

# **Data-Over-Cable Service Interface Specifications**

## **IPv4 and IPv6 eRouter Specification**

### **CM-SP-eRouter-I07-111117**

#### **ISSUED**

#### **Notice**

This DOCSIS® specification is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs®. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. 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.

© 2006-2011 Cable Television Laboratories, Inc.

All rights reserved.

## Document Status Sheet

|                                   |  |                      |                             |                   |
|-----------------------------------|--|----------------------|-----------------------------|-------------------|
| <b>Document Control Number:</b>   | CM-SP-eRouter-I07-111117   |                      |                             |                   |
| <b>Document Title:</b>            | IPv4 and IPv6 eRouter Specification  |                      |                             |                   |
| <b>Revision History:</b>          | I01 – 12/7/06<br>I02 – 2/23/07<br>I03 – 5/18/07<br>I04 – 6/11/10<br>I05 – 2/10/11<br>I06 – 6/23/11<br>I07 – 11/17/11 |                      |                             |                   |
| <b>Date:</b>                      | November 17, 2011  |                      |                             |                   |
| <b>Status:</b>                    | <del>Work in Progress</del>  | <del>Draft</del>     | Issued                      | <del>Closed</del> |
| <b>Distribution Restrictions:</b> | <del>Author Only</del>   | <del>CL/Member</del> | <del>CL/Member/Vendor</del> | Public            |

### Key to Document Status Codes:

- Work in Progress** An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.
- Draft** A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
- Issued** A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
- Closed** A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

### Trademarks:

CableCARD™, CableHome®, CableLabs®, CableNET®, CableOffice™, CablePC™, DCAS™, DOCSIS®, DPoE™, EBIF™, eDOCSIS™, EuroDOCSIS™, EuroPacketCable™, Go2BroadbandSM, M-Card™, M-CMTS™, OCAP™, OpenCable™, PacketCable™, PCMM™, PeerConnect™, and tru2way® are marks of Cable Television Laboratories, Inc. All other marks are the property of their respective owners.

# Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>SCOPE.....</b>  | <b>1</b>  |
| 1.1      | Introduction and Purpose.....                                | 1         |
| 1.2      | Requirements .....   | 1         |
| <b>2</b> | <b>REFERENCES .....</b>                                      | <b>2</b>  |
| 2.1      | Normative References .....                                   | 2         |
| 2.2      | Informative References.....                                  | 4         |
| 2.3      | Reference Acquisition .....                                  | 5         |
| <b>3</b> | <b>TERMS AND DEFINITIONS .....</b>                           | <b>6</b>  |
| <b>4</b> | <b>ABBREVIATIONS AND ACRONYMS .....</b>                      | <b>7</b>  |
| <b>5</b> | <b>THEORY OF OPERATION .....</b>                             | <b>9</b>  |
| 5.1      | eDOCSIS eRouter and TR-069 Architecture .....                | 11        |
| 5.2      | eRouter Device Management .....                              | 12        |
| <b>6</b> | <b>EROUTER INITIALIZATION .....</b>                          | <b>13</b> |
| <b>7</b> | <b>IPV4 PROVISIONING .....</b>                               | <b>14</b> |
| 7.1      | DHCPv4 Fields Used by the eRouter.....                       | 15        |
| 7.2      | Router DHCPv4 Server Sub-element.....                        | 16        |
| 7.2.1    | <i>DHCPv4 Server Function Goals .....</i>                    | <i>16</i> |
| 7.2.2    | <i>DHCPv4 Server Function System Description.....</i>        | <i>17</i> |
| 7.2.3    | <i>DHCPv4 Server Function Requirements.....</i>              | <i>17</i> |
| 7.3      | Operator-Facing IPv4 Address Release Behavior .....          | 18        |
| 7.4      | Customer-Facing IPv4 Address Release Behavior .....          | 18        |
| <b>8</b> | <b>IPV6 PROVISIONING .....</b>                               | <b>19</b> |
| 8.1      | Obtain Link-Local Address .....                              | 20        |
| 8.2      | Perform router discovery .....                               | 20        |
| 8.3      | Obtain IPv6 address and other configuration parameters ..... | 20        |
| 8.4      | Use of T1 and T2 Timers .....                                | 22        |
| 8.5      | IPv6 Provisioning of CPE Devices .....                       | 22        |
| 8.5.1    | <i>SLAAC Requirements for eRouter .....</i>                  | <i>23</i> |
| 8.5.2    | <i>DHCPv6 Requirements for eRouter .....</i>                 | <i>23</i> |
| 8.6      | Operator-Facing IPv6 Address Release Behavior .....          | 24        |
| 8.7      | Customer-Facing IPv6 Address Release Behavior .....          | 25        |
| <b>9</b> | <b>IPV4 DATA FORWARDING AND NAPT OPERATION.....</b>          | <b>26</b> |
| 9.1      | Introduction .....   | 26        |
| 9.1.1    | <i>Assumptions.....</i>                                      | <i>26</i> |
| 9.1.2    | <i>Overview.....</i>   | <i>26</i> |
| 9.2      | System Description.....                                      | 26        |
| 9.2.1    | <i>Overview.....</i>   | <i>26</i> |
| 9.3      | IPv4 Router.....   | 28        |
| 9.4      | NAPT.....  | 29        |
| 9.4.1    | <i>Dynamically Triggered NAPT Translations.....</i>          | <i>30</i> |
| 9.4.2    | <i>Application Layer Gateways (ALGs).....</i>                | <i>31</i> |
| 9.4.3    | <i>Multicast NAPT .....</i>                                  | <i>31</i> |
| 9.5      | ARP .....  | 31        |

|                    |   |           |
|--------------------|---|-----------|
| 9.6                | IPv4 Multicast.....   | 32        |
| 9.6.1              | IGMP Proxying.....  | 33        |
| 9.6.2              | IPv4 Multicast Forwarding .....   | 34        |
| 9.6.3              | IPv4 Multicast Forwarding Example .....                                 | 35        |
| 9.7                | Dual-Stack Lite Operation .....   | 36        |
| <b>10</b>          | <b>IPv6 DATA FORWARDING .....</b>                                       | <b>38</b> |
| 10.1               | Overview .....  | 38        |
| 10.2               | System Description .....  | 39        |
| 10.3               | IPv6 Multicast.....   | 41        |
| 10.3.1             | MLD Proxying .....  | 42        |
| 10.3.2             | IPv6 Group Membership Database.....                                     | 42        |
| 10.3.3             | IPv6 Multicast Forwarding .....   | 43        |
| 10.3.4             | IPv6 Multicast Forwarding Example .....                                 | 43        |
| <b>11</b>          | <b>QUALITY OF SERVICE .....</b>   | <b>46</b> |
| 11.1               | Downstream Quality of Service Operation.....                            | 46        |
| 11.2               | Upstream Quality of Service Operation.....                              | 46        |
| <b>12</b>          | <b>EROUTER MANAGEMENT .....</b>   | <b>47</b> |
| 12.1               | eRouter SNMP Management Interface Requirements.....                     | 47        |
| 12.2               | eRouter TR-069 Management Interface Requirements .....                  | 47        |
| 12.2.1             | ACS Discovery.....  | 47        |
| 12.2.2             | ACS Selection .....   | 48        |
| 12.2.3             | Dynamic ACS Updates .....   | 48        |
| 12.2.4             | TR-069 CWMP Control and Credentials.....                                | 48        |
| <b>13</b>          | <b>SECURITY .....</b>   | <b>49</b> |
| <b>ANNEX A</b>     | <b>SNMP MIB OBJECTS SUPPORTED BY THE EROUTER .....</b>                  | <b>50</b> |
| A.1                | eRouter Interface Numbering .....                                       | 50        |
| <b>ANNEX B</b>     | <b>CONFIGURATION OF EROUTER OPERATIONAL PARAMETERS.....</b>             | <b>51</b> |
| B.1                | eRouter SNMP Configuration .....  | 51        |
| B.1.1              | eRouter SNMP Modes of Operation .....                                   | 51        |
| B.1.2              | eRouter SNMP Access Control Configuration .....                         | 51        |
| B.1.3              | SNMPv1v2c Coexistence Configuration.....                                | 51        |
| B.2                | eCM Proxy mechanism for configuration of eRouter.....                   | 57        |
| B.3                | eRouter Configuration Encodings .....                                   | 57        |
| B.3.1              | eRouter TLV Processing .....  | 57        |
| B.3.2              | eRouter Initialization Mode Encoding.....                               | 57        |
| B.3.3              | TR-069 Management Server.....   | 58        |
| B.3.4              | SNMPv1v2c Coexistence Configuration.....                                | 59        |
| B.3.5              | SNMPv3 Access View Configuration.....                                   | 61        |
| B.3.6              | Vendor Specific Information.....  | 62        |
| <b>ANNEX C</b>     | <b>TR-069 MANAGED OBJECTS REQUIREMENTS .....</b>                        | <b>63</b> |
| C.1                | Profiles from [TR-181i2a3] .....  | 63        |
| <b>APPENDIX I</b>  | <b>ACKNOWLEDGEMENTS (INFORMATIVE) .....</b>                             | <b>67</b> |
| <b>APPENDIX II</b> | <b>REVISION HISTORY .....</b>   | <b>68</b> |
| II.1               | The following ECN was incorporated into CM-SP-eRouter-I02-070223: ..... | 68        |
| II.2               | The following ECN was incorporated into CM-SP-eRouter-I03-070518: ..... | 68        |
| II.3               | The following ECN was incorporated into CM-SP-eRouter-I04-100611: ..... | 68        |

|      |   |    |
|------|---|----|
| II.4 | The following ECN was incorporated into CM-SP-eRouter-I05-110210: .....   | 68 |
| II.5 | The following ECN was incorporated into CM-SP-eRouter-I06-110623: .....   | 68 |
| II.6 | The following ECNs were incorporated into CM-SP-eRouter-I07-111117: ..... | 68 |

## Figures

|  |    |
|--|----|
| Figure 5-1 - Logical Components of an eDOCSIS device with an IPv4 eRouter .....        | 9  |
| Figure 5-2 - Logical Components of an eDOCSIS device with an IPv6 eRouter .....        | 9  |
| Figure 5-3 - Logical Components of an eDOCSIS device with an IPv4 + IPv6 eRouter ..... | 10 |
| Figure 5-4 - TR-069 Interface Model Applied to eDOCSIS eRouter .....                   | 12 |
| Figure 7-1 - IPv4 Provisioning Message Flow .....                                      | 14 |
| Figure 8-1 - IPv6 Provisioning Message Flow .....                                      | 19 |
| Figure 9-1 - eRouter IPv4 Forwarding Block Diagram.....                                | 27 |
| Figure 9-2 - eRouter IPv4 Multicast Forwarding Block Diagram.....                      | 33 |
| Figure 9-3 - IPv4 Multicast Forwarding Example.....                                    | 35 |
| Figure 10-1 - eRouter IPv6 Forwarding Block Diagram.....                               | 38 |
| Figure 10-2 - eRouter IPv6 Multicast Forwarding Block Diagram.....                     | 41 |
| Figure 10-3 - IPv6 Multicast Forwarding Example.....                                   | 44 |

## Tables

|   |    |
|---|----|
| Table 6-1 - eRouter Modes .....                               | 13 |
| Table 7-1 - eRouter DHCP Retransmission Interval .....        | 15 |
| Table 7-2 - DHCPv4 Server Options.....                        | 17 |
| Table B-1 - vacmViewTreeFamilyTable .....                     | 51 |
| Table B-2 - SNMPv1v2c Coexistence Configuration Mapping ..... | 52 |
| Table B-3 - snmpCommunityTable .....                          | 53 |
| Table B-4 - snmpTargetAddrTable .....                         | 53 |
| Table B-5 - snmpTargetAddrExtTable.....                       | 54 |
| Table B-6 - vacmSecurityToGroupTable .....                    | 55 |
| Table B-7 - vacmAccessTable.....                              | 55 |
| Table B-8 - SNMPv3 Access View Configuration Encoding .....   | 56 |
| Table B-9 - vacmViewTreeFamilyTable .....                     | 56 |
| Table C-1 - TR-181 Profiles for eRouter.....                  | 63 |

# 1 SCOPE

This specification is part of the DOCSIS family of specifications developed by Cable Television Laboratories, Inc. (CableLabs). This specification was developed for the benefit of the cable industry, and includes contributions by operators and vendors from North America, Europe, and other regions.

## 1.1 Introduction and Purpose

This specification defines a core set of features that enable multiple subscriber devices to gain access to operator provided high-speed data service using DOCSIS. This core set of features allows for both IPv4- and IPv6-enabled devices to gain connectivity to the Internet.

The eRouter is specified as an Embedded Service/Application Functional Entity (eSAFE) device as defined in [eDOCSIS] that is implemented in conjunction with a DOCSIS cable modem device.

The core set of features defined in this specification includes the ability to provision multiple CPE devices, a description of how to forward data to and from CPE devices, and also the ability to forward IP Multicast traffic to CPE devices.

## 1.2 Requirements

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

### 2.1 Normative References <sup>1</sup>

In order to claim compliance with this specification, it is necessary to conform to all or part of 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 DHCP] | CableLabs DHCP Options Registry Specification, CL-SP-CANN-DHCP-Reg-I08-111117, November 17, 2011, Cable Television Laboratories, Inc.                    |
| [eDOCSIS]   | eDOCSIS™ Specification, CM-SP-eDOCSIS-I22-110623, June 23, 2011, Cable Television Laboratories, Inc.   |
| [MULPI]     | DOCSIS MAC and Upper Layer Protocol Interface Specification, CM-SP-MULPIv3.0-I17-111117, November 17, 2011, Cable Television Laboratories, Inc.          |
| [OSSIV3.0]  | DOCSIS Operations Support System Interface Specification. CM-SP-OSSIV3.0-I16-111117, November 17, 2011, Cable Television Laboratories, Inc.              |
| [SECV3.0]   | DOCSIS Security Specification, CM-SP-SECV3.0-I13-100611, June 11, 2010, Cable Television Laboratories, Inc.  |
| [RFC 792]   | IETF RFC 792, Internet Control Message Protocol, J. Postel, September 1981.  |
| [RFC 826]   | IETF RFC 826, An Ethernet Address Resolution Protocol, David C. Plummer, November, 1982.   |
| [RFC 868]   | IETF RFC 868, Time Protocol, J. Postel & K. Harrenstien, May 1983.   |
| [RFC 1122]  | IETF RFC 1122, Requirements for Internet Hosts - Communication Layers, R. Braden, October, 1989.   |
| [RFC 1812]  | IETF RFC 1812, Requirements for IP Version 4 Routers, F. Baker, June 1995.   |
| [RFC 1918]  | IETF RFC 1918, Address Allocation for Private Internets, Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, February 1996.                |
| [RFC 2131]  | IETF RFC 2131, Dynamic Host Configuration Protocol, R. Droms, March, 1997.   |
| [RFC 2132]  | IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, S. Alexander, R. Droms, March 1997.   |
| [RFC 2461]  | IETF RFC 2461, Neighbor Discovery for IP Version 6 (IPv6), T. Narten, E. Nordmark, W. Simpson, December, 1998.   |
| [RFC 2462]  | IETF RFC 2462, IPv6 Stateless Address Autoconfiguration, S. Thomson, T. Narten, December 1998.   |
| [RFC 2463]  | IETF RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, A. Conta, S. Deering, December 1998. |
| [RFC 2710]  | IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6, S. Deering, W. Fenner, B. Haberman, October 1999.  |
| [RFC 2827]  | IETF RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, P. Ferguson, D. Senie, May 2000.  |

<sup>1</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 by JB. Revised per eRouter N-11.1014-3 on 10/27/11 and by per eRouter N-11.1015-2 on 11/04/11 by JB.



- [RFC 3022] IETF RFC 3022, Traditional IP Network Address Translator (Traditional NAT), P. Srisuresh, K. Egevang, January 2001.
- [RFC 3203] IETF RFC 3203, DHCP reconfigure extension, Y. T'Joens, C. Hublet, P. De Schrijver, December, 2001.
- [RFC 3315] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, July 2003.
- [RFC 3319] IETF RFC 3319, Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers, H. Schulzrinne, B. Volz, July 2003.
- [RFC 3376] IETF RFC 3376, Internet Group Management Protocol, Version 3, B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, October, 2002.
- [RFC 3412] IETF RFC 3412, Configuring Networks and Devices with Simple Network Management Protocol (SNMP), M. MacFaden, D. Partain, J. Saperia, W. Tackabury, April 2003.
- [RFC 3413] IETF RFC 3413, Internet Protocol Version 6 (IPv6) Addressing Architecture, R. Hinden, S. Deering, April 2003.
- [RFC 3415] IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), B. Wijnen, R. Presuhn, K. McCloghrie, December 2002.
- [RFC 3417] IETF RFC 3417, A Conservative Selective Acknowledgment (SACK)-based Loss Recovery Algorithm for TCP, E. Blanton, M. Allman, K. Fall, L. Wang, April 2003.
- [RFC 3419] IETF RFC 3419, Mobile IP Traversal of Network Address Translation (NAT) Devices, H. Levkowitz, S. Vaarala, May 2003.
- [RFC 3489] IETF RFC 3489, STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, March 2003.
- [RFC 3513] IETF RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture, R. Hinden, S. Deering, April, 2003.
- [RFC 3584] IETF RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, R. Frye, D. Levi, S. Routhier, B. Wijnen, August 2003.
- [RFC 3633] IETF RFC 3633, IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, O. Troan, R. Droms, December 2003.
- [RFC 3646] IETF RFC 3646, DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), R. Droms, December 2003.
- [RFC 3736] IETF RFC 3736, Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6, R. Droms, April 2004.
- [RFC 3810] IETF RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6, R. Vida, Ed., L. Costa, Ed., June 2004.
- [RFC 4075] IETF RFC 4075, Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6, V. Kalusivalingam, Cisco Systems, May 2005.
- [RFC 4242] IETF RFC 4242, Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6), S. Venaas, T. Chown, B. Volz, November 2005.
- [RFC 4291] IETF RFC 4291, IP Version 6 Addressing Architecture, R. Hinden, S. Deering, February 2006.
- [RFC 4293] IETF RFC 4293, Management Information Base for the Internet Protocol (IP), S. Routhier, (Editor), Bill Fenner, Brian Haberman, Dave Thaler, April 2006.

- [RFC 4361] IETF RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), T. Lemon, B. Sommerfeld, February 2006.
- [RFC 4443] IETF RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, A. Conta, S. Deering, M. Gupta, Ed., March 2006.
- [RFC 4632] IETF RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, V. Fuller, T. Li, August 2006.
- [RFC 4861] IETF RFC 4861, T. Narten, E. Nordmark, W. Simpson, H. Soliman, Neighbor Discovery for IP Version 6 (IPv6), September 2007.
- [RFC 4862] IETF RFC 4862, S. Thomson, T. Narten, T. Jinmei, IPv6 Stateless Address Autoconfiguration, September 2007.
- [RFC 4884] IETF RFC 4884, Extended ICMP to Support Multi-Part Messages, R. Bonica, D. Gan, D. Tappan, C. Pignataro, April 2007.
- [RFC 5006] IETF RFC 5006, J. Jeong, S. Park, L. Beloeil, S. Madanapalli, IPv6 Router Advertisement Option for DNS Configuration, September 2007.
- [RFC 6092] IETF RFC 6092, Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, J. Woodyatt, Ed., January 2011.
- [RFC 6106] IETF RFC 6106, IPv6 Router Advertisement Options for DNS Configuration, November 2010.
- [RFC 6204] IETF RFC 6204, Basic Requirements for IPv6 Customer Edge Routers, H. Singh, W. Beebee, C. Donley, B. Stark, O. Troan, Ed., April 2011.
- [RFC 6333] IETF RFC 6333, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, A. Durand, R. Droms, J. Woodyatt, Y. Lee, August 2011.
- [TR-064] TR-064 LAN-Side DSL CPE Configuration Specification, May 2004, Broadband Forum Technical Report.
- [TR-069a4] TR-069 CPE WAN Management Protocol v1.2, Issue 1 Amendment 2, July 2011, Broadband Forum Technical Report.
- [TR-143  
Corrigendum1] TR-143 Enabling Network Throughput Performance Tests and Statistical Monitoring, Issue 1, Corrigendum 1, December 2008, Broadband Forum Technical Report.
- [TR-181i2a3] TR-181 Device Data Model for TR-069, Issue 2 Amendment 3, July 2011, Broadband Forum Technical Report.

## 2.2 Informative References

This specification uses the following informative references.

- [MR-230] TR-069 Deployment Scenarios, Issue 1, MR-230, August 2010, Broadband Forum Marketing Report.
- [TR-106a5] TR-106 Data Model Template for TR-069-Enabled Devices, Issue 1, Amendment 5, November 2010, Broadband Forum Technical Report.
- [WI-FI MGMT] Wi-Fi Provisioning Framework Specification, WR-SP-WiFi-MGMT-I02-101005, October 5, 2010, Cable Television Laboratories, Inc.

## 2.3 Reference Acquisition <sup>2</sup>

- Broadband Forum, 48377 Fremont Blvd, Suite 117 Fremont, CA. 94538,  
Phone: +1-510-492-4020, Fax: +1-510-492-4001, <http://www.broadband-forum.org>
- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;  
Phone:+1-303-661-9100; Fax:+1-303-661-9199; Internet: <http://www.cablelabs.com>
- 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. Internet: <http://www/ietf.org>

---

<sup>2</sup> Revised per eRouter N-11.1014-3 on 10/27/11 by JB.

### 3 TERMS AND DEFINITIONS <sup>3</sup>

This specification uses the following terms:

|  |  |
|--|--|
| <b>Customer-Facing Interface</b>         | An eRouter interface used for connecting CPE devices. Defined in [RFC 6204] as a Local Area Network (LAN) Interface, the Customer-Facing Interface is represented by a physical port.  |
| <b>Customer-Facing IP Interface</b>      | An IP Interface connected to the eRouter that is not necessarily mapped one-to-one with the number of Customer-Facing ports on the eRouter. As defined in [RFC 6204], this is an IP LAN interface in which one or many physical ports are associated with an IP address.                       |
| <b>Customer-Facing Logical Interface</b> | A logical Interface connected to the eRouter that is not necessarily mapped one-to-one with the number of Customer-Facing ports on the eRouter. As defined in [RFC 6204], this is a LAN interface in which one or more physical ports are associated with a logical interface, such as a VLAN. |
| <b>eRouter</b>                           | An eSAFE device that is implemented in conjunction with the DOCSIS embedded cable modem.   |
| <b>Internet Gateway Device</b>           | A remotely managed gateway device as defined in CPE WAN Management Protocol [TR-069a4].  |
| <b>Multicast Subscription Database</b>   | A simple table of entries for the IPv4 or IPv6 Multicast Group Membership information maintained by the eRouter on respective interfaces. Implementation details for storage of records are completely vendor-defined.   |
| <b>Operator-Facing Interface</b>         | The eRouter interface that is connected to the Embedded cable modem. As defined in [RFC 6204], this is a Wide Area Network (WAN) interface. In CWMP this is called an upstream interface.  |
| <b>Operator-Facing IP Interface</b>      | IP Interface that is connected to the Embedded Cable Modem and is provisioned with an IP Address provided by the Operator. As defined in [RFC 6204], this is a WAN interface.  |
| <b>TR-069</b>                            | Term used to refer to the CPE WAN Management Protocol suite defined in [TR-069a4].   |
| <b>TR-069 CPE</b>                        | Term used to refer to the CPE managed using the CPE WAN Management Protocol suite defined in [TR-069a4].   |

<sup>3</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 by JB. Revised per eRouter N-11.1014-3 on 10/27/11 and by per eRouter N-11.1015-2 on 11/04/11 by JB.

## 4 ABBREVIATIONS AND ACRONYMS <sup>4</sup>

This specification uses the following abbreviations:

|              |  |
|--------------|--|
| <b>ACS</b>   | Auto-configuration Server                      |
| <b>ALG</b>   | Application Layer Gateway                      |
| <b>ARP</b>   | Address Resolution Protocol                    |
| <b>ASN.1</b> | Abstract Syntax Notation One                   |
| <b>CM</b>    | Cable Modem                                    |
| <b>CPE</b>   | Customer Premises Equipment                    |
| <b>CWMP</b>  | CPE WAN Management Protocol                    |
| <b>DAD</b>   | Duplicate Address Detection                    |
| <b>DNS</b>   | Domain Name Service                            |
| <b>DUID</b>  | DHCP unique identifier                         |
| <b>EAE</b>   | Early Authentication and Encryption            |
| <b>eSAFE</b> | Embedded Service/Application Functional Entity |
| <b>EUI</b>   | Extended Unique Identifier                     |
| <b>FTP</b>   | File Transfer Protocol                         |
| <b>ID</b>    | Identifier                                     |
| <b>IDG</b>   | Internet Gateway Device                        |
| <b>IP</b>    | Internet Protocol                              |
| <b>IRT</b>   | Initial Retransmission Times                   |
| <b>LAN</b>   | Local Area Network                             |
| <b>LLC</b>   | Logical Link Control                           |
| <b>ND</b>    | Neighbor Discovery                             |
| <b>MAC</b>   | Media Access Control                           |
| <b>MIB</b>   | Management Information Base                    |
| <b>MLD</b>   | Multicast Listener Discovery                   |
| <b>MRC</b>   | Maximum Retransmission Count                   |
| <b>MRD</b>   | Maximum Retransmission Duration                |
| <b>MRT</b>   | Maximum Retransmission Time                    |
| <b>NAT</b>   | Network Address Translation                    |
| <b>NAPT</b>  | Network Address Port Translation               |
| <b>OID</b>   | Object ID                                      |
| <b>OUI</b>   | Organization Unique Identifier                 |
| <b>RFC</b>   | Request For Comment                            |

---

<sup>4</sup> Revised per eRouter N-11.1014-3 on 10/27/11 by JB.

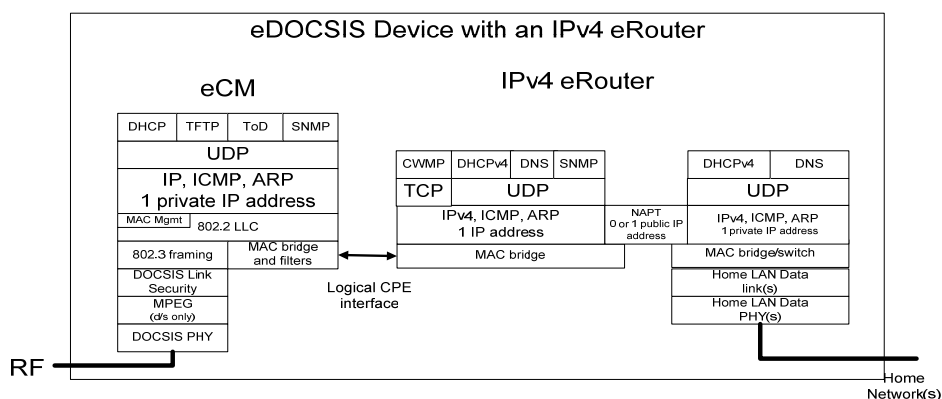
|              |                                     |
|--------------|-------------------------------------|
| <b>RA</b>    | Router Advertisement                |
| <b>RD</b>    | Router Discovery                    |
| <b>RG</b>    | Residential Gateway                 |
| <b>SIP</b>   | Session Initiation Protocol         |
| <b>SLAAC</b> | Stateless Address Autoconfiguration |
| <b>TCP</b>   | Transmission Control Protocol       |
| <b>TLV</b>   | Type/Length/Value                   |
| <b>TTL</b>   | Time To Live                        |
| <b>UDP</b>   | User Datagram Protocol              |
| <b>WAN</b>   | Wide Area Network                   |

## 5 THEORY OF OPERATION <sup>5</sup>

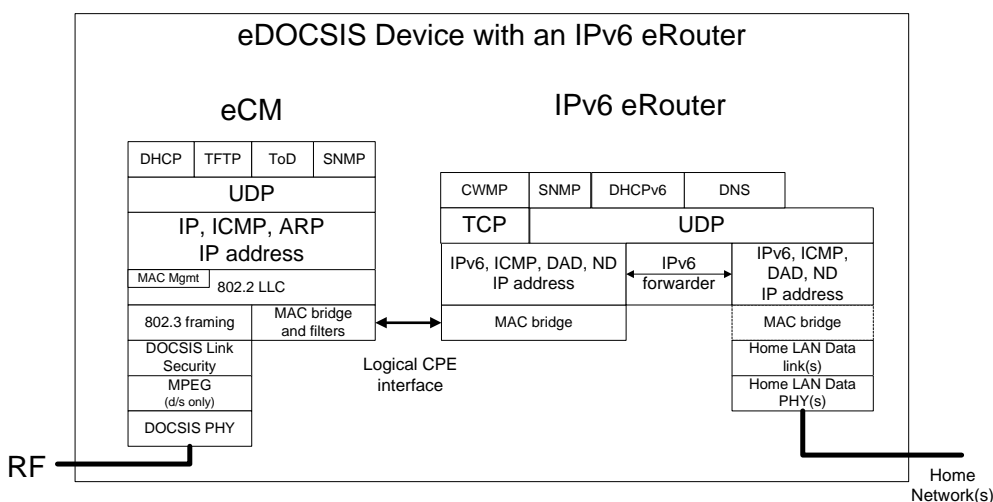
The eRouter device is intended to provide networking functionality in conjunction with an embedded DOCSIS eCM in an eDOCSIS device.

This specification defines a set of features for an IPv4 eRouter and a set of features for an IPv6 eRouter. Both sets of features can be implemented together as an IPv4 + IPv6 eRouter.

The figures below depict implementations of an eDOCSIS device with an IPv4 eRouter, an IPv6 eRouter, and an IPv4 + IPv6 eRouter.

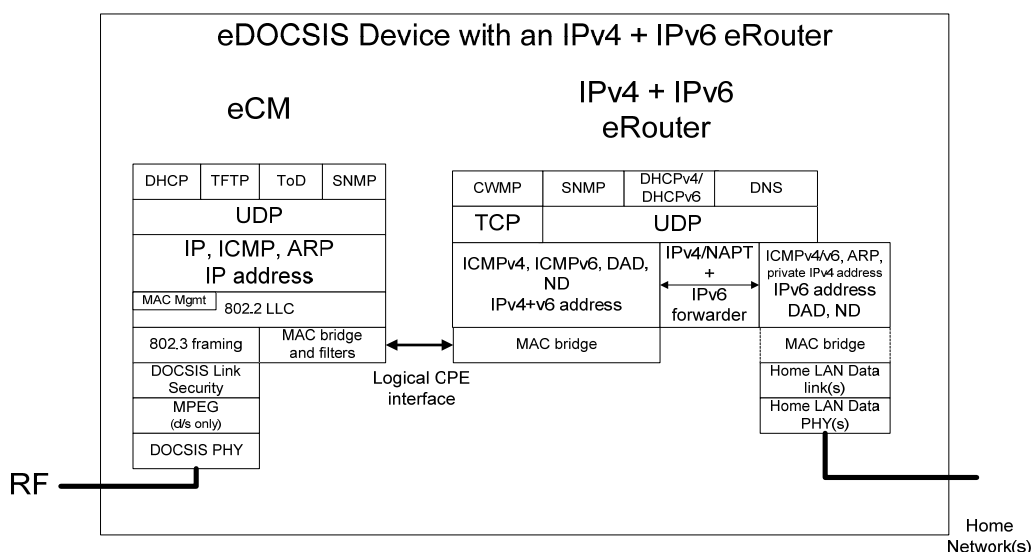


**Figure 5-1 - Logical Components of an eDOCSIS device with an IPv4 eRouter**



**Figure 5-2 - Logical Components of an eDOCSIS device with an IPv6 eRouter**

<sup>5</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 by JB. Revised per eRouter N-11.1014-3 on 10/27/11 by JB.



**Figure 5-3 - Logical Components of an eDOCSIS device with an IPv4 + IPv6 eRouter**

The primary function of the eRouter device is to allow subscribers to connect multiple CPE devices to the operator-provided DOCSIS high-speed Internet service. DOCSIS specifications allow subscribers to directly connect multiple CPE devices to the cable modem; however, that requires operators to provide provisioning to each of the CPE devices. The eRouter is delegated the responsibility of provisioning multiple CPE devices at the subscriber end. Depending on which version of the eRouter is included with the eDOCSIS implementation, the eRouter allows provisioning of IPv4 CPEs, IPv6 CPEs, or both IPv4 and IPv6 CPEs simultaneously.

This specification defines the core set of functions that are performed by the eRouter; however, in most implementations, vendors would include additional features that would enhance the eRouter device. This may include additional networking features as well as the ability to provision and manage the eRouter from the subscriber side.

The specification defines: a) CPE provisioning with IPv4 and IPv6 addresses, b) IPv4 data forwarding with NAT and IPv6 data forwarding, c) ability to forward IP Multicast traffic, and d) preserving IP QoS markings on IP data to and from the CPE devices.

This specification uses the terms Customer-Facing Interface and Operator-Facing Interface as defined in Section 3.

This specification defines requirements for an eRouter device with a single Operator-Facing IP Interface. This specification defines requirements for an eRouter device with a single Customer-Facing logical IP Interface that is not necessarily mapped one-to-one with the number of Customer-Facing ports on the eRouter. Though it is possible that an eRouter could have multiple Customer-Facing IP interfaces, such cases are outside of the scope of this specification.

This specification defines SNMP [RFC 3412] and TR-069 C WMP [TR-069a4] as the Operator-Facing management interface alternative options for eRouter.



## 5.1 eDOCSIS eRouter and TR-069 Architecture <sup>6</sup>

This section defines TR-069 requirements for the eRouter management architecture which is based on the [eDOCSIS] specification.

The TR-069 specification suite defines the Device 2.x entity in [TR-181i2a3]. It refers to a CPE device management space for holding the device itself and root of other services specifications (e.g., VoIP, Storage, IPTV, etc.). See [MR-230] for more details on TR-069 deployment scenarios.

Both eDOCSIS and TR-069 architectures define two equivalent components:

- Access Modem: eDOCSIS defines the eCM; TR-069 may accommodate any access technology.
- Services: eDOCSIS defines eSAFEs; TR-069 defines CPE Services.

The cable modem is not referred to as a CPE in [MULPI] and [eDOCSIS]. Only devices in the Customer-Facing Interfaces attached to a cable modem are termed CPEs in [MULPI] and [eDOCSIS]. In TR-069, all devices located in the customer premises are considered CPEs. For the eRouter case, the term CPE has the same meaning within DOCSIS and TR-069. However, in this specification the eSAFE term is used when referring to the eRouter nature.

The main differences between both architectures are:

- A TR-069 Device 2.x [TR-181i2a3] is a TR-069 enabled CPE such as Residential Gateways (RGs) and other type of network devices (e.g., Access Modem). Different services can be implemented on a TR-069 Device. The Access Modem could be part of the device itself, by modeling it as an upstream interface of the entire TR-069 CPE, or the device contains only CPE services. In eDOCSIS the eCM is the Access Modem and eRouter is an application or functional entity (eSAFE). DOCSIS specifications define CMs and eSAFEs such as eRouters (embedded eRouters within an eCM).
- The management of eSAFEs in eDOCSIS is separated from the eCM. In TR-069 the management of services is integrated with the CPE device management.

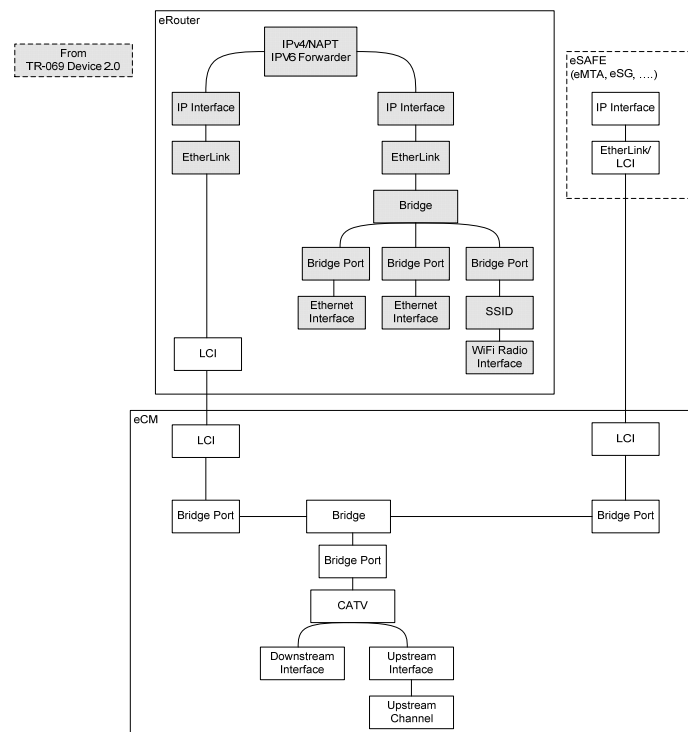
TR-069 allows the transparent integration of access network technologies within the RG and CPE Services by combining the multiple components and their respective management data. The TR-069 device can either configure and monitor the Access Modem managed elements, simply report the Access Modem status and configuration, or do nothing with the Access Modem. The latter is the case of TR-069 in the context of eDOCSIS where the eCM is managed and provisioned independently of any eSAFE supporting TR-069 management.

Figure 5-4 shows the alignment of eDOCSIS, eRouter, and TR-069 device architectures where the reuse of the TR-069 protocol stack and data models for eDOCSIS devices such as eRouter can be seen. A general purpose eSAFE is shown for illustration purposes. The main difference between both models is the separation of the CM bridge of the internal WAN/LAN bridging function at the eRouter compared to the integrated TR-069 Device 2.x.

Figure 5-4 is based on the "Simple Router Example (Interfaces Visualized)" figure of [TR-181i2a3]. In Figure 5-4, the stack layers are seen as interfaces per [TR-181i2a3], physical interfaces (e.g., Ethernet, SSID, Wi-Fi Radio), bridges, ports, Bridges, EthernetLink interfaces (LLC), and IP Interfaces. The Operator-Facing TR-069 Etherlink Interfaces correspond to the eDOCSIS Logical CPE Interfaces (LCI). IP additional interfaces can represent IP Tunnels and other IP forwarding models.

---

<sup>6</sup> Added per eRouter N-11.1014-3 on 10/27/11 by JB.



**Figure 5-4 - TR-069 Interface Model Applied to eDOCSIS eRouter**

## 5.2 eRouter Device Management <sup>7</sup>

The eRouter device that supports TR-069 implies the support of dual stack management, SNMP for the eCM component, and TR-069 for the eRouter component, as shown in Figure 5-4 - TR-069 Interface Model Applied to eDOCSIS eRouter.

eRouter eSAFEs can be modeled as a stack of interfaces, and, in the future, other eSAFEs might support TR-069 protocol. This specification does not address architecture requirements such those listed in section 5.1 of [eDOCSIS], specifically, whether two TR-069-capable eSAFEs share the same TR-069 management stack or have separate stacks (as in the SNMP model). This is outside of the scope of this specification and within the scope of [eDOCSIS].

<sup>7</sup> Added per eRouter N-11.1014-3 on 10/27/11 by JB.

## 6 eROUTER INITIALIZATION <sup>8</sup>

Prior to its initialization, the eRouter is enabled or disabled through the TLVs in Annex B. The eRouter may operate in any one of four possible modes – Disabled, IPv4 Protocol Enabled, IPv6 Protocol-Enabled, or Dual IP Protocol-Enabled, as summarized in Table 6-1. The eRouter **MUST** support the Disabled Mode and at least one other Mode. The eRouter **MAY** support the IPv4 Protocol Enabled Mode. The eRouter **MAY** support the IPv6 Protocol Enabled Mode. The eRouter **MAY** support the Dual IP Protocol Enabled Mode. The eRouter **MUST** persist its initialization mode across reinitialization. The eRouter **MAY** reinitialize itself when its initialization mode changes.

**Table 6-1 - eRouter Modes**

| Mode                     | IPv4                                      | IPv6                                     |
|--------------------------|---|--|
| Disabled                 | CM bridges all traffic per [MULPI] spec.  | CM bridges all traffic per [MULPI] spec. |
| IPv4 Protocol Enabled    | eRouter forwards IPv4 traffic with NAPT.  | eRouter does not forward IPv6 traffic.   |
| IPv6 Protocol Enabled    | eRouter does not forward IPv4 traffic.    | eRouter forwards IPv6 traffic.           |
| Dual IP Protocol Enabled | eRouter forwards IPv4 packets using NAPT. | eRouter forwards IPv6 packets.           |

In Disabled Mode, the eRouter transparently forwards all traffic directly between its Customer-Facing Interface and its Operator-Facing Interface. In this mode, it appears as if there is no eRouter present. The CM bridges all traffic (regardless of IP protocol version) to the CPE ports that would have been behind the eRouter had it been enabled. In this mode, the eRouter specification is irrelevant – the interfaces become part of the cable modem. All behavior will occur according to the DOCSIS specifications.

When configured to operate in IPv4 Protocol Enabled Mode, the eRouter performs IPv4 provisioning and forwards IPv4 traffic between its Customer-Facing Interface and its Operator-Facing Interface. The eRouter operating in IPv4 Protocol Enabled Mode will not perform any IPv6 provisioning. An eRouter configured to operate in IPv4 Protocol Enabled Mode will not forward any IPv6 traffic. The IPv4 traffic is forwarded using NAPT according to Section 9.

When configured to operate in IPv6 Protocol Enabled Mode, the eRouter performs IPv6 provisioning and forwards IPv6 traffic between its Customer-Facing Interface and its Operator-Facing Interface. The eRouter operating in IPv6 Protocol Enabled Mode will not perform any IPv4 provisioning. An eRouter configured to operate in IPv6 Protocol Enabled Mode will not forward any IPv4 traffic.

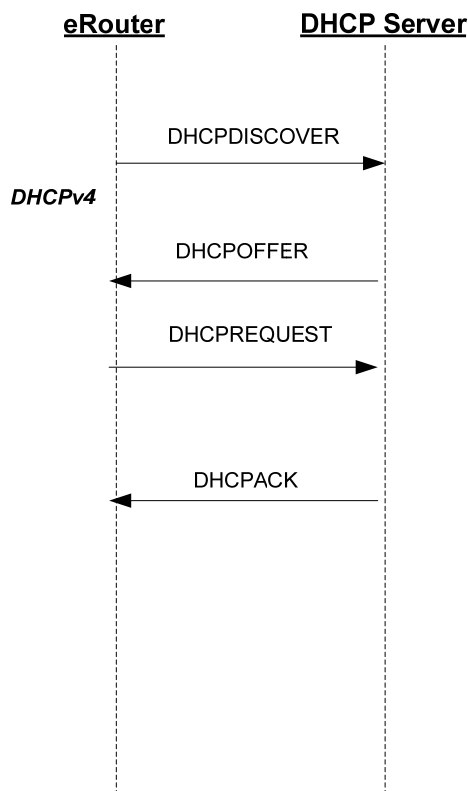
In Dual IP Protocol Enabled Mode, the eRouter is configured to forward both IPv4 and IPv6 traffic between its Customer-Facing Interface and its Operator-Facing Interface. IPv4 traffic is forwarded using NAPT, according to Section 9. IPv6 traffic is forwarded according to Section 10.

<sup>8</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 by JB. Revised per eRouter N-11.1015-2 on 11/04/11 by JB.

## 7 IPV4 PROVISIONING

The normative requirements of this section are mandatory for an eRouter that implements the IPv4 Protocol Enabled Mode and/or the Dual IP Protocol Enabled Mode as defined in Section 6.

After the CM has completed provisioning, if the eRouter is configured to route IPv4 packets, the eRouter **MUST** use DHCPv4 [RFC 2131] via its Operator-Facing Interface in order to obtain an IP address and any other parameters needed to establish IP connectivity, as illustrated in Figure 7-1.



**Figure 7-1 - IPv4 Provisioning Message Flow**

The eRouter may receive multiple DHCPOFFER messages in response to its DHCPDISCOVER message. If a received DHCPOFFER message does not include all of the required DHCPv4 fields and options as described in Section 7.2, the eRouter **MUST** discard the DHCPOFFER message and wait for another DHCPOFFER message. If none of the received DHCPOFFER messages contain all the required DHCPv4 fields and options, the eRouter **MUST** retransmit the DHCPDISCOVER message.

The backoff values for retransmission of DHCPDISCOVER messages **SHOULD** be chosen according to a uniform distribution between the minimum and maximum values in the rows of Table 7-1.

**Table 7-1 - eRouter DHCP Retransmission Interval**

| Backoff Number | Minimum (sec.) | Maximum (sec.) |
|----------------|----------------|----------------|
| 1              | 3              | 5              |
| 2              | 7              | 9              |
| 3              | 15             | 17             |
| 4              | 31             | 33             |
| 5              | 63             | 65             |

The eRouter **SHOULD** also implement a different retransmission strategy for the RENEWING and REBINDING states, as recommended in [RFC 2131], which is based on one-half of the remaining lease time.

The eRouter **MUST** limit the number of retransmissions of the DHCPDISCOVER and DHCPREQUEST messages to five or fewer. The eRouter **MUST NOT** forward IPv4 traffic between its Customer-Facing Interface and its Operator-Facing Interface until it has completed IPv4 provisioning, including the successful receipt of a DHCPACK message. The eRouter **MUST NOT** forward IPv4 traffic if, at any time, it does not have an IPv4 address for its Operator-Facing Interface.

The eRouter **MUST** be able to accept a unicast response from the DHCP server/relay agent.

[RFC 3203] describes an extension to DHCPv4 that allows a server to send a FORCERENEW message that forces a client to renew its lease. The eRouter **MUST** ignore all received FORCERENEW messages.

## 7.1 DHCPv4 Fields Used by the eRouter

The eRouter **MUST** include the following fields in the DHCPDISCOVER and DHCPREQUEST messages:

- The hardware type (htype) **MUST** be set to 1.
- The hardware length (hlen) **MUST** be set to 6.
- The client hardware address (chaddr) **MUST** be set to the 48-bit MAC address associated with the IPv4 CM-facing interface of the eRouter.
- The Broadcast bit **MUST NOT** be set.
- The client-identifier option **MUST** be included, using the format defined in [RFC 4361].
- The parameter request list option **MUST** be included. The following option codes (defined in [RFC 2132] and [RFC 4361]) **MUST** be included in the list:
  - Option code 1 (Subnet Mask)
  - Option code 3 (Router Option)
  - Option code 6 (DNS Server Option)
  - Option code 60 (Vendor Class Identifier) [eRouter1.0]
  - Option Code 43 (see [eDOCSIS])
  - Option 55 Parameter Request List

The following fields are expected in the DHCP OFFER and DHCP ACK messages returned to the eRouter. The eRouter MUST configure itself with the listed fields from the DHCP ACK:

- The IP address to be used by the eRouter (yiaddr) (critical).
- The IP Address lease time, option 51 (critical).
- The Server identifier, option 54 (critical).
- The subnet mask to be used by the eRouter (Subnet Mask, option 1) (critical).

A list of addresses of one or more routers is to be used for forwarding eRouter-originated IP traffic (Router Option, option 3). The eRouter is not required to use more than one router IP address for forwarding (critical):

- A list of DNS Server addresses (critical).
- A list of options under the CL\_V4EROUTER\_CONTAINER\_OPTION option which are passed on to CPE devices as defined in the [CANN DHCP].

If a critical field is missing or invalid in the DHCP ACK received during initialization, the eRouter MUST restart the DHCP cycle, beginning with an initial DHCP DISCOVER.

If a non-critical field is missing or invalid in the DHCP ACK received during initialization, the eRouter MUST ignore the field, and continue the provisioning process.

If the yiaddr, Server Address, or Lease Time field is missing or invalid in the DHCP ACK received during a renew or rebind operation, the eRouter MUST retry the renew or rebind operation until either: (1) it receives a response containing valid values of the yiaddr, Server Address, and Lease Time fields; or (2) the lease expires. If the lease expires, the eRouter MUST restart the DHCP cycle, beginning with an initial DHCP DISCOVER.

If any field other than the yiaddr, Server Address or Lease Time is missing, or is invalid in the DHCP ACK received during a renew or rebind operation, the eRouter MUST ignore the field if it is invalid and remain operational.

## 7.2 Router DHCPv4 Server Sub-element

The DHCP server is responsible for assigning network address leases to LAN IP devices associated with Customer-Facing Interfaces. It is also responsible for providing LAN IP devices with configuration information via DHCP Option codes, as specified in [RFC 2132].

### 7.2.1 DHCPv4 Server Function Goals

Goals for the DHCP server include the following:

- Assign network address leases to CPE devices according to [RFC 2131].
- Assign private CPE addresses according to [RFC 1918].
- Assign configuration information according to [RFC 2132].

### 7.2.2 DHCPv4 Server Function System Description

The eRouter DHCPv4 server responsibilities include:

- Assigning IP Addresses and delivering DHCP configuration parameters to CPE Devices. The server relies on built-in default values for initial IP Address pool configuration, lease parameter configuration, and DHCP options values.
- Optional logging of DHCPv4 server errors to a local event log.

### 7.2.3 DHCPv4 Server Function Requirements

The eRouter **MUST** include a DHCPv4 server compliant with [RFC 2131].

In addition, the following requirements apply to the DHCPv4 Server function:

- When the DHCP server assigns an active lease for an IP address to a CPE Device, the server **MUST** remove that IP address from the pool of IP addresses available for assignment.
- The DHCP server function of the eRouter **MUST** support the DHCP options indicated as mandatory in Table 7-2.
- The DHCP server function of the eRouter **MUST NOT** respond to DHCP messages that are received through the Operator-Facing Interface, nor originate DHCP messages from the Operator-Facing Interface.
- The DHCP server function of the eRouter **MUST NOT** deliver any DHCP option with null value to any CPE device.
- The DHCP server function **SHOULD** be operational independent of the eRouter Operator-Facing Interface connectivity state.
- If the eRouter Operator-Facing Interface is not successfully provisioned, the eRouter DHCP server function **SHOULD** assign a short lease time to CPE devices and may omit options it has not acquired.
- The DHCP server function **MUST** assign private IP address space as defined in [RFC 1918].
- The DHCP server function **SHOULD** log errors to a local event log.

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

|             |   |                 |                     |
|-------------|---|-----------------|---------------------|
| 10.0.0.0    | - | 10.255.255.255  | (10/8 prefix)       |
| 172.16.0.0  | - | 172.31.255.255  | (172.16/12 prefix)  |
| 192.168.0.0 | - | 192.168.255.255 | (192.168/16 prefix) |

**Table 7-2 - DHCPv4 Server Options**

| Option Number | Option Function       |
|---------------|-----------------------|
| 0             | Pad                   |
| 255           | End                   |
| 1             | Subnet Mask           |
| 3             | Router Option         |
| 6             | Domain Name Server    |
| 50            | Requested IP Address  |
| 51            | IP Address Lease Time |
| 54            | Server Identifier     |

| Option Number | Option Function  |
|---------------|--|
| 55            | Parameter Request List   |
| X             | Option(s) acquired under CL_V4EROUTER_CONTAINER_OPTION from the Operator |

### 7.3 Operator-Facing IPv4 Address Release Behavior <sup>9</sup>

There is a number of situations in which it is desirable for eRouter to release its associated IPv4 address leases in order to protect the integrity of the DHCP database. Examples of such circumstances include situations in which the eRouter needs to be administratively reset (i.e., for configuration change, software update, or other reasons), or a change to the IPv4 address during DHCPv4 renewal. Due to the eRouter's dependency on the eCM for maintaining operator-facing connectivity, the eRouter **MUST** release its lease information prior to an SNMP or administratively imposed re-initialization of the embedded CM in order to prevent loss of the communications path with the DHCP server.

Whenever the eRouter is instructed to reset, the eRouter **MUST** send a DHCP\_RELEASE message [RFC 2131] for the IPv4 public address assigned by the DHCPv4 server to the eRouter's Operator-Facing Interface. The eRouter **MUST** send the DHCP\_RELEASE message [RFC 2131] for the IPv4 public address assigned by DHCPv4 to the eRouter's Operator-Facing Interface whenever the eRouter receives a DHCPv4 server renewal response contains a different IPv4 address. The eRouter **MUST NOT** wait for a confirmation of the receipt of the release by the DHCPv4 server in order to re-initialize.

### 7.4 Customer-Facing IPv4 Address Release Behavior <sup>10</sup>

After initiating an administrative device reset in which the public address has been released, the eRouter customer-facing interfaces will be limited to inter-LAN forwarding until the device completes any necessary resets and a new address lease is acquired. Prior to the operator-facing interface acquiring an IPv4 address from the operator's DHCPv4 server, local network services and data forwarding of the customer-facing LAN interfaces will continue so long as the DHCPv4 server of the eRouter is enabled.

<sup>9</sup> Added per eRouter N-11.1015-2 on 11/04/11 by JB.

<sup>10</sup> Added per eRouter N-11.1015-2 on 11/04/11 by JB.

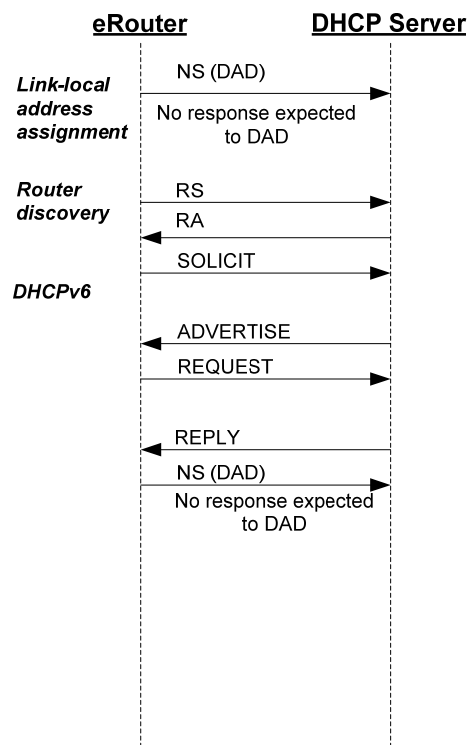


## 8 IPV6 PROVISIONING <sup>11</sup>

IPv4 address space is nearly exhausted. The IANA pool of free IPv4 address space is expected to be completely depleted before customers have been fully migrated to IPv6. The features necessary to facilitate transition to IPv6 are described in the following sections.

The normative requirements of this section are mandatory for an eRouter that implements the IPv6 Protocol Enabled Mode and/or the Dual IP Protocol Enabled Mode, as defined in Section 6.

After the CM has completed provisioning, if the eRouter is operating in the IPv6 Protocol Enabled Mode or the Dual IP Protocol Enabled Mode, the eRouter **MUST** use DHCPv6 [RFC 3315] in order to obtain an IP address for its Operator-Facing IP Interface and any other parameters needed to establish IP connectivity, as illustrated in Figure 8-1.



**Figure 8-1 - IPv6 Provisioning Message Flow**

The eRouter establishes IPv6 connectivity including assignment of:

- Link-local IPv6 address
- IPv6 address of a Default router
- Operator-Facing Interface IPv6 address (used for both management access to the eRouter and data forwarding)
- Other IPv6 configuration

These steps are described in the following subsections.

<sup>11</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 by JB.

## 8.1 Obtain Link-Local Address <sup>12</sup>

The eRouter MUST construct a link-local address for its Operator-Facing Interface and each of its Customer-Facing Interface(s) according to the procedure in section 5.3 of [RFC 4862]. The eRouter MUST use the EUI-64 identifier as a link-local address for each of its interfaces as described in [RFC 3513]. For each of its interfaces, the eRouter MUST join the all-nodes multicast address and the solicited-node multicast address of the corresponding link-local address [RFC 4862], [RFC 2710]. The eRouter MUST use Duplicate Address Detection (DAD), as described in section 5.4 of [RFC 4862], to confirm that the constructed link-local addresses are not already in use prior to sending any Router Solicitations on the interface. If the eRouter determines that the constructed link-local address is already in use, the eRouter MUST terminate IPv6 operation on that interface.

## 8.2 Perform router discovery <sup>13</sup>

The eRouter MUST perform router discovery as specified in section 6.3 of [RFC 4861] on its Operator-Facing Interface. The source address used in the Router Solicitation MUST be the link-local address on the Operator-Facing Interface. The eRouter identifies neighboring routers and default routers from the received RAs.

## 8.3 Obtain IPv6 address and other configuration parameters <sup>14</sup>

An eRouter MUST examine the contents of RAs it receives and obey the following rules:

- If the M bit in the RA is set to 1, the eRouter MUST use DHCPv6 to obtain its IPv6 address for its Operator-Facing Interface and other configuration information (and ignore the A and 0 bits).

If an RA contains a prefix advertisement for an IPv6 network prefix on which the eRouter does not have an address and the M bit in the RA is set to 1, the eRouter MUST use DHCPv6 to obtain its IPv6 address for its Operator-Facing Interface and renew any current IA\_PD lease(s).

The eRouter MUST act as a requesting router for the purposes of DHCPv6 prefix delegation ([RFC 3633]). DHCPv6 address assignment (IA\_NA) and DHCPv6 prefix delegation (IA\_PD) SHOULD be done as a single DHCPv6 session.

The eRouter sends a DHCPv6 Solicit message as described in section 17.1.1 of [RFC 3315]. The Solicit message MUST include:

1. A Client Identifier option containing the DHCP Unique Identifier (DUID) for this eRouter (as specified by [RFC 3315]), the DUID should be formatted as follows:
  - a. The eRouter MUST use a DUID that is one of DUID-LL, DUID-EN or DUID\_UUID type and;
  - b. The eRouter MUST use a DUID that is persistent across administrative reset or reboot following a loss of power per [RFC 6204] W-6.
2. An IA\_NA option to obtain its IPv6 address.
3. An IA\_PD option (as specified in [RFC 3633]) to obtain its delegated IPv6 prefix.
4. A Reconfigure Accept option to indicate the eRouter is willing to accept Reconfigure messages.
5. An Options Request option, which MUST include the DNS Recursive Name Server option [RFC 3646].

<sup>12</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 and per eRouter-N-11.1015-2 on 11/4/11 by JB.

<sup>13</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 and per eRouter-N-11.1015-2 on 11/4/11 by JB.

<sup>14</sup> Revised per eRouter-N-09.0877-2 on 5/11/10, per eRouter-N-10.0974-2 on 1/24/11 and per eRouter-N-11.1015-2 on 11/4/11 by JB.

6. A Vendor Class option containing 32-bit number 4491 (the Cable Television Laboratories, Inc., enterprise number) and the string "eRouter1.0".
7. A DOCSIS Device Identifier Option, as defined in [CANN DHCP].
8. A Vendor-specific option, containing:
  - a. The 32-bit number 4491 (the Cable Television Laboratories, Inc., enterprise number).
  - b. A CableLabs Vendor Specific Option Request sub-option, which request CL\_OPTION\_ORO CableLabs Vendor-specific options as defined in [CANN DHCP].
  - c. A list of options under the CL\_EROUTER\_CONTAINER\_OPTION option which are passed on to CPE devices as defined in the [CANN DHCP].

The eRouter MUST use the prefix assigned by the next successful operator DHCPv6 operation even if the new prefix differs from the prefix previously assigned. This new prefix will overwrite any stored prefix information preserved across resets by the eRouter.

If the eRouter does not have a previously assigned prefix, the eRouter MUST indicate a non-zero prefix size as DHCPv6 "hint" information [RFC 3633]. The eRouter MUST ask for a prefix large enough to assign one /64 for each of its Customer-Facing Logical Interfaces rounded up to the nearest nibble. The eRouter MUST be able to accept a delegated prefix length different from what was provided in the hint. If the delegated prefix is too small to address all of its interfaces, the eRouter SHOULD assign a single /64 for all Customer-Facing Logical Interfaces and log an error message.

If the delegated prefix(es) are aggregate route(s) of multiple, more-specific routes, the eRouter MUST silently discard packets that match the aggregate route(s), but not any of the more-specific routes. In other words, the next hop for the aggregate route(s) should be the null destination. For example, if the delegated prefix is a /56 but only 12 /64 are in active use, the eRouter should discard all traffic destined to the 242 unused /64. This is necessary to prevent forwarding loops and is also helpful in preventing malicious (DoS, network scanning, etc.) traffic from entering the LAN or using eRouter resources.

The eRouter MUST use the following values for retransmission of the Solicit message (see section 14 of [RFC 3315] for details):

- IRT (Initial Retransmission Time) = SOL\_TIMEOUT
- MRT (Maximum Retransmission Time) = SOL\_MAX\_TIMEOUT
- MRC (Maximum Retransmission Count) = 0
- MRD (Maximum Retransmission Duration) = 0

The DHCP server responds to Solicit messages and Request messages with Advertise and Reply messages. The Advertise and Reply messages may include other configuration parameters, as requested by the eRouter, or as configured by the administrator, to be sent to the eRouter. If any of the following options is absent from the Advertise message, the eRouter MUST discard the message and wait for another Advertise message. If any of the following options is absent from the Reply message, the eRouter MUST consider IPv6 provisioning to have failed. In addition the eRouter MAY log an event.

1. The IA\_NA option containing the eRouter's IPv6 address;
2. The IA\_PD option containing the delegated IPv6 prefix for use by the eRouter;
3. Reconfigure Accept option.

The eRouter interface MUST join the All-Nodes multicast address and the Solicited-Node multicast address of the IPv6 address acquired through DHCPv6. The eRouter MUST perform Duplicate Address Detection (DAD) with the IPv6 address acquired through DHCPv6.

If the eRouter determines through DAD that the IPv6 address assigned through DHCPv6 is already in use by another device, the eRouter MUST:

- Send a DHCP Decline message to the DHCP server, indicating that it has detected that a duplicate IP address exists on the link.
- Discontinue using the duplicate IP address.
- Consider the IPv6 provisioning process to have failed and log the event in the local log.

The eRouter MUST support the Reconfigure Key Authentication Protocol, as described in section 21.5 of [RFC 3315].

The eRouter MUST NOT forward any IPv6 traffic between its Customer-Facing Interface and its Operator-Facing Interface until it has successfully completed the IPv6 provisioning process. The eRouter MUST NOT forward any IPv6 traffic between its Customer-Facing Interface and its Operator-Facing Interface if, at any time, it does not have a Globally-assigned IPv6 address on its Operator-Facing Interface.

## 8.4 Use of T1 and T2 Timers <sup>15</sup>

The eRouter MUST initiate the lease renewal process when timer eRouter-T1 expires. The eRouter MUST initiate the lease rebinding process when timer eRouter-T2 expires. Timers eRouter-T1 and eRouter-T2 are called T1 and T2, respectively, in the DHCP specifications. If the DHCP server sends a value for eRouter-T1 to the eRouter in a DHCP message option, the eRouter MUST use that value. If the DHCP server does not send a value for eRouter-T1, the CM MUST set eRouter-T1 to 0.5 times the duration of the lease [RFC 3315]. If the DHCP server sends a value for eRouter-T2 to the eRouter in DHCP message options, the eRouter MUST use that value. If the DHCP server does not send a value for eRouter-T2, the eRouter MUST set eRouter-T2 to 0.875 times the duration of the lease [RFC 3315].

## 8.5 IPv6 Provisioning of CPE Devices <sup>16</sup>

The eRouter MUST generate and assign a globally unique /64 prefix for each Customer-Facing Logical Interface. These individual prefixes are allocated out of the prefix acquired from the IA\_PD option per Section 8.3 by the eRouter during the provisioning process.

The eRouter MUST assign a global IPv6 address to each Customer-Facing IP Interface. The eRouter SHOULD generate each Customer-Facing IP Interface Identifier using the Modified EUI-64 process as described per [RFC 4291]. The Modified EUI-64 IPv6 Interface Identifier is created by converting the IEEE 802 MAC address assigned to each Customer-Facing IP Interface to an EUI-64 formatted 64-bit address, and complementing the U/L bit; then, pre-pending 64 bits of the prefix acquired under IA\_PD in Section 8.3 to create the 128-bit IPv6 Interface Identifier address.

<sup>15</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 by JB.

<sup>16</sup> Revised per eRouter-N-11.1015-2 on 11/4/11 by JB.

### 8.5.1 SLAAC Requirements for eRouter

When the eRouter provides SLAAC on Customer-Facing Interfaces:

The /64 prefix length is required for the dynamic numbering of CPE devices using SLAAC [RFC 4862].

The eRouter **MUST** generate Router Advertisements (RA) on each Customer-Facing IP Interface as per [RFC 4862]. The RA **MUST** include the following by default unless administratively reconfigured:

- have the M bit set to 0,
- have the O bit set to 1,
- contain a Prefix Information Option with both the ICMPv6 options 'flags' L-Bit (On-link) bit and A-Bit (Autonomous) bit set to 1 derived from the prefix acquired under IA\_PD in Section 8.3,
- set the Preferred and Valid lifetimes in the Prefix Information Option equal to the Preferred and Valid lifetimes communicated in the IA-PD option on the Operator-Facing Interface. This requirement ensures prefix lifetime synchronization between the eRouter aggregate prefix and the prefix/es assigned to each Customer-Facing Interface.

These settings in the RA will cause CPE devices to use auto-configuration by default for assigning their global IPv6 address.

On the Customer-Facing Interface the eRouter **MUST** be able to pass the following set of DHCPv6 options received from the Cable Operator for the configuration of CPE devices.

- The OPTION\_DNS\_SERVERS option as specified in [RFC 3646]. This option carries a list of Domain Name Servers for the CPE devices.
- The list of options under the CL\_V4EROUTER\_CONTAINER\_OPTION option which are passed to the eRouter by the operator.

The eRouter **SHOULD** include DNS configuration options in its RA message as specified in [RFC 6106]. If the eRouter supports the RDNSS option, it **MUST** include the list of DNS servers included in the OPTION\_DNS\_SERVERS option.

### 8.5.2 DHCPv6 Requirements for eRouter

The DHCPv6 requirements of this section are optional. The eRouter **SHOULD** provide DHCPv6 on Customer-facing interfaces, as described in the following RFCs:

- [RFC 3315] Dynamic Host Configuration Protocol for IPv6 (DHCPv6).
- [RFC 3319] Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers.
- [RFC 3646] DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).
- [RFC 3633] IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.
- [RFC 3736] Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6.
- [RFC 4075] Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6.
- [RFC 4242] Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).

When the eRouter provides DHCPv6 on Customer-Facing Interfaces:

The DHCPv6 server **MUST** be able to manage at least one IA\_NA for each client, and at least one address in each IA\_NA. The DHCPv6 server **MUST** be able to assign an address to a client constructed from the client's EUI-64 identifier.

The DHCPv6 server **SHOULD** be able to manage at least one IA\_PD for each client, and at least one delegated prefix in each IA\_PD. The prefix delegated to the client is derived from the prefix delegated to the eRouter from the Cable Operator.

The DHCPv6 server **MAY** implement vendor-defined default lifetimes for assigned addresses and delegated prefixes.

The eRouter **MUST** generate Router Advertisements (RA) on each Customer-Facing IP Interface as per [RFC 4862]. The RA **MUST** include the following by default unless administratively reconfigured:

- have the M bit set to 1,
- have the O bit set to 1,
- contain a Prefix Information Option with both the ICMPv6 options 'flags' L-Bit (On-link) bit and A-Bit (Autonomous) bit set to 1 derived from the prefix acquired under IA\_PD in Section 8.3,
- set the Preferred and Valid lifetimes in the Prefix Information Option equal to the Preferred and Valid lifetimes communicated in the IA-PD option on the Operator-Facing Interface. This requirement ensures prefix lifetime synchronization between the eRouter aggregate prefix and the prefix/es assigned to each Customer-Facing Interface.

These settings in the RA will cause CPE devices to use DHCPv6 configuration for assigning their global IPv6 address.

The eRouter **MUST** be able to pass a set of options received from the Cable Operator to the DHCPv6 server for configuration of CPEs.

The eRouter **MAY** relax the requirements on non-volatile storage of assigned addresses and delegated prefixes and **MAY** glean information about assigned addresses and delegated prefixes from Advertise, Renew, and Rebind messages received from clients.

## 8.6 Operator-Facing IPv6 Address Release Behavior <sup>17</sup>

There are a number of situations in which it is desirable for the eRouter to release its associated IPv6 address leases in order to ensure the integrity of the DHCP database. Examples of such circumstances include situations in which the eRouter needs to be administratively reset (say for configuration change, software update or other reason) or a change to the IPv6 address during DHCPv6 renewal.

Due to the eRouter's dependency on the eCM for maintaining operator-facing connectivity, the eRouter **MUST** release its lease information prior to a SNMP or administratively imposed re-initialization of the embedded CM in order to prevent loss of the communications path with the DHCP server. The eRouter **MUST NOT** wait for confirmation of receipt of the release by the DHCPv6 server in order to re-initialize.

---

<sup>17</sup> Revised per eRouter-N-11.1015-2 on 11/4/11 by JB.

The eRouter MUST send a DHCP\_RELEASE message [RFC 3315] for the IPv6 IA\_NA and IA\_PD assigned by the DHCPv6 server to the eRouter's Operator-Facing Interface for the following events:

- Whenever the eRouter is instructed to reset,
- Whenever the eRouter receives a DHCPv6 Reply message containing a different IPv6 prefix or IPv6 address.

The eRouter SHOULD NOT wait for a confirmation of the RELEASE by the DHCPv6 server to re-initialization itself.

## 8.7 Customer-Facing IPv6 Address Release Behavior <sup>18</sup>

After initiating an administrative device reset in which the IA\_NA and IA\_PD addresses have been released, the eRouter customer-facing interfaces will be limited to inter-LAN forwarding until the device completes any necessary resets and new address and prefix leases are acquired. Prior to the eRouter's operator-facing interface acquiring IPv6 prefix information from the operator's DHCPv6 server, the eRouter will retain the IPv6 prefix information beyond the remaining valid lifetime of the prefix for the purposes of customer-facing LAN addressing. This additional measure on the customer-facing interfaces will insure that local network services and data forwarding of the customer-facing LAN interfaces will continue.

The eRouter MUST declare that it is no longer a Default Router by setting the Router Lifetime field to zero in the Router Advertisement.

The eRouter MUST NOT clear the prefix information from the Router Advertisement when the PD is released, preserving the previously acquired prefix until such time as the eRouter successfully completes DHCPv6. Clearing the prefix information would effectively disable IPv6 networking within the home network, or force use of IPv4 networking. Preserving the prefix information even beyond the valid lifetime until the eRouter completes DHCP address acquisition is another failsafe to ensure v6 connectivity remains even if operator-facing connectivity is lost for a protracted period of time.

The eRouter MUST preserve the prefix information across eRouter resets for the purpose of client configuration in advance of IPv6 address acquisition on the operator-facing interface. By preserving the prefix assigned to the eRouter, the home network can continue to operate until the expiration of the valid lifetime.

---

<sup>18</sup> Revised per eRouter-N-11.1015-2 on 11/4/11 by JB.

## 9 IPV4 DATA FORWARDING AND NAPT OPERATION

### 9.1 Introduction

The normative requirements of this section are mandatory for an eRouter that implements the IPv4 Protocol Enabled Mode and/or the Dual IP Protocol Enabled Mode as defined in Section 6.

#### 9.1.1 Assumptions

- There is only a single Operator-Facing IP Interface on the eRouter.
- There is typically a single Customer-Facing IP interface on the eRouter.
- At least one globally-routable IPv4 address is available to the eRouter's Operator-Facing IP Interface.
- The Operator-Facing IP Interface is Ethernet encapsulated.
- The Customer-Facing IP interface is Ethernet encapsulated.

#### 9.1.2 Overview

IPv4 Forwarding in the eRouter consists of three logical sub-elements:

- IPv4 Router
- NAPT (Network Address Port Translation)
- ARP (Address Resolution Protocol)

The IPv4 Router sub-element is responsible for forwarding packets between the Operator-Facing IP Interface and the Customer-Facing IP interfaces. This includes looking up the IPv4 Destination address to make a forwarding decision on whether to forward the packet from one of its interfaces to another one of its interface or to its internal stack.

Packet handling in the eRouter for NAPT includes:

- Providing a form of IPv4 address translation that allows for multiple IPv4 hosts on the Customer-Facing IP interfaces while presenting a small number of IPv4 addresses on the Operator-Facing IP Interface.
- Preventing unnecessary traffic on the Customer-Facing IP interfaces.
- Preventing traffic from one CPE device to another CPE device from traversing to the Operator-Facing Interface.

The ARP protocol on the eRouter provides a mechanism for converting IPv4 network addresses to Ethernet MAC addresses on both Customer-Facing IP interfaces and the Operator-Facing IP Interface.

### 9.2 System Description

#### 9.2.1 Overview

Some eRouters may have multiple customer ports that are connected to the same logical IP router interface. One scenario would be when the eRouter has an 802.11 wireless port and an 802.3 Ethernet port on the single Customer-Facing logical IP interface. The text in this section uses the term "Customer-

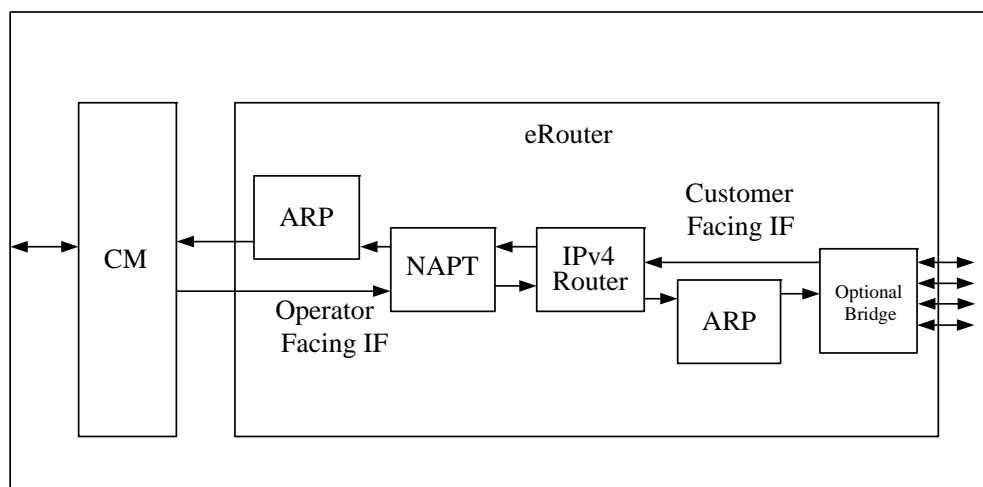


Facing IP interface" to refer to a single Customer-Facing logical IP router interface connected to the eRouter that is not necessarily mapped one-to-one with the number of Customer-Facing ports on the eRouter. This text documents the behavior of a single Customer-Facing IP interface, though it is possible that an eRouter could have multiple Customer-Facing IP interfaces. It is vendor-specific how to route between Customer-Facing Interfaces and the Operator-Facing IP Interface when there are multiple Customer-Facing IP interfaces.

Packets need to be processed by each of the three sub-elements in a very specific order (see Figure 9-1). The order is different depending on whether packets are received from a Customer-Facing IP interface or the Operator-Facing IP Interface.

When receiving packets from the Customer-Facing IP interface, the eRouter first attempts to route the packet through the router sub-element. If the router sub-element forwards the packet to the Operator-Facing Interface, the packet is passed to the NAPT sub-element to see if the packet requires NAPT translation. Once the NAPT sub-element has completed its work, the packet is sent to the ARP sub-element to resolve the IPv4 network address to Ethernet MAC. Then the packet is encapsulated in an Ethernet header and sent out the operator interface. If the router sub-element forwards the packet back out the Customer-Facing IP interface (perhaps because the client is on a different private subnet), the packet is sent to the ARP sub-element to resolve the IPv4 network address to Ethernet MAC. Then the packet is encapsulated in an Ethernet header and sent out the appropriate interface. No NAPT processing is necessary for packets routed back out the Customer-Facing IP interface.

When packets are received from the Operator-Facing Interface, they are immediately sent to the NAPT sub-element to translate the IPv4 network addresses back to addresses within the domain of the router sub-element. Once the NAPT has been performed on the packet, it is then sent to the router sub-element. If the router sub-element forwards the packet to the Customer-Facing IP interface, it sends the packet to the ARP sub-element to resolve the IPv4 network address to Ethernet MAC, encapsulates the packet in an Ethernet header, and sends the packet out the appropriate interface. If the router sub-element forwards the packet back to the Operator-Facing IP Interface, it is vendor-specific how to deal with the packet. Some implementations may choose to forward the packet back to the operator network; some may choose to drop the packet. Regardless, traffic should not be sent to a given eRouter from the operator network unless it is destined for a subnet known to the Customer-Facing IP interface.



**Figure 9-1 - eRouter IPv4 Forwarding Block Diagram**

### 9.3 IPv4 Router

When the eRouter's IPv4 Router sub-element receives a packet from its NAPT sub-element (received initially by its Operator-Facing IP Interface), it validates the IPv4 header in the packet. The eRouter MAY validate the IPv4 header in accordance with [RFC 1812], section 5.2.2. As defined in [RFC 1812], section 5.3.1, the eRouter MUST decrement the IP TTL field by at least one when forwarding the packet either back to the Customer-Facing IP interface, or out the Operator-Facing Interface. Packets forwarded to the eRouter's local IP stack for processing, MUST NOT decrement the TTL. Once the IPv4 header has been validated, the eRouter processes the destination IPv4 address of the packet. If the destination IPv4 address matches the eRouter's public address assigned to its Operator-Facing IP Interface, the eRouter sends the packet to its local IP stack for processing. If the destination IPv4 address does not match this address, the eRouter determines the next-hop address of the destination in order to forward the packet. The next-hop can be another router or a client directly connected to its Customer-Facing IP interface. The next-hop is determined by comparing the destination IPv4 address to the subnets assigned to its Customer-Facing IP interface. If the destination IPv4 address matches any of the prefixes assigned to the Customer-Facing IP interface, the destination is considered directly connected, or "on-link", and the next-hop to use for ARP purposes is the destination IPv4 address. If it does not match, the destination is considered remote or "off-link", and the next-hop to use for ARP purposes is the address of the intermediate router. Discovering other routers on the Customer-Facing IP interface is vendor-specific. If the eRouter cannot determine the next-hop of the IPv4 destination, then it MUST drop the packet.

When the eRouter's IPv4 Router sub-element receives a packet from its Customer-Facing IP interface, it validates the IPv4 header in the packet. The eRouter MAY validate the IPv4 header in accordance with [RFC 1812], section 5.2.2. As defined in [RFC 1812], section 5.3.1, the eRouter MUST decrement the IP TTL field by at least one when forwarding the packet, either back to the Customer-Facing IP Interface, or out the Operator-Facing Interface. Packets forwarded to the eRouter's local IP stack for processing, MUST NOT decrement the TTL. Once the IPv4 header has been validated, the eRouter processes the destination IPv4 address of the packet. If the destination IPv4 address matches one of the private addresses assigned to the eRouter, it sends the packet to its local IP stack for processing. If the destination IPv4 address does not match one of these addresses, the eRouter determines the next-hop address of the destination in order to forward the packet. The next-hop can be another router or a client directly connected to either its Operator-Facing IP Interface, or back out its Customer-Facing IP Interface. The next-hop is determined by comparing the destination IPv4 address to the subnets assigned to the IP interface on which the eRouter is transmitting. If the destination IPv4 address matches a sub-net prefix, the destination is considered directly connected or "on-link", and the next-hop to use for ARP purposes is the destination IPv4 address. If it does not match, the destination is considered remote or "off-link", and the next-hop to use for ARP purposes is the address of the intermediate router. The typical scenario for packets routed to the Operator-Facing IP Interface is that the next-hop router will be the eRouter's default, learned via DHCP, Section 7.2, which will be the CMTS. Discovering other routers, aside from the CMTS (or routing delegate chosen by the DHCP server if the CMTS is a bridge) on the Operator-Facing IP Interface, is vendor-specific. Discovery of other directly connected devices on the Operator-Facing IP Interface is also vendor-specific. The typical scenario for packets routed back out the Customer-Facing IP Interface is that the next-hop is a local host on a different subnet than that of the source, but directly connected to the eRouter. If the eRouter cannot determine the next-hop of the IPv4 destination address, it MUST drop the packet.

Regardless of whether the packet was received from the Customer-Facing IP Interface or the Operator IP Interface, the eRouter MUST generate an appropriate ICMP error message as described in [RFC 792] to identify the reason for dropping an IPv4 datagram, except in the follow cases:

- The drop is due to congestion.

- The packet is itself an ICMPv4 error message.
- The packet is destined for an IPv4 broadcast or multicast address.
- The source IPv4 address of the packet is invalid as defined by [RFC 1812], section 5.3.7.
- The packet is a fragment and is not the first fragment (i.e., a packet for which the fragment offset in the IPv4 header is nonzero).
- The eRouter's IPv4 router sub-element MUST process and/or generate the following ICMPv4 messages when appropriate:

|    |                         |           |
|----|-------------------------|-----------|
| 0  | Echo Reply              | [RFC 792] |
| 3  | Destination Unreachable | [RFC 792] |
| 11 | Time Exceeded           | [RFC 792] |

**NOTE:** It is considered inappropriate for the eRouter's IPv4 router sub-element to generate ICMPv4 Destination Unreachable messages on the operator-facing interface.<sup>19</sup>

The eRouter MUST have at least one MAC address for its Operator-Facing IP Interface and one MAC address for its Customer-Facing IP Interface. The eRouter MUST share these source MAC addresses for IPv4 and IPv6. The eRouter MUST use the MAC address assigned to its Operator-Facing IP Interface as the source MAC address for all packets that it sends out its Operator-Facing IP Interface. The eRouter MUST use the MAC address assigned to the Customer-Facing IP Interface as the source MAC address for all packets that it sends out its Customer-Facing IP Interfaces.

The eRouter MUST forward broadcast packets received on either interface only to the eRouter's IP stack. The eRouter MUST NOT forward broadcast packets received on either interface to any interface other than the eRouter's IP stack.

## 9.4 NAPT

The eRouter MUST implement an NAPT function compliant with traditional Network Address Port Translation (NAPT) [RFC 3022], section 2.2. Per [RFC 3022], NAPT "is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports, are translated into a single network address and its TCP/UDP ports". Also, per [RFC 3022], the purpose of NAPT functionality is to "provide a mechanism to connect a realm with private addresses to an external realm, with globally unique registered addresses". The text in the NAPT sections below uses the term "public address(es)" to refer to the addresses reachable by the eRouter on its Operator-Facing IP Interface, assuming that they are globally-unique registered addresses. Note that an IP address that the eRouter views as globally unique, may be private to the operator's network. However, from the eRouter's perspective, these addresses are unique enough to ensure proper delivery to the next router upstream, and assumed to be globally unique.

Traditional NAPT is the simplest and most straightforward version of NAPT. Other versions that allow for mixtures of public and private network addresses on the Customer-Facing IP interface, or that allow users from the Operator-Facing IP Interface to establish translations to the Customer-Facing IP Interface, are not required by the eRouter and not discussed in this specification. Traditional NAPT requires that addresses used within the private network on Customer-Facing IP Interfaces cannot overlap with any public addresses reachable by the Operator-Facing IP Interface. Therefore, the eRouter MUST use any of the private IPv4 network addresses described in [RFC 1918] for its Customer-Facing IP interface. The

<sup>19</sup> Revised per eRouter-N-11.0991-1 on 5/6/11 by JB.

Customer-Facing IP Interface is considered to be a member of one private realm. A private realm is a single domain of private addresses. This means that an eRouter cannot connect to multiple private realms or private address domains.

The eRouter MAY advertise routes to destinations on the Operator-Facing IP Interface on the private network. The eRouter MUST NOT advertise routes to private destinations on the Customer-Facing IP Interface. Destinations on the Customer-Facing IP Interface MUST NOT be propagated onto the Operator-Facing IP Interface.

The eRouter MUST create NAPT translations dynamically based on receiving a packet from a private source on the Customer-Facing IP Interface attempting to access a public address on the Operator-Facing IP Interface, as described in Section 9.4.1.

For packets that traverse the NAPT function, the eRouter MUST always map a combination of private IPv4 address and port number to the same combination of public IPv4 address and port number. That is, the eRouter does not implement a symmetric Network Address Translation (NAT) as defined in [RFC 3489].

The eRouter MUST NOT create NAPT translations when public sources on the Operator-Facing IP Interface attempt to access private destinations on the Customer-Facing IP Interface. Connectivity between two devices that both live on the Customer-Facing IP Interface, but on different subnets, do not require NAPT translations, as they are required to be part of the same private realm. Therefore, the eRouter MUST NOT create NAPT translations to allow connectivity between CPEs that live on the Customer-Facing IP Interface.

In the following sections, the term Private Network Address Port (PNAP) refers to the network address and TCP/UDP port of a device on Customer-Facing IP interface that is using a private network address. The term Global Network Address Port (GNAP) refers to the network address and TCP/UDP port of that same device on Operator-Facing IP Interface after it has been translated by NAPT.

#### **9.4.1 Dynamically Triggered NAPT Translations**

Dynamically-triggered NAPT is invoked when a device on the Customer-Facing IP Interface with a private network address attempts to initiate one or more sessions to a public destination on the Operator-Facing IP Interface. In this case, the eRouter creates a mapping of source PNAP to GNAP and simultaneously creates a mapping of destination GNAP to PNAP for the return packets. The eRouter then replaces the source PNAP fields of the packet with its corresponding GNAP fields and forwards the packet out the Operator-Facing IP Interface. Once the external destination responds, the eRouter intercepts the reply and changes the previously inserted GNAP fields (now destination) back to the original PNAP values.

The eRouter MUST timeout dynamically-created NAPT translations to ensure that stale entries get removed. This timeout value MUST default to 300 seconds. This time value MAY be configurable. Other mechanisms can be used (like analyzing TCP session state) to time out the translations sooner, but the eRouter MUST still time out translations based on the timeout time in case the more advanced mechanism fails (e.g., because packet loss occurred and the eRouter did not see the final packets of a TCP flow).

### 9.4.2 Application Layer Gateways (ALGs)

Many applications are hampered by NAT for various reasons. A common problem is the appearance of IPv4 address and/or port information inside the application payload that is too deep into the packet to be manipulated by NAT, which operates at the network and transport layers. ALGs can be deployed to work around some of the problems encountered, but if the payload of such packets is secured, (by secure transport or application level security) the application cannot work. Another common reason NAT causes problems is when applications exchange address/port information to establish new connections, creating interdependencies that NAT cannot know about. The subsections following describe specific ALGs required by the eRouter.

#### 9.4.2.1 ICMP Error Message ALG

ICMP error messages are required for the well-known trace-route network debugging tool to work across the eRouter. This ALG is described in detail in [RFC 3022], section 4.3. The ICMP error message ALG **MUST** be implemented by the eRouter. Briefly stated, the eRouter **MUST** translate both the outer and inner IPv4 headers in the ICMP error message in order for the protocol to work correctly, when packets traverse through the NAT sub-element.

#### 9.4.2.2 FTP ALG

FTP is a fairly widely-used protocol, so the FTP ALG is one of the most important ALGs. The issue with FTP is that it uses the body of the control session packets to signal the data session parameters, including the new TCP ports, to use for the data session. Since NAT relies heavily on the TCP port field in order to translate between the private and public realm, this ALG is necessary to understand the new ports to be used by the ensuing data session. This ALG is described in detail in [RFC 3022], section 4.4. The FTP ALG **MUST** be implemented by the eRouter.

### 9.4.3 Multicast NAT

IPv4 Multicast packets are a special case for NAT and will need special handling at the eRouter. One scenario where forwarding of IP Multicast packets at the eRouter will need special handling is when a video source is using a private network address on a Customer-Facing IP Interface. In general, for video sources on the Customer-Facing IP Interface to work, the eRouter would be required to run at least one industry-standard multicast routing protocol to advertise the flows.

Since the eRouter will support IGMP proxy for IGMP v2 and v3, there is no reason to support a special translation for multicast packets in the eRouter for IGMP messages from private network addresses arriving on the Customer-Facing IP interface, as they will be consumed by the eRouter and new IGMP messages will be sent by the proxy agent from a public source network address on the Operator-Facing IP Interface.

## 9.5 ARP

The ARP function in the eRouter **MUST** be compliant with the following RFCs:

- An Ethernet Address Resolution Protocol [RFC 826].
- Requirements for IP Version 4 Routers [RFC 1812], section 3.3.2.
- Requirements for Internet Hosts [RFC 1122], section 2.3.2.

The ARP function in the eRouter is limited to IPv4 network addresses (pln= 4) and Ethernet hardware addresses (hln=6). When the eRouter needs to forward an IPv4 packet to a given IP address on either the Operator-Facing IP Interface or the Customer-Facing IP Interface, it consults a table of IPv4 network addresses that each map to Ethernet addresses. If the corresponding IPv4 network address is found in the table, its corresponding Ethernet address **MUST** be used as the Ethernet destination address of the packet. If the corresponding IPv4 network address is not found, the eRouter **MUST** start the ARP protocol in hopes that it will learn the IPv4 network address to Ethernet address association. The eRouter **MUST** use its own MAC address, as described in Section 9.3, as the source MAC address and source hardware address of all ARP packets.

The eRouter creates ARP translations, dynamically based on the eRouter, receiving an ARP reply destined for one of the eRouter's IPv4 network addresses. The eRouter also creates ARP translations, dynamically based on the eRouter, receiving an ARP request destined for one of the eRouter's IPv4 network addresses.

ARP entries maintained by the eRouter need careful examination before being aged. Both voice and video present humanly noticeable negative affects when ARP entries are removed in the middle of a session. [RFC 1122] suggests several different ways to age ARP entries in section 2.3.2.1. The eRouter **SHOULD** use option 2 – "Unicast polling", which allows for the ARP entry to stay fresh and in the ARP table as long as possible. This option is well-suited for routers that expect to have fairly small ARP tables and want long-term uninterrupted connectivity.

## 9.6 IPv4 Multicast

The eRouter learns IP multicast group membership information received on the Customer-Facing Interfaces and proxies it on the Operator-Facing Interface towards the next upstream multicast router. The eRouter forwards IPv4 multicast packets downstream based on the information learned at each Customer-Facing Interface.

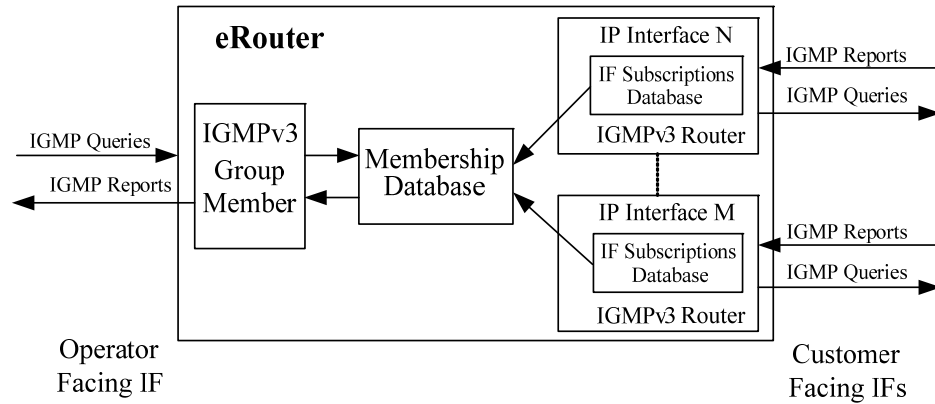
The eRouter proxies IGMP information upstream actively by implementing mutually-independent IGMPv3 router functionality on Customer-Facing Interfaces, and IGMPv3 group member functionality on the Operator-Facing Interface. On each IP interface, and independently of other IP interfaces, the eRouter generates, terminates, and processes IGMP messages according to IGMPv3 requirements. For example, the version of IGMP used on the cable network or the local area network will be defined locally at each network. The eRouter may send IGMPv2 reports on the Operator-Facing Interface while generating IGMPv3 queries on Customer-Facing Interfaces.<sup>20</sup>

The following elements define the eRouter IPv4 multicast behavior (also shown in Figure 9-2):

- An IGMPv3 Group Member that implements the group member part of IGMPv3[RFC 3376] on the Operator-Facing Interface.
- An IGMPv3 Router that implements the router portion of IGMPv3 [RFC 3376] on each Customer-Facing Interface.
- A subscription database per Customer-Facing Interface with multicast reception state of connected CPEs.
- An IPv4 Group Membership Database that merges subscription information from all the Customer-Facing Interfaces.

---

<sup>20</sup> Sentence modified by eRouter-N-06.0352-1 by kb 2/2/07.



**Figure 9-2 - eRouter IPv4 Multicast Forwarding Block Diagram**

Central to the operation of the IGMPv3 Router(s) and IGMPv3 Group Member is the IPv4 Group Membership Database, through which the IGMPv3 Router(s) and IGMPv3 Group Member indirectly relate. This database condenses multicast reception state collected by the IGMPv3 Router(s) from connected CPEs. This information is used by the IGMPv3 Group Member on the Operator-Facing Interface as its own multicast reception interface state.

### 9.6.1 IGMP Proxying

The eRouter maintains the multicast reception state of CPEs on each Customer-Facing Interface in the interface's multicast subscription database. The eRouter obtains multicast reception state information of CPEs through the implementation of an IGMPv3 Router on each Customer-Facing Interface. Multicast reception state arrives at the eRouter in the form of IGMP Report messages transmitted by CPEs. The eRouter MUST implement the router portion of IGMPv3 [RFC 3376] on each Customer-Facing Interface. The eRouter MUST maintain, for each Customer-Facing Interface, the IPv4 multicast reception state of connected CPEs.

In the event of multiple queriers on one subnet, IGMPv3 elects a single querier-based on the querier IP address. However, the querier election rules defined for IGMPv3 do not apply to the eRouter. The eRouter MUST always act as an IGMP querier on its Customer-Facing Interfaces.

On the Operator-Facing Interface, the eRouter MUST implement the group member portion of IGMPv3 [RFC 3376]. The eRouter MUST merge the multicast reception state of connected CPEs into an IPv4 group membership database as described in Section 9.6.1.1. The eRouter MUST use the IPv4 group membership database as multicast reception interface state per [RFC 3376], section 3.2, on the Operator-Facing Interface. Thus, when the composition of the group membership database changes, the eRouter reports the change with an unsolicited report sent on the Operator-Facing Interface. When queried by an upstream multicast router, the eRouter also responds with information from the group membership database.

The eRouter MUST NOT perform the router portion of IGMPv3 on the Operator-Facing Interface.

### 9.6.1.1 IPv4 Group Membership Database

The eRouter's Membership Database is formed by merging the multicast reception state records of Customer-Facing Interfaces. In compliance with [RFC 3376], the eRouter keeps per Customer-Facing Interface and per multicast address joined one record of the form:

(multicast address, group timer, filter-mode, (source records))

With source records of the form:

(source address, source timer)

The eRouter keeps an IPv4 Group Membership Database with records of the form:

(multicast-address, filter-mode, source-list)

The eRouter uses the IPv4 Group Membership Database records as the interface state for the IGMPv3 Group Member implementation on the Operator-Facing Interface. Each record of the IPv4 Group Membership Database is the result of merging all subscriptions for that record's multicast-address on Customer-Facing Interfaces. For each IPv4 multicast group joined on any Customer-Facing Interface, the eRouter MUST abide by the following process to merge all customer interface records for the group, into one Group Membership Database record:

- First, the eRouter pre-processes all customer interface group records by:
  - Converting IGMPv1 and IGMPv2 records into IGMPv3 records.
  - Removing group and source timers from IGMPv3 and converted records.
  - Removing every source whose source timer is greater than zero from records with a filter mode value of EXCLUDE.
- Then the eRouter creates an IPv4 Group Membership Database record by merging the pre-processed records, using the merging rules for multiple memberships on a single interface specified in section 3.2 of the IGMPv3 specification [RFC 3376].

### 9.6.2 IPv4 Multicast Forwarding

The forwarding of IPv4 multicast packets received on any interface onto a Customer-Facing Interface is determined by the known multicast reception state of the CPEs connected to the Customer-Facing Interface. The eRouter MUST replicate an IPv4 multicast session on a Customer-Facing Interface, if at least one CPE device connected to the interface has joined the session. The eRouter MUST NOT replicate an IPv4 multicast session on a Customer-Facing Interface, if no CPE device connected to the interface has joined the session.

The eRouter MUST NOT forward IPv4 multicast packets received on any interface, i.e., any Customer-Facing or the Operator-Facing Interface, back to the same interface.



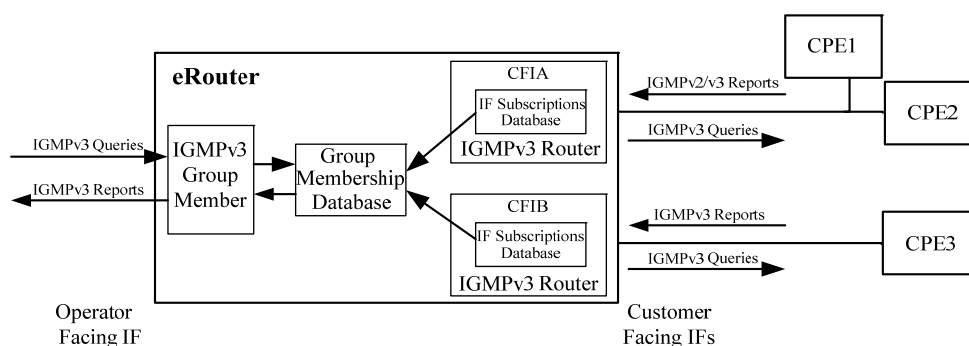
The eRouter MUST NOT forward IGMP messages received on any IP interface onto another IP interface. Except for IGMP packets, the eRouter MUST forward all IPv4 multicast traffic received on Customer-Facing Interfaces onto the Operator-Facing Interface. Operator control of multicast traffic forwarding onto the cable network, if desired, can be done through the implementation of filters at the eCM.

### 9.6.3 IPv4 Multicast Forwarding Example

The eRouter in this example has two Customer-Facing Interfaces; CFIA, and CFIB, connected to one LAN segment each. On CFIA, there are two CPEs connected; CPE1 and CPE2. CPE1 is IGMPv2 capable and will attempt to join group 224.0.100.1. CPE2 is IGMPv3 capable and will attempt to join group 224.128.100.1 from all sources. On CFIB, there is one CPE connected, CPE3, which is IGMPv3 capable and that will attempt to join group 224.128.100.1, except from source 198.200.200.200.

The router upstream of the eRouter (e.g., the CMTS) supports and is configured to operate in IGMPv3 mode, and thus the eRouter works in IGMPv3 mode on the Operator-Facing Interface.<sup>21</sup>

The setup is shown in Figure 9-3:



**Figure 9-3 - IPv4 Multicast Forwarding Example<sup>22</sup>**

The CPEs send reports as follows:<sup>23</sup>

| Report From | Report Version | Multicast Address | Record Type | Source Address  |
|-------------|----------------|-------------------|-------------|-----------------|
| CPE1        | IGMPv2         | 224.0.100.1       | N/A         | N/A             |
| CPE2        | IGMPv3         | 224.128.100.1     | EXCLUDE     | Null            |
| CPE3        | IGMPv3         | 224.128.100.1     | EXCLUDE     | 198.200.200.200 |

Because CPE1 sends an IGMPv2 report for group 224.0.100.1, CFIA operates in IGMPv2 compatibility mode for this group. On the other hand, CFIA and CFIB operate in IGMPv3 mode for group 224.128.100.1, because they receive IGMPv3 reports for this group from CPE2 and CPE3, respectively. The eRouter multicast reception state at each Customer-Facing Interface is the following:<sup>24</sup>

<sup>21</sup> Paragraph added per eRouter-N-06.0352-1 by kb 2/2/07.

<sup>22</sup> Figure revised per eRouter-N-06.0352-1 by kb 2/2/07.

<sup>23</sup> This paragraph and table below modified per eRouter-N-06.0352-1 by kb 2/2/07.

<sup>24</sup> This paragraph and table below modified per eRouter-N-06.0352-1 by kb 2/2/07.

| Interface | Multicast Address | Group Timer | Filter-Mode | Source Address  | Source Timer |
|-----------|-------------------|-------------|-------------|-----------------|--------------|
| CFIA      | 224.0.100.1       | A           | EXCLUDE     | Null            | 0            |
| CFIA      | 224.128.100.1     | B           | EXCLUDE     | Null            | 0            |
| CFIB      | 224.128.100.1     | C           | EXCLUDE     | 198.200.200.200 | 0            |

The interface state at the eRouter's Operator-Facing Interface, stored in the Group Membership Database, is the following:

| Multicast Address | Filter-Mode | Source Address |
|-------------------|-------------|----------------|
| 224.0.100.1       | EXCLUDE     | Null           |
| 224.128.100.1     | EXCLUDE     | Null           |

The eRouter uses the information in the table above as multicast reception state at the Operator-Facing Interface. For example, in response to an IGMPv3 general query, the eRouter sends an IGMPv3 report for the two records shown.

Assuming that the CMTS is transmitting downstream four multicast streams, the eRouter forwards them as follows:<sup>25</sup>

| Stream # | Multicast Address | Source Address  | eRouter forwards on interfaces |      |
|----------|-------------------|-----------------|--------------------------------|------|
|          |                   |                 | CFIA                           | CFIB |
| 1        | 224.0.200.2       | 198.100.100.100 | NO                             | NO   |
| 2        | 224.0.100.1       | 198.100.100.100 | YES                            | NO   |
| 3        | 224.128.100.1     | 198.100.100.100 | YES                            | YES  |
| 4        | 224.128.100.1     | 198.200.200.200 | YES                            | NO   |

## 9.7 Dual-Stack Lite Operation<sup>26</sup>

Even as operators migrate customers from IPv4 to IPv6 addressing, a significant percentage of Internet resources and content will remain accessible only through IPv4. As a consequence of the slow transition to IPv6 on the part of content providers, operators require mechanisms to allow customers to continue to access content and resources using IPv4 even after the last IPv4 allocations have been fully depleted. This necessitates multiplexing several customers behind a single IPv4 address. One technology that satisfies operator requirements for IPv4 address extension is dual-stack lite.

Dual-stack lite enables an operator to share IPv4 addresses among multiple customers by combining two well-known technologies: IP in IP (IPv4-in-IPv6) tunneling and NAT. More specifically, dual-stack lite encapsulates IPv4 traffic inside an IPv6 tunnel and sends it to an operator NAT device.

To facilitate IPv4 extension over an IPv6 network, the eRouter MAY implement dual-stack lite B4 (client) functionality, as specified in section 5 of [RFC 6333]. When dual-stack lite is enabled, the eRouter acquires an IPv6 address on its Operator-Facing Interface and learns the address of the operator

<sup>25</sup> Table below modified per eRouter-N-06.0352-1 by kb 2/2/07.

<sup>26</sup> Section added per eRouter-N-09.0877-2 on 5/11/10 by JB. Revised per eRouter-N-11.1015-2 on 11/4/11 by JB.

NAT device via DHCPv6. It encapsulates IPv4 traffic inside IPv6 sourced from its Operator-Facing Interface and destined for the operator NAT device.

## 10 IPV6 DATA FORWARDING

The normative requirements of this section are mandatory for an eRouter that implements the IPv6 Protocol Enabled Mode and/or the Dual IP Protocol Enabled Mode, as defined in Section 6.

### Assumptions

- There is only a single Operator-Facing IP Interface on the eRouter.
- There is typically a single Customer-Facing IP Interface on the eRouter.
- The Operator-Facing IP Interface is Ethernet encapsulated.
- The Customer-Facing IP Interface is Ethernet encapsulated.
- The eRouter advertises itself as a router (using ND) on both the Operator-Facing and Customer-Facing Interfaces so clients and routers on either interface learn about the eRouter.
- All the eRouters are on separate links and therefore will not see each other's RAs.

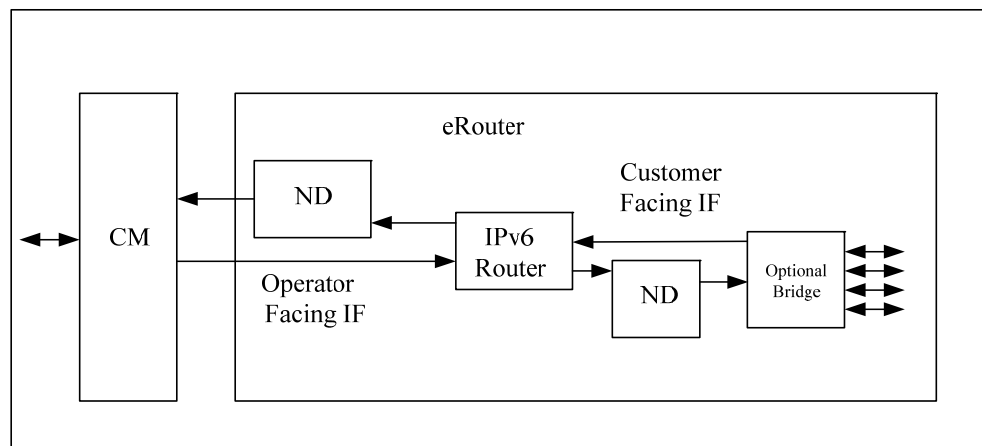
### 10.1 Overview

The IPv6 eRouter is responsible for implementing IPv6 routing. This includes looking up the IPv6 Destination address to decide which of the eRouter interfaces to send the packet.

The ND protocol is required on the eRouter. Like ARP in IPv4, it provides a mechanism for converting IPv6 network addresses to Ethernet MAC addresses on both the Customer-Facing IP interfaces and the Operator-Facing IP Interface. It also provides a mechanism for the eRouter to advertise its presence, host configuration parameters, routes, and on-link preferences.

Figure 10-1 shows a block diagram of the IPv6 eRouter with an IPv6 Router block and an ND block. The IPv6 functionality, however, does not have the clean separation indicated by these blocks. The IPv6 Routing and Neighbor Discovery blocks are closely intertwined and, therefore, are discussed together under the same subsection.

The IPv6 eRouter uses a local IPv6 routing table to forward packets. The eRouter creates the IPv6 routing table upon initialization of the IPv6 portion of the eRouter and adds entries according to the receipt of Router Advertisement messages containing on-link prefixes and routes.



**Figure 10-1 - eRouter IPv6 Forwarding Block Diagram**

## 10.2 System Description <sup>27</sup>

Except when noted, the ND function in the eRouter MUST comply with the Neighbor Discovery for IPv6 [RFC 2461]. Per [RFC 4861], ND is used "to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid."

Several sections of [RFC 4861] do not apply to the eRouter. These sections include:

- section 6.2.7 - RA Consistency
- section 6.2.8 - Link-local Address Change
- section 7.2.8 - Proxy Neighbor Advertisements
- section 8 - Redirect Function
- section 11 - Security Considerations
- section 12 - Renumbering Considerations

The eRouter MUST support the following ND messages per [RFC 4861]: Router Solicitation, Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement.

The eRouter receives a packet and checks the destination address of the packet. If the destination IPv6 address matches the address assigned to the eRouter's IP interface, the eRouter forwards the packet to its local IP stack for processing. If the destination IPv6 address does not match the eRouter's address, the eRouter determines the next-hop address of the destination in order to forward the packet. The next-hop can be a router, or the destination itself. The next-hop is determined by comparing the destination IPv6 address to the subnets assigned to the IP interface on which the eRouter is transmitting out. If the destination IPv6 address matches a sub-net prefix, the destination is considered directly connected or "on-link", and the next-hop to use for ND purposes is the destination IPv6 address. If it does not match, the destination is considered remote or "off-link", and the next-hop to use for ND purposes is the address of the intermediate router.

The typical scenario for packets routed to the Operator-Facing IP Interface is that the next-hop router will be the eRouter's default, learned via Router Advertisement [RFC 3315], from the CMTS. Discovering other routers, aside from the CMTS (or routing delegate chosen if the CMTS is a bridge), on the Operator-Facing IP Interface is vendor-specific. Discovery of other directly-connected devices on the Operator-Facing IP Interface is also vendor-specific. The typical scenario for packets routed back out the Customer-Facing IP Interface is that the next-hop is a local host on a different subnet than that of the source, but directly connected to the eRouter. If the eRouter cannot determine the next-hop of the IPv6 destination address, then it MUST drop the packet.

Once a next-hop is determined, the eRouter's Neighbor Cache is consulted for the link-layer address of the next-hop address. If necessary, address resolution is performed. Address resolution is accomplished by multicasting a Neighbor Solicitation that prompts the addressed neighbor to return its link-layer address in a Neighbor Advertisement. The neighbor cache entry is then updated with this link-layer address, and the eRouter then forwards the packet to the link-layer address contained in this cache entry.

<sup>27</sup> Revised per eRouter-N-09.0877-2 on 5/11/10 and per eRouter N-11.1015-2 on 11/4/11 by JB.

If an error occurs at any point in the process, the eRouter discards the packet. Regardless of whether the packet was received from the Customer-Facing IP Interface or the Operator IP Interface, the eRouter **MUST** generate an appropriate ICMP error message, as described in [RFC 4884], to identify the reason for dropping an IPv6 datagram, except in the follow cases:

- The drop is due to congestion.
- The packet is itself an ICMPv6 error message.
- The packet is destined for an IPv6 multicast address (except if the packet is the "Packet Too Big Message" or the "Parameter Problem Message", as explained in [RFC 4884], section 2.4, paragraph (e)).
- The packet is destined for a link-layer broadcast address, except as noted above.
- The packet is destined for a link-layer multicast address, except as noted above.
- The source IPv6 address of the packet does not uniquely identify a single node, as explained in detail in [RFC 4884], section 2.4, paragraph (e).
- The eRouter **MUST** process and/or generate the following ICMPv6 messages when appropriate:

|     |                                     |            |
|-----|-------------------------------------|------------|
| 1   | Destination Unreachable             | [RFC 2463] |
| 3   | Time Exceeded                       | [RFC 2463] |
| 129 | Echo Reply                          | [RFC 2463] |
| 130 | Multicast Listener Query            | [RFC 3810] |
| 131 | Multicast Listener Report           | [RFC 3810] |
| 132 | Multicast Listener Done             | [RFC 3810] |
| 133 | Router Solicitation                 | [RFC 4861] |
| 134 | Router Advertisement                | [RFC 4861] |
| 135 | Neighbor Solicitation               | [RFC 4861] |
| 136 | Neighbor Advertisement              | [RFC 4861] |
| 143 | Version 2 Multicast Listener Report | [RFC 3810] |

**NOTE:** It is considered inappropriate for the eRouter to generate ICMPv6 Destination Unreachable messages on the operator-facing interface.<sup>28</sup>

The eRouter is responsible for decrementing the Hop Limit field in the IPv6 packet that it is going to forward. If the eRouter receives an IPv6 packet with a Hop Limit of zero, or the eRouter decrements an IPv6 packet's Hop Limit to zero, it **MUST** discard that packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of that IPv6 packet.

The eRouter is also responsible for reinserting the Ethernet header of IPv6 packets. The eRouter has at least one MAC address for its Operator-Facing IP Interface and one MAC address for its Customer-Facing IP Interface that are shared for IPv4 and IPv6 (see Section 8.3). The eRouter **MUST** use the MAC address assigned to its Operator-Facing IP Interface as the source MAC address for all IPv6 packets that it sends out its Operator-Facing IP Interface. The eRouter **MUST** use the MAC address assigned to the Customer-Facing IP Interface as the source MAC address for all IPv6 packets that it sends out its Customer-Facing IP Interfaces. Per [RFC 4861], the eRouter uses the MAC address of the next-hop address learned via Neighbor Discovery as the destination MAC address for the IPv6 packet.

<sup>28</sup> Revised per eRouter-N-11.0991-1 on 5/6/11 by JB.

The eRouter MUST forward link-local multicast packets received on either interface only to the eRouter's IP stack. The eRouter MUST NOT forward link-local multicast packets received on either interface to any interface other than the eRouter's IP stack.

### 10.3 IPv6 Multicast

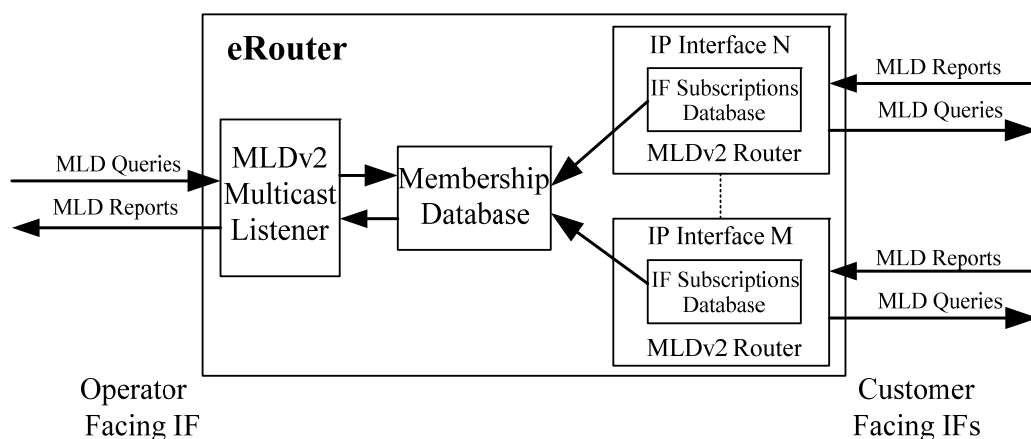
The eRouter learns IP multicast group membership information received on the Customer-Facing Interfaces and proxies it on the Operator-Facing Interface towards the next upstream multicast router. The eRouter forwards IPv6 multicast packets downstream based upon the information learned at each Customer-Facing Interface.

The eRouter proxies MLD information upstream actively by implementing mutually-independent MLDv2 router functionality on Customer-Facing Interfaces and MLDv2 multicast listener functionality on the Operator-Facing Interface. On each IP interface, and independently of other IP interfaces, the eRouter generates, terminates, and processes MLD messages according to MLDv2 requirements. For example, the version of MLD used on the cable network or the local area network will be defined locally at each network. The eRouter may send MLDv1 reports on the Operator-Facing Interface while generating MLDv2 queries on Customer-Facing Interfaces.<sup>29</sup>

The following elements define the eRouter IPv6 multicast behavior (also shown in Figure 10-2):

- An MLDv2 Multicast Listener that implements the multicast listener part of MLDv2 [RFC 3810] on the Operator-Facing Interface;
- An MLDv2 Router that implements the router part of MLDv2 [RFC 3810] on each Customer-Facing Interface;
- A Subscription Database per Customer-Facing Interface with multicast reception state of connected CPEs;
- An IPv6 Group Membership Database that merges subscription information from all the Customer-Facing Interfaces.

These logical sub-elements are shown in Figure 10-2.



**Figure 10-2 - eRouter IPv6 Multicast Forwarding Block Diagram**

<sup>29</sup> Sentence modified per eRouter-N-06.0352-1 by kb 2/2/07.

### 10.3.1 MLD Proxying

The eRouter maintains the multicast reception state of CPEs on each Customer-Facing Interface in the interface's multicast subscription database. The eRouter obtains CPE's multicast reception state information through the implementation of an MLDv2 Router on each Customer-Facing interface. Multicast reception state arrives at the eRouter in the form of MLD Report messages transmitted by CPEs. The eRouter **MUST** implement the router portion of the MLDv2 protocol, [RFC 3810], on each Customer-Facing Interface. The eRouter **MUST** maintain, for each Customer-Facing Interface, the IPv6 multicast reception state of connected CPEs.

In the event of multiple queriers on one subnet, MLDv2 elects a single querier based on the querier IP address. However, the querier election rules defined for MLDv2 do not apply to the eRouter. The eRouter **MUST** always act as an MLD querier on its Customer-Facing Interfaces.

On the Operator-Facing Interface, the eRouter **MUST** implement the multicast listener portion of the MLDv2 protocol, [RFC 3810]. The eRouter **MUST** merge the multicast reception state of connected CPEs into an IPv6 group membership database, as described in Section 10.3.2, IPv6 Group Membership Database. The eRouter **MUST** use the membership database as multicast reception interface state per [RFC 3810], section 4.2, for the Operator-Facing Interface. Thus, when the composition of the IPv6 multicast membership database changes, the eRouter reports the change with an unsolicited report sent on the Operator-Facing Interface. When queried by an upstream multicast router, the eRouter also responds with information from the membership database.

The eRouter **MUST NOT** perform the router portion of MLDv2 on the Operator-Facing Interface.

### 10.3.2 IPv6 Group Membership Database

The eRouter's Membership Database is formed by merging the multicast reception state records of Customer-Facing Interfaces. In compliance with [RFC 3810], the eRouter keeps per Customer-Facing Interface and per multicast address joined one record of the form:

(multicast address, group timer, filter-mode, (source records))

With source records of the form:

(source address, source timer)

The eRouter keeps an IPv6 Group Membership Database with records of the form:

(multicast-address, filter-mode, source-list)

The eRouter uses the IPv6 Group Membership Database records as interface state for the MLDv2 Multicast Listener implementation on the Operator-Facing Interface. Each record of the IPv6 Group Membership Database is the result of merging all subscriptions for that record's IPv6 multicast-address on Customer-Facing Interfaces. For each IPv6 multicast group joined on any Customer-Facing Interface, the eRouter **MUST** abide by the following process to merge all customer interface records for the group into one Group Membership Database record:

- First, the eRouter pre-processes all customer interface group records by:
  - Converting MLDv1 records into MLDv2 records.
  - Removing group and source timers from MLDv2 and converted records.



Removing every source whose source timer is greater than zero from records with a filter mode value of EXCLUDE.

- Then the eRouter creates an IPv6 Group Membership Database record by merging the pre-processed records, using the merging rules for multiple memberships on a single interface specified in section 4.2 of the MLDv2 specification [RFC 3810].

### 10.3.3 IPv6 Multicast Forwarding

The forwarding of IPv6 multicast packets received on any interface onto a Customer-Facing Interface is determined by the known multicast reception state of the CPEs connected to the Customer-Facing Interface. The eRouter **MUST** replicate an IPv6 multicast session on a Customer-Facing Interface if at least one CPE device connected to the interface has joined the session. The eRouter **MUST NOT** replicate an IPv6 multicast session on a Customer-Facing Interface if no CPE device connected to the interface has joined the session.

The eRouter **MUST NOT** forward IPv6 multicast packets received on any interface, i.e., any Customer-Facing or the Operator-Facing Interface, back to the same interface.

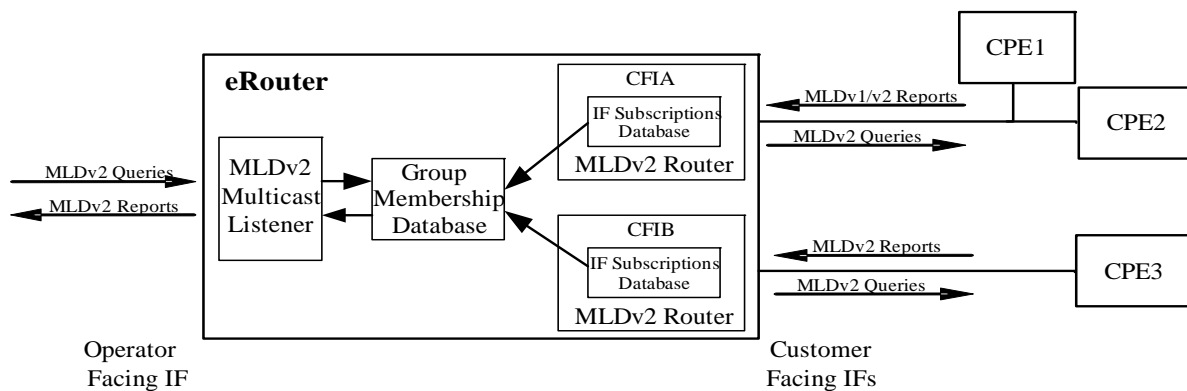
In compliance with IPv6 link-scope packet forwarding rules, the eRouter **MUST NOT** forward MLD messages received on an IP interface onto another IP interface. Also, the eRouter **MUST NOT** forward link-scoped IPv6 multicast packets received on an IP interface onto another IP interface. The eRouter **MUST** forward all non-link-scoped IPv6 multicast traffic received on Customer-Facing Interfaces onto the Operator-Facing Interface. Operator control of multicast traffic forwarding onto the cable network, if desired, can be done through the implementation of filters at the eCM.

### 10.3.4 IPv6 Multicast Forwarding Example

The eRouter in this example has two Customer-Facing Interfaces; CFIA and CFIB, connected to one LAN segment each. On CFIA, there are two CPEs connected; CPE1 and CPE2. CPE1 is MLDv1-capable and will attempt to join group FF1E::100. CPE2 is MLDv2-capable and will attempt to join group FF1E::128 from all sources. On CFIB, there is one CPE connected, CPE3, which is MLDv2 capable and that will attempt to join group FF1E::128, except from source 3FFE:2900::200.

The router upstream of the eRouter (e.g., the CMTS) supports and is configured to operate in MLDv2 mode, and thus the eRouter works in MLDv2 mode on the Operator-Facing Interface.

The setup is shown in Figure 10-3:



**Figure 10-3 - IPv6 Multicast Forwarding Example<sup>30</sup>**

The CPEs send reports as follows:<sup>31</sup>

| Report From | Report Version | Multicast Address | Record Type | Source Address |
|-------------|----------------|-------------------|-------------|----------------|
| CPE1        | MLDv1          | FF1E::100         | N/A         | N/A            |
| CPE2        | MLDv2          | FF1E::128         | EXCLUDE     | Null           |
| CPE3        | MLDv2          | FF1E::128         | EXCLUDE     | 3FFE:2900::200 |

Because CPE1 sends an MLDv1 report for group FF1E::100, CFIA operates in MLDv1 compatibility mode for this group. On the other hand, CFIA and CFIB operate in MLDv2 mode for group FF1E::128, because they receive MLDv2 reports for this group from CPE2 and CPE3, respectively. The eRouter multicast reception state at each Customer-Facing Interface is the following:<sup>32</sup>

| Interface | Multicast Address | Group Timer | Filter-Mode | Source Address | Source Timer |
|-----------|-------------------|-------------|-------------|----------------|--------------|
| CFIA      | FF1E::100         | A           | EXCLUDE     | Null           | 0            |
| CFIA      | FF1E::128         | B           | EXCLUDE     | Null           | 0            |
| CFIB      | FF1E::128         | C           | EXCLUDE     | 3FFE:2900::200 | 0            |

The eRouter merges the multicast reception state of connected CPEs shown above into the Group Membership Database as follows:

| Multicast Address | Filter-Mode | Source Address |
|-------------------|-------------|----------------|
| FF1E::100         | EXCLUDE     | Null           |
| FF1E::128         | EXCLUDE     | Null           |

The eRouter uses the information in the Group Membership Database as multicast reception state at the Operator-Facing Interface. For example, in response to an MLDv2 general query, the eRouter sends an MLDv2 report for the two records shown.

<sup>30</sup> Figure modified per eRouter-N-06.0352-1 by kb 2/2/07.

<sup>31</sup> This paragraph and table below modified per eRouter-N-06.0352-1 by kb 2/2/07.

<sup>32</sup> This paragraph and table below modified per eRouter-N-06.0352-1 by kb 2/2/07.

Assuming that the CMTS is transmitting four multicast streams downstream, the eRouter forwards them as follows:<sup>33</sup>

| Stream # | Multicast Address | Source Address | eRouter forwards on interfaces |      |
|----------|-------------------|----------------|--------------------------------|------|
|          |                   |                | CFIA                           | CFIB |
| 1        | FF1E::200         | 3FFE:2900::100 | NO                             | NO   |
| 2        | FF1E::100         | 3FFE:2900::100 | YES                            | NO   |
| 3        | FF1E::128         | 3FFE:2900::100 | YES                            | YES  |
| 4        | FF1E::128         | 3FFE:2900::200 | YES                            | NO   |

<sup>33</sup> Table below modified per eRouter-N-06.0352-1 by kb 2/2/07.

## 11 QUALITY OF SERVICE

QoS on the eRouter is optional. The eRouter **SHOULD** support Layer 2 and Layer 3 QoS, as defined in this section. The QoS functionality described herein allows the operator to selectively provide a level of differentiation among the various data streams destined for CPE behind the eRouter. Typical applications could include Internet Protocol Television services (IPTV) and other enhanced data services, though it is anticipated that overall packet counts will still be dominated by largely undifferentiated best-effort data traffic.

Because Layer 2 (e.g., 802.1 p/Q Ethernet) headers will be stripped off as packets traverse the eRouter, the eRouter **MUST** prioritize the forwarding of IP packets based on the values marked in the IPv4 ToS byte or IPv6 Traffic Class field.

### 11.1 Downstream Quality of Service Operation

This section deals with the requirements regarding traffic going to CPEs, through the eRouter, from the Cable network.

The eRouter **MUST** provide two or more priority queues on each Customer-Facing Interface for traffic going to CPEs. The eRouter **MAY** provide a configuration mechanism to map ToS/Traffic Class field priority values to the high- and low-priority queues. As a default setting, the eRouter might use the most significant bit of the ToS/Traffic Class field to determine priority to queue mappings.

### 11.2 Upstream Quality of Service Operation

This section deals with traffic coming from the CPEs attached to the eRouter to the cable network.

For the purposes of QoS of upstream traffic from CPE devices, the interface between the eRouter and the embedded CM must be considered to be of infinite bandwidth, and thus no congestion should be expected to occur on this interface. Thus, the eRouter does not need to provide any queues in the upstream direction. The eRouter **MAY** provide a configuration mechanism to determine whether the eRouter allows CPE devices to pass QoS-tagged packets with the IP ToS/Traffic Class field intact, or whether the eRouter resets the IP ToS/Traffic Class field to 0. The eRouter **MAY** use the IP ToS/Traffic Class field to populate Layer 2 QoS headers to ensure upstream QoS treatment. Although other implementations are possible, one such implementation is to directly map the three most significant bits of the IP ToS/Traffic Class field into the 802.1Q priority field.

In the case where multiple Customer-Facing Interfaces are implemented, the eRouter may support additional QoS mechanisms to prioritize upstream traffic based on ingress interface.

## 12 EROUTER MANAGEMENT<sup>34</sup>

The eRouter allows the implementation of different management interfaces as described in this section. Management interfaces in this specification refer to the protocols, data models, and semantic representation of the data exchange to perform the conventional management functions in the device.

The eRouter **MUST** support either SNMP [RFC 3412] or TR-069 [TR-069a4] from the Operator-Facing management interface.

The eRouter is not required to support both management interfaces simultaneously for a given system boot instance.

User management from the Customer-Facing interface is vendor specific. Remote management of the eRouter (from the Operator-Facing interface) by the customer is outside of the scope of this specification.

Other specifications referring to the eRouter specification might add requirements to the eRouter management interface for additional functionality.

### 12.1 eRouter SNMP Management Interface Requirements

The eRouter SNMP Management Interface requirements are listed in Annex A and Annex B. Annex A lists the management objects requirements for the eRouter to support. Annex B, sections B.1, B.3.4, and B.3.5 provide the provisioning elements to secure the SNMP access control by SNMP entities.

If SNMP is supported from the Operator-Facing Interface, the eRouter **MAY** support SNMP [RFC 3412] from the Customer-Facing Interface.

### 12.2 eRouter TR-069 Management Interface Requirements

The eRouter TR-069 Management Interface requirements are listed in Annex C.

If TR-069 is supported from the Operator-Facing Interface, the eRouter **MAY** support [RFC 3412] for Customer-Facing Interface management.

#### 12.2.1 ACS Discovery

The eRouter performs initial ACS discovery via the mechanisms in the following sections:

##### 12.2.1.1 eRouter TR-069 Management Server Configuration File TLV Encapsulation.

The eRouter **MUST** support the TR-069 Management Server Configuration File TLV Encapsulation as defined in Annex B.3.3.2 for ACS selection.

##### 12.2.1.2 TR-069 Management Server URL DHCP Option

The eRouter **MAY** support the DHCPv4 option CL\_V4OPTION\_TR-069\_MANAGEMENT\_SERVER\_URL, and DHCPv6 option CL\_OPTION\_TR-069\_MANAGEMENT\_SERVER\_URL [CANN DHCP] for the ACS selection as part of the eRouter

---

<sup>34</sup> Section added per eRouter N-11.1014-3 on 10/27/11 by JB.

DHCP ACK and/or REPLY messages. The eRouter MUST follow the DHCP requirements in [TR-069a4] for the initial ACS discovery with the exception of using the CableLabs-defined DHCP options.

### 12.2.2 ACS Selection

If the TR-069 Management Server URL is present in only one of TR-069 Management Server Configuration File TLV Encapsulation or TR-069 Management Server URL DHCP Option, the eRouter MUST use the present URL as the initial ACS URL. If the TR-069 Management Server URL is present in both TR-069 Management Server Configuration File TLV Encapsulation and TR-069 Management Server URL DHCP Option, the eRouter MUST use the former as the ACS URL. If the TR-069 Management Server URL is present in neither the CM configuration file nor the DHCP Offer/Response, the eRouter MUST NOT communicate with any ACS.

### 12.2.3 Dynamic ACS Updates

After the initial discovery, the ACS URL can be changed by updating the Device.ManagementServer.URL attribute value. The eRouter MUST ignore the ACS URL if it is present in DHCP renew/rebind messages.

### 12.2.4 TR-069 CWMP Control and Credentials

The TR-069 Device.ManagementServer object defines controls for CWMP operations and credentials for authentication of connection requests between the CPE and ACS. All TR-069 Device.ManagementServer objects can be configured by the ACS via [TR-069a4] procedures.

In addition, the parameter Device.ManagementServer.URL can be delivered via DHCP or Configuration File TLV, as specified in Section 12.2.2.

For security reasons, the TR-069 Device.ManagementServer object credential attributes (Username, Password, ConnectionRequestUsername and ConnectionRequestPassword) are also configurable via the TR-069 Management Server Configuration File TLV Encapsulation (see Annex B.3.3).

To prevent dead-lock situations that would require user interventions, the Device.ManagementServer.EnableWCMP is also configurable via the TR-069 Management Server Configuration File TLV Encapsulation (see Annex B.3.3.1).

## 13 SECURITY <sup>35</sup>

It is considered a best practice to filter obviously malicious traffic (e.g., spoofed packets, "Martian" addresses, etc.). Thus, the eRouter ought to support basic stateless egress and ingress filters. The eRouter is also expected to offer mechanisms to filter traffic entering the customer network; however, the method by which vendors implement configurable packet filtering is beyond the scope of this document.

The eRouter **MUST** enable [RFC 6092] stateful firewall by default. In particular, the eRouter **SHOULD** support functionality sufficient for implementing the set of recommendations in [RFC 6092], section 4. The eRouter **MUST** support ingress filtering in accordance with BCP 38 [RFC 2827].

---

<sup>35</sup> Added per eRouter-N-11.1015-2 on 11/8/11 by JB.

## Annex A SNMP MIB Objects supported by the eRouter

This Annex defines the SNMP MIBs that the eRouter is required to implement.

The eRouter MUST support the following MIB objects:

- ipNetToPhysicalTable [RFC 4293];
- vacmAccessTable [RFC 3415];
- vacmSecurityToGroupTable [RFC 3415];
- vacmViewTreeFamilyTable [RFC 3415];
- vacmAccessReadViewName [RFC 3415];
- vacmAccessWriteViewName [RFC 3415];
- snmpCommunityTable [RFC 3584];
- snmpTargetAddrTable [RFC 3413] ;
- snmpTargetAddrTAddress [RFC 3413];
- snmpTargetAddrTMask [RFC 3584];
- snmpTargetAddrExtTable [RFC 3584].

Additional information for the configuration and use of the above MIB objects is defined in Annex B.

### A.1 eRouter Interface Numbering

The eRouter MUST use in its MIB tables, when appropriate, an ifIndex number of '1' for the Operator-Facing Interface and an ifIndex number of '2' for the first Customer-Facing Interface. Any additional Customer-Facing Interfaces MUST be numbered sequentially from '3' onwards.



## Annex B Configuration of eRouter Operational Parameters

This Annex defines the configuration TLVs used by the eRouter and describes how the configuration parameters are transferred from the eCM to the eRouter.

### B.1 eRouter SNMP Configuration

This Annex subsection defines the configuration of SNMP access to the eRouter.

#### B.1.1 eRouter SNMP Modes of Operation

The eRouter **MUST** support SNMPv1, SNMPv2c, in SNMP-coexistence mode as defined in [RFC 3584]. The eRouter **MAY** support SNMPv3 as defined in [OSSIV3.0].

#### B.1.2 eRouter SNMP Access Control Configuration

The eRouter uses the View-based Access Control Model (VACM) for configuration of SNMPv1v2c co-existence as defined in [RFC 3584].

##### B.1.2.1 View-based Access Control Model (VACM) Profile

This section addresses the default VACM profile for the eRouter.

The eRouter **MUST** support a pre-installed entry in the vacmViewTreeFamilyTable [RFC 3415] as follows:

**Table B-1 - vacmViewTreeFamilyTable**

| Column Name (* = Part of Index) | Column Value                    |
|---------------------------------|---------------------------------|
| * vacmViewTreeFamilyViewName    | eRouterManagerView              |
| * vacmViewTreeFamilySubtree     | <1.3.6.1>                       |
| vacmViewTreeFamilyMask          | Zero-length String              |
| vacmViewTreeFamilyType          | 'included'                      |
| vacmViewTreeFamilyStorageType   | volatile (2) or nonvolatile (3) |
| vacmViewTreeFamilyStatus        | active (1)                      |

The eRouter **MAY** also support additional views to be configured by the operator during the provisioning process, as defined in the SNMPv1v2c Access View Name encoding Annex B.3.4.4 and the SNMPv3 Access View Configuration encoding.

#### B.1.3 SNMPv1v2c Coexistence Configuration

This section specifies eRouter handling of the SNMPv1v2c Coexistence Configuration encodings as defined in Annex B.3.3.1 when included in the eRouter configuration information. The SNMPv1v2c Coexistence Configuration encoding is used to configure SNMPv3 framework tables for SNMPv1 and v2c access.

The eRouter uses the SNMPv1v2c Coexistence Configuration encodings to create entries in the following tables:

- snmpCommunityTable;
- snmpTargetAddrTable;
- vacmSecurityToGroupTable;
- vacmAccessTable;
- snmpTargetAddrExtTable.

### **B.1.3.1 Mapping SNMPv1v2c Coexistence Configuration**

This section describes the mapping of SNMPv1v2c Coexistence Configuration into SNMPv3 entries.

Table B-2 provides a Variable Name as a short-hand reference to be used in the SNMPv3 tables defined in subsections below for each of the SNMPv1v2c Coexistence Configuration encodings. The table also defines the mapping between each of the SNMPv1v2c Coexistence Configuration encodings and the associated SNMP MIB objects.

**Table B-2 - SNMPv1v2c Coexistence Configuration Mapping**

| Encodings  | Variable Name   | Associated MIB Object  |
|--|---|--|
| SNMPv1v2c Community Name                                   | <i>CommunityName</i>                                  | snmpCommunityName [RFC 3584]                                     |
| <b>SNMPv1v2c Transport Address Access</b>                  |   |  |
| SNMPv1v2c Transport Address                                | <i>TAddress</i>                                       | snmpTargetAddrTAddress [RFC 3413]                                |
| SNMPv1v2c Transport Address Mask                           | <i>TMask</i>  | snmpTargetAddrTMask [RFC 3584]                                   |
| SNMPv1v2c Access View Type                                 | <i>AccessViewType</i>                                 |  |
| SNMPv1v2c Access View Name (optional, see Section B.3.4.4) | <i>AccessViewName</i><br>or <i>eRouterManagerView</i> | vacmAccessReadViewName and<br>vacmAccessWriteViewName [RFC 3415] |

The eRouter is not required to verify the consistency across tables.

Table B-3 through Table B-7 describe the eRouter procedures to populate the SNMPv3 framework tables to conform to the "SNMP Management Framework Message Processing and Access Control Subsystems" [RFC 3412].

When configuring entries in these SNMPv3 tables:

- The ReadViewName and WriteViewName may correspond to default entries as defined in Annex B.1.3.1 or entries created using SNMPv3 Access View Configuration (see Annex B.3.5).
- Multiple columnar objects can be configured with indexes containing the string "@eRouterRouterconfig". If these tables are configured through other mechanisms, network operators should not use values beginning with "@eRouterconfig", to avoid conflicts.

#### **B.1.3.1.1 snmpCommunityTable**

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

The eRouter MUST create one row in snmpCommunityTable for each SNMPv1v2c Coexistence Configuration TLV as follows:

- The eRouter sets the value of snmpCommunityIndex to "@eRouterconfig\_n" where 'n' is a sequential number starting at 0 for each TLV processed (e.g., "@eRouterconfig\_0", "@eRouterconfig\_1", etc.)
- The eRouter creates space separated tags in snmpCommunityTransportTag for each SNMPv1v2c Community Name sub-TLV of the SNMPv1v2c Coexistence Configuration encoding.

**Table B-3 - snmpCommunityTable**

| Column Name<br>(* = Part of Index) | Column Value  |
|------------------------------------|---|
| * snmpCommunityIndex               | "@eRouterconfig_n" where n is 0..m-1 and m is the number of SNMPv1v2c Community Name TLVs               |
| snmpCommunityName                  | <CommunityName>   |
| snmpCommunitySecurityName          | "@eRouterconfig_n"  |
| snmpCommunityContextEngineID       | <the engineID populated by the SNMP>  |
| snmpCommunityContextName           | <Zero-length OCTET STRING>  |
| snmpCommunityTransportTag          | "@eRouterconfigTag_n" where n is 0..m-1 and m is the number of SNMPv1v2c Coexistence Configuration TLVs |
| snmpCommunityStorageType           | volatile (2)  |
| snmpCommunityStatus                | active (1)  |

#### B.1.3.1.2 snmpTargetAddrTable

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

The eRouter MUST create one row in snmpTargetAddrTable for each SNMPv1v2c Transport Address Access sub-TLV of the SNMPv1v2c Coexistence Configuration encoding.

**Table B-4 - snmpTargetAddrTable**

| Column Name<br>(* = Part of Index)                  | Column Value   |
|---|--|
| * snmpTargetAddrName                                | "@eRouterconfigTag_n_i" where 'n' is 0..m-1 and 'm' is the number of SNMPv1v2c Coexistence Configuration TLVs.<br>Where 'i' is 0..p-1 and p is the number of SNMPv1v2c Transport Address Access sub-TLV within the SNMPv1v2c Coexistence Configuration TLV n |
| snmpTargetAddrTDomain                               | IPv4: snmpUDPDDomain [RFC 3417]<br>IPv6: transportDomainUdpIpv6 [RFC 3419]   |
| snmpTargetAddrTAddress<br>(IP Address and UDP Port) | IPv4: SnmpUDPAddress [RFC 3417]<br>OCTET STRING (6) Octets 1-4: <TAddress> Octets 5-6: <TAddress><br>IPv6: TransportAddressIPv6 [RFC 3419]<br>OCTET STRING (18) Octets 1-16: <TAddress> Octets 17-18: <TAddress>   |
| snmpTargetAddrTimeout                               | Default from MIB   |
| snmpTargetAddrRetryCount                            | Default from MIB   |
| snmpTargetAddrTagList                               | "@eRouterconfigTag_n" where n is 0..m-1 and m is the number of SNMPv1v2c Coexistence Configuration TLVs  |

| Column Name<br>(* = Part of Index) | Column Value           |
|------------------------------------|------------------------|
| snmpTargetAddrParams               | '00'h (null character) |
| snmpTargetAddrStorageType          | volatile (2)           |
| snmpTargetAddrRowStatus            | active (1)             |

#### B.1.3.1.3 *snmpTargetAddrExtTable*

The snmpTargetAddrExtTable is defined in the "SNMP Community MIB Module" section of [RFC 3584].

The eRouter MUST create one row in snmpTargetAddrExtTable for each SNMPv1v2c Transport Address Access sub-TLV of the SNMPv1v2c Coexistence Configuration encoding.

**Table B-5 - snmpTargetAddrExtTable**

| Column Name<br>(* = Part of Index) | Column Value   |
|------------------------------------|--|
| * snmpTargetAddrName               | "@eRouterconfigTag_n_i" where 'n' is 0..m-1 and 'm' is the number of SNMPv1v2c Coexistence Configuration TLVs.<br><br>Where 'i' is 0..p-1 and p is the number of SNMPv1v2c Transport Address Access sub-TLV within the SNMPv1v2c Coexistence Configuration TLV n   |
| snmpTargetAddrTMask                | <Zero-length OCTET STRING> when <TMask> is not provided in the i-th SNMPv1v2c Transport Address Access sub-TLV<br>IPv4: SnmpUDPAddress [RFC 3417]<br>OCTET STRING (6) Octets 1-4: <TMask> Octets 5-6: <UDP Port><br>IPv6: TransportAddressIPv6 [RFC 3419]<br>OCTET STRING (18) Octets 1-16: <TMask> Octets 17-18: <UDP Port> |
| snmpTargetAddrMMS                  | Maximum Message Size   |

#### B.1.3.1.4 *vacmSecurityToGroupTable*

The vacmSecurityToGroupTable is defined in the "Definitions" section of [RFC 3415].

The eRouter MUST create two rows in vacmSecurityGroupTable for each SNMPv1v2c Coexistence Configuration TLV as follows:

- The eRouter sets the value of vacmSecurityName to "@eRouterconfig\_n" where 'n' is a sequential number starting at 0 for each SNMPv1v2c Coexistence Configuration TLV processed (e.g., "@eRouterconfig\_0", "@eRouterconfig\_1", etc.);
- The eRouter sets the value of vacmGroupName to "@eRouterconfigV1\_n" for the first row and "@eRouterconfigV2\_n" for the second row where 'n' is a sequential number starting at 0 for each SNMPv1v2c Coexistence Configuration TLV processed (e.g., "@eRouterconfigV1\_0", "@eRouterconfigV1\_1", etc.).

**Table B-6 - vacmSecurityToGroupTable**

| Column Name<br>(* = Part of Index) | First Row Column Value | Second Row Column Value |
|------------------------------------|------------------------|-------------------------|
| * vacmSecurityModel                | SNMPV1 (1)             | SNMPV2c (2)             |
| * vacmSecurityName                 | "@eRouterconfig_n"     | "@eRouterconfig_n"      |
| vacmGroupName                      | "@eRouterconfigV1_n"   | "@eRouterconfigV2_n"    |
| vacmSecurityToGroupStorageType     | volatile (2)           | volatile (2)            |
| vacmSecurityToGroupStatus          | active (1)             | active (1)              |

**B.1.3.1.5 vacmAccessTable**

The vacmAccessTable is defined in the "Definitions" section of [RFC 3415].

The eRouter MUST create two rows in vacmAccessTable for each SNMPv1v2c Coexistence Configuration encoding as follows:

- The eRouter sets the value of vacmGroupName to "@eRouterconfigV1\_n" for the first row and "@eRouterconfigV2\_n" for the second row where 'n' is a sequential number starting at 0 for each SNMPv1v2c Coexistence Configuration encoding processed (e.g., "@eRouterconfigV1\_0", "@eRouterconfigV1\_1", etc.);

In case the eRouter does not support the SNMPv3 Access View Name encoding in Annex B.3, the eRouter MUST use the default view defined in Annex B.1.2.1 and ignore the Sub-TLV SNMPv1v2c Access View Name.

**Table B-7 - vacmAccessTable**

| Column Name<br>(* = Part of Index) | Column Value  | Column Value  |
|------------------------------------|---|---|
| * vacmGroupName                    | "@eRouterconfigV1_n"  | "@eRouterconfigV2_n"  |
| * vacmAccessContextPrefix          | <zero-length string>  | <zero-length string>  |
| * vacmAccessSecurityModel          | SNMPV1 (1)  | SNMPV2c (2)   |
| * vacmAccessSecurityLevel          | noAuthNoPriv (1)  | noAuthNoPriv (1)  |
| vacmAccessContextMatch             | exact (1)   | exact (1)   |
| vacmAccessReadViewName             | Set <AccessViewName><br>or eRouterManagerView   | Set <AccessViewName><br>or eRouterManagerView   |
| vacmAccessWriteViewName            | When <AccessViewType> == '2'<br>Set <AccessViewName><br>or eRouterManagerView<br>When <AccessViewType> != '2' Set<br><Zero-length OCTET STRING> | When <AccessViewType> == '2'<br>Set <AccessViewName><br>or eRouterManagerView<br>When <AccessViewType> != '2' Set<br><Zero-length OCTET STRING> |
| vacmAccessNotifyViewName           | <Zero-length OCTET STRING>  | <Zero-length OCTET STRING>  |
| vacmAccessStorageType              | volatile (2)  | volatile (2)  |
| vacmAccessStatus                   | active (1)  | active (1)  |

**B.1.3.2 Mapping SNMPv3 Access View Configuration**

If SNMPv3 is supported by the eRouter, the SNMPv3 Access View Configuration encoding is used to configure the vacmViewTreeFamilyTable.

Table B-8 provides a Variable Name as a short-hand reference to be used in the SNMPv3 tables defined in the subsections below for each of the SNMPv3 Access View Configuration encodings. The table also defines the mapping between each of the SNMPv3 Coexistence Configuration encodings and the associated SNMP MIB objects.

**Table B-8 - SNMPv3 Access View Configuration Encoding**

| Encodings                  | Variable Name            | Associated MIB Object [RFC 3415] |
|----------------------------|--------------------------|----------------------------------|
| SNMPv3 Access View Name    | <i>AccessViewName</i>    | vacmViewTreeFamilyViewName       |
| SNMPv3 Access View Subtree | <i>AccessViewSubTree</i> | vacmViewTreeFamilySubtree        |
| SNMPv3 Access View Mask    | <i>AccessViewMask</i>    | vacmViewTreeFamilyMask           |
| SNMPv3 Access View Type    | <i>AccessViewType</i>    | vacmViewTreeFamilyType           |

The eRouter is not required to verify the consistency across tables.

Table B-9 describes the eRouter procedures to populate the vacmViewTreeFamilyTable to conform to the "SNMP Management Framework Message Processing and Access Control Subsystems" [RFC 3412].

When configuring entries in these SNMPv3 tables:

- One entry is created for each SNMPv3 Access View Configuration encoding. Some Access Views may have a number of included/excluded OID branches. Only Access View Name will be common for all these OID branches. To support such type of Access View, multiple SNMPv3 Access View Configuration encodings need to be defined.

#### **B.1.3.2.1 vacmViewTreeFamilyTable**

The vacmViewTreeFamilyTable is defined in the "Definitions" section of [RFC 3415].

If the SNMPv3 Access View Configuration encoding is supported by the eRouter, then the eRouter **MUST**:

- Create one row in vacmViewTreeFamilyTable for each SNMPv3 Access View Configuration TLV;
- Reject the configuration if two or more SNMPv3 Access View Configuration encodings have identical index components (*AccessViewName* and *AccessViewSubTree*);
- Set the object vacmViewTreeFamilySubtree to 1.3.6 when no sub-TLV SNMPv3 Access View Subtree is defined;
- Set the object vacmViewTreeFamilyMask to the default zero-length string when no sub-TLV SNMPv3 Access View Mask is defined;
- Set the object vacmViewTreeFamilyType to the default value 1 (included) when no sub-TLV SNMPv3 Access View Type is defined.

**Table B-9 - vacmViewTreeFamilyTable**

| Column Name (* = Part of Index) | Column Value        |
|---------------------------------|---------------------|
| * vacmViewTreeFamilyViewName    | <AccessViewName>    |
| * vacmViewTreeFamilySubtree     | <AccessViewSubTree> |
| vacmViewTreeFamilyMask          | <AccessViewMask>    |
| vacmViewTreeFamilyType          | <AccessViewType>    |
| vacmViewTreeFamilyStorageType   | volatile (2)        |

|                          |            |
|--------------------------|------------|
| vacmViewTreeFamilyStatus | active (1) |
|--------------------------|------------|

## B.2 eCM Proxy mechanism for configuration of eRouter

The eRouter configuration encodings are encapsulated in the 'eCM Config File Encapsulation' encoding defined in [eDOCSIS]. The eCM receives the configuration file and parses its contents. The encodings in the eCM configuration file encapsulated in Type 202 are for exclusive use of the eRouter, and these TLVs are transferred from the eCM to the eRouter in a vendor specific manner. After the eCM successfully completes registration, the eRouter uses these encapsulated TLVs for initialization.

The eRouter initializes per the 'eRouter Operation Mode' encoding, encapsulated under the TLV 202 in the eCMs configuration file. During the eRouter initialization process, the eCM reports the eRouter state with the Flow Step information and status in the esafeProvisioningStatusTable [eDOCSIS].

The eCM configuration download process includes certain security aspects; e.g., EAE and secure download which provide for confidentiality and authenticity of the information contained in the CM configuration file as defined in [MULPI] and [SECv3.0].

## B.3 eRouter Configuration Encodings<sup>36</sup>

This section defines the encodings required for eRouter configuration and how those are processed by the eRouter.

### B.3.1 eRouter TLV Processing

The eRouter MUST disregard encodings that are not defined in this section.

The following subsections provide definitions of Configuration Encodings that are valid for eRouter use. The eRouter MUST reject invalid eRouter Configuration Encodings. When the eRouter Configuration Encodings are rejected, the eRouter MUST operate in 'Disabled Mode' per Section 6, eRouter Initialization.

The eRouter MUST reject the eRouter Configuration Encoding if that encoding results in an entry in the SNMP table that cannot be created because of a conflict with an existing entry.

### B.3.2 eRouter Initialization Mode Encoding

This encoding defines the eRouter initialization mode (Section 6) configured by the Operator.

A valid eRouter Initialization Mode Encoding contains exactly one instance of this TLV.

| Type | Length | Value                       |
|------|--------|-----------------------------|
| 1    | 1      | 0: Disabled                 |
|      |        | 1: IPv4 Protocol Enabled    |
|      |        | 2: IPv6 Protocol Enabled    |
|      |        | 3: Dual IP Protocol Enabled |
|      |        | 4-255: Invalid              |

<sup>36</sup> Revised per eRouter N-11.1014-3 on 10/27/11 by JB.

### B.3.3 TR-069 Management Server

This encoding specifies some aspects of TR-069 Device.ManagementServer object to be used by the cable provisioning system. Whenever a TLV or sub-TLV is absent, default values from [TR-069a4] and [TR-181i2a3] apply.

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value     |
|------|--------|-----------|
| 2    | N      | Composite |

#### B.3.3.1 EnableCWMP

This encoding specifies the Device.ManagementServer.EnableCWMP parameter from [TR-181i2a3].

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value               |
|------|--------|---------------------|
| 2.1  | 1      | 0: false<br>1: true |

#### B.3.3.2 URL

This encoding specifies the Device.ManagementServer.URL parameter from [TR-181i2a3].

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value  |
|------|--------|--------|
| 2.2  | n      | String |

#### B.3.3.3 Username

This encoding specifies the Device.ManagementServer.Username parameter from [TR-181i2a3].

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value  |
|------|--------|--------|
| 2.3  | n      | String |

#### B.3.3.4 Password

This encoding specifies the Device.ManagementServer.Password parameter from [TR-181i2a3].

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value  |
|------|--------|--------|
| 2.4  | n      | String |



### **B.3.3.5 ConnectionRequestUsername**

This encoding specifies the Device.ManagementServer.ConnectionRequestUsername parameter from [TR-181i2a3].

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value  |
|------|--------|--------|
| 2.5  | n      | String |

### **B.3.3.6 ConnectionRequestPassword**

This encoding specifies the Device.ManagementServer.ConnectionRequestPassword parameter from [TR-181i2a3].

A valid eRouter Initialization Mode Encoding contains at most one instance of this TLV.

| Type | Length | Value  |
|------|--------|--------|
| 2.6  | n      | String |

### **B.3.3.7 ACSOverride**

If enabled, the CPE MUST accept the ACS URL from the CM configuration file, even if the ACS has overwritten the values.

If disabled, the CPE accepts the CM configuration file values only if the ACS has not overwritten the ACS URL.

| Type | Length | Value |
|------|--------|-------|
|------|--------|-------|

## **B.3.4 SNMPv1v2c Coexistence Configuration**

This encoding specifies the SNMPv1v2c Coexistence Access Control configuration for the eRouter. This encoding creates entries in the SNMPv3 framework tables as specified in Annex B.1.3.1 above.

A valid SNMPv1v2c Coexistence Configuration (Type 53) encoding contains the SNMPv1v2c Community Name and one or more instance(s) of SNMPv1v2c Transport Address Access. A valid SNMPv1v2c Coexistence Configuration (Type 53) encoding may also contain the SNMPv1v2c Access View Type and the SNMPv1v2c Access View Name.

The eRouter does not make persistent entries in the SNMP framework table.

The eRouter MUST support a minimum of 5 SNMPv1v2c Coexistence Configuration encodings.

| Type | Length | Value     |
|------|--------|-----------|
| 53   | N      | Composite |

### **B.3.4.1 SNMPv1v2c Community Name**

This sub-TLV specifies the Community Name (community string) used in SNMP requests to the eRouter.

| Type | Length | Value |
|------|--------|-------|
| 53.1 | 1..32  | Text  |

#### **B.3.4.2     *SNMPv1v2c Transport Address Access***

This sub-TLV specifies the Transport Address and Transport Address Mask pair used by the eRouter to grant access to the SNMP entity querying the eRouter.

| Type | Length | Value    |
|------|--------|----------|
| 53.2 | N      | Variable |

A valid SNMPv1v2c Transport Address Access encoding contains one instance of SNMPv1v2c Transport Address and may contain one instance of SNMPv1v2c Transport Address Mask.

The eRouter accepts one or more instances of sub-TLV 53.2 SNMPv1v2c Transport Address Access within a TLV 53.

##### **B.3.4.2.1     *SNMPv1v2c Transport Address***

This sub-TLV specifies the Transport Address to use in conjunction with the Transport Address Mask used by the eRouter to grant access to the SNMP entity querying the eRouter.

| Type   | Length  | Value             |
|--------|---------|-------------------|
| 53.2.1 | 6 or 18 | Transport Address |

Transport addresses are 6 or 18 bytes in length for IPv4 and IPv6 type addresses respectively.

##### **B.3.4.2.2     *SNMPv1v2c Transport Address Mask***

This sub-TLV specifies the Transport Address Mask to use in conjunction with the Transport Address used by the eRouter to grant access to the SNMP entity querying the eRouter. This sub-TLV is optional.

| Type   | Length  | Value                  |
|--------|---------|------------------------|
| 53.2.2 | 6 or 18 | Transport Address Mask |

Transport addresses are 6 or 18 bytes in length for IPv4 and IPv6 type addresses respectively.

#### **B.3.4.3     *SNMPv1v2c Access View Type***

The SNMPv1v2c Access View Type encoding specifies the type of access to grant to the community name specified in the SNMPv1v2c Community Name encoding. This TLV is optional. If this TLV is not present, the eRouter MUST set the value of the SNMPv1v2c Access View Type to Read-Only.

| Type | Length | Value                         |
|------|--------|-------------------------------|
| 53.3 | 1      | 1: Read-only<br>2: Read-write |

#### **B.3.4.4     *SNMPv1v2c Access View Name***

This sub-TLV specifies the name of the view that provides the access indicated in the SNMPv1v2c Access View Type. This sub-TLV is optional.

| Type | Length | Value  |
|------|--------|--------|
| 53.4 | 1..32  | String |

#### **B.3.5     *SNMPv3 Access View Configuration***

This encoding specifies the SNMPv3 Simplified Access View configuration of the eRouter. This TLV creates entries in SNMPv3 tables.

The eRouter supports SNMPv3 Access View Configuration encoding only if the eRouter supports SNMPv3.

A valid SNMPv3 Access View Configuration encoding contains one instance of SNMPv3 Access View Name. The eRouter does not make persistent entries in the SNMP framework table.

The eRouter MUST reject the eRouter Configuration Encoding if an eRouter created entry in an SNMP table is rejected due reaching the limit in the number of entries supported for that table.

| Type | Length | Value     |
|------|--------|-----------|
| 54   | N      | Composite |

##### **B.3.5.1     *SNMPv3 Access View Name***

This encoding specifies the administrative name of the view defined by the SNMPv3 Access View Configuration.

| Type | Length | Value |
|------|--------|-------|
| 54.1 | 1..32  | Text  |

##### **B.3.5.2     *SNMPv3 Access View Subtree***

This encoding specifies an ASN.1 formatted object identifier (OID) that represents the filter sub-tree included in the SNMPv3 Access View Configuration encoding.

A valid SNMPv3 Access View Subtree encoding starts with the ASN.1 Universal type 6 (OID) byte, followed by the ASN.1 length field, and then followed by the ASN.1 encoded object identifier components. For example, the sub-tree 1.3.6 is encoded as 0x06 0x03 0x01 0x03 0x06.

If this encoding is not included under the SNMPv3 Access View Name encoding, the eRouter MUST use the default OID sub-tree of 1.3.6.

| Type | Length | Value |
|------|--------|-------|
| 54.2 | N      | OID   |

**B.3.5.3 SNMPv3 Access View Mask**

This sub-TLV specifies the bit mask to apply to the Access View Subtree of the Access View TLV.

| Type | Length | Value |
|------|--------|-------|
| 54.3 | 0..16  | Bits  |

This sub-TLV is optional. If this sub-TLV is not present, the eRouter MUST assign a zero-length string to SNMPv3 Access View Mask.

**B.3.5.4 SNMPv3 Access View Type**

This sub-TLV specifies the inclusion or exclusion of the sub-tree indicated by SNMPv3 Access View Subtree. The value of 1 indicates that the sub-tree of SNMPv3 Access View SubTree is included in the Access View. The value of 2 indicates that the sub-tree of SNMPv3 Access View Sub Tree is excluded from the Access View.

| Type | Length | Value                      |
|------|--------|----------------------------|
| 54.4 | 1      | 1: included<br>2: excluded |

This sub-TLV is optional. If this sub-TLV is not present, the eRouter MUST assign the value 'included' to SNMPv3 Access View Type.

**B.3.6 Vendor Specific Information**

The Vendor Specific Information encoding is used to extend the capabilities of the eRouter specification, through the use of vendor-specific features. A valid Vendor Specific Information encoding contains only one Vendor ID field (Annex B.3.6.1) to indicate that the settings apply to a specific vendor device.

The eRouter MUST ignore a Vendor Specific Information encoding that includes a Vendor ID different to the one of the eRouter.

| Type | Length | Value    |
|------|--------|----------|
| 43   | N      | Variable |

**B.3.6.1 Vendor ID Encoding**

The Vendor ID encoding contains the vendor identification specified by the three-byte vendor-specific Organization Unique Identifier of the eRouter's MAC addresses.

The Vendor ID 0xFFFFFFFF is reserved.

| Type | Length | Value |
|------|--------|-------|
| 43.8 | 3      | OUI   |

## Annex C TR-069 Managed Objects Requirements<sup>37</sup>

The eRouter MUST support the objects associated with the Profiles and Components listed below. See [TR-106a5] for information about Components and Profiles in TR-069. N/A indicates the profile does not apply to eRouter.

### C.1 Profiles from [TR-181i2a3]

*Table C-1 - TR-181 Profiles for eRouter*

| Profile              | Requirement | Notes  |
|----------------------|-------------|--|
| Download:1           | MAY         |  |
| DownloadTCP:1        | MAY         |  |
| Upload:1             | MAY         |  |
| UploadTCP:1          | MAY         |  |
| UDPEcho:1            | MAY         |  |
| UDPEchoPlus:1        | MAY         |  |
| SupportedDataModel:1 | MAY         |  |
| MemoryStatus:1       | MAY         |  |
| ProcessStatus:1      | MAY         |  |
| TempStatus:1         | MAY         |  |
| TempStatusAdv:1      | MAY         |  |
| TempStatusAdv:2      | MAY         |  |
| User:1               | MUST        |  |
| UPnPDev:1            | MUST        | Support Data model, other specs to detail UPNP functional requirements |
| UPnPDiscBasic:1      | MUST        | Support Data model, other specs to detail UPNP functional requirements |
| UPnPDiscAdv:1        | MAY         |  |
| SelfTestDiag:1       | MAY         |  |
| NSLookupDiag:1       | MAY         |  |
| SimpleFirewall:1     | MUST        |  |
| AdvancedFirewall:1   | MUST        |  |
| USBHostsBasic:1      | N/A         |  |
| USBHostsAdv:1        | N/A         |  |
| PeriodicStatsBase:1  | MUST        |  |

<sup>37</sup> Annex added per eRouter N-11.1014-3 on 10/27/11 by JB.

| Profile             | Requirement                 | Notes |
|---------------------|-----------------------------|-------|
| PeriodicStatsAdv:1  | MAY                         |       |
| DownloadAnnounce:1  | MAY                         |       |
| DownloadQuery:1     | MAY                         |       |
| Baseline:2          | MUST                        |       |
| DNSRelay:1          | MUST                        |       |
| Routing:1           | MUST                        |       |
| Routing:2           | MUST                        |       |
| IPv6Routing:1       | MUST                        |       |
| IPInterface:2       | MUST                        |       |
| IPv6Interface:1     | MUST                        |       |
| PPPInterface:1      | N/A                         |       |
| PPPInterface:2      | N/A                         |       |
| VLANTermination:1   | MUST                        |       |
| EthernetLink:1      | MUST                        |       |
| Bridge:1            | MUST                        |       |
| VLANBridge:1        | MUST                        |       |
| BridgeFilter:1      | MUST                        |       |
| BridgeFilter:2      | MUST                        |       |
| ATMLink:1           | N/A                         |       |
| PTMLink:1           | N/A                         |       |
| EthernetInterface:1 | MUST                        |       |
| ADSL:1              | N/A                         |       |
| ADSL2:1             | N/A                         |       |
| VDSL2:1             | N/A                         |       |
| BondedDSL:1         | N/A                         |       |
| HPNA:1              | MUST if interface supported |       |
| HPNADiagnostics:1   | MUST if interface supported |       |
| HPNAQoS:1           | MUST if interface supported |       |
| HomePlug:1          | MUST if interface supported |       |

| Profile                   | Requirement                 | Notes |
|---------------------------|-----------------------------|-------|
| MoCA:1                    | MUST if interface supported |       |
| UPA:1                     | MUST if interface supported |       |
| UPADiagnostics:1          | MUST if interface supported |       |
| WiFiRadio:1               | Per [WI-FI MGMT]            |       |
| WiFiSSID:1                | Per [WI-FI MGMT]            |       |
| WiFiAccessPoint:1         | Per [WI-FI MGMT]            |       |
| WiFiEndPoint:1            | Per [WI-FI MGMT]            |       |
| USBInterface:1            | MUST if interface supported |       |
| USBPort:1                 | MUST if interface supported |       |
| NAT:1                     | MUST                        |       |
| QoS:2                     | MAY                         |       |
| QoSDynamicFlow:1          | MAY                         |       |
| QoSStats:1                | MAY                         |       |
| NeighborDiscovery:1       | MUST                        |       |
| RouterAdvertisement:1     | MUST                        |       |
| IPv6rd:1                  | MAY                         |       |
| DSLite:1                  | MAY                         |       |
| Hosts:2                   | MUST                        |       |
| GatewayInfo:1             | MUST                        |       |
| DeviceAssociation:1       | MUST                        |       |
| UDPConnReq:1              | MAY                         |       |
| CaptivePortal:1           | MAY                         |       |
| Time:1                    | MUST                        |       |
| IEEE8021xAuthentication:1 | Per [WI-FI MGMT]            |       |
| IPPing:1                  | MAY                         |       |
| TraceRoute:1              | MAY                         |       |
| ATMLoopback:1             | N/A                         |       |
| DSLDiagnosics:1           | N/A                         |       |
| ADSL2Diagnostics:1        | N/A                         |       |

| Profile                      | Requirement | Notes |
|------------------------------|-------------|-------|
| VDSL2Diagnostics:1           | N/A         |       |
| DHCPv4Client:1               | MUST        |       |
| DHCPv4Server:1               | MUST        |       |
| DHCPv4CondServing:1          | MAY         |       |
| DHCPv4Relay:1                | MUST NOT    |       |
| DHCPv4ServerClientInfo:1     | MUST        |       |
| DHCPv6Client:1               | MUST        |       |
| DHCPv6ClientServerIdentity:1 | MUST        |       |
| DHCPv6Server:1               | MUST        |       |
| DHCPv6ServerAdv:1            | MAY         |       |
| DHCPv6ServerClientInfo:1     | MUST        |       |
| Processors:1                 | MAY         |       |
| VendorLogFiles:1             | MAY         |       |
| DUStateChngComplPolicy:1     | MAY         |       |
| SM_ExecEnvs:1                | MAY         |       |
| SM_DeployAndExecUnits:1      | MAY         |       |
| SM_Baseline:1                | MAY         |       |



## Appendix I      Acknowledgements (Informative)

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.

| <b>Contributor</b> | <b>Company Affiliation</b> |
|--------------------|----------------------------|
| Ben Bekele         | Cox                        |
| Amol Bhagwat       | CableLabs                  |
| Ralph Brown        | CableLabs                  |
| John Brzozowski    | Comcast                    |
| Eduardo Cardona    | CableLabs                  |
| Margo Dolas        | Broadcom                   |
| Chris Donley       | CableLabs                  |
| Ralph Droms        | Cisco Systems              |
| Alain Durand       | Comcast                    |
| Toerless Eckert    | Cisco Systems              |
| Kirk Erichsen      | Time Warner Cable          |
| Doc Evans          | ARRIS                      |
| Roger Fish         | Broadcom                   |
| Deepak Kharbanda   | CableLabs                  |
| Michelle Kuska     | CableLabs                  |
| Diego Mazzola      | Texas Instruments          |
| John McQueen       | Broadcom                   |
| Jean-Francois Mule | CableLabs                  |
| Harsh Parandekar   | Cisco Systems              |
| Michael Patrick    | Motorola                   |
| Saifur Rahman      | Comcast                    |
| Lakshmi Raman      | CableLabs                  |
| Ryan Ross          | Juniper                    |
| Matt Schmitt       | CableLabs                  |
| Ron da Silva       | Time Warner Cable          |
| Madhu Sudan        | Cisco Systems              |
| Dan Torbet         | ARRIS                      |
| Greg White         | CableLabs                  |

We would particularly like to thank Ralph Droms (Cisco) and Doc Evans (ARRIS) for their extensive contributions to the specification and also for defining the eRouter Provisioning details for DHCPv4 and DHCPv6. We would like to thank Ryan Ross (Juniper) for his detailed work on the eRouter NAT and IPv6 data-forwarding behavior. We would like to thank Margo Dolas (Broadcom) for her work in numerous areas of the specification, including the eRouter IPv4 data forwarding functionality. We would like to thank Diego Mazzola and Deepak Kharbanda for defining the eRouter IP Multicast functionality. We would like to thank John McQueen (Broadcom) for helping define the eRouter DHCPv4 server behavior. We would like to thank Dan Torbