistent with a configured "per hop behavior (PHB)" that will provide MAP messages with the highest priority and lowest latency across the CIN to the EQAM. Marking of the DHCP field is optional and part of the operator’s overall network design. In the upstream direction, the request can be copied from the DOCSIS frame and sent on an independent L2TPv3 flow that has a unique DSCP.

The net result of prioritizing the MAP and REQ messages, combined with a good CIN design, is to make the operation and performance of the centralized upstream scheduler similar to that of an I-CMTS system.

5.7 MHAv2 Summary

In summary, the RPD is used to transfer DOCSIS frames between an IP network interface and an RF interface. The RPD does not participate in the DOCSIS MAC protocol. Instead, MHAv2 provides an IP pseudowire that seamlessly transports the DOCSIS frames between the CCAP-Core and the RPD. As such, for most DOCSIS functions, the MHAv2 CCAP system functions almost identically to an I-CCAP. This preserves common functionality and features between the two systems.

6 RPD INITIALIZATION

6.1 Overview

When the RPD device first powers up, it goes through a series of steps before becoming operational. These steps are shown in Figure 6 and explained in this section. Note that Figure 6 is a simplified sequence and does not attempt to show error paths. Error handling during each operation is described in a subsequent, relevant section of the document.

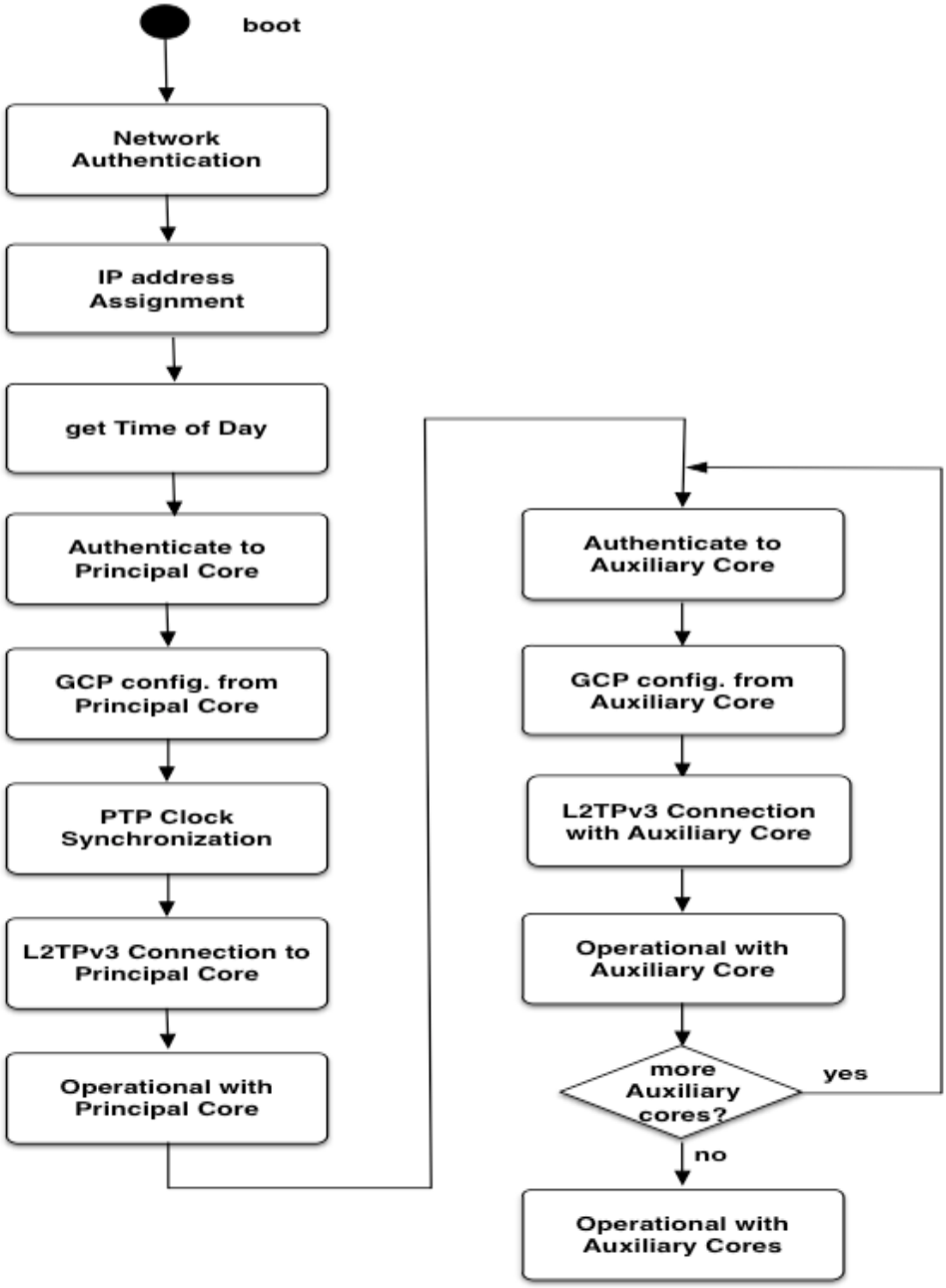

Figure 6 - RPD Initialization

6.2 Security

The Remote PHY security architecture consists of a trusted domain and an untrusted domain (see Figure 7 below). To access the trusted domain and connect to the CCAP-Core, RPDs may be required to be authenticated to the trusted network. This is accomplished using 802.1x. When the RPD connects to the CCAP-Core, a control session is established which can be secured using IPsec. Both of these mechanisms perform mutual authentication using digital certificate credentials issued from a trusted public key infrastructure (PKI). RPDs support both of these mechanisms (802.1x or IPsec). MSOs can enable them as needed for their specific deployments.

Details for both mechanisms are provided in the following sections.

6.3 Network Authentication

6.3.1 Problem Definition

In many cases, an RPD will be located in an untrusted part of the MSO network, such as a pole-mounted fiber node or remote cabinet but must connect to devices inside the trusted network. When this occurs, it presents a potential security vulnerability. An RPD in an environment like this is shown in Figure 7.

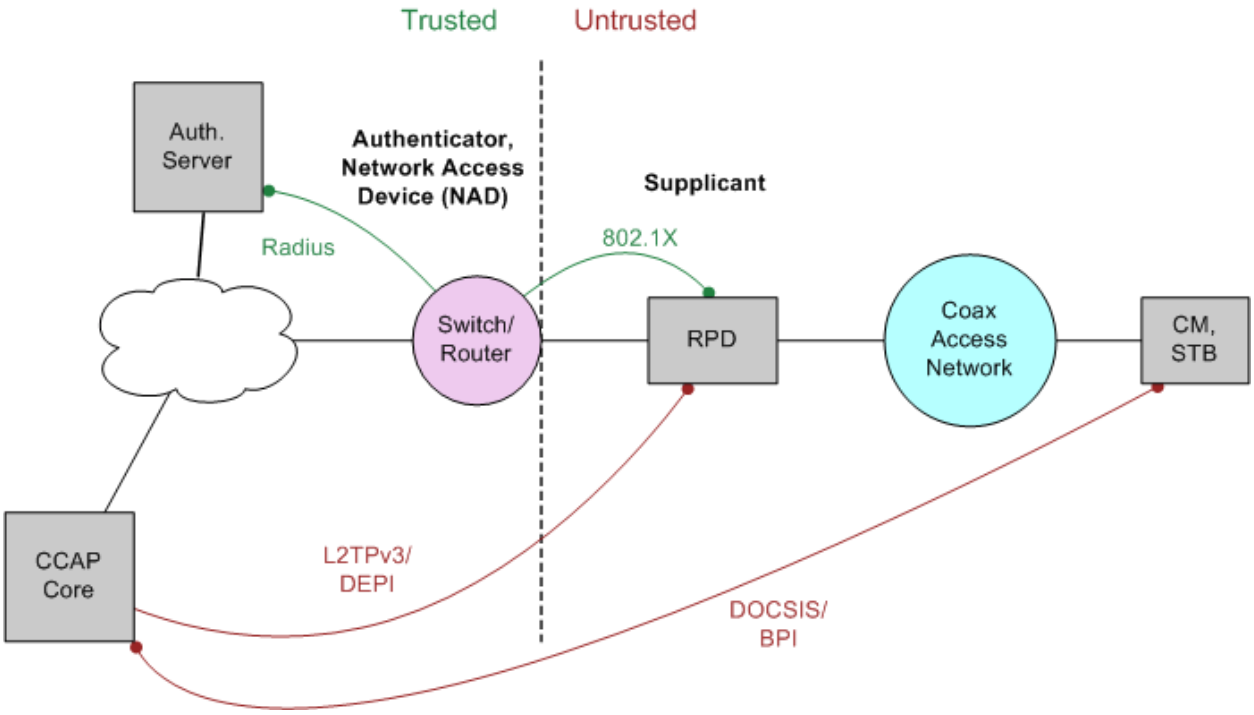

Figure 7 - Remote PHY: Trusted Domain and Untrusted Domain

To mitigate this threat, an MSO may require that the RPD is authenticated before it is allowed access to the trusted network. An RPD may of course be located within the trusted network boundary, such as in a physically secured hub site. In this case, authentication may not be required. Thus, the RPD must be able to operate in both authenticated and unauthenticated networks. Whether authentication is required for an RPD is determined by the network that it is connected to rather than the RPD itself. To support "out of box" operation, an RPD should first attempt to authenticate to the network. If no response to authentication is received, it should assume authentication is not supported by the network and attempt to operate without it (refer to Section 6.3.3.4 for details).

6.3.2 Authentication from an Untrusted Portion of the Network

In Figure 8, the RPD is located in an untrusted area of the network so the network is configured to require authenticated access. The CCAP-Core is located in a trusted area of the network. A single RPD may connect to more

than one CCAP-Core. This is because there may be different CCAP-Cores for DOCSIS and video, or for primary and standby. The RPD will also need to connect to other network services such as DHCP and to allow connections from network management servers.

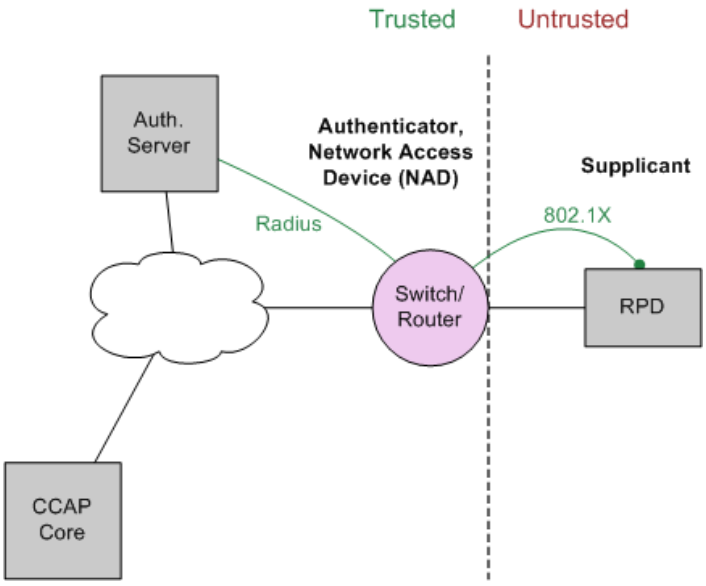

Figure 8 - Authentication Network Diagram

The two authentication scenarios that an RPD MUST support are:

- No authentication in which case the RPD can send to and receive packets from the trusted network with no additional requirements.
- 802.1x based authentication, which requires the RPD to act as an 802.1x supplicant, as described in Section 6.3.3.

A fundamental objective for deployment of RPD is to not require configuration.

To achieve this "out of the box" operation, the RPD MUST be able to determine which security option is in place without configuration.

The RPD MUST determine whether 802.1x authentication is operating, as described in Section 6.3.3.

6.3.3 802.1x Authentication

Authentication is performed based on the 802.1x [IEEE 802.1x] and MACsec [IEEE 802.1ae] standards.

802.1x is a Layer 2 protocol that uses EAP (Extensible Authentication Protocol) to provide authentication services.

For the RPD, EAP-TLS is used based on digital certificate credentials issued from the DOCSIS PKI.

The standard defines three entities:

Supplicant	This is the RPD that requires authentication.
Authenticator/NAD	This is a network element that prevents the RPD from gaining network access until authentication is achieved. The Authenticator is also known as a Network Access Device (NAD).
Authentication Server	This is a standard 802.1x authentication server that validates the authentication.

MHAv2 uses a standard version of the 802.1x protocol with EAP-TLS. This method is referred to as network authentication since the entire authentication process happens between the RPD and a Network Access Device (NAD) without the involvement of the CCAP-Core.

Figure 9 shows how the EAP messages between the Authentication Server and the Authenticator are carried over the Radius or Diameter, while the EAP messages from the Authentication Server to the RPD are carried over the combination of Radius/Diameter and 802.1x (EAPoL).

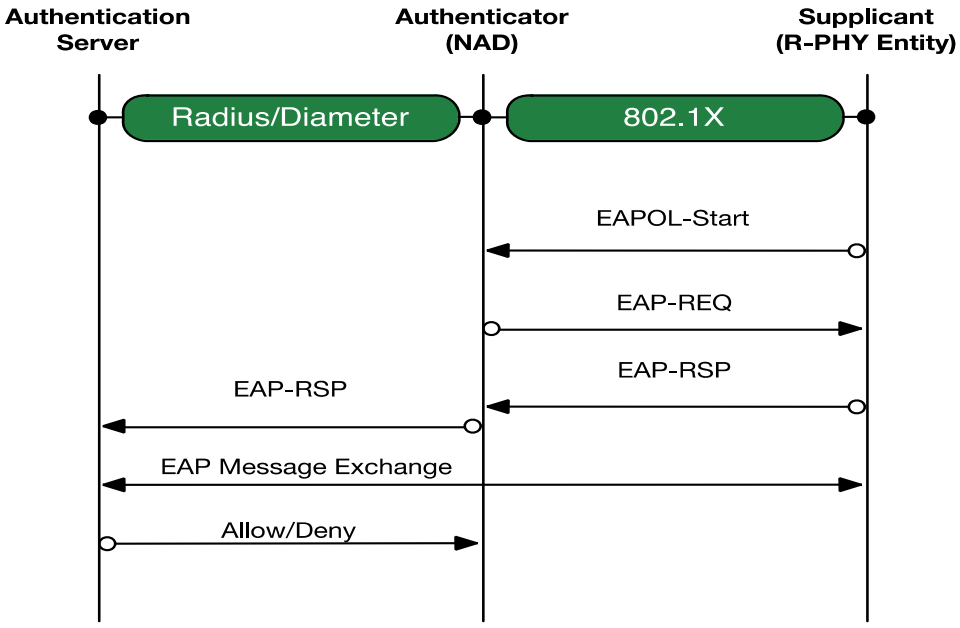

Figure 9 - Network Authentication Signaling

The Authenticator will transmit a Layer 2 broadcast EAP-Request message periodically or in response to an EAPoLstart message from a supplicant. An RPD will respond with a Layer 2 unicast EAP-Response. The Authenticator will forward the EAP response to the Authentication server using a RADIUS or DIAMETER protocol. The Authentication server and the RPD then communicate directly using the Authenticator as a relay agent. When the Authentication server has made a decision, it communicates that decision to the Authenticator. The Authenticator will then provide or deny network access to the RPD.

6.3.3.1 MACsec

MACsec (see [IEEE 802.1ae] is a link layer encryption mechanism used to provide additional security to 802.1x.

MACsec may be used to provide link level encryption between the RPD and the NAD. A security association is created between the NAD and each authenticating RPD based on keying material created during the EAP exchanges. This is used to encrypt data between the NAD and each RPD, providing a higher level of security than basic 802.1x. With 802.1x, after authentication of an RPD, the NAD port is opened to any messages from the authenticated RPD MAC address. This creates the possibility for a device to spoof the RPD MAC address to gain access to the network. With MACsec only devices in possession of legitimate security keys can send traffic to the network.

The use of MACsec provides the following advantages:

- It enables secure access for multiple devices per port
- It provides protection against potential man in middle attacks in both single and multiple devices per port use cases.

MACsec is relatively new and is not yet supported by all switches and all silicon. If MACsec is supported

- The RPD MUST support the MACsec Key Agreement protocol (MKA) for key exchange and management.
- The RPD MUST derive the Connectivity Association Key (CAK) from the EAP-MSK as defined by EAP-TLS and 802.1x.
- The RPD MUST not use pre-shared CAKs.

6.3.3.2 RPD Topology Support for 802.1x

Figure 10 shows a number of potential topologies for RPD deployment and connectivity to the NAD. The various topologies are discussed in the subsections of this section.

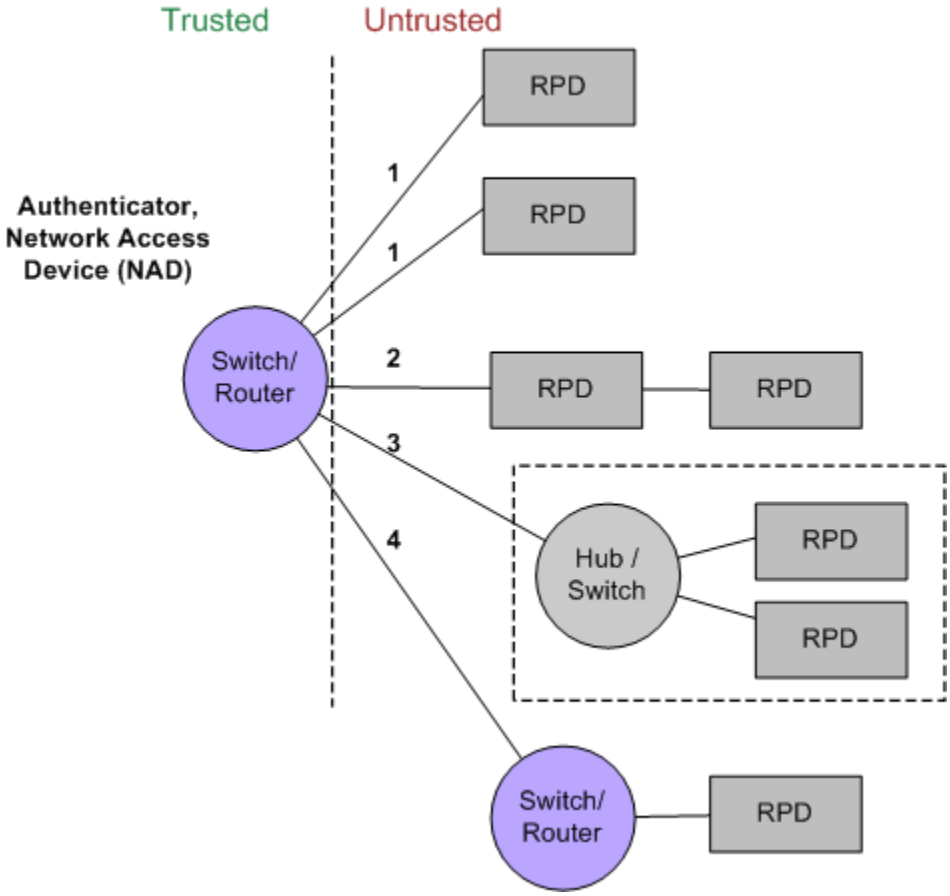

Figure 10 - RPD Topologies for 802.1x

6.3.3.2.1 Type 1: Single Host per Port

In its most basic form, 802.1x supports access by a single host per Ethernet switch port. This is defined in the 802.1x standard and is widely supported by existing switches.

The RPD MUST support this topology.

The RPD MUST support 802.1x in this configuration.

The RPD SHOULD support MACsec in this configuration.

6.3.3.2.2 Type 2: Daisy Chained RPDs

In this topology, a single NAD port is connected to multiple RPDs connecting over a single port. In this topology MACsec may be used to establish independent security associations with each RPD. This is defined in the standard but is not widely supported in current switches.

The RPD MAY support this daisy chain topology.

If a daisy chain topology is supported:

- The RPD SHOULD support 802.1x in this configuration;

- The RPD SHOULD support MACsec in this configuration.
- 802.1x request messages are carried in a multicast packet with the well-known PAE group address as the destination address. Normal Ethernet switches are required to block this address so that 802.1x is typically a single hop protocol with the authenticator directly connected to the supplicant.
- The RPD SHOULD propagate the 802.1x EAP-REQ multicast messages between the NAD and the daisy chain port.

6.3.3.2.3 Type 3: Multiple RPDs in Single Device

In this topology, a single NAD port is connected to an integrated device such as a node with multiple RPDs connecting via an internal hub or switch. Thus the NAD sees multiple devices (and multiple MAC source addresses) on the port. In this topology, MACsec may be used to establish independent security associations with each RPD, based on the RPD MAC address. This is defined in [IEEE 802.1ae], but is not widely supported in current switches.

If this topology is supported:

- Each RPD MUST have a unique MAC address per Ethernet port;
- The internal hub / switch SHOULD propagate the 802.1x EAP-REQ multicast messages to the RPDs;
- The RPD SHOULD support 802.1x in this configuration;
- The RPD SHOULD support MACsec in this configuration.

6.3.3.2.4 Type 4: Intermediate External Switch / Router

In this topology, a one or more RPDs are connected to the NAD through an intermediate switch or router.

MSOs deploying this topology may not be able to utilize 802.1x or MACsec due to the forwarding restrictions on PAE multicast in Ethernet bridges and switches. Definition of the external switch behavior that would be required to support this topology is outside the scope of this specification.

6.3.3.3 Authenticator Location

The Authenticator is hosted in the device at the border of the trusted network. This may be a Layer 2 switch, a Layer 3 router or the CCAP-Core.

There can be zero or more Layer 2 switches and/or Layer 3 routers between the Authenticator and the CCAP-Core. There can be zero or more Layer 2 switches and/or Layer 3 routers between the Authenticator and the Authentication Server.

6.3.3.4 Operation

After powering up (and prior to obtaining an IP address) the RPD MUST attempt to authenticate itself to the network using 802.1x as shown in Figure 11.

The RPD MUST send an EAPOL-START message to the Authenticator and wait for an EAP-REQ. If there is no EAP-REQ in response to the EOPOL-Start within "EAP-REQ-TIMEOUT", the EAPOL-START MUST be resent and the RPD MUST return to wait mode. If no EAP-REQ is received after EAPOL-START-RETRIES have been exhausted, the RPD MUST assume that the network is not authenticated, operate in a non-authenticated mode, and proceed with the DHCP phase of the initialization sequence (this is standard operating procedure for an 802.1x device).

If an EAP-REQ is received the RPD MUST proceed with 802.1x authentication. If the RPD authentication is rejected or if the authentication process fails after an EAP-REQ has been received, the RPD MUST hold off for the defined 802.1x wait period before trying to re-authenticate.

Once authentication is completed succesfully, the RPD MUST proceed with the DHCP phase of the initialization sequence.

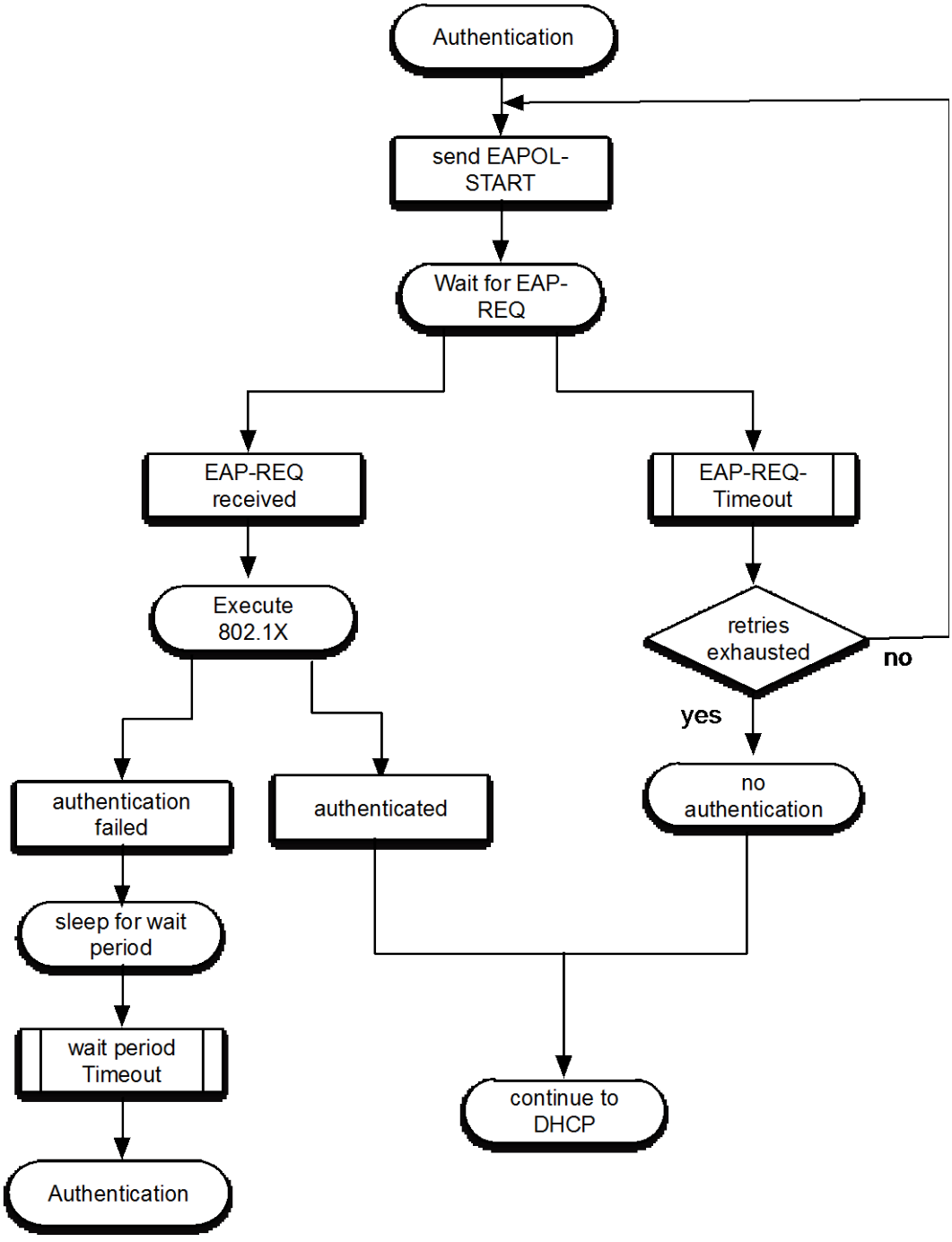

Figure 11 - RPD Authentication using 802.1x

6.3.3.5 802.1x Mutual Authentication

802.1x with EAP-TLS provides mutual authenticaton of the RPD and the Authentication server. The RPD MUST use EAP-TLS per [RFC 5216] with certificates issued from the DOCSIS PKI managed by CableLabs (see Annex E). The CableLabs Root CA certificate is installed in the Authentication server and RPD as a trust anchor for validating received certificates. The RPD Certificate and its private key, along with the issuing intermediate Device CA certificate are installed in the RPD. The Authentication Server Certificate and its private key, along with the issuing

intermediate Service Provider CA certificate, are installed on the Authentication server. During the EAP-TLS message exchange, the RPD and Authentication server will send their device/server certifcates and the issuing intermediate CA certificate to each other to be validated against the root CA trust anchor certificate. The RPD and Authentication server MUST use the "Basic Path Validation" procedure defined in [RFC 5280] for validating received certificates.

6.3.3.6 CCAP-Core Requirements

The CMTS Core MAY act as a NAD if it is directly connected to the RPD. In ths case, it MUST support the 802.1x protocol and act as a relay agent to the Authentication server.

6.3.3.7 Authentication Failures

If an EAP-REQ message has been received indicating that authentication is in effect for the network, any subsequent failures during the authentication process MUST be handled per the [IEEE 802.1x] specification. The wait period timer (which defines the time a device must wait after a failed authentication attempt before another attempt is permitted) SHOULD not be reduced below the 60 second default time.

Retransmission behavior for EAP messages (which are forwarded from the authenticator to the authentication server) MUST follow [RFC 3748].

Constant	Value
EAP-REQ-TIMEOUT	10 sec
EAPOL-START-RETRIES	3

6.4 Address Assignment

Figure 12 shows a simplified access network containing an RPD, a CCAP-Core and a DHCP Server.

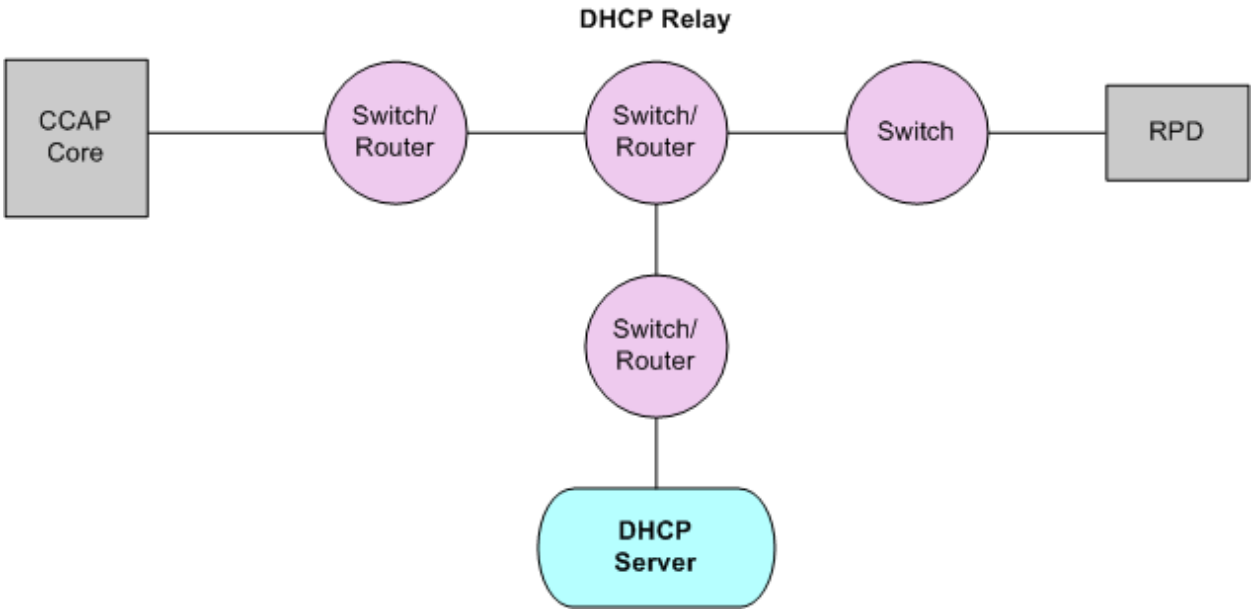

Figure 12 - DHCP Network Diagram

Once the RPD is successfully authenticated to the trusted network, it requests an IP address using DHCP. The standard DHCPv6 or DHCPv4 protocol is used with extensions.

The RPD MUST initially run DHCPv6. If that fails, then the RPD MUST run DHCPv4.

This method is referred to as network DHCP since the entire address assignment of the RPD can take place without the involvement of the CCAP-Core. The CCAP-Core MAY run a DHCP Relay agent but is not required to if relay is provided by another network component.

There may be zero or more Layer 2 switches between the RPD and the DHCP Relay. The DHCP Relay may be hosted by a Layer 2 switch, a Layer 3 router or the CCAP-Core. There may be zero or more Layer 2 switches and/or Layer 3 routers between the network element that is hosting the DHCP Relay and the CCAP-Core. There may be zero or more Layer 2 switches and/or Layer 3 routers between the DHCP Relay and the DHCP Server.

Figure 13 shows the DHCP signaling protocol. The RPD issues a broadcast DHCP discovery message when it needs to obtain an IP address. The DHCP agent responds with a unicast DHCP offer that contains the IP address of one or more DHCP servers. The RPD picks one of the DHCP servers and sends a DHCP request to it. The DHCP server sends a DHCP acknowledgement with an IP address for the RPD device.

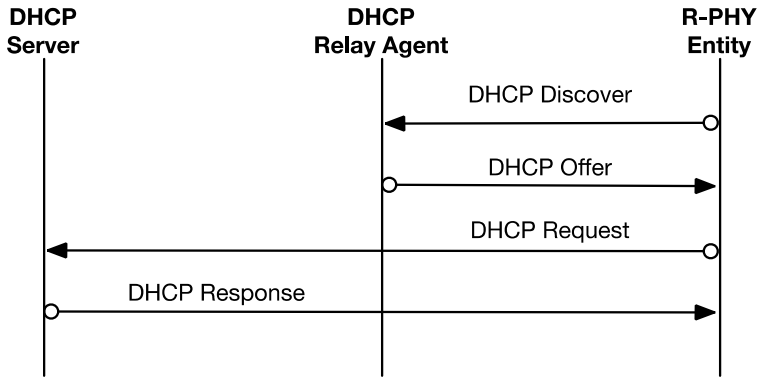

Figure 13 - DHCP Signaling

Unlike the DOCSIS DHCP process where the CCAP is always the DHCP relay agent and can always snoop and append to the DHCP messages, the CCAP-Core may not have any direct access to the DHCP message exchange and thus will not be directly aware of the IP address assignment of the RPD. The following mechanism MUST be used to create an association between the CCAP-Core and the RPD:

1. The CCAP-Core and the DHCP Server MUST be provisioned with the same IP/MAC Address pair for the RPD. The provisioning can be done manually or with an automated system.
2. The DHCP Server MUST provide the IP address of the CCAP-Core to the RPD. An additional DHCP option <CCAP-Cores> is added to support this mechanism. The CCAP-Core MUST either accept the connection from the RPD, deny the connection, or redirect the RPD to another CCAP-Core.

6.4.1 DHCP Options

Refer to [CANN] for details on specific options.

The RPD MUST support the following DHCP options when they are received in a DHCP message.

Option	Value	Use
2	Time Offset	Used for authentication, logging, and software upgrade
4	Time Server	Used for authentication, logging, and software upgrade
7	Log Server	Used for logging

The RPD MUST support the following CableLabs suboptions under DHCP option 43.

Suboption	Value	Use
2	<Device Type>	MUST be set to “RPD”

3	<ECM: eSAFE>	Not used
4	<serial number>	Refer to [CANN]
5	<hw version>	Refer to [CANN]
6	<sw version>	Refer to [CANN]
7	<Boot ROM version>	Refer to [CANN]
8	<OUI>	Refer to [CANN]
9	<Model Number>	Refer to [CANN]
10	<Vendor Name>	Refer to [CANN]
TBD	<CCAP-Cores>	Address of all CCAP-Cores RPD MUST attempt to connect to. The Principal Core is the first entry in the list.

6.4.1.1 CCAP-Cores Suboption

CMTS Cores suboption describes either IPv4 or IPv6 addresses, as shown in Figure 14 and Figure 15.

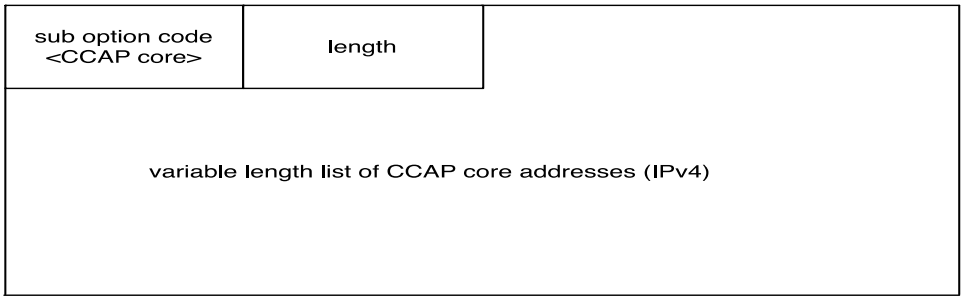

Figure 14 - CCAP-Cores DHCP Suboption IPv4

The CMTS Cores suboption can also be used with DHCPv6.

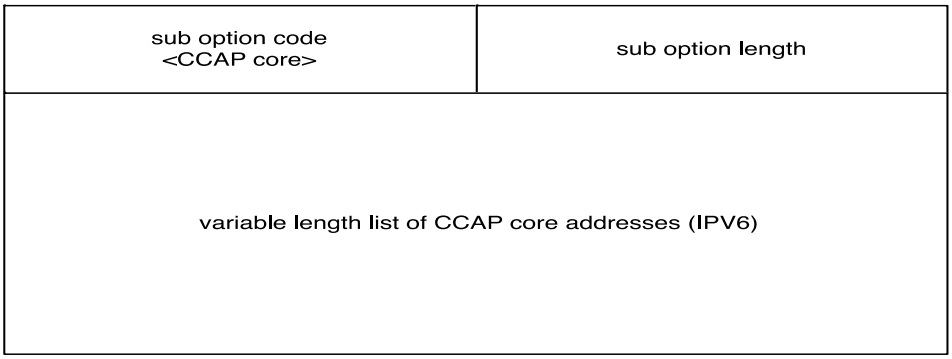

Figure 15 - CCAP-Cores DHCP Suboption IPv6

The cores may have different roles, such as primary, standby, DOCSIS, EQAM, etc. The specific role of each core is determined during the GCP configuration phase.

- The RPD MUST attempt to connect to all cores in the options list as described in Section 6.6.

6.4.2 Failures

The RPD MUST respond to any errors during the DHCP process as per [RFC 2131].

NOTE: This results in the RPD entering a time out and retry loop with a randomized exponential back off.

6.4.3 Security Implications

The RPD MUST attempt to contact the DHCP server via the CIN interface. If 802.1x and MACsec are in place this will provide secure access to the trusted network.

6.5 Time of Day

The RPD acquires the time of day for the purpose of timestamping warnings, error logs and messages, validation of the CVC during a software upgrade, and validation of the CCAP-Core certificate during mutual authentication.

6.5.1 ToD Acquisition

The RPD MUST attempt to obtain the current date and time by using the Time Protocol (see [RFC 868]) from one of the servers listed in the `Time Server Option` DHCP field. If this field is missing or invalid, the RPD MUST initialize the current time to Jan 1, 1970, 0h00. If the time is initialized (reset), the RPD MUST ignore the value, if any, of the Time Offset DHCP option.

The RPD MUST use its DHCP-provided IP address for exchange of messages with the Time Protocol server. The RPD MUST transmit the request using UDP. The RPD MUST listen for the response on the same UDP port as is used to transmit the request. The RPD MUST combine the time retrieved from the server (which is UTC) with the time offset received from the DHCP server to create a valid "local" time.

Once the RPD acquires time, it MUST stop requesting, unless any of its ToD related parameters (such as time offset or server address) are modified. If the RPD's ToD related parameters are modified, the RPD MAY re-request ToD from the Time Protocol server(s).

6.5.2 ToD Conflicts and Problems

The DHCP server may return multiple IP addresses from multiple Time Protocol servers. The RPD MUST attempt to obtain time of day from all the servers listed until it receives a valid response from any of the servers. The RPD MUST contact the servers in batches of tries with each batch consisting of one try per server and each successive try within a batch at most one second later than the previous try and in the order listed by the DHCP message. If the RPD fails to acquire time after any batch of tries, it MUST retry a similar batch using a truncated randomized binary exponential backoff with an initial backoff of 1 second and a maximum backoff of 256 seconds.

If an RPD is unable to establish time of day it MUST log the failure in the local log. If the RPD does not obtain ToD in the initial request against the first server, the RPD MUST initialize the current time to Jan 1, 1970, 0h00, and then subsequently initialize its current time once it receives a response from a Time Server.

If the RPD fails to establish TOD it will not be able to validate the CCAP-Core certificate.

The failure may be due to time server failure or to an error in the DHCP option list.

The RPD will follow the same mechanism as for a DHCP failure and restart the DHCP process as described in Section 6.4.2

6.5.3 ToD Security Implications

The RPD MUST attempt to contact the time server via the CIN-facing port on which the DHCP response was received. If 802.1x and MACsec are in place this will provide secure access to the trusted network.

6.6 Connection to CCAP-Cores

Following successful IP address assignment the RPD attempts to connect to all of the CCAP-Cores that have been identified in the DHCP option list as described below.

6.6.1 Core Types

Cores are defined to be either Principal or Auxiliary.

An RPD can be connected to multiple CCAP-Cores. Each CCAP-Core manages and configures an independent subset of the RPD resources, e.g., one or more RF channels. There are certain types of parameters, which are common across resource sets such as downstream power. The Principal Core is responsible for the configuration of these common parameters for the RPD and for certain device management functions.

Auxiliary cores are responsible for providing DOCSIS, video, or OOB services. They are restricted to the resource set assigned to them by the Principal Core.

The RPD MUST complete configuration with a Principal Core before allowing configuration from Auxiliary cores.

In general, it is expected that the first core in the DHCP option list will be the Principal, but the RPD MUST be able to accommodate out-of-order lists.

The RPD MUST accept configuration from only one Principal core (refer to Section 6.6.2.4 for details).

Principal and Auxiliary cores may operate in Active or Standby roles. {Note 1}

Note 1: High Availability actions will be defined in a future version of the specification

6.6.2 Connection Process

The connection process between RPD and each CCAP-Core (whether Principal or Auxiliarry) consists of two phases:

1. Establish a mutually authenticated secure connection between the RPD and Core.
2. RPD configuration using GCP.

6.6.2.1 Mutual Authentication

Mutual authentication is used when establishing a secure connection between the RPD and CCAP-Core(s). It is independent from the authentication used for trusted network access described in Section 6.3.

Mutual authentication is always required between the RPD and CCAP-Core but a secure connection may not be required in all cases (e.g., when the RPD is inside the trusted network or MACsec is used to secure access to the trusted network). This is negotiated as described below.

Authentication can be initiated by either the CCAP-Core or the RPD.

Whether the RPD is required to authenticate is under control of the CCAP-Core.

The RPD and the CCAP-Core MUST support mutual authentication based on IKEv2 [RFC 7296] using public key signatures based on the digital certificate credentials issued from the CableLabs DOCSIS PKI (see Annex E). The RPD certificate provisioning requirements are the same as what is defined in Section 6.3.3.5. The CCAP-Core MUST be provisioned with the CableLabs Root CA certificate as a trust anchor. CCAP-Core MUST be provisioned with a CCAP-Core Device Certificate and its private key along with the CableLabs Device CA certificate which are issued by the CableLabs Root CA.

The RPD MUST use UDP port 500 for IKEv2 exchanges.

The CCAP-Core MUST use UDP port 500 for IKEv2 exchanges.

The RPD MUST initiate the IKE_SA_INIT process per [RFC 7296].

The CCAP-Core MAY initiate the IKE_SA_INIT process per [RFC 7296] if the RPD address is known in order to facilitate faster reconnection (for example, following a CCAP error).

The RPD MUST attempt to recontact a CCAP-Core following a connection loss.

The RPD MUST include its [X.509] certificate in the IKEv2 exchanges.

The CCAP-Core MUST include its [X.509] certificate in the IKEv2 exchanges.

The RPD MUST use the value of the common name field from the [X.509] certificate as the identifier in IKEv2 messages it generates.

The CCAP-Core MUST use the value of the common name field from the [X.509] certificate as the identifier in IKEv2 messages it generates.

The mechanism by which the CMTS Core determines whether to accept the connection from the RPD is a local matter but could include:

- Local configuration of RPD identifier, or
- Forwarding to an authentication policy server.

The CCAP-Core MUST determine the security profile for the GCP control plane during the IKEv2 exchange.

The GCP control plane SHOULD be authenticated by the CCAP-Core. The CCAP-Core MAY encrypt the GCP Control Plane.

If authentication or encryption are in operation, IPsec ESP in transport mode MUST be used to protect the GCP control plane.

If authentication or encryption are in operation, IKEv2 MUST be used to generate the keying material required to secure the GCP control plane.

The IKEv2 traffic selector MUST be the 5-tuple identifying the GCP connection.

The CCAP-Core MUST determine the security profile for the L2TPv3 control plane during the IKEv2 exchange.

The L2TPv3 control plane MAY be authenticated and MAY be encrypted by the CCAP-Core.

If authentication or encryption are in operation, IPsec ESP in transport mode MUST be used to protect the L2TPv3 control plane.

If authentication or encryption are in operation, IKEv2 MUST be used to generate keying material to secure the L2TPv3 control plane.

The IKEv2 traffic selector MUST be the 5-tuple identifing the L2TPv3 connection.

Different security associations MUST be used for GCP and L2TPv3 control.

The following cryptographic methods as defined in [RFC 4307] MUST be supported:

- Message integrity using HMAC-SHA1-96;
- Data Encryption using AES 128 CBC;
- Pseudo-random function for key generation HMAC-SHA1;
- Certificate authentication using RSA Signature Algorithm [RSA 3] with SHA-256 hash (see [FIPS 180-4]) per Annex E.

6.6.2.1.1 No Authentication Option

If the CCAP-Core does not wish to use encryption or authentication, it signals this by selecting null encryption and no authentication options (see [RFC 4307]) during the IKEv2 exchange.

6.6.2.1.2 Certificate Validation

The RPD MUST use the “Basic Path Validation” procedure defined in [RFC 5280] for validating received certificates.

The CCAP-Core MUST use the “Basic Path Validation” procedure defined in [RFC 5280] for validating received certificates.

6.6.2.1.3 Authentication Failure

Failures during the authentication process MUST be handled per [RFC 7296].

If the authentication is terminated due to a failure, the RPD will attempt to connect to the next core in the list.

6.6.2.2 RPD Configuration via GCP

Following authentication, the CCAP-Core MUST configure the RPD using the GCP (Generic Control Plane) protocol (see [GCP]). Since the RPD is an extension of the CCAP-Core, the CCAP-Core contains all the necessary configuration information.

GCP allows control plane data structures from other protocols to be tunneled through its generic control plane. For example, GCP can directly use DOCSIS TLVs for the configuration of the RPD PHY parameters.

Note that the [R-DEPI] and [R-UEPI] protocols also contain a certain amount of configuration information. The MHAv2 paradigm is to keep the R-DEPI and R-UEPI configuration focused on session signaling and to use GCP for RPD-specific configuration and operation.

The specific RPD configuration parameters used in GCP are listed in Annex B.

The GCP protocol is authenticated and secured using IPsec. Encryption and/or message authentication codes (HMAC) can be applied to protect packets. IPsec keys are derived from the keying material created during the IKEv2 authentication process. IPsec session key exchange and renewal during the life of the GCP connection will be supported using IKEv2.

6.6.2.3 GCP Connection Failures

If a CCAP-Core has not responded after CORE_CONNECT_TIMEOUT, then the RPD MUST retry the connection CONFIG_RETRY_COUNT. If no response is received after retries are exhausted, the RPD MUST move on to the next Core in the list.

Constant	Value
CORE_CONNECT_TIMEOUT	5 seconds
CONFIG_RETRY_COUNT	3

6.6.2.4 Connection to Principal Core

Following successful IP address assignment, the RPD MUST follow the process shown in Figure 16 to connect to a Principal core.

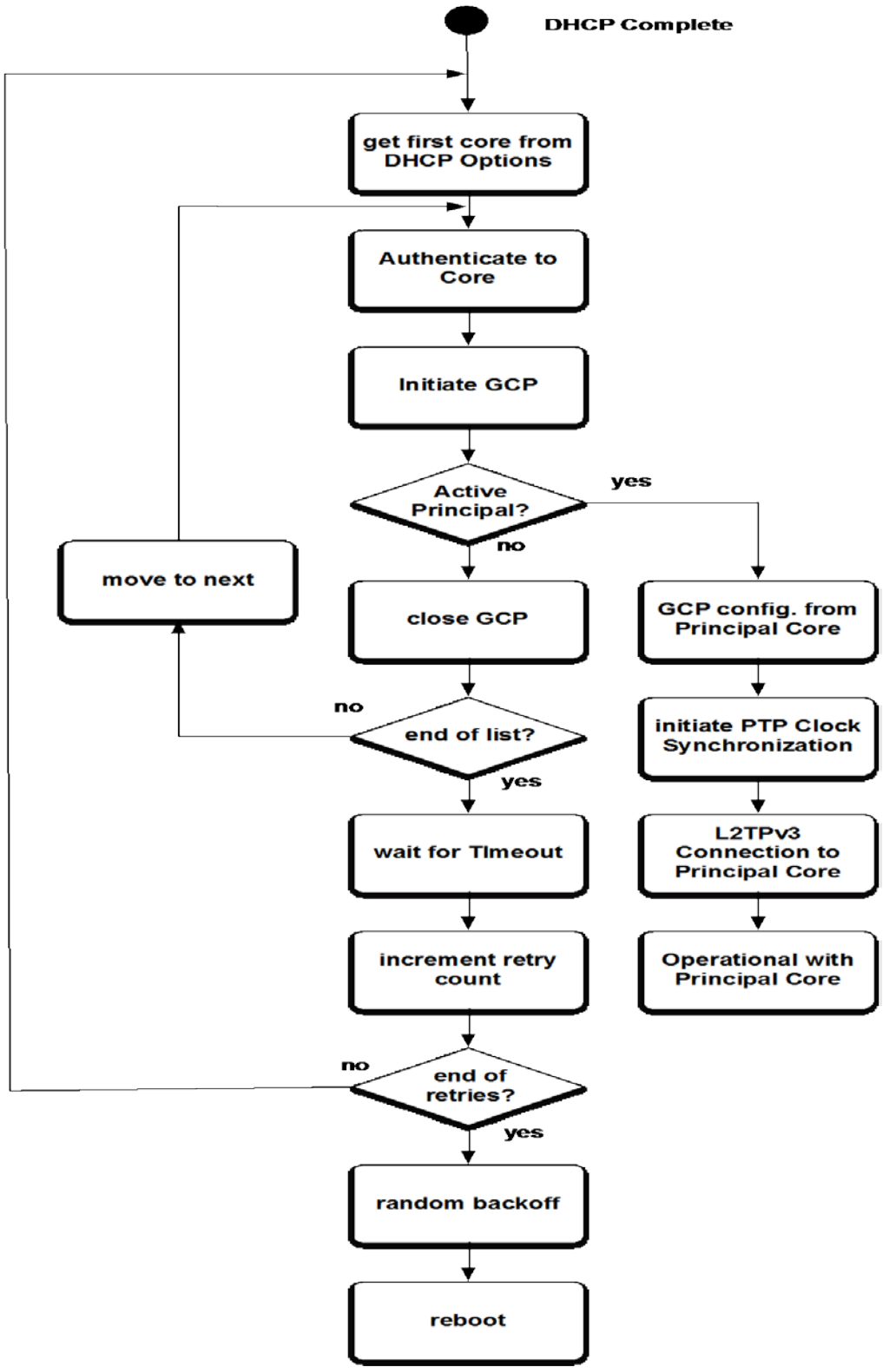

Figure 16 - Process for Connecting to the Principal Core

The RPD MUST establish a GCP connection with a Principal Core following the process shown in Figure 16 and described below. It MUST start the process with the first core in the DHCP option list and move sequentially through the list until a successful connection is achieved.

The RPD MUST attempt to authenticate with the core as described in Section 6.6.2.1.

Following authentication, the RPD MUST initiate a TCP connection to the GCP well-known port on the CCAP-Core. When the connection is established, the RPD MUST issue a GCP Notify message to the CCAP-Core to initiate configuration and determine if the core can act as a Principal.

If the core identifies as a Principal core in active mode (as opposed to standby) the RPD MUST proceed with GCP configuration.

If the configuration received from the Principal core overwrites any of parameter values communicated via the DHCP Options previously received, the RPD MUST use the parameter values received from the Principal Core. Alternatively, a new list of Auxiliary cores could be provided.

When configuration by the Principal core is complete, the RPD MUST initiate PTP clock synchronization. The PTP may take some time to reach a steady state, so the RPD should start the synchronization process as soon as possible.

The RPD MUST establish L2TPv3 connectivity with the Principal core as described in Section 6.8.

Following successful L2TPv3 establishment, the RPD is operational with the Principal Core and MUST move on to any Auxiliary cores defined by DHCP Options or defined during configuration from the Principal core.

6.6.2.5 Failures

If the core contacted is not a Principal Core, the RPD MUST move to the next core in the options list and attempt to contact this core.

If the end of the option list is reached with no Principal Core found, the RPD MUST wait NO_PRINCIPAL_CORE_FOUND_TIMEOUT then retry from the start of the list.

If no Principal Core can be contacted after PRINCIPAL_CORE_RETRY_COUNT attempts, the RPD must wait for a random backoff time between PC_BACKOFF_MIN and PC_BACKOFF_MAX, and then reboot.

Constant	Value
NO PRINCIPAL_CORE_FOUND_TIMEOUT	60 seconds
PRINCIPAL_CORE_RETRY_COUNT	3
PC_BACKOFF_MIN	60 seconds
PC_BACKOFF_MAX	300 seconds

6.6.2.6 Redirection

If a Principal CCAP-Core does not have configuration data for an RPD or is not aware of the RPD, the core SHOULD either reject the connection and log an error or use GCP to redirect the RPD to another core.

A CCAP-Core MAY elect to redirect an RPD to one or more alternate cores for further configuration, e.g., to act as a standby or to provide additional services.

The CCAP-Core MUST use the GCP (Generic Control Plane) protocol to redirect the RPD.

The redirecting CCAP-Core MUST transfer a variable length list of IPv4 or IPv6 addresses to the RPD.

6.6.3 Connection to Auxiliary Cores

After becoming operational with a Principal core, the RPD MUST follow the process shown in Figure 17 to connect to any Auxiliary cores that have been configured.

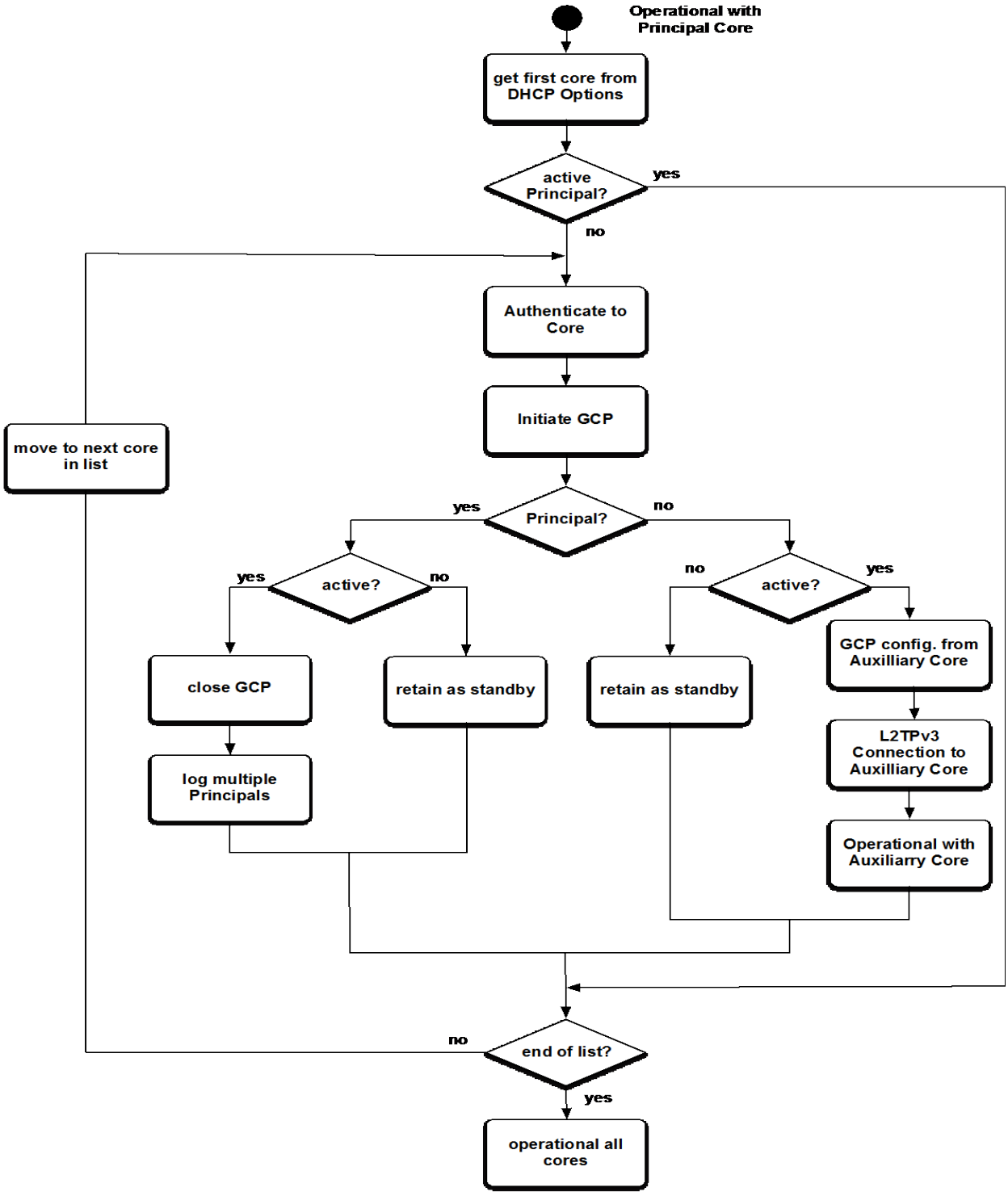

Figure 17 - Process for Connecting to Auxiliary Cores

For each core in the list:

- If this is the active Principal core (to which it is already connected) the RPD MUST move to the next entry in the list.

- The RPD MUST try to authenticate with the core.
- Following authentication the RPD MUST initiate a TCP connection to the GCP well-known port on the CCAP-Core. When the connection is established, the RPD MUST issue a GCP Notify message to the CCAP-Core to initiate configuration.
- If the core is an additional Principal core operating in active mode, the RPD MUST log an error and close the GCP connection because only one active Principal core is allowed. The CCAP-Core MUST also log an error.
- If the core is a Principal core operating in standby mode the RPD MUST retain this information in case the active Principal core fails.
- If the core is an auxiliary operating in standby mode the RPD MUST retain this information in case the active Auxiliary core fails.
- If the core is an auxiliary core operating in active mode:
    - The RPD MUST proceed with GCP configuration.
    - The RPD MUST establish L2TPv3 connectivity with the Auxiliary core as described in Section 6.8.
    - Following successful L2TPv3 establishment, the RPD is operational with the Auxiliary Core and MUST move on to any additional Auxiliary cores defined by DHCP Options or defined during configuration from the Principal core.

6.7 Synchronization

Once the RPD has been configured, the RPD chooses its method of synchronization. The RPD can be directed to either be internally synchronized where the RPD is the clock master (Option A) or externally synchronized where the RPD is a clock slave (Option B).

In a Remote PHY system, the downstream and upstream PHY timing are always aligned because the downstream and upstream PHY are co-located. The only timing requirement is to be able to share a timestamp value between the CCAP-Core and the RPD for upstream scheduling. These timing techniques are described in [R-DTI].

Note that if the upstream scheduler is located in the RPD, then all the timing elements are local to the RPD and no adjustments are necessary. This scenario is equivalent (from a timing standpoint) to having the entire CMTS in the RPD. This is a future option for the R-PHY architecture should it ever be needed.

The net effect of all methods is that the timestamp used in the SYNC message, the MAP message, the REQ message, the RPD upstream burst receiver, and the upstream scheduler are aligned.

The protocol used in [R-DTI] between the CMTS Core and the RPD is the Precision Time Protocol (PTP) as defined by [IEEE 1588]. PTP is used because it is a standard protocol whose accuracy can be enhanced when the CIN is built with [IEEE 1588] compliant equipment. Note that it is not necessary for the network to be compliant to [IEEE 1588].

Encryption or authentication of PTP messages between the master clock and the RPD (e.g., by using IPsec) would result in some loss of accuracy because intermediate nodes could not update the timing data. If security of PTP messages is required, MACsec encryption can be used.

The synchronization requirements can be summarized as follows:

- All specific operational requirements are stated in the [R-DTI] specification.
- The RPD MUST be able to support PTP messages received over a MACsec (see [IEEE 802.1ae]) secured link from the CIN.
- If the CCAP-Core has specified a PTP Master source during GCP configuration the RPD MUST use it.

6.7.1 Synchronization Failures

6.7.1.1 RPD Operating as a Timing Slave

If the RPD does not receive a sync message within PTP_SYNC_TIMEOUT, it MUST log a LOSS_OF_SYNC error and operate in a non-synchronized local clocking mode. It will continue to attempt to synchronize with a PTP clock master. When synchronization is re-established, a SYNC_ESTABLISHED message MUST be logged.

6.7.1.2 RPD Operating as a Timing Master

If the RPD does not receive a delay request message within PTP_DELAY_TIMEOUT, it MUST log a LOSS_OF_SLAVE error. It will continue to act as PTP clock master. When communication with a slave is re-established a SLAVE_FOUND message MUST be logged.

Constant	Value
PTP_SYNC_TIMEOUT	5 seconds
PTP_DELAY_TIMEOUT	5 seconds

6.8 Connectivity

Once clocking has been established, the RPD and the CCAP-Core are ready to set up the L2TPv3 data tunnel and control plane connectivity.

Downstream data plane connectivity between the CMTS Core and the RPD is described in [R-DEPI]. Upstream data plane connectivity between the RPD and the CMTS Core is described in [R-UEPI]. [R-DEPI] is an extension of the Layer 2 Tunneling Protocol described in [RFC 3931].

R-DEPI and R-UEPI establish one overall control plane connection between a CMTS Core and an RPD pair. Within this tunnel, there are separate pseudowires consisting of L2TPv3 sessions for each MAC-PHY functional pair. The data plane encapsulation is managed per session. Depending upon the type of pseudowire encapsulation used, a pseudowire may contain one or more channels.

After the R-DEPI and R-UEPI session initializes, the CMTS Core and RPD are ready to use.

The connectivity requirements can be summarized as follows:

- If the RPD is provided with a Principal CCAP-Core IP address, the RPD MUST try to establish connectivity to that CCAP-Core using the DEPI primary session.
- If the RPD is provided with a Auxiliary CCAP-Core IP address, the RPD MUST try to establish connectivity to that Auxiliary CCAP-Core using the auxiliary DEPI sesison.
- The CMTS Core MUST be compliant with [R-DEPI] and [R-UEPI].
- The RPD MUST be compliant with [R-DEPI] and [R-UEPI].
- The CMTS Core MUST support the R-DEPI MPT pseudowire type for DOCSIS 3.0 and MPEG-TS Video.
- The CMTS Core SHOULD support the R-DEPI MCM pseudowire type for DOCSIS 3.0 and MPEG-TS Video.
- The CMTS Core MUST support all R-DEPI PSP pseudowire types for DOCSIS 3.1.
- The CMTS Core MUST support all R-UEPI PSP pseudowire types.
- The RPD MUST support the R-DEPI MPT pseudowire type for DOCSIS 3.0 and MPEG-TS Video.
- The RPD MUST support the R-DEPI MCM pseudowire type for DOCSIS 3.0 and MPEG-TS Video.
- The RPD MUST support all R-DEPI PSP pseudowire types for DOCSIS 3.1.
- The RPD MUST support all R-UEPI PSP pseudowire types.

7 SECURE SOFTWARE DOWNLOAD

7.1 Introduction

Remote PHY architecture supports downloading code to RPDs. Authenticating the source and verifying the integrity of downloaded code is vital to the overall operation and security of Remote PHY architecture. The methods for secure software download as well as the relevant specification text have been adopted from DOCSIS 3.1 Security Specification [SECv3.1].

Broadly speaking, with respect to secure software downloads; the RPD assumes the functions of a DOCSIS cable modem. It is envisioned that such an approach will allow the operators to reuse the majority of the OSS infrastructure deployed for CM software and security certificate management to perform equivalent functions for RPDs. However, there are important changes to the upgrade procedure. These changes are summarized below and explained further within section 7.

- The RPD upgrade process relies on certificates from the new CableLabs PKI. The legacy certificates are not supported.
- Unlike a DOCSIS CM, the RPD does not receive a configuration file from a provisioning system. RPD initialization involves connecting to and obtaining configuration information from a Principal CCAP-Core via GCP. The software upgrade TLVs received via GCP effectively replace equivalent TLVs received by a CM in a configuration file.
- Unlike a CM SSU process, which needs to be enabled by inclusion of CVC in the CM configuration file, the RPD is implicitly enabled for SSU, unless the Principal CCAP-Core disables this feature.
- A DOCSIS CM receives time service from the provisioning system via the DOCSIS Time Protocol, while an active RPD is time synchronized via the PTP protocol. The RPD needs to receive time service via the DOCSIS Time Protocol before it establishes the PTP protocol connection.

The RPD code is signed with a certificate from the new PKI defined in [SECv3.1] and then validated by the RPD. The software download module is an attractive target for an attacker. If an attacker were able to mount an attack against the software download module, s/he could potentially install code to disrupt service on a wide scale or to redirect the content. To thwart these attacks, the attacker is forced to overcome several security barriers.

7.2 Overview

The requirements defined in this section address these security objectives for the code download process:

- The RPD needs to have a means to authenticate that the originator of any download code is a known and trusted source;
- The RPD needs to have a means to verify that the downloaded code has not been altered from the original form in which it was provided by the trusted source;
- The process needs to simplify the operator's code file-handling requirements and provide mechanisms for the operator to upgrade or downgrade the code version of RPDs on their network;
- The process allows operators to dictate and control their policies with respect to: 1) which code files will be accepted by RPDs within their network; and 2) security controls that establish the security of the process on their network;
- RPDs are able to move freely among systems controlled by different operators;
- Support updating the Root CA Certificate in the RPD (optional);
- Support updating the Device CA Certificate in the RPD (optional).

The concerns of individual operators or RPD manufacturers may result in additional security related to the distribution or installation of code into a RPD. This specification does not restrict the use of further protections, as long as they do not conflict with the requirements of this specification.

Multiple levels of protection are required to protect and verify the code download:

- The manufacturer of the RPD code always applies a digital signature to the code file. The signature is verified with a certificate chain that extends up to the Root CA before accepting a code file. The manufacturer signature affirms the source and integrity of the code file to the RPD;
- Though the manufacturer always signs its code file, an operator may later apply its code signature in addition to the manufacturer signature. If a second signature is present, the RPD verifies both signatures with a certificate chain that extends up to the Root CA before accepting a code file;
- OSS mechanisms for the provisioning and control of the RPD are critical to the proper execution of this process. Code downloads are initiated by the Principal CCAP-Core during the initial RPD configuration process, or can be initiated in normal operation using an SNMP command.

The RPD code file is built using a [PKCS#7]-compliant structure that is defined below, which is identical to the code structure used to upgrade CM software. Included in this structure are:

- The upgrade code image;
- The Code Verification Signature (CVS); i.e., the digital signature over the code image and any other authenticated attributes as defined in the structure;
- The Code Verification Certificate (CVC); i.e., an [X.509]-compliant certificate that is used to deliver and validate the public code verification key that will verify the signature over the code image. The DOCSIS Certificate Authority (CA), a trusted party whose public key is already stored in the RPD, signs this certificate.

Figure 18 shows the basic steps required for the signing of a code image when the code file is signed only by the RPD manufacturer, and when the code file is signed by the RPD manufacturer *and* co-signed by an operator.

In DOCSIS, the Root CA certificate is installed in each RPD as a trust anchor. The code manufacturer builds the code file by signing the code image using a DOCSIS [PKCS#7] digital signature structure with a Manufacturer CVC certificate and the issuing CVC CA certificate. The code file is then sent to the operator. The operator verifies that the code file is from a trusted DOCSIS manufacturer and has not been modified. At this point, the operator has the option of loading the code file on the Software Download server as-is, or of adding its signature and operator CVC and issuing CVC CA certificate to the code file. During the code upgrade process, the RPD retrieves the code file from the Software Download server and verifies the new code image using the Root CA Certificate trust anchor before installing it. See Annex E for CVC chain details.

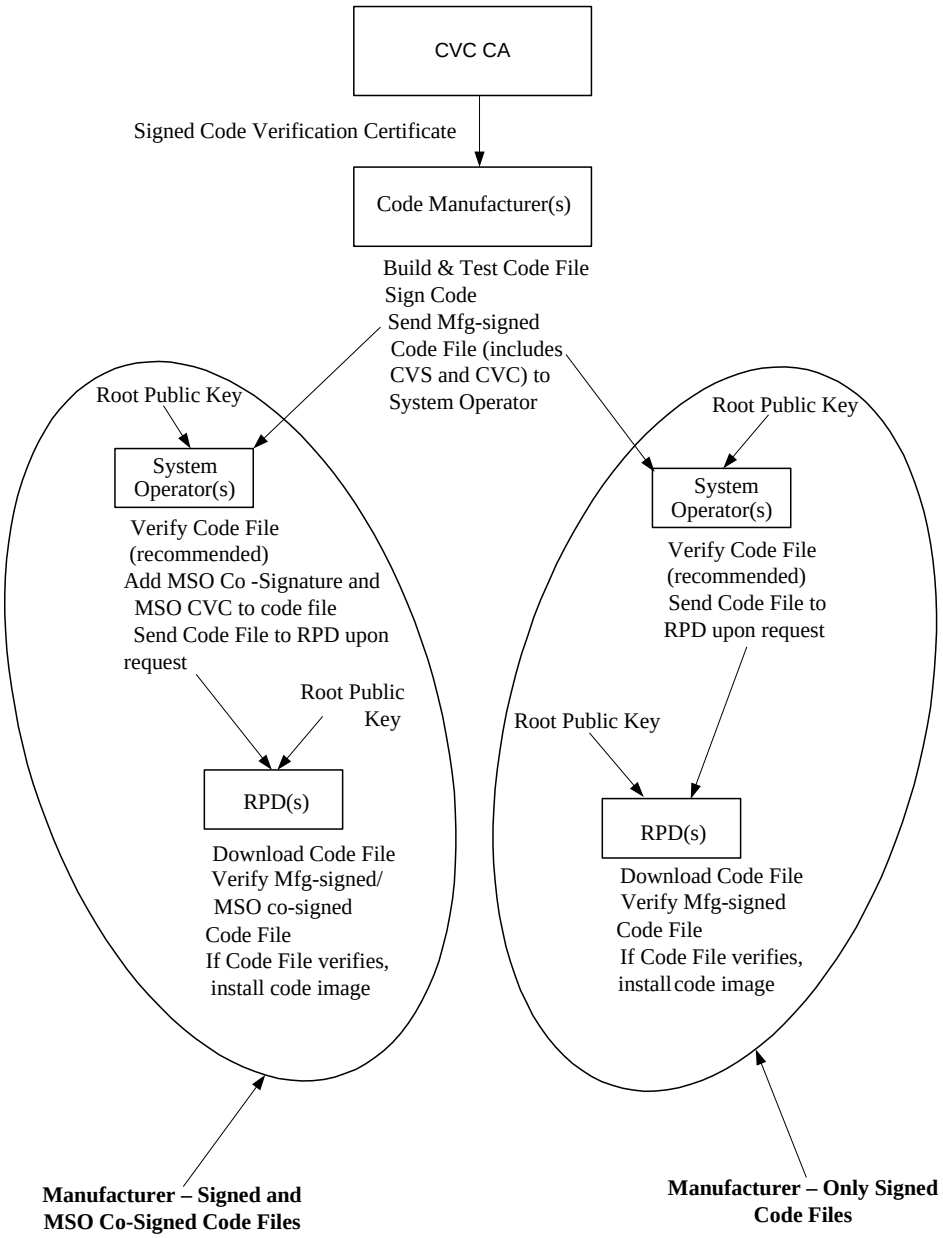

Figure 18 - Typical Code Validation Hierarchy

7.3 RPD Software Upgrade Procedure

Once the RPD is authenticated (or bypasses authentication) and has obtained an IP address, it may receive a software update. The software of the RPD may occur by one of the following methods:

1. During RPD operational configuration from the Principal CCAP-Core or at any time when operational, the software may be updated using the GCP software update option.
2. An external management system can connect to the R-PHY and command it to update its software via SNMP. This option is available even before the RPD is connected to any CCAP device.

The RPD MUST support a software update initiated through the GCP software update feature. The RPD MUST support a software update initiated via SNMP.

A software update is accomplished by providing the RPD a filename, an IP address (v4 or v6) for a software download server and a Code Validation Certificate (CVC). The RPD then uses TFTP or HTTP to go to that server to obtain the software update.

NOTE: This method of software update is intentionally similar to how a DOCSIS CM is assigned a new software image so that the existing DOCSIS infrastructure may be leveraged.

The RPD MUST implement a TFTP client compliant with [RFC 1350] for software file downloads. The RPD MAY implement an HTTP-client compliant with [RFC 1945] or [RFC 2616] for software file downloads. The transfer is SNMP-initiated, as described in [CCAP-OSSI v3.1], or initiated by the CCAP-Core via GCP, as described here.

The RPD MUST include the TFTP block size option [RFC 2348] when requesting the software image file.

The RPD MUST request a block size of 1448 octets if using TFTP over IPv4.

The RPD MUST request a block size of 1428 octets if using TFTP over IPv6.

If the file specified in the GCP Software Upgrade File Name TLV does not match the current software image of the RPD, the RPD MUST request the specified file via TFTP from the software server. The RPD selects the software download server as follows:

- If the RPD communicates with CCAP-Core via IPv4 and receives the Software Upgrade IPv4 TFTP Server TLV via GCP, the RPD MUST use the server specified by this TLV. The RPD MUST ignore the Software Upgrade IPv6 TFTP Server TLV when it communicates with CCAP-Core via using IPv4.
- If the RPD communicates with CCAP-Core via IPv6 and receives the Software Upgrade IPv6 TFTP Server TLV via GCP, the RPD MUST use the server specified by this TLV. The RPD MUST ignore the Software Upgrade IPv4 TFTP Server TLV when it communicates with CCAP-Core via IPv6.

When performing a GCP-initiated software download, the RPD MAY defer normal operation until the download is complete. The RPD MUST verify that the downloaded image is appropriate for itself. If the image is appropriate, the RPD MUST write the new software image to non-volatile storage. Once the file transfer is completed successfully, and the software image is verified, the RPD MUST restart itself with the new code image with a RPD Initialization Reason of SW_UPGRADE_REBOOT.

If the RPD is unable to complete the file transfer for any reason, it MUST remain capable of accepting new software download requests (without operator or user interaction), even if power or connectivity is interrupted between attempts. The RPD MUST log the failure. The RPD MAY report the failure asynchronously to the network manager. The RPD MUST continue to operate with the existing software if an upgrade cannot be performed.

If the RPD receives a valid image, it will automatically upgrade its software, reboot and repeat the entire initialization process, including authentication. Image validation uses the same method involving digital signatures and the PKI certificate as defined in the DOCSIS secure software download process.

If a Principal CCAP-Core initiates a Remote PHY software upgrade during operational configuration or at any time during active operation, then the following events occur:

- The GCP session to the Principal CCAP-Core initiating the update is terminated;
- Any L2TPv3 connections to the Principal CCAP-Core initiating the update are terminated;
- Any active GCP and L2TPv3 connections to other CCAP-Cores are terminated;
- The software upgrade is performed;
- The RPD reboots.

If a network management entity initiates the software upgrade, then the following events occur:

- Any active GCP and L2TPv3 connections to all CCAP-Cores are terminated;
- The software upgrade is performed;
- The RPD reboots.

7.4 Software Code Upgrade Requirements

The following sections define the requirements of the RPD software code upgrade verification process. All RPD code upgrades are prepared and verified as described. All RPDs MUST verify code upgrades according to this specification. The new PKI used for issuing CVCs consists of three types of certificates: a Root CA, a CVC CA, and the CVC. CableLabs manages the new PKI and the certificates issued from its CAs (CableLabs Root CA and CableLabs CVC CA); see [SECv3.1] for certificate profile and extension definitions. The RPD MUST process CVC extensions as defined by [RFC 5280]

NOTE: The CableLabs Root CA is used to issue both RPD Device Certificates and CVC Certificates. RPDs do not support the code upgrade requirements that use the legacy PKI defined in DOCSIS 3.0.

7.4.1 Code File Processing Requirements

The code file format is defined in the [SECv3.1].

The RPD MUST reject the DOCSIS [PKCS#7] code file if the `signedData` field does not match the DER-encoded structure represented in [SECv3.1].

The RPD MUST be able to verify DOCSIS code file signatures that are signed using key modulus lengths of 1024, 1536, and 2048 bits. The public exponent is F_4 (65537 decimal).

The RPD MUST reject the CVC if it does not match the DER-encoded structure represented in [SECv3.1].

The RPD MUST NOT install the upgraded code image unless the code image has been verified as being compatible with the RPD.

If the code download and installation is successful, then the RPD MUST replace its currently stored Root CA Certificate with the Root CA Certificate in the `SignedContent` field, if one was present.

If the code download and installation is successful, then the RPD MUST replace its currently stored Device CA Certificate with the Device CA Certificate received in the `SignedContent` field, if any were present.

7.4.2 Code File Access Controls

In addition to the cryptographic controls provided by the digital signature and the certificate, special control values are included in the code file for the RPD to check before it accepts a code image as valid. The conditions placed on the values of these control parameters MUST be satisfied before the RPD attempts to validate the CVC and the CVS (see Sections 7.4.3.1 and 7.4.3.2).

7.4.2.1 Subject Organization Names

The RPD MUST recognize up to two names that it considers a trusted code-signing agent if present in the subject field of a code file CVC. These are:

- **The RPD manufacturer:** The RPD MUST verify that the manufacturer name in the manufacturer CVC subject field exactly matches the manufacturer name stored in the RPD's non-volatile memory by the manufacturer. A manufacturer CVC is always included in the code file.
- **A co-signing agent:** DOCSIS technology permits another trusted organization to co-sign code files destined for the RPD. In most cases this organization is the operator. The organization name of the co-signing agent is communicated to the RPD via a co-signer CVC via GCP when initializing the RPD's code verification process. The RPD MUST verify that the co-signer organization name in the co-signer CVC subject field exactly matches the co-signer organization name previously received in the co-signer initialization CVC, and stored by the RPD.

7.4.2.2 Time Varying Controls

In support of the code upgrade process, the RPD MUST keep two UTC time values associated with each code-signing agent. These values are known as `codeAccessStart` and `cvcAccessStart`. The RPD MUST store and maintain one pair of time values for the RPD manufacturer signing agent. If the RPD is assigned a code co-signing agent, the RPD MUST maintain a pair of time values for the code co-signing agent.

These values are used to control code file access to the RPD by individually controlling the validity of the CVS and the CVC. Stored and maintained time values in the RPD MUST have a precision of one second. Stored and maintained time values in the RPD MUST be capable of representing all times (with one second precision) between midnight, January 1 1950 and midnight January 1 2050.

The RPD MUST NOT allow the values of `codeAccessStart` and `cvcAccessStart` corresponding to the RPD's manufacturer signing agent to decrease. The RPD MUST NOT allow the value of `codeAccessStart` and `cvcAccessStart` corresponding to the co-signing agent to decrease as long as the co-signing agent does not change and the RPD maintains co-signer time-varying control values (see Section 7.4.5).

7.4.3 RPD Code Upgrade Initialization

Before the RPD can upgrade code, it should be properly initialized. The manufacturer first initializes the RPD.

7.4.3.1 Manufacturer Initialization

It is the responsibility of the manufacturer to install the initial code version in the RPD.

In support of code upgrade verification, values for the following parameters MUST be loaded into the RPD's non-volatile memory:

- RPD manufacturer `organizationName`;
- `codeAccessStart` initialization value;
- `cvcAccessStart` initialization value.

The RPD MUST initialize the values of `codeAccessStart` and `cvcAccessStart` to an `UTCTime` equal to the validity start time of the manufacturer's latest CVC. These values will be updated periodically under normal operation via manufacturer CVCs that are received and verified by the RPD.

7.4.3.2 Operational Initialization

The method for obtaining RPD code download files is defined in Section 7.4.3. The RPD receives settings relevant to code upgrade verification from the Principal CCAP-Core via GCP. The RPD MUST NOT use these settings until after the Principal CCAP-Core has successfully completed the operational bringup of the RPD.

The GCP TLVs normally include the most up-to-date CVC applicable for the destination RPD. When the CCAP-Core initiates a code upgrade, it provides a CVC to initialize the RPD for accepting code files according to this specification. Regardless of whether a code upgrade is required, a CVC in the GCP TLVs MUST be processed by the RPD.

The Principal CCAP-Core enables or disables the RPD's capability to initiate SSU from SNMP through "SSU Control" TLV. This mechanism can be utilized to prevent software upgrades from SNMP interrupting vital services. The Principal CCAP-Core can, for example, restrict the time interval in which software upgrades can be performed to coincide with the MSO's service window.

The RPD is effectively enabled for SSU from SNMP unless it is connected to a Principal CCAP-Core and the Principal CCAP-Core explicitly disables SSU. When the SSU is disabled via GCP, the RPD MUST reject any attempt to initiate SSU from SNMP.

After the RPD is disconnected from the Principal CCAP-Core, the SSU upgrade capability is effectively enabled regardless of the settings established earlier by the Principal CCAP-Core.

GCP TLVs may contain:

- A "SSU Control" TLV disabling or enabling the SW upgrade capability.
- No CVCs;
- From DOCSIS 3.1 PKI:
    - A Manufacturer CVC Chain (the Manufacturer CVC and its issuing CA certificate);
    - A Co-signer CVC Chain (the Co-signer CVC and its issuing CA certificate);

- Both Manufacturer CVC Chain and Co-signer CVC Chain

When the RPD has not received a co-signer CVC, the RPD MUST NOT accept code files that have been co-signed.

If the RPD is configured to accept code co-signed by a code-signing agent, the following parameters MUST be stored in the RPD's memory when the co-signer CVC is processed:

- Co-signing agent's `organizationName`;
- Co-signer `cvcAccessStart`;
- Co-signer `codeAccessStart`.

Unlike the manufacturer `organizationName` and time varying control values, the co-signer `organizationName` and time varying control values are not required to be stored in non-volatile memory.

7.4.3.2.1 Processing the CVC Received via GCP

When a CVC is included in the GCP TLVs, the RPD MUST verify the CVC before accepting any of the code upgrade settings it contains. Upon receipt of the CVC the RPD MUST perform the following validation and procedural steps.

- If any of the following verification checks fail, the RPD MUST immediately halt the CVC verification process.
- If the GCP TLVs do not include a valid CVC, the RPD MUST NOT download upgrade code files, triggered by the GCP.
- If the GCP TLVs do not include a valid CVC, the RPD MUST NOT accept information from a CVC subsequently delivered via an SNMP MIB.

Following receipt of a CVC via GCP, and after the RPD has successfully became operational with the Principal CCAP-Core, the RPD MUST:

1. Verify that the Extended Key Usage extension is present in the CVC, as specified in Appendix III of [SECv3.1].
2. Verify that the manufacturer CVC validity start time is greater than or equal to the manufacturer `cvcAccessStart` value currently held in the RPD if the CVC is a Manufacturer CVC and the subject `organizationName` is identical to the RPD's manufacturer name.
3. Reject this CVC and log an error if the CVC is a Manufacturer CVC and the subject `organizationName` is not identical to the RPD's manufacturer name.
4. Verify that the validity start time is greater than or equal to the co-signer `cvcAccessStart` value currently held in the RPD if the CVC is a Co-signer CVC and the subject `organizationName` is identical to the RPD's current code co-signing agent.
5. After the CVC has been validated, make this subject organization name become the RPD's new code co-signing agent if the CVC is a Co-signer CVC and the subject `organizationName` is not identical to the current code co-signing agent name.
6. Verify that the CVC and any CVC CA Certificate signatures chain up to the Root CA Certificate of the new PKI held by the RPD.
7. Verify that the validity periods for the CVC and the issuing CA certificate have not expired.
8. Update the RPD's current value of `cvcAccessStart` corresponding to the CVC's subject `organizationName` (i.e., manufacturer or code co-signing agent) with the validity start time value from the validated CVC. If the validity start time value is greater than the RPD's current value of `codeAccessStart`, update the RPD's `codeAccessStart` value with the validity start time value.

7.4.3.2.2 Processing the SNMP CVC

The RPD MUST process CVCs received via SNMP when it is enabled to perform SSU. When the RPD is disabled from performing SSU it MUST reject all CVCs received via SNMP. CVCs received via SNMP will also chain up to the same Root CA certificate or public key that was used to validate the CVC from GCP (see Section 7.4.5). When validating a CVC received via SNMP, the RPD MUST perform the following validation and procedural steps. If any

of the following verification checks fail, the RPD MUST immediately halt the CVC verification process, log the error if applicable, and remove all remnants of the process up to that step.

When a RPD receives a CVC via SNMP, it MUST:

1. Verify that the Extended Key Usage extension is in the CVC as specified in Appendix III of [SECv3.1].
2. Verify that the manufacturer CVC validity start time is greater than the manufacturer `cvcAccessStart` value currently held in the RPD if the CVC subject `organizationName` is identical to the RPD's manufacturer name.
3. Verify that the validity start time is greater than the co-signer `cvcAccessStart` value currently held in the RPD if the CVC subject `organizationName` is identical to the RPD's current code co-signing agent.
4. Reject this CVC if the CVC subject `organizationName` is not identical to RPD's manufacturer or current code co-signing agent name.
5. Verify that the CVC and any CVC CA Certificate signatures chain up to the same Root CA Certificate or Root CA key that was used to validate the corresponding CVC (manufacturer or co-signer) from GCP.
6. Verify that the validity periods for the CVC and the issuing CA certificate have not expired.
7. Update the current value of the subject's `cvcAccessStart` values with the validated CVC's validity start time value. If the validity start time value is greater than the RPD's current value of `codeAccessStart`, the RPD MUST replace its `codeAccessStart` value with the validity start value.

7.4.4 Code Signing Guidelines

Manufacturer and operator code signing guidelines are provided in Appendix III of [SECv3.1].

7.4.5 Code Verification Requirements

The RPD MUST NOT install upgraded code unless the code has been verified.

7.4.5.1 RPD Code Verification Steps

When downloading code, the RPD MUST perform the verification checks presented in this section. If any of the verification checks fail, or if any section of the code file is rejected due to invalid formatting, the RPD MUST immediately halt the download process and log the error if applicable, remove all remnants of the process to that step, and continue to operate with its existing code. The verification checks can be made in any order.

1. The RPD MUST verify that:
   - The value of `signingTime` is equal to or greater than the manufacturer `codeAccessStart` value currently held in the RPD;
   - The value of `signingTime` is equal to or greater than the manufacturer CVC validity start time;
   - The value of `signingTime` is less than or equal to the manufacturer CVC validity end time.
2. The RPD MUST verify that:
   - The manufacturer CVC subject `organizationName` is identical to the manufacturer name currently stored in the RPD's memory;
   - The manufacturer CVC validity start time is equal to or greater than the manufacturer `cvcAccessStart` value currently held in the RPD;
   - The Extended Key Usage extension in the Manufacturer CVC meets the requirements of Appendix III of [SECv3.1];
3. The RPD MUST verify that the Mfr CVC chains up to the Root CA held by the RPD.
4. Verify that the validity periods for the CVC and the issuing CA certificate have not expired.
5. The RPD MUST verify the manufacturer code file signature. If the signature does not verify, the RPD MUST reject all components of the code file (including the code image), and any values derived from the verification process should be immediately discarded.

6. If the manufacturer signature verifies and a co-signing agent signature is required:

    a) The RPD MUST verify that:
        (1) The co-signer signature information is included in the code file;
        (2) The value of `signingTime` is equal to or greater than the corresponding `codeAccessStart` value currently held in the RPD;
        (3) The value of `signingTime` is equal to or greater than the corresponding CVC validity start time;
        (4) The value of `signingTime` is less than or equal to the corresponding CVC validity end time.

    b) The RPD MUST verify that:
        (1) The co-signer CVC subject `organizationName` is identical to the co-signer organization name currently stored in the RPD's memory;
        (2) The co-signer CVC validity start time is equal to or greater than the `cvcAccessStart` value currently held in the RPD for the corresponding subject `organizationName`;
        (3) The Extended Key Usage extension in the Co-signer CVC meets the requirements of Appendix III of [SECv3.1].

    c) The RPD MUST verify that the Co-Signing CVC Certificate chains up to the Root CA held by the RPD.
    d) The RPD MUST verify that the validity periods for the CVC and the issuing CA certificate have not expired.
    e) The RPD MUST verify the co-signer code file signature. If the signature does not verify, the RPD MUST reject all components of the code file (including the code image), and any values derived from the verification process should be immediately discarded.

7. Once the manufacturer, and optionally the co-signer, signature has been verified, the code image can be trusted and installation may proceed. Before installing the code image, all other components of the code file and any values derived from the verification process except the [PKCS#7] `signingTime` values and the CVC validity start values SHOULD be immediately discarded.
8. The RPD upgrades its software by installing the code file according to Section 7.3.
9. If the code installation is unsuccessful, the RPD MUST discard the [PKCS#7] `signingTime` values and CVC validity start values it just received in the code file. The procedure for handling this failure condition is specified in [MULPI v3.1].
10. Once the code installation is successful, the RPD MUST:

    a) Update the current value of manufacturer `codeAccessStart` with the [PKCS#7] `signingTime` value;
    b) Update the current value of manufacturer `cvcAccessStart` with the CVC validity start value.

11. If the code installation is successful, and if the code file was co-signed, the RPD MUST:

    a) Update the current value of the co-signer `codeAccessStart` with the [PKCS#7] `signingTime` value;
    b) Update the current value of the co-signer `cvcAccessStart` with the CVC validity start value.

7.4.6 DOCSIS Interoperability

Images for RPD secure software download are to be signed using certificates from the new PKI defined in the [SECv3.1] specification. Images for legacy secure software download are signed using certificates from the legacy PKI defined in [SECv3.0]are not supported by RPDs. The RPD supports secure software downloads using certificates only from the new PKI.

7.4.7 Error Codes

The RPD MUST log the following error events when they occur during the code verification process. RPD event logging requirements and event message format are defined in [R-OSSI].

1. Improper code file controls

    Conditions:

    a) CVC subject `organizationName` for manufacturer does not match the RPD's manufacturer name.

b) CVC subject `organizationName` for code co-signing agent does not match the RPD's current code co-signing agent.
c) The manufacturer [PKCS#7] `signingTime` value is less-than the `codeAccessStart` value currently held in the RPD.
d) The manufacturer [PKCS#7] validity start time value is less-than the `cvcAccessStart` value currently held in the RPD.
e) The manufacturer CVC validity start time is less-than the `cvcAccessStart` value currently held in the RPD.
f) The manufacturer [PKCS#7] `signingTime` value is less-than the CVC validity start time.
g) Missing or improper extended key-usage extension in the manufacturer CVC.
h) The co-signer [PKCS#7] `signingTime` value is less-than the `codeAccessStart` value currently held in the RPD.
i) The co-signer [PKCS#7] validity start time value is less-than the `cvcAccessStart` value currently held in the RPD.
j) The co-signer CVC validity start time is less-than the `cvcAccessStart` value currently held in the RPD.
k) The co-signer [PKCS#7] `signingTime` value is less-than the CVC validity start time.
l) Missing or improper extended key-usage extension in the co-signer CVC.

2. Code file manufacturer CVC validation failure

   Conditions:

   a) The manufacturer CVC in the code file does not chain to the same root CA as the manufacturer CVC received via GCP.

3. Code file manufacturer CVS validation failure
4. Code file co-signer CVC validation failure

   Conditions:

   a) The co-signer CVC in the code file does not chain to the same root CA as the co-signer CVC received via GCP.

5. Code file co-signer CVS validation failure.
6. Improper format of CVC received via GCP.

   Conditions:

   a) Missing or improper key usage attribute.

7. Validation failure of CVC received via GCP.
8. Improper SNMP CVC format.

   Conditions:

   a) CVC subject `organizationName` for manufacturer does not match the RPD's manufacturer name.
   b) CVC subject `organizationName` for code co-signing agent does not match the RPD's current code co-signing agent.
   c) The CVC validity start time is less-than or equal-to the corresponding subject's `cvcAccessStart` value currently held in the RPD.
   d) Missing or improper key usage attribute.

9. SNMP CVC validation failure.

   Conditions:

   a) The manufacturer CVC received via SNMP does not chain to the same root CA as the manufacturer CVC received via GCP.
   b) The co-signer CVC received via SNMP does not chain to the same root CA as the co-signer CVC in the received via GCP.

7.5 Security Considerations (Informative)

The method(s) used to protect private keys are a critical factor in maintaining security. Users authorized to sign code, i.e., manufacturers and operators who have been issued code verification certificates (CVCs) by the DOCSIS root CA, should protect their private keys. An attacker with access to the private key of an authorized code-signing user can create, at will, code files that are potentially acceptable to a large number of RPDs.

The defense against such an attack is for the operator to revoke the certificate whose associated code-signing private key has been learned by the attacker. To revoke a certificate, the operator delivers to each affected RPD, an updated CVC with a validity start time that is newer than that of the certificate(s) being revoked. The new CVC can be delivered via any of the supported mechanisms: GCP, code file, or SNMP. The new CVC implicitly revokes all certificates whose validity start time is earlier than that of the new CVC.

To reduce the vulnerability to this attack, operators should regularly update the CVC in each RPD, at a frequency comparable to how often the operator would update a CRL if one were available. Regular updates help manage the time interval during which a compromised code-signing key is useful to an attacker. CVCs should also be updated if it is suspected that a code-signing key has been compromised. To update the CVC, the user needs a CVC whose validity start time is newer than the CVC in the RPD. This implies that the DOCSIS root CA regularly issues new CVCs to all authorized code-signing manufacturers and operators, to make the CVCs available for update.

When an RPD is attempting to become operational with the Principal CCAP-Core for the first time or after being off-line for an extended period, it should receive a trusted CVC as soon as possible. This provides the RPD with the opportunity to receive the most up-to-date CVC available and deny access to CVCs that needed to be revoked since the RPD's last initialization. The first opportunity for the RPD to receive a trusted CVC is via GCP from the Principal CCAP-Core. The Principal Core has the ability to control RPD's ability to perform the SSU through a dedicated GCP TLV. If the Principal Core disables SSU, the RPD will not request or have the ability to remotely upgrade code files. In addition, the RPD will not accept CVCs subsequently delivered via SNMP.

To mitigate the possibility of an RPD receiving a previous code file via a replay attack, the code files include a signing-time value in the [PKCS#7] structure that can be used to indicate the time the code image was signed. When the RPD receives a code file signing-time that is later than the signing-time it last received, it will update its internal memory with this value. The RPD will not accept code files with an earlier signing-time than this internally stored value. To upgrade an RPD with a new code file without denying access to past code files, the signer may choose not to update the signing-time. In this manner, multiple code files with the same code signing-time allow an operator to freely downgrade an RPD's code image to a past version (that is, until the CVC is updated). This has a number of advantages for the operator, but these advantages should be weighed against the possibilities of a code file replay attack.

Without a reliable mechanism to revert back to a known good version of code, any code-update scheme, including the one in this specification, has the weakness that a single, successful forced update of an invalid code image may render the RPD useless, or may cause the RPD to behave in a manner harmful to the network. Such an RPD may not be repairable via a remote code update, since the invalid code image may not support the update scheme.

8 X.509 CERTIFICATE PROFILE AND MANAGEMENT

R-PHY employs X.509 version 3 digital certificates for authenticating key exchanges between RPD and NAD and between RPD and CCAP-Core. [X.509] is a general-purpose standard; the certificate profile, described here, further specifies the contents of the certificate's defined fields. This certificate profile also defines the hierarchy of trust for the management and validation of certificates.

Except where otherwise noted in Annex E, the certificates used comply with [RFC 5280].

8.1 Certificate Management Architecture Overview

The certificate management architecture for RPD authentication uses the DOCSIS 3.1 PKI defined by [SECv3.1]. The PKI consists of a three-level hierarchy of trust supporting three types of certificates:

- Root CA Certificate;
- Device CA Certificate;
- RPD Device Certificates.

The Root CA Certificate is used as a trust anchor for the PKI and issues the Device CA Certificate that issues the RPD Device Certificates. The PKI uses a "centralized" model where the Device CA is hosted by CableLabs or an approved 3rd party that issues RPD Device Certificates to approved manufacturers. CableLabs manages the PKI and the certificates issued from its CAs (for information about CableLabs Root CA and CableLabs Device CA, see Annex E).

The Root CA will also be used as a trust anchor for issuing and validating CA and Code Verification Certificates (CVCs) for the Secure Software Download (SSD) process specified in Section 7.

The Root CA generates and distributes to operators a Certificate Revocation List (CRL), identifying revoked manufacturer certificates. The manner in which CRLs are distributed is outside the scope of this specification. In order to reduce the burden on RPD devices that are designed to work in multiple geographic regions, an effort will be made to consolidate the DOCSIS 3.1 PKI hierarchy such that the same device certificate for DOCSIS 3.1 will also be valid for EuroDOCSIS 3.1 and other international versions of DOCSIS 3.1 and above.

8.2 RPD Certificate Storage and Management in the RPD

The RPD MUST have a factory installed RPD Device Certificate (and associated private keys) that is issued from the new PKI. The RPD uses the RPD Device Certificate when authenticating with a NAD or CCAP-Core.

The RPD's non-volatile memory MUST contain a Root CA certificate for SSD image verification.

The RPD MAY be capable of updating or replacing the Device CA Certificate via the DOCSIS code download file (see Section 7).

The RPD MUST be able to process certificate serial number values containing 20 octets or fewer. The RPD MUST accept certificates that have serial numbers that are negative or zero.

8.3 Certificate Processing and Management in the CCAP-Core

IKEv2 (see [RFC 7296]) employs digital certificates to verify the binding between a device's identity (encoded in a digital certificate's subject name) and its public key. The CCAP-Core does this by validating the RPD Device Certificate's certification path. This path will typically consist of three chained certificates: the RPD Device Certificate, the Device CA certificate and the Root CA certificate (see section 8.1). Validating the chain follows the "Basic Path Validation" rules defined in [RFC 5280].

The CCAP-Core MUST support validating certificate chains from the DOCSIS 3.1 PKI.

[RFC 4131] requires that CCAP-Cores support administrative controls that allow the operator to override certification chain validation by identifying a particular CA or RPD Device Certificate as trusted or untrusted. This section specifies the management model for the exercise of these controls, as well as the processing a CCAP-Core undertakes

to assess a RPD Device Certificate's validity, and thus verify the binding between the RPD's identity and its public key.

The CCAP-Core MUST be able to process certificate serial number values containing 20 octets or fewer. The CCAP-Core MUST accept certificates that have serial numbers that are negative or zero.

Annex E describes the format of the subject name field for each type of DOCSIS certificate. The issuer field of a certificate exactly matches the subject field of the issuing certificate. DOCSIS 3.1 PKI certificates transmitted by an RPD have name fields that conform to the format described in Annex E. A CCAP-Core MUST be capable of processing the name fields of a certificate if the name fields conform to the indicated format in Annex E. A CCAP-Core MAY choose to accept a certificate that has name fields that do not conform to the indicated format in Annex E.

The CCAP-Core MUST process certificate extensions as defined by [RFC 5280] (see Annex E for certificate profile and extension definitions).

8.3.1 CCAP-Core Certificate Management Model

The CCAP-Core holds copies of the Root CA, Device CA, and RPD Device Certificates (see Section 8.1), which it obtains in one of two ways: 1) provisioning, or 2) IKEv2 messaging. Each certificate learned by a CCAP-Core MUST be assigned one of four states:

- Untrusted,
- Trusted,
- Chained, or
- Root.

The CCAP-Core MUST support the ability to provision at least two Root CA Certificates. The CCAP-Core MUST support the ability to display the entire Root Certificate(s) and/or its thumbprint to the operator.

A CCAP-Core learns of Device CA certificates through either the CCAP-Core's provisioning interface or through receipt and processing of the client RPDs' Authentication Information messages. Regardless of how a CCAP-Core obtains its Device CA certificates, the CCAP-Core MUST mark them as either Untrusted, Trusted, or Chained. If a CA Certificate is not self-signed, the CCAP-Core MUST mark the certificate as Chained. The CCAP-Core, however, MUST support administrative controls that allow an operator to override the Chained marking and identify a given CA certificate as Trusted or Untrusted.

If a Device CA Certificate is self-signed, the CCAP-Core MUST mark the certificate as either Trusted or Untrusted, according to administratively controlled CCAP-Core policy.

A CCAP-Core obtains copies of RPD Device Certificates in the IKEv2 messages it receives from RPDs. RPD Device Certificates are issued by a Device CA. Thus, the CCAP-Core MUST mark RPD Device Certificates as Chained unless overridden by CCAP-Core administrative control and configured as Trusted or Untrusted.

8.3.2 Certificate Validation

The CCAP-Core validates the certification paths of CA and RPD Device Certificates using Basic Path Validation rules defined in [RFC 5280] and the criteria below.

The CCAP-Core MUST label CA and RPD Certificates as Valid or Invalid if their certification paths are valid or invalid respectively. Trusted certificates, provisioned in the CCAP-Core, MUST be Valid; this is true even if the current time does not fall within the Trusted certificate's validity period. Untrusted certificates, provisioned in the CCAP-Core, MUST be Invalid.

The CCAP-Core MUST mark a chained certificate as Valid only if:

1. The certificate chains to a Root CA, Trusted, or Valid certificate that has not been revoked as defined by the Basic Path Validation section in [RFC 5280]; and
2. The current time falls within the validity period of each Chained or Root certificate within the certificate chain; and

3. The certificate is not identified as revoked (see Section 8.4); and
4. In the case of a RPD Device Certificate, the RPD MAC address encoded in its `tbsCertificate`.subject field and RSA public key encoded in its `tbsCertificate.subjectPublicKeyInfo` field match the RPD MAC address and RSA public key encoded in the IKEv2 messaging; and
5. In the case of an RPD Device Certificate, if the KeyUsage extension is present, the digitalSignature and/or keyAgreement bits are turned on, the keyEncipherment bit is turned on, and the keyCertSign and cRLSign bits are off. In the case of a Device CA Certificate, if the KeyUsage extension is present, the keyCertSign bit is turned on.

Whether criterion 2 above is ignored MUST be subject to CCAP-Core administrative control.

If validity period checking is enabled and the time of day has not been acquired by the CCAP-Core, a (non-permanent) authorization reject message MUST be returned by the CCAP-Core in response to an authorization request.

The CCAP-Core MUST NOT invalidate certificates that have non-specified critical extensions (contrary to [RFC 5280]) as long as the certificates satisfy the validity criteria above.

8.4 Certificate Revocation

Providing a mechanism for certificate revocation is a normal part of PKI management. When a certificate is issued, it is expected to be in use for its entire validity period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name, change of association between subject and CA, and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA needs to revoke the certificate.

Two methods of supporting certificate revocation are defined in this specification: 1) Certificate Revocation Lists (CRLs), and 2) Online Certificate Status Protocol (OCSP). The CCAP-Core MUST support configuration of none, one, or both certificate revocation methods to be enabled at the same time.

8.4.1 Certificate Revocation Lists

[RFC 5280] defines a method for revoking certificates using [X.509] Certificate Revocation Lists (CRLs).

Figure 19 shows a framework for managing and distributing CRLs. A CRL is a digitally signed, timestamped list of certificate serial numbers revoked by a Certificate Authority (CA). When a CA identifies the compromised certificates, the CA could generate the CRLs itself, or a CA could delegate the CRL generation to a third party CRL Issuer. The CRL Repository is a system that maintains a database of revoked certificates. A description of the interface between the CA or CRL Issuer and CRL Repository is outside the scope of this specification.

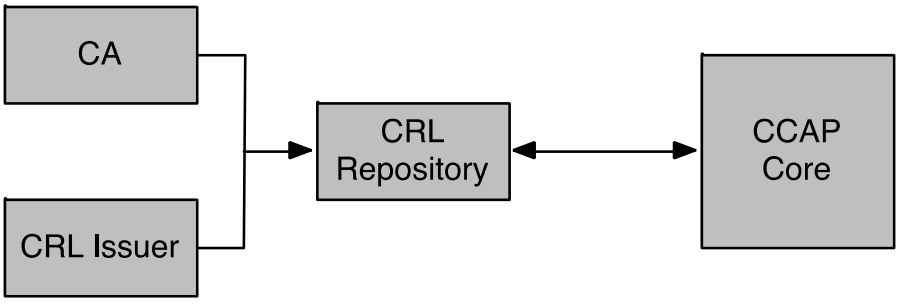

Figure 19 - CRL Framework

The CCAP-Core retrieves CRL entries from the CRL Repository and uses this information to verify if a certificate received during the RPD authentication process is revoked.

8.4.1.1 CCAP-Core CRL Support

The CCAP-Core MUST support retrieval of CRL files formatted as defined in [RFC 5280]. CRL files may identify revoked certificates that were issued from different CAs. Therefore, the CCAP-Core MUST support extensions related to indirect CRL files, as defined in [RFC 5280]. The CCAP-Core MUST support HTTP as defined in [RFC 2616] for downloading CRL files.

Before using the information in a CRL file, the CCAP-Core MUST verify that its digital signature chains to a trusted root CA. Trusted root CAs are administratively provisioned in the CCAP-Core. If the CRL file digital signature cannot be verified, the CCAP-Core MUST discard the CRL file. The CCAP-Core MUST validate if a CA certificate or RPD Device Certificate is revoked during the certificate validation process specified in Section 8.3.2.

If the CRL contains the nextUpdate value, the CCAP-Core MUST refresh the CRL after the specified time has passed. If the CCAP-Core fails to retrieve the new CRL, it MUST log an event (see [CCAP-OSSI v3.1]) and continue to use its current CRL. If the CCAP-Core fails to retrieve the new CRL it should attempt to retry retrieval of the CRL file on a periodic basis. If the CRL does not contain the nextUpdate value, the CCAP-Core MUST refresh the CRL according to the configured value as defined in [CCAP-OSSI v3.1].

When the CCAP-Core is configured to use a CRL it MUST attempt to retrieve the CRL file each time it starts up. During CCAP-Core startup it is possible that some RPDs may perform IKEv2 authorization before the CRL file has been retrieved. When the CCAP-Core is configured to use a CRL and an RPD's device certificate chain is validated during CCAP-Core startup before the CRL file is retrieved, the CCAP-Core MUST log an event for that RPD [CCAP-OSSI v3.1] and bypass CRL checking.

8.4.2 Online Certificate Status Protocol

[RFC 6960] defines an Online Certificate Status Protocol (OCSP) for querying the status of a digital certificate. The CCAP-Core sends a certificate status request to an OCSP responder when it receives a CA certificate or an RPD Device Certificate (see Figure 20). The OCSP responder sends a status response indicating that the certificate is either "good," "revoked," or "unknown." The OCSP responder checks only the revocation status of a certificate; it does not verify the validity of the certificate itself. The CCAP-Core uses the result from the OCSP responder during the certificate validation process specified in Section 8.3.2.

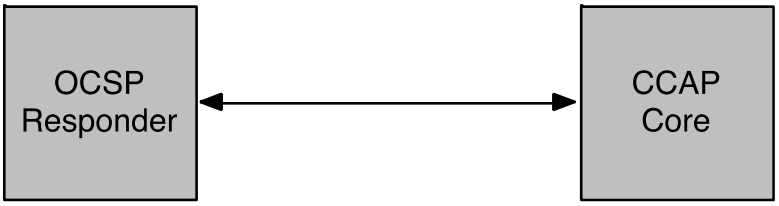

Figure 20 - OCSP Framework

The CCAP-Core MUST be capable of acting as an OCSP client as defined in [RFC 6960]. The CCAP-Core SHOULD cache the OCSP response status for a certificate if the nextUpdate value is present in the OCSP response. If the CCAP-Core caches the OCSP response status for a given certificate, it MUST retrieve the revocation status from the cache. Once the nextUpdate time for that certificate has passed, the CCAP-Core MUST continue using the revocation status value from the cache until an update is retrieved from the OCSP Responder. If the CCAP-Core is unable to retrieve the OCSP status for an uncached certificate or if the retrieved status is "unknown," the CCAP-Core MUST log an event [CCAP-OSSI v3.1] and assume the certificate status to be "good."

If the nextUpdate value is not present in the OCSP response, the CCAP-Core MUST NOT cache the OCSP response status for a certificate. If the CCAP-Core is configured with OCSP Responder information, it MUST send an OCSP request when a CA certificate or RPD Device Certificate is obtained using the Authentication Information message, or Authentication Request message respectively, unless there is a valid certificate status in the cache.

When the CCAP-Core is attempting to communicate with the OCSP Responder, the exchange should not significantly delay the RPD provisioning process. If no response is received, the CCAP-Core MUST proceed using the currently cached revocation status. For uncached certificate states, the CCAP-Core MUST proceed as if a response with the status "good" has been received.

The CCAP-Core MUST support OCSP over HTTP as described in [RFC 6960]. The CCAP-Core MAY generate a signature in the OCSP request. The CCAP-Core MUST bypass validation of the signature in an OCSP response based on the configured value as defined in [CCAP-OSSI v3.1].

9 PHYSICAL PROTECTION OF KEYS IN THE RPD

RPDs MUST store and maintain the RPD Device Certificate RSA private/public key pairs. The RPD MUST store the RPD Device Certificate private keys in a manner that deters unauthorized disclosure and modification. Also, RPDs SHOULD prevent debugger tools from reading the RPD Device Certificate private key in production devices by restricting or blocking physical access to memory containing this key.

The RPD MUST meet [FIPS 140-2] security requirements for all instances of private and public permanent key storage.

The RPD MUST meet [FIPS 140-2] Security Level 1. FIPS 140-2 Security Level 1 requires minimal physical protection through the use of production-grade enclosures. The reader should refer to the cited document for the formal requirements; however, below is a summary of those requirements.

Under the [FIPS 140-2] classification of "physical embodiments" of cryptographic modules, external RPDs are "multiple-chip stand-alone cryptographic modules. FIPS 140-2 specifies the following Security level 1 requirements for multiple-chip stand-alone modules:

- The chips are to be of production-grade quality, which shall include standard passivation techniques (i.e., a sealing coat over the chip circuitry to protect it against environmental or other physical damage);
- The circuitry within the module is to be implemented as a production grade multiple-chip embodiment (i.e., a printed circuit board, a ceramic substrate, etc.);
- The module is to be entirely contained within a metal or hard plastic production-grade enclosure, which may include doors or removable covers.

10 SYSTEM OPERATION (NORMATIVE)

Once the system is operational, there is very little that happens with the MHAv2 protocols. Most of the operational features are managed within the DOCSIS protocol that is run transparently over MHAv2.

This section explains some variations to the MHAv2 operational state. One of those variations is the location of the upstream scheduler.

10.1 DOCSIS Upstream Scheduling

The RPD is intended to be a simple and lightweight extension of the CCAP. MHAv2 permits the upstream scheduler to be located either centrally or remotely. Note that the [R-UEPI] protocol provides sufficient quality of service mechanisms that the upstream scheduler can be run centrally.

The advantages of running a centralized upstream scheduler are:

- Similar CMTS software model to an Integrated CMTS.
- Similar operational model to an Integrated CMTS.
- Scheduler software is from the same vendor as the CMTS software.
- Fewer interoperability problems between different vendors of CCAP-Core and the RPD.
- Access to Debug mode if there are problems with the remote scheduler.
- Scalable resources for the scheduler if more CPU power is needed.

The advantages of running a distributed upstream scheduler are:

- Shorter round-trip delay from request to grant that may impact some aspects of performance.

For plant distances of 100 miles or less, the Remote PHY and I-CMTS systems have nearly identical performance as the I-CMTS, since the I-CMTS is a centralized scheduler system (because the PHY is also centralized). With the PHY removed from the CMTS Core, the CMTS Core can be located at distances much greater than the original 100 mile limit for DOCSIS. In these cases, the REQ-GNT turn around time could be extended by several additional milliseconds. However, the DOCSIS scheduler is a pipelined system. If the time between grants increases, then the number of bytes per grant will increase to compensate.

The R-PHY system defaults to a centralized scheduler because the differences in performance are negligible and the benefits are measureable. Support for a distributed scheduler is not included at this time.

10.1.1 Centralized Scheduling Requirements

The requirements regarding centralized scheduling are:

- The RPD MUST support operation with a centralized scheduler.
- The RPD MAY support operation with a distributed scheduler.

10.2 Daisy-chaining of the Backhaul Ethernet Port

The RPD may be located in a node enclosure with other entities that aggregate to the same backhaul link to the CIN. Two distinct forms of aggregation are supported:

1. All RPDs connect to an Ethernet switch or hub which then connects to the CIN.
2. Each RPD is daisy-chained with the next RPD, and the last RPD connects to the CIN. In the case of daisy-chaining, it is as if each RPD has a three-port Ethernet switch associated with it that lets traffic either pass through, or to be injected/removed by the device.

10.2.1 Backhaul Daisy-chaining Requirements

The requirements regarding backhaul daisy-chaining are:

- Each RPD that is to be individually authenticated MUST have its own MAC address and its own IP address assignment.
- When operating in a daisy-chained topology, the RPD MUST support the authentication requirements defined in Section 6.3.

10.3 Networking Considerations

It is important to distinguish between the terms “PHB-ID” and “DSCP” as used in the MHAv2 specifications:

- A “PHB-ID” is a 6-bit value appearing in an L2TPv3 Attribute Value Pair (AVP)
- A “DSCP” is a 6-bit value appearing in an IP packet header

All L2TPv3 packets in [R-DEPI] are in a control session, a PSP session, or a non-PSP session. All PSP sessions contain both downstream and upstream data “flows”. PHB-IDs apply to flows of PSP data sessions. DSCPs apply to the IP packets that encapsulate all L2TPv3 packets, i.e., DSCPs apply to control sessions, PSP sessions, and non-PSP sessions.

For a downstream PSP flow, the CCAP-Core assigns via L2TPv3 AVPs the PHB-ID for each downstream PSP flow. The assigned downstream flow PHB-ID selects the scheduling behavior for that flow *only on the RPD*, i.e., for the scheduling of multiple downstream PSP flows on the single hop from CIN to RF network. At a minimum, an RPD SHOULD provide highest-priority strict priority service to PSP flows assigned to the Expedited Forwarding(46) PHB-ID. Support for more complex scheduling disciplines, e.g. multiple strict priorities or weighted fair queueing, is for further study.

The RPD advertises via GCP to the CCAP-Core what PHB-IDs it supports for downstream PSP flow scheduling. An RPD MUST support at least the Expedited Forwarding (46) and BestEffort(0) PHB-IDs. The use of PHB-IDs other than ExpeditedForwarding(46) and BestEffort(0) is for further study.

For a downstream PSP flow, The CCAP-Core selects the DSCP to send in the IP header of the L2TPv3 data session packets for the flow. The DSCP selects the per-hop behavior *on each CIN router* between the CCAP-Core and RPD. The 6-bit DSCP of the IP headers of downstream L2TPv3 data packets on a PSP flow may or may not equal the 6-bit PHB-ID assigned to the flow on the RPD itself. For example, the CCAP-Core may use more than two different DSCP values when the CIN supports them. The RPD ignores the DSCP of a downstream IP packet and uses only the flow ID in the inner PSP sub-layer to select the queue with which it schedules downstream data for the flow.

For an upstream PSP flow, the CCAP-Core assigns via L2TPv3 AVPs the PHB-ID for each upstream PSP flow. For the upstream case, the PHB-ID corresponds to a “recommended DSCP value” as described in [RFC 3140]. The RPD sets the DSCP in the IP headers of all upstream L2TPv3 data packets for a PSP flow to the PHB-ID value assigned to that flow. The PHB-ID assigned to an upstream PSP flow does not identify any per-hop beviour in the RPD itself.

10.3.1 Per Hop Behavior

The IETF has defined a number of Per Hop Behaviors (PHBs) to be used for offering network-based QoS. DEPI supports use of the 6-bit Expedited Forwarding (EF) PHB as described in [RFC 3246], Assured Forwarding (AF) PHBs as described in [RFC 2597], and best effort forwarding as described in [RFC 2597]. DEPI negotiates six-bit Per-Hop Behavior Identifiers (PHBIDs) between the CCAP-Core and the RPD.

The RPD advertises the PHB-IDs it supports for its downstream PSP packet scheduler. The RPD MUST support Expedited Forwarding(46) and BestEffort(0) PHB-IDs. The RPD SHOULD provide highest strict priority scheduling service to PSP flows assigned to the Expedited Forwarding(46) PHB-ID. The CCAP-Core SHOULD support assigning the Expedited Forwarding(46) PHB-ID to a separate PSP flow for MAPs+UCDs with Best Effort (0) for all other traffic.

For upstream flows, the RPD MUST support signaling of an arbitrary 6-bit PHB-ID as the transmitted 6-bit DSCP value.

NOTE: Table 1 lists the PHBs explicitly supported by the DEPI specification. This specification does not prohibit support for other PHBs not defined in Table 1.

Table 1 - PHBs and Recommended DSCP Values

PHB	PHB ID(s) and Recommended DSCP Value(s)
EF	46
AF (multiple levels)	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38
Best effort	0

The DEPI interface supports multiple traffic types including DOCSIS MAC and DOCSIS data traffic. Within both traffic types, there may be different levels of priority. For PSP operation, the CCAP-Core SHOULD provide a mechanism to map traffic of different priorities to DEPI flows with different PHB values. The CCAP-Core SHOULD NOT use the same PHB across multiple DEPI flows within a session.

The CIN should provide the appropriate Per Hop Behavior for the differentiated traffic types. The level of granularity provided for differentiated traffic is determined by the network operator, but at a minimum, it is expected that DOCSIS MAP messages and VoIP data traffic are prioritized higher than best effort data traffic.

The RPD uses the PHB signaled in the establishment of the DEPI flow when scheduling multiple DEPI PSP flows onto one QAM channel as described in [R-DEPI].

10.3.2 DiffServ Code Point Usage

An operator sets up CIN network elements to support a particular set of DSCPs. The selected DSCPs should select appropriate per-hop behavior at each network element for differentiated traffic types.

For L2TPv3 data sessions, packets in the same direction have the same DSCP; packets in different directions may have different DSCPs. For PSP L2TPv3 sessions, each PSP “flow” in the session and in a particular direction may have a different DSCP value. Different PSP flows in the same PSP session may have the same DSCP.

The CCAP-Core is responsible for selecting the DSCP values of all L2TPv3 control and data session packets, including the DSCP sent by the RPD.

The CCAP-Core and RPD MUST:

- set the same DSCP on all L2TPv3 control packets;
- set the same DSCP on all L2TPv3 data packets of the same non-PSP session in a direction;
- set the same DSCP on all L2TPv3 data packets of the same PSP flow in a direction.

DOCSIS frames encapsulated in L2TPv3 packets may contain IP packets which also have a DSCP assigned. The RPD is not required to schedule packets based upon the original DSCP contained within the DOCSIS frame.

10.3.3 Packet Sequencing

For a stream of packets transmitted on a DEPI flow, the packet sequence number is incremented by one for each packet sent, as described in [R-DEPI].

If the RPD detects a discontinuity in the packet sequence numbers indicating that one or more packets were dropped or delayed, an error is logged and the RPD SHOULD transfer the current packet to the QAM channel without waiting for the missing packets. If the RPD detects a discontinuity in the packet sequence numbers indicating that one or more packets have arrived late, those packets SHOULD be discarded.

The RPD MUST NOT forward packets that were skipped due to a discontinuity in the sequence numbers. Storing and re-ordering of packets so that they can be delivered to the QAM channel in the correct sequence is not prohibited by these requirements and the RPD MAY perform such re-ordering as long as the latency requirements of Section 5.6 are met.

10.3.4 Network MTU

The network between the CCAP-Core and the RPD has a certain Maximum Transmission Unit (MTU). If a maximum size DOCSIS frame were to be tunneled from the CCAP-Core to the RPD without fragmentation, the size of the resulting packet could be greater than the CIN can handle. Both the D-MPT and PSP modes avoid this issue by offering streaming and fragmentation. As such, IP fragmentation is not required. IP fragmentation is also undesirable because the RPD may forward packets based upon the destination UDP port, and the UDP port is only available in the first IP fragment.

Determining the MTU to use for the L2TPv3 tunnel between the CCAP-Core and the RPD is a two-step process:

1. Choose the payload size.
2. Determine the MTU of the path between the CCAP-Core and the RPD.

The first step is done as part of L2TPv3 session establishment (see [R-DEPI]) using the DEPI MTU AVPs. When the CCAP-Core sends the session ICRQ message it MUST supply the DEPI Local MTU AVP with a payload size that is the lesser of its receive capabilities and the receive capabilities defined by its lower layer. The receive capabilities of the CCAP-Core are defined by its internal constraints, and any configured maximums. The receive capabilities defined by its lower layer are calculated based on referencing the payload size constraints of the interface below which this tunnel is being created, as defined in Annex A.1.

The CCAP-Core MUST support an MTU size of at least 2000 bytes, as calculated in Annex A.1. The RPD MUST send L2TPv3 frames with a payload size less than or equal to this maximum. If the RPD cannot meet this criterion then it MUST fail session creation by generating a CDN message. The RPD needs to consider the same criteria in calculating its MTU.

The RPD MUST support an MTU size of at least 2000 bytes, as calculated in Annex A.1. The RPD MUST insert the DEPI Remote MTU AVP in the ICRP message with its MTU size. The CCAP-Core MUST send L2TPv3 frames with a payload size less than or equal to this maximum. If the CCAP-Core cannot meet this criterion then it MUST fail session creation by generating a CDN message.

The second step is to determine the MTU of the path between the CCAP-Core and the RPD. The CCAP-Core MUST provide a mechanism to prevent sending packets larger than the network MTU. This SHOULD be done using Path MTU Discovery, as described in [RFC 1191]. Annex A.3 gives a brief overview of the Path MTU discovery protocol.

Alternatively, this MAY be done via a static configuration option. Both the CCAP-Core and the RPD MUST have a way to statically configure an MTU for each L2TPv3 session. To avoid IP fragmentation, the CCAP-Core and the RPD MUST set the Don't Fragment bit (DF) in the IPv4 header for all transmissions into the L2TPv3 pseudowire.

10.4 Pilot Tone Generation

Pilot tones in the HFC network are required to ensure that amplifiers in the network are operating correctly. Amplifiers use these tones to adjust gain and keep signals at the appropriate output level. The RPD in a distributed CCAP architecture is required to be capable of generating these tones and placing these tones in the appropriate portion of the downstream spectrum under control of the CCAP-Core. Pilot tones, in this context, are used for Automatic Gain Control (AGC) and should not be confused with the pilots used in OFDM/OFDMA channels.

The RPD MUST support pilot tone generation.

The RPD MUST support up to four frequencies for CW pilot tones per chassis simultaneously.

The RPD MUST support a minimum of two CW pilot tones output per downstream RF port.

The RPD MUST support placing CW pilot tones from 54 to 535 MHz.

The RPD SHOULD support placing CW pilot tones from 54 to 1218 MHz.

The RPD MUST allow the pilot tone to be set in a range of +3 dB to +9 dB in 0.2 dB steps relative to the 256-QAM level.

The RPD SHOULD allow pilot tones to be set in absolute dBmV across that range.

The RPD MUST support a pilot tone power accuracy of ±2 dB. Time and temperature stability requirements are expected to be defined in a product specification document.

The RPD MUST support a minimum pilot tone quality (e.g., 2nd and 3rd harmonics, 2nd and 3rd inter-modulation distortion, spurs, etc.) of 65 dBc relative to the pilot tone output power, in the case where $N_{eq}' \geq N_{eq}/4$ where:

- N_{eq}' = Number of equivalent active 6 MHz channels combined per RF port
- N_{eq} = Number of equivalent channels the RPD is capable of per RF port

The RPD MUST meet the requirements for noise in other channels (47 MHz to 1002 MHz) as defined in the CMTS Output Out-of-Band Noise and Spurious Emissions Requirements table of [PHY v3.1] for the given N_{eq} and N_{eq}', with the exception of channels coinciding with the pilot tones' harmonics products. For this purpose, channels occupied by pilots are considered active channels, but the noise is calculated relative to the 6 MHz equivalent channels' power.

11 MULTIPLE CCAP-CORE OPERATION

11.1 Introduction

The MHAv2 architecture permits RPDs to be managed by more than one CCAP-Core. An RPD is controlled by exactly one "principal" CCAP-Core and zero or more "auxiliary" CCAP-Core(s). An "auxiliary" core manages a subset of RPD resources, e.g., particular channels or RF ports. Each auxiliary CCAP-Core establishes its own GCP session and L2TPv3 control sessions with the RPD. The specification term "CCAP-Core" can refer to either the principal core or an auxiliary core.

Potential auxiliary CCAP-Cores include but are not limited to the following:

- A "Broadcast EQAM" CCAP-Core that controls only downstream video broadcast channels;
- A "Narrowcast EQAM" CCAP-Core that controls only downstream video narrowcast channels;
- A "Forward OOB" CCAP-Core that controls and sources NDF, typically broadcast to multiple RPD ports;
- A "Reverse OOB" CCAP-Core that controls and receives NDR channels, always received one per RPD port.
- A CMTS CCAP that controls the downstream and upstream channels of a separate MAC domain;

A CMTS Core is programmed or configured in a vendor-specific manner to operate as an auxiliary core.

11.2 RPD Startup with Multiple Cores

An RPD MUST implement an *ActivePrincipalCore* object into which the principal CCAP-Core controlling the RPD writes its IP address.

Attribute Name	Type	Access	Type Constraints	Units	Default
ActivePrincipalCore	IpAddress	RW			

An RPD MUST implement an *ActiveAuxCoreTable* object into which auxiliary CCAP-Cores connected to the RPD write their IP addresses.

Attribute Name	Type	Access	Type Constraints	Units	Default
ActiveAuxCoreTable		RW			
ActiveAuxCoreIp	IpAddress	RW	key		

An RPD MUST implement a *ConfiguredCoreTable* object that contains the list of principal and auxiliary cores to which the RPD attempts to attach. This table is originally populated by the RPD itself based on DHCP, but may be modified by the principal core.

Attribute Name	Type	Access	Type Constraints	Units	Default
ConfiguredCoreTable		RW			
ConfiguredCoreIp	IpAddress	RW	key		

A resetting RPD MUST clear its *ConfiguredCoreTable*, *ActivePrincipalCore* and *ActiveAuxiliaryCoreTable* objects. This requirement applies to both cold-reset and warm-reset.

An RPD MUST accept up to six *CCAP-Core-IP-Address* options (a new [CANN] 42.x option) in its DHCP response. A starting RPD initially populates its *ConfiguredCoreTable* with the *CCAP-Core-IP-Address* list learned from DHCP.

After completing initial DHCP, an RPD MUST attempt to establish EAP-TLS authentication and a GCP TCP session with each of the *ConfiguredCoreTable* IP addresses until a Principal core identifies itself by writing to the *ActivePrincipalCore* RPD object.

After a GCP TCP session is established, the Principal CCAP-Core MUST write its IP address into the *ActivePrincipalCore* object of the RPD before attempting any other GCP write operations.

After a GCP TCP session is established, an auxiliary CCAP-Core MUST add its IP address to the RPD's *ActiveAuxiliaryCores* table. The Principal core MAY add IP addresses to the *ActiveAuxiliaryCores* table.

The RPD MUST attempt to maintain an IPsec-authorized GCP session to each core IP address in its *ActivePrincipalCore* object and *ActiveAuxiliaryCores* table.

11.3 Downstream Channel Constraint Table

Downstream QAM modulators are often implemented with hardware "channel blocks" that constrain consecutively identified channels to have the same or related physical attribute. A Principal CCAP-Core attempting to dynamically determine resource sets of downstream channels is made aware of those constraints by a read-only object table on the RPD.

An RPD MUST implement a read-only *DownChannelConstraintTable* to identify constraints imposed by its hardware on the configuration of physical parameters of blocks of downstream channels.

The set of described constraints are implied as present on all downstream RF ports of the RPD.

Attribute Name	Type	Access	Type Constraints	Units	Default
DownChannelConstraintTable	Na				
Index	unsignedInt		key		
DownChanIndexStart	unsignedInt		0..159		
DownChanIndexEnd	unsignedInt		0..159, > DownChanIndexStart		
LockParameters	LockParamBits				

The constraints are defined as a `LockParameters` bitmask:

```
LockParameters EnumBits {
   frequency(0),
   bandwidth(1),
   power(2),
   modulation(3),
   interleaver(4),
   j83Annex(5),
   symbolRate(6)
   mute(7)
}
```

The `LockParameters` field is a bitmask from which constraints apply to the range of channels defined by `DownChanIndexStart` through `DownChanIndexEnd`, inclusive. Note that different *DownChannelConstraintTable* objects may describe different `LockParameter` values on overlapping or partially overlapping channel ranges of other `DownChannelContraintTable` objects:

"frequency(0)" means the channels are constrained to have consecutive frequencies;

"bandwidth(1)" means the channels are constrained to have the same channel width;

"power(2)" means the channels are constrained to have the same power adjustment;

"modulation(3)" means the channels are constrained to have the same modulation;

"interleaver(4)" means the channels are constrained to have the same interleave value;

"j83Annex(5)" means the channels are constrained to have the same j83Annex definition;

"symbolRate(6)" means the channels are constrained to have the same symbol rate;

"mute(7)" means the channels are constrained to be muted or unmuted together.

11.4 Resource Sets and Auxiliary Resource Assignment

An RPD MUST implement the `ResourceSet` table , which identifies which auxiliary cores may control which RPD object.

Attribute Name	Type	Access	Type Constraints	Units	Default
ResourceSet					
ResourceSetIndex	Integer	RW	key		
DsRfPortStart	Integer	RW	-1 if unused		
DsRfPortEnd	Integer	RW	-1 if unused		
DsChanIndexStart	Integer	RW	-1 if unused		
DsChanIndexEnd	Integer	RW	-1 if unused		
UsRfPortStart	Integer	RW	-1 if unused		
UsRfPortEnd	Integer	RW	-1 if unused		
UsChanIndexStart	Integer	RW	-1 if unused		
UsChanIndexEnd	Integer	RW	-1 if unused		

A resource set consists of a range of channels from start to end (inclusive) on particular RF ports from start to end (inclusive). The RPD MUST enforce that no two entries in the `ResourceSet` table overlap, i.e., include the same channel on the same RF port.

A Principal CCAP-Core MUST implement R-OSSI tables that permit CCAP-Core configuration of the `ResourceSet` table objects to be written to an RPD.

An RPD MUST implement the `AuxResourceAssignment` table, which identifies which auxiliary core is authorized to manage which resource set. The RPD MUST implement sufficient entries in `AuxResourceAssignment` to assign each supported auxiliary core to one resource set.

Attribute Name	Type	Access	Type Constraints	Units	Default
AuxResourceAssignment	List				
ResourceSetIndex	key	RW	See text.		
AuxCoreIpAddress	key	RW			

The RPD MUST permit more than one `AuxCoreIpAddress` to be configured to the same `ResourceSetIndex`.

An RPD MUST implement the `PermitAuxSelfConfiguration` object to control whether auxiliary cores are permitted to configure their own resource sets.

Attribute Name	Type	Access	Type Constraints	Units	Default
PermitAuxSelfConfiguration	Boolean	RW	Writeable by Principal core only		false

An RPD MUST enforce the policy that only the Principal core can write to `PermitAuxSelfConfiguration`.

The Principal core is by default solely responsible for writing the `ResourceSet` and `AuxResourceAssignment` tables. When `PermitAuxSelfConfiguration` is ‘false’ (the default), the RPD MUST enforce that only the Principal core may write to the `ResourceSetTable` and `AuxResourceAssignmentTable`. When `PermitAuxSelfConfiguration` is ‘true’ (as changed by the Principal core) the RPD MUST permit any auxiliary core to write to `ResourceSetTable` and to assign those entries to its own IP address by writing to the `AuxResourceAssignment` table. Even when `PermitAuxSelfConfiguration` is ‘true’, the RPD MUST enforce the policy that an auxiliary core writes only its own IP address into the `AuxResourceAssignment` table.

11.5 RPD Reads and Writes

The RPD MUST support concurrent reads of any objects by any connected CCAP-Core, whether a Principal core or an Auxiliary core.

The RPD MUST reject an attempt by an Auxiliary core to write to any object not specifically authorized to it by the `AuxResourceAssignment` table. The RPD MUST reject an attempt by the Principal core to write to any object assigned to an Auxiliary core in the `AuxResourceAssignment` table.

Annex A DEPI MTU (Normative)

A.1 L2TPv3 Lower Layer Payload Size

Typically, an interface calculates its default maximum payload size by asking the interface below it in the interface channel what is its maximum payload size and considering its own encapsulation. For example, by default, Ethernet has a frame size of 1518 (without VLANs). The Ethernet encapsulation is 18 bytes, leaving 1500 bytes of payload (MTU) for its upper layer. IP then subtracts the IP header size (typically 20 bytes) to arrive at 1480 bytes available to its upper layer. For D-MPT the remainder becomes 1472 bytes, because the Session Field and the L2TPv3 Data Session Header comprise 8 bytes. For PSP, the PSP header including the maximum PSP segment table size needs to be taken into account.

The CCAP-Core and the RPD MUST support expanded Ethernet Frame sizes, up to 2000 bytes long, in compliance with [MULPI v3.1].

A.2 Maximum Frame Size for DEPI

This section documents the maximum frame size of the DEPI when a PSP pseudowire is used without fragmenting or concatenation.

Table 2 - MTU of DEPI (for PSP)

Field				Size
DEPI Frame	Ethernet Header			14 bytes
	802.1Q Header			4 bytes
	DEPI MTU	IPv4 Header		20 bytes
		IPv6 Header		40 bytes
		L2TPv3 Header		8 bytes
		DEPI-PSP Header***		6 bytes
		DOCSIS Frame	DOCSIS Header****	6-246 bytes
			Ethernet Header	14 bytes
			802.1Q Header	4 bytes
			Ethernet PDU	1500 or 2000 bytes
			Ethernet CRC	4 bytes
	Ethernet CRC			4 bytes
Total with PSP, no UDP, IPv4, no VLAN				**1570 to 1862 (or 2362)**

*** A PSP header is 4 bytes plus 2 bytes for each segment. Only one segment is shown. (A D-MPT header is 4 bytes.)

**** A typical DOCSIS header with BPI and no other extended headers is 11 bytes.

For simplicity, only one PSP segment is included in the above calculations. Additional segments are needed when PSP is concatenating or fragmenting. Note that a 2000 byte payload in a PSP frame could contain as many as 26 uncompressed TCP ACKs (64 byte Ethernet packets plus 6 to 11 bytes of DOCSIS overhead) which could create as many as 22 segments (first and last packets are fragmented) which would create a segment table size of 44 bytes, in addition to the standard 4 byte PSP header. For other payload types such as VoIP packets with high codec compression and with PHS disabled, or with larger MTUs, the number of segments could be even higher.

A.3 Path MTU Discovery

Path MTU Discovery relies on the fact that the network elements between the CCAP-Core and the RPD all support this functionality [RFC 1191]. If these network elements do not support Path MTU Discovery then this mechanism cannot be used and the static configuration option should be used.

Path MTU Discovery (PMTUD) works when the IP path MTU between the CCAP-Core and the RPD is less than the total IP datagram size generated when using the payload size negotiated during L2TPv3 session establishment, and the

Don’t Fragment (DF) bit is set in the IP header. If the CCAP-Core sends packets larger than the network can support, then network elements between the CCAP-Core and the RPD may generate an ICMP Destination Unreachable message with the code "Fragmentation needed and DF set" (ICMP Type 3 Code 4, also referred to as "Datagram Too Big" message), toward the source of the tunneled packet, if ICMP unreachables are allowed.

This ICMP error message includes at least the IP header and the next 8 bytes of the IP data (corresponding to the UDP header when using L2TPv3 over UDP, or to the Session ID and first 4 bytes of the L2SS when using L2TPv3 over IP) from the offending packet. The CCAP-Core and the RPD should have a way to map the source and destination IP address contained in the IP header embedded in the ICMP data to an L2TP Control Connection. As defined in [RFC 1191], a "PMTU is associated with a path, which is a particular combination of IP source and destination address and perhaps a Type-of-Service (TOS)".

Upon successfully processing the ICMP Destination Unreachable message, the CCAP-Core and RPD should reduce the Max Payload of all the sessions associated with the control connection mapped from the ICMP Destination Unreachable message to the size requested in the Next-Hop MTU field of the message. Both the Max Payload and the size contained in the Next-Hop MTU field express a Layer 3 payload of a Layer 2 frame, including the IP header and IP data.

The Max Payload MUST NOT be increased by receiving an ICMP Destination Unreachable message. The CCAP-Core and RPD may periodically attempt to increase the Max Payload of the session to its negotiated maximum and restart this process in case the path through the network has changed and larger MTUs are allowed. This technique is described in [RFC 1191]. The Max Payload size learned through this process will never be greater than the negotiated maximum learned during session establishment. The Path MTU Discovery procedures for IPv6 are described in [RFC 1981].

Annex B GCP Usage (Normative)

GCP (Generic Control Plane) is described in [GCP]. GCP is fundamentally a control plane tunnel that allows data structures from other protocols to be reused in a new context. This is useful if there is configuration information that is well defined in an external specification. GCP can repurpose the information from other specifications rather than redefining it. For example, MHAv2 uses GCP to reuse predefined DOCSIS TLVs for configuration and operation of the RPD. GCP has three basic features:

- Device management, such as power management;
- Structured access, such as TLV tunneling;
- Diagnostic access.

GCP defines the structured access using a combination of:

- 32 bit Vendor ID as defined in [Vendor ID];
- 16 bit Structure ID as uniquely defined by the vendor. For MHAv2, the default vendor ID is the CableLabs vendor ID of 4491 (decimal).

When GCP tunnels the data structures of another protocol, the syntax GCP(protocol name) can be used. For example, if the DOCSIS UCD command is tunneled over GCP, the combination of the DOCSIS UCD over GCP can be referred to as GCP(UCD).

B.1 RPD Configuration with GCP(UCD)

To configure the RPD upstream PHY, the DOCSIS UCD command is tunneled through GCP using the following GCP parameters:

- Vendor ID = 4491 (CableLabs)
- Structure ID = 35 (DOCSIS UCD)

The UCD is sent unicast to an RPD with a GCP Exchange Data Structures Request message. The RPD responds with a GCP Exchange Data Structures Response message.

B.2 RPD Upstream Scheduler with GCP(DSx)

MHAv2 permits the upstream scheduler to be located either centrally in the CMTS Core or in the RPD. When the scheduler is located in the RPD, the CMTS Core needs to be able to add, change, and delete service flows in the remote upstream scheduler. The semantics for doing this are fully described in the DOCSIS DSA (Dynamic Service Flow Add), DSC (Dynamic Service Flow Change), and DSD (Dynamic Service Flow Delete) commands.

These commands are tunneled through GCP with the following parameters:

- Vendor ID = 4491 (CableLabs)
- Structure ID as defined in Table 3.

The DSx command headers are not needed, because GCP contains all header information and a transaction ID. The specific payload of the DSx commands that are used in the corresponding GCP commands are shown in Table 3. GCP does not have a separate ACK command since GCP is transported over a reliable transport protocol such as TCP. If the DSx-ACK TLVs are needed, they are carried over a second GCP Request Response pair.

Table 3 - GCP Encoding for the Upstream Scheduler

Structure ID	Function	GCP Message	GCP Payload
15	DSA-REQ	EDS-REQ	TLVs
16	DSA-RSP	EDS-RSP	Confirmation Code, TLVs
17	DSA-ACK	EDS-REQ	Confirmation Code, TLVs
17	n/a	EDS-RSP	No content
18	DSC-REQ	EDS-REQ	TLVs

Structure ID	Function	GCP Message	GCP Payload
19	DSC-RSP	EDS-RSP	Confirmation Code, TLVs
20	DSC-ACK	EDS-REQ	Confirmation Code, TLVs
20	n/a	EDS-RSP	No content
21	DSD-REQ	EDS-REQ	SFID, TLVs
22	DSD-RSP	EDS-RSP	Confirmation Code

B.3 R-PHY Control Protocol

The following section defines the rules for the application of GCP as a Remote PHY control plane protocol. This set of rules is referred to as R-PHY Control Protocol or RCP.

RCP operates as an abstraction layer over the foundation of GCP protocol as defined in [GCP]. RCP provides the set of CCAP-Core with to ability to remotely manage a set of objects, such as channels, ports, performance variables, etc.

RCP relies on the following GCP messages: Notify, Device Management and Exchange Data Structures. The encodings of the GCP messages are provided in tables below.

B.3.1 RCP over GCP EDS Message

Table 4 shows the encodings of the RCP over GCP EDS message.

Table 4 - RCP Encodings for GCP EDS Messages

Description	Length	Contents
Message ID	1 byte	6 (Exchange Data Structures Request)
Message Length	2 bytes	12 + N (length excludes three first bytes (Id +Len) of the header)
Transaction ID	2 bytes	Unique value
Mode	1 byte	0
Port	2 bytes	N/A
Channel	2 bytes	N/A
Vendor ID	4 bytes	4491 (IANA Enterprise Number assigned to CableLabs)
Vendor Index	1 byte	1
Message Body	N bytes	TLV encoded RCP Message

B.3.2 RCP over GCP EDS Response Messages

The EDS Normal Response message shown in Table 5 has a format identical to the Request message (except Message ID == 7) and permits the inclusion of the TLV-encoded information.

Table 5 - RCP Encodings for GCP EDS Normal Response Messages

Description	Length	Contents
Message ID	1 byte	7 (Exchange Data Structures Request Normal Response)
Message Length	2 bytes	12 + N (length excludes three first bytes (Id +Len) of the header)
Transaction ID	2 bytes	Unique value, same as request
Mode	1 byte	0
Port	2 bytes	N/A
Channel	2 bytes	N/A
Vendor ID	4 bytes	4491 (IANA Enterprise Number assigned to CableLabs)
Vendor Index	1 byte	1

Description	Length	Contents
Message Body	N bytes	TLV encoded RCP Message

The EDS Error Response (Message Id == 8) format shown in Table 6 does not include TLV encoding information. This message can be used to communicate errors in those cases which are defined by the GCP specification [GCP]. The types of errors which are not covered by GCP Error Response Message are conveyed in EDS Normal Response Message in TLV-encoded format.

Table 6 - RCP Encodings for GCP EDS Error Response Messages

Description	Length	Contents
Message ID	1 byte	135 (Exchange Data Structures Error Response)
Message Length	2 bytes	3
Transaction ID	2 bytes	Same as request
Exception code	1 byte	See section 6.4 of [GCP]

B.3.3 RCP over GCP Device Management Message

The RCP encodings of GCP Device Management messages are shown in Table 7.

Table 7 - RCP Encodings for GCP Device Management Messages

Description	Length	Contents
Message ID	1 byte	4 (Device Management)
Message Length	2 bytes	8
Transaction ID	2 bytes	Unique value
Mode	1 byte	Bit 7: 0 = Send normal response 1 = Suppress normal response Bit 6-0: Reserved. Set to 0.
Port	2 bytes	N/A
Channel	2 bytes	N/A
Command	N bytes	0 – Null 1 – Cold Reset 2 – Warm Reset 3 – Standby 4 – Wakeup 5 – Power-Down 6 – Power-Up 7 to 255 – Reserved

The RPD MUST set bit 7 of the Mode field to ‘1’.

B.3.4 RCP over GCP Notify Message

GCP Notify messages are sent from the RPD to the CCAP-Core. RCP utilizes Event Code 1 and the TLV-encoded portion of the GCP Notify message. CCAP-Core does not respond to Notify messages.

The RPD MUST set bit 7 to '1' and bit 6 to '1' in the Mode field. The RPD MUST set the value of the Event Code field to "1".

The RCP encodings of GCP Notify messages are shown in Table 8.

Table 8 - RCP Encodings for GCP Notify Messages

Description	Length	Contents
Message ID	1 byte	2 (Notify)
Message Length	2 bytes	8 + N (length does not include first 3 bytes of the message)
Transaction ID	2 bytes	Unique value, selected by the RPD.
Mode	1 byte	Bit 7: 0 = Send normal response 1 = Suppress normal response Bit 6: 0 = Event data is text 1 = Event data is raw Bit 5-0: Reserved. Set to 0.
Status	1 byte	0 – Null (default) 1 – Cold Reset 2 – Warm Reset 3 – Standby 4 – Wakeup 5 – Power-Down 6 – Power-Up 7 to 255 – Reserved
Event Code	4 bytes	1
Event Data	N bytes	TLV-encoded RCP message

B.3.5 RCP TLV Format

The information carried in RCP protocol is formatted into TLV tuples. RCP operates with TLV format and usage rules which are similar to those defined in DOCSIS protocol. Each RPC TLV consists of a one byte long Type field, two byte long Length field and an optional, variable length Value field. The RPC TLV Type field can have the value of 1-255. The use of the value of "0" is reserved. The RPC TLV Length field denotes the total length of the Value field. The valid range for the Length field is 0-65535. When a TLV does not include the Value field, the Length field is set to zero. The encoding of the Value field varies, depending on the type field. The RCP protocol allows for nesting of sub-TLVs.

Using these encodings, new parameters may be added which some devices cannot interpret. A CCAP-Core or RPD which does not recognize a parameter type MUST skip over this parameter and not treat the event as an error condition.

B.3.6 RCP Message Structure

The RCP Messages are embedded in a single TLV tuple. The value field of these TLV consists of multiple tuples in the form `{operation-TLV, Object Set-TLV}`. The RCP protocol defines three operation types: "Read", "Write", and "Delete". The definition of the managed objects, also referred to as information model or schema is provided further in this specification.

The RCP TLV format imposes a size limit on RCP messages of 64 kB. RCP messages are never fragmented. When necessary, for example if the volume of information exceeds 64 kB, the CCAP-Core can issue multiple messages.

B.3.7 RCP Messages Types

The RCP protocol defines three message types. These messages, their TLV encoding, description and GCP usage are presented in Table 9.

Table 9 - Summary of RCP Messages

Message Name	Message TLV Type	Description	GCP Mapping
IRA, Identification and Resource Advertising	01	An initial message exchanged after authentication in which the CCAP-Core obtains all parameters identifying the RPD and its available resources.	Sent by CCAP-Core in GCP EDS message.
REX, RCP Object Exchange	02	A message in which CCAP-Core allocates or de-allocates resources and configures the resources in the RPD or requests information from the RPD i.e. statistics or other status data.	Sent by the CCAP-Core in GCP EDS message. Responded to by the RPD when operation is complete.
NTF, Notification	03	A message sent by the RPD to inform the CC about a specific event or a set of events.	Sent by the RPD in GCP Notify Message. CC does not respond to NTF messages.

B.3.8 RCP Protocol Rules

The CCAP-Core can issue multiple RCP messages before it receives acknowledgement from the RPD. Each RPD MUST support a minimum of 16 outstanding messages per CCAP-Core. A CCAP-Core MAY issue a single IRA or REX message with a combination of read, write and delete tuples. The NTF issue by the RPD may only contain write tuples. A CCAP-Core may issue a "Read" operation for a set individual objects (leaves) or object trees.

Responses to IRA and REX messages indicate the result of request processing with granularity of each {operation-TLV, Object Set-TLV} tuple. When the RPD response indicates a failure for a particular tuple, the RPD MUST make no change to the objects indicated in the tuple.

The RPD MUST respond to RCP request messages with one second of receiving the request message. The response messages sent by the RPD may be issued in a different order from the order of reception of request messages.

Since GCP operates over a reliable TCP connection) the protocol does not define explicit "acknowledgement" messages or other mechanism to deal with loss of individual messages.

B.3.9 Extensibility

This section will be written for a future version of this specification.

B.3.10 Protocol Versioning

The RCP protocol uses versioning as the primary means for future extensibility. The initial RCP protocol version defined by this specification is "1.0". Future versions of this specification may define new RCP protocol versions with additional capabilities or protocol options. During the initialization the CCAP-Core will read the RPD's capabilities, including the set of RCP protocol versions supported by the RCP via the IRA message. The CCAP will then select the highest RCP protocol version that both the CCAP-Core and the RPD can support and instruct the RPD to use the selected version.

B.3.11 Information Model Extensibility

The RPHY information model/schema is versioned separately from the protocol. The method for schema version selection is similar to the protocol version selection. The initial RCP information schema version defined by this specification is "1.0" Future versions of this specification may define new RCP information schema versions. For each version of the schema this specification will define a set of mandatory objects and a set of optional objects organized in sets, referred to as features. During initialization, the CCAP-Core will read which schema features the RPD supports in the IRA message. The CCAP-Core will also let the RPD know (write) which versions of the schema and which features it supports to control objects sent in Notify messages.

The CCAP-Core MUST convey in RCP protocol only those objects that the RPD supports. RPD MUST convey in RCP protocol only those objects that the CCAP-Core supports. These requirements are not applicable to vendor specific extensions.

B.3.12 Vendor Specific Extensions

The RCP protocol permits for exchange of vendor specific information by defining a method for inclusion of vendor specific TLVs. Vendor specific TLVs are complex TLVs with a Type of "Vendor-Specific". The first sub-TLV of a vendor specific TLV is the TLV identifying the vendor with length of 4 and the value field containing the vendor's Private Enterprise Number (http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers). A vendor specific TLV includes one or more vendor defined sub-TLVs. The definition of the formats and the usage of these TLVs are outside of the scope of this specification.

An example of vendor specific TLV is provided below.

```
{T= Vendor-Specific, Length: variable (minimum)
    {T = Vendor-Id, L = 4, V = Vendor ID: Enterprise number identifying vendor}
    {
        A sequence consisting of one or more vendor specific TLVs
    }
}
```

Vendor- specific TLVs are ignored by RPDs and CCAP-Cores which do not recognize vendor id.

B.3.13 Inclusion of DOCSIS Messages

The CCAP-Core can include in RCP certain messages describing the majority of the parameters of US TDMA and OFDMA channels and DS OFDM channels. These messages are transmitted in the form of an TLVs in REX messages.

The RPD MUST support the reception of three types of DOCSIS messages, including UCD, OCD and DPD Messages as the means for configuration of the DOCSIS channels for which these messages provide description. The RPD MUST decode these messages using DOCSIS rules in order to configure certain channel resources.

An example of an RCP message containing an embedded DOCSIS message is provided in Section B.3.14.4.

B.3.14 RCP Message Examples

B.3.14.1 RCP Rex Message Request Example

The following example presented below represents a message with a single "Read" operation for a set of statistical counters for two upstream channels. Curly braces "{" and "}" denote the boundaries of TLVs. Note, that the outer envelope (GCP EDC Request) is not shown.

```
{ T = REX, L= 43, V=                                ; top-level "container" type
    { T = Sequence, L = 40, V =                      ; a seq. of TLVs starting with oper.
      { T = Operation, L = 1, V = READ }
      { T = Channel, L = 15, V =                     ; L = 6 + 3*3 = 15
          { T= ChannelSelector,   L = 3, V: byte0 = portnum, byte1: channel type, byte2:
channelIndex }
          { T = TotalCW, L = 0  }
          { T = UncorrectedCW, L=0 }
          { T = CorrectableCW, L=0  }
      }
      { T = Channel, L =  15, V =
          { T = ChannelSpecifier, L =  3, V:  byte0 = portnum, byte1: channel type, byte2:
channelIndex }
          { T = TotalCW, L = 0 }
          { T = UncorrectedCW, L=0 }
          { T = CorrectableCW, L=0  }
      }
   }
```

B.3.14.2 RCP REX Message Normal Response Example

The message below represents a successful (no error) REX Response for stats counters for two upstream channels.

This is a response to the request outlined in Section B.3.14.1. As in previous examples, the outer envelope (GCP EDC Normal Response) is not shown.

```
{ T = REX, L= 67, V=                                    ; top-level “container” type
    { T = Sequence, L = 64, V =
      { T = Operation, L = 1, V = READ }
      { T = Channel, L =  27, V =                        ; L = 6 + 3*7 = 27
          { T= ChannelSelector,   L = 3, V: byte0 = portnum, byte1: channel type, byte2:
channelIndex }
          { T = TotalCW, L = 4, V = 32-bit counter}
          { T = UncorrectedCW, L= 4, V = 32-bit counter}
          { T = CorrectableCW, L=4, V = 32-bit counter}
      }
      { T = Channel, L =  27, V =
          { T = ChannelSpecifier, L =  3, V:  byte0 = portnum, byte1: channel type, byte2:
channelIndex }
          { T = TotalCW, L = 4, V = 32-bit counter}
          { T = UncorrectedCW, L= 4, V = 32-bit counter}
          { T = CorrectableCW, L=4, V = 32-bit counter}
      }
   }
}
```

B.3.14.3 RCP Rex Message Error Response Example

The example shown below represents a REX Response message for stats counters for two upstream channels. This is a response to the request outlined in Section B.3.14.1. As in the previous examples, the outer envelope (GCP EDC Normal Response) is not shown. The values of the response code (rspCode) are (TBD).

```
{ T = REX, L= 67, V =
   { T = Sequence, L = 64, V =
      { T = Operation, L = 1, V = READ-RSP }
      { T=RESP-CODE, L=1, V= rspCode  }         ;A Status TLV , only required on an error;
                                                 ; if omitted, oper. was successful
      { T=ERROR-MSG, L=15, V="Unknown channel" } ; Optional RPD vendor specific msg for
the log
      { T = Channel, L =  15, V =                ; L = 6 + 3*3 = 15
          { T= ChannelSelector,   L = 3, V: byte0 = portnum, byte1: channel type, byte2:
channelIndex }
          { T = TotalCW, L = 0, }
          { T = UncorrectedCW, L= 0}
          { T = CorrectableCW, L=0}
      }
      { T = Channel, L =  15, V =
          { T = ChannelSpecifier, L =  3, V:  byte0 = portnum, byte1: channel type, byte2:
channelIndex }
          { T = TotalCW, L = 0}
          { T = UncorrectedCW, L= 0}
          { T = CorrectableCW, L=0}
      }
   }
}
```

B.3.14.4 An Example of an Embedded DOCSIS Message

The example shown below represents a REX Request Message, in which the CCAP-Core communicates to the RPD the content of a DOCSIS message.

```
{ T = REX, L= nn + 13, V=                                ; top-level “container” type
   { T = Sequence, L = nn +13, V =                 ; nn is the length of the DOCSIS Message
      { T = Operation, L = 1, V = Write }
      { T = Channel, L =  3, V =  nn + 15
         {  T= ChannelSelector,   L = 3, V: byte0 = portnum; byte1: channel type, byte2:
channelIndex }
         {T = DocsisMsg , L = nn, V = “Opaque Hex String forming a complete DOCSIS message”
}
       }
   }
}
```

Annex C R-DEPI Extensions of R-UEPI Usage (Normative)

The R-UEPI control plane is the same as the R-DEPI control plane with additional AVPs. The R-DEPI control plane is explained in [R-DEPI].

Annex D MPEG Stream Analysis (Normative)

The RPD MAY support MPEG Stream Analysis as described in this annex.

In order to validate that the MPEG stream served from the CCAP-Core does not have issues that will cause video outages or other service impairments, the RPD will optionally be capable of performing tests on an MPEG stream to verify its integrity. These checks are designed to detect video disruption and outages by detecting Packet Identifier (PID) discontinuities and PID bitrate (or PID count) thresholds. The RPD monitors PIDs within both multi-program and single-program transport streams (MPTS and SPTS) used to carry various MPEG system and control information, video payloads, and audio payloads. PIDs monitored include the Program Association Table (PAT), the Program Map Table (PMT), Program and System Information Protocol (PSIP), 0x1FFC carousel, and PIDs within a PMT program such as video, audio, SCTE-35/Digital Program Insertion (DPI), and Enhaced TV Binary Interchange Format (EBIF).

If the RPD supports MPEG Stream Analysis, it MUST monitor MPEG synchronization by detecting transport stream synchronization loss. A device synchronizes on a transport stream via the reception of correct sync bytes, which are the 8 bits that precede the header of an MPEG packet (always 0x47). When the decoder first detects the sync byte, it looks again for the next sync byte after 188 or 204 bytes in the stream. After finding three sync bytes in a row in this pattern, synchronization has been established and packet boundaries are then known. However, if packets arrive with incorrect sync bytes, synchronization loss occurs and the decoder again establishes MPEG synchronization. The RPD will consider synchronization lost when two or more consecutive incorrect sync bytes are received.

Once the RPD has achieved MPEG synchronization, the following evaluations can be performed:

- If the RPD supports MPEG Stream Analysis, it MUST be capable of reading the transport stream ID (TSID) from the PAT. This value can be reported in enterprise MIBs. Note that a TSID is not available in DOCSIS streams.
- If the RPD supports MPEG Stream Analysis, it MUST detect program PID discontinuity resulting in media loss.
- If the RPD supports MPEG Stream Analysis, it MUST be capable of detecting the existence of the following program PIDs in the transport stream:
    - PAT
    - PMT
    - Video
    - Audio
    - SCTE-35/DPI
    - EBIF
- When loss of one of these PIDs is detected, it is expected that the RPD, using an SNMP trap or Syslog event, will provide notification to the operator.
- If the RPD supports MPEG Stream Analysis, it MUST be capable of detecting the existence of the mini-carousel PID (0x1FEE) and reading the service group ID (SGID) from the PID.

In addition, the bit rates of certain PIDs can provide insight into the health of a given stream. For example, a too-low bit rate could mean failure of the component providing the PID stream; a too-high bit rate could indicate an error condition on that device. Either of these occurrences can cause service disruption. The rates of these can be monitored via counters and a rate calculated on a time scale of minutes or several minutes to determine the health of the stream. If the RPD supports MPEG Stream Analysis, it MUST monitor the PID bit rate of the following PIDs:

- DOCSIS PID 0x1FFE
- ATSC A65 PSIP base PID 0x1FFB
- In-band DTA PIDs, including SI PID, 0x1FFC, and 0x1FF0

When an abnormal bit rate is detected, it is expected that the RPD, using an SNMP trap or Syslog event, will provide notification to the operator.

Annex E Certificate Hiearchy and Profiles (Normative)

This section describes the certificate format and extensions used by CableLabs certification authorities (CA) and summarizes the fields of [X.509] version 3 certificates used for this specification. The CableLabs certificate PKI hierarchy is shown below:

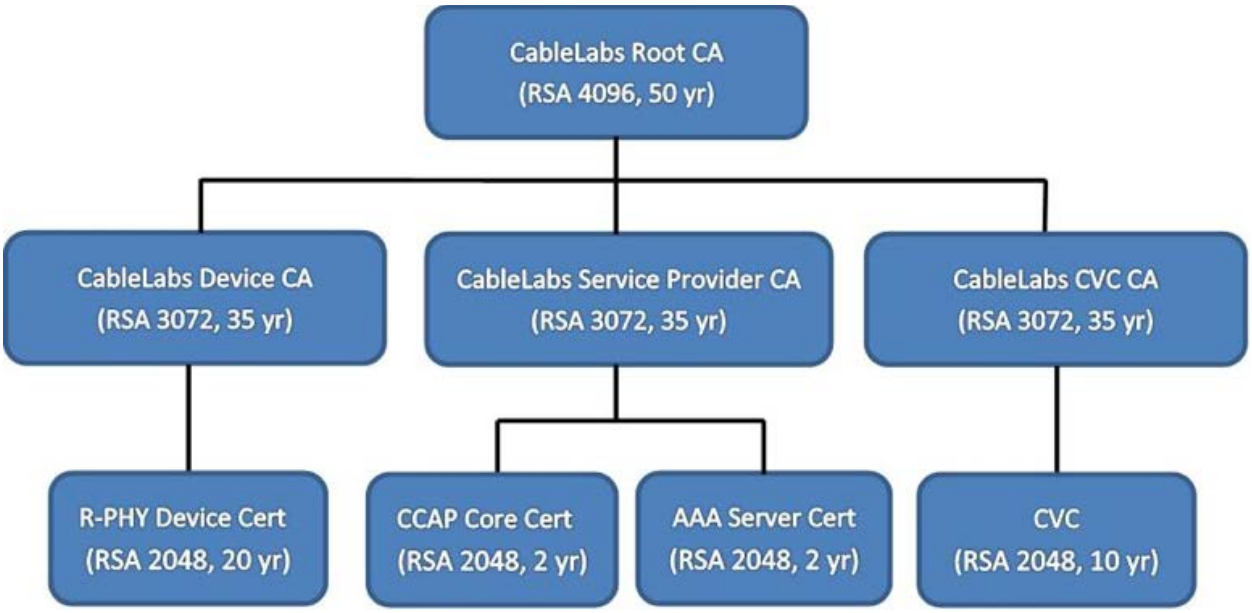

Figure 21 - Certificate Hiearchy

All certificates and CRLs described in this specification are signed with the RSA signature algorithm, using SHA-256 as the hash function. The RSA signature algorithm is described in PKCS #1 [RSA 1]; SHA-256 is described in [FIPS 180-4].

E.1 CableLabs Root CA Certificate

The contents of the CableLabs Root CA Certificate is shown in Table 10.

Table 10 - CableLabs Root CA Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Root CA01 cn=CableLabs Root Certification Authority		
Subject DN		c=US o=CableLabs ou=Root CA01 cn=CableLabs Root Certification Authority		
Validity Period		50 yrs		
Public Key Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		4096 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA

E.2 CableLabs Device CA Certificate

The contents of the CableLabs Device CA Certificate is shown in Table 11.

Table 11 - CableLabs Device CA Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Root CA01 cn=CableLabs Root Certification Authority		
Subject DN		c=US o=CableLabs ou=Device CA01 cn=CableLabs Device Certification Authority		
Validity Period		35 yrs		
Public Key Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		3072-bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				0
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA for online CAs

E.3 RPD Certificate

The contents of the RPD Certificate is shown in Table 12.

Table 12 - RPD Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA01 cn=CableLabs Device Certification Authority		
Subject DN		c=<Country of Manufacturer> o=<Company Name> ou=DCA Remote Device Certificate cn=<MAC Address>		
Validity Period		20 yrs		
Public Key Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<MAC Address>: MAC address of the RPD.

The MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (:), e.g., `00:60:21:A5:0A:23`. Hexadecimal digits greater than 9 are expressed as uppercase letters.

E.4 CableLabs Service Provider CA Certificate

The contents of the CableLabs Service Provider Certificate is shown in Table 13.

Table 13 - CableLabs Service Provider CA Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Root CA01 cn=CableLabs Root Certification Authority		
Subject DN		c=US o=CableLabs ou=Service Provider CA01 cn=CableLabs Service Provider Certification Authority		
Validity Period		35 yrs		
Public Key Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		3072 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				0
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA for online CAs

E.5 CCAP-Core Device Certificate

The contents of the CCAP-Core Device Certificate is shown in Table 14.

Table 14 - CCAP-Core Device Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou= Service Provider CA01 cn= CableLabs Service Provider Certification Authority		
Subject DN		c=<Country of Manufacturer> o=<Company Name> ou=DCA Headend/Hub Certificate cn=<MAC Address>		
Validity Period		2 yrs		
Public Key Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<MAC Address>: MAC address of the CCAP-Core Device.

The MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (:), e.g., `00:60:21:A5:0A:23`. Hexadecimal digits greater than 9 are expressed as uppercase letters.

E.6 AAA Server Certificate

The contents of the AAA Server Certificate is shown in Table 15.

Table 15 - AAA Server Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Service Provider CA01 cn=CableLabs Service Provider Certification Authority		
Subject DN		c=<Country> o=<Company Name> ou=AAA Server Certificate cn=<server FQDN>		
Validity Period		20 yrs		
Public Key Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	X	FALSE	
dNSName				<server FQDN>

Appendix I Plant Sweep in a Distributed Architecture (Informative)

Today, operators in HFC plants deploy test equipment that allows sweep tests to be performed, measuring plant frequency response in the upstream and downstream direction. Traditionally, these have been closed, proprietary systems with these characteristics:

- In the downstream, proprietary equipment in the plant generates sweep signals that are measured by field test equipment; a control channel between the headend equipment and test equipment controls how and when these signals are generated.
- In the upstream, the test equipment in the field generates signals that are measured by proprietary equipment in the headend; a similar control channel between the test equipment and headend equipment is used to feed measurements back to the test equipment so that adjustments can be made.

In a Remote PHY architecture, supporting the telemetry/control channel between the headend and the field test equipment becomes a challenge. In a traditional architecture, the headend equipment is connected through the combining network; this connection is eliminated in the R-PHY architecture. Other methods for performing sweep are needed.

In this appendix, three alternatives to using currently available plant maintenance systems are discussed:

- Using current transmitter and receiver technology, developed as part of the DOCSIS Proactive Network Maintenance (PNM) toolset, to perform measurements;
- Introducing modules to the R-PHY Node that perform the role of the headend test equipment;
- Developing an API in the R-PHY Node that allows interaction with field test equipment.

I.1 Plant Sweep Using Transmitter and Receiver Capabilities

With the full-band capture capabilities introduced for DOCSIS 3.0 and 3.1 equipment, frequency response measurements can be taken by either the CM or the R-PHY node receiver. Existing signals in the plant can be used in the downstream for these measurements and the results of the measurements can be made available to test equipment in the field via SNMP. To measure portions of the spectrum where no signals exist (for example, when evaluating regions where services will be expanded for DOCSIS 3.1), the CCAP-Core can instruct the R-PHY node to generate signals that can be measured by the CM.

In the upstream, existing signals can be measured and test modes on the CM can generate carrier signals that can be measured at the R-PHY Node burst receiver. These measurements too can be exposed to field test equipment via SNMP.

In addition, PNM enables symbol capture in both the upstream and downstream direction, allowing impairments to also be detected in the time domain, rather than just the frequency domain.

Details on the PNM toolset can be found in the following DOCSIS 3.1 specifications: [CCAP-OSSI v3.1], [CM-OSSI v3.1], [MULPI v3.1], and [PHY v3.1].

I.2 Hardware Module in the Node

Test equipment vendors may develop modules that will be deployed within a node that supports the R-PHY architecture that performs the same function as the equipment that was previously deployed in the headend. Since the module is located in the R-PHY Node, the same telemetry and control channels can be used. In this approach, the sweep vendors can work with the node vendors to develop the sweep module and therefore the topic is not covered in detail in this specification.

I.3 R-PHY Node API Support

In this approach, an API is developed by R-PHY Node and test equipment vendors that can be used by test equipment to control the placement and configuration of signals in the RF spectrum. This API provides more control of sweep carrier generation and access to measurements by the test equipment, without the need to support a specific hardware module in the node, as described in the previous approach. Since the sweep signal itself is a CW signal, no additional

RF capability is required above what is defined in the R-PHY specifications (i.e., the ability to generate CW carriers at any frequency and the ability to measure RF receive levels).

Appendix II Acknowledgements

On behalf of the cable industry and our member companies, CableLabs would like to thank the following individuals for their contributions to the development of this specification:

Contributor	Company Affiliation
John T. Chapman	Cisco
Pawel Sowinski	Cisco
Gerry White	Cisco
Stuart Hoggan	CableLabs
Michael Patrick	Harmonic

On behalf of the cable industry and our member companies, CableLabs would like to thank the following individuals for their contributions to the development of the technology and participation in the Remote PHY Working Group.

Contributor	Company Affiliation	Contributor	Company Affiliation
Bill Powell	Alcatel-Lucent	Nagesh Nandiraju	Comcast
Brian Kurtz	Altera	Saifur Rahman	Comcast
Carlton Lane	Analog	Jorge Salinger	Comcast
Linda Mazaheri	Analog	Joe Solomon	Comcast
Tom Ferreira	Arris	Douglas Will	Comcast
Steve Foley	Arris	Jeff Ford	Complex IQ
Anand Goenka	Arris	Al Garrett	Complex IQ
Jeff Howe	Arris	Ony Anglade	Cox Communications
Hari Nair	Arris	Mike Cooper	Cox Communications
Andrew Chagnon	Broadcom	Samir Parikh	Gainspeed Networks
Victor Hou	Broadcom	João Campos	Get
Niki Pantelias	Broadcom	Even Kristoffersen	Get
David Pullen	Broadcom	Adi Bonen	Harmonic
Stuart Hoggan	CableLabs	Mike Patrick	Harmonic
Volker Leisse	CableLabs	Jim Chen	Huawei
Karthik Sundaresan	CableLabs	Hesham ElBakoury	Huawei
Nikhil Tayal	CableLabs	Karl Moerder	Huawei
Jun Tian	CableLabs	Jack Moran	Huawei
Andrew Sundelin	CableLabs Consultant	Guangsheng Wu	Huawei
Naor Goldman	Capacicom	Phil Oakley	LGI
Dave Fox	Casa Systems	Stan Bochenek	Maxim Integrated
Maike Geng	Casa Systems	Ajay Kuckreja	Maxim Integrated
David Claussen	Charter	Len Dauphinee	MaxLinear
Nobo Akiya	Cisco	David Huang	MaxLinear
Alon Bernstein	Cisco	Louis Park	MaxLinear
Brian Bresnahan	Cisco	Sridhar Ramesh	MaxLinear
John T. Chapman	Cisco	Patrick Tierney	MaxLinear
Hang Jin	Cisco	Scott Walley	MaxLinear
Tong Liu	Cisco	Rei Brockett	Pace/Aurora
Carlos Pignataro	Cisco	Nasir Ansari	Rogers
Sangeeta Ramakrishnan	Cisco	George Hart	Rogers
John Ritchie	Cisco	Kevin Kwasny	Shaw
Pawel Sowinski	Cisco	Lee Johnson	ST Micro
Don Strausberger	Cisco	Paul Brooks	Time Warner Cable

Contributor	Company Affiliation	Contributor	Company Affiliation
Yi Tang	Cisco	Kirk Erichsen	Time Warner Cable
Bill Wall	Cisco	Colin Howlett	Vecima
Gerry White	Cisco	Douglas Johnson	Vecima
Philippe Perron	Cogeco	Faten Hijazi	Xilinx
John Bevilacqua	Comcast	Alex Luccisano	Xilinx

Additionally, CableLabs would like to thank the DCA MSO team for their continued support in driving the specification development and the decision-making process.

Karthik Sundaresan, CableLabs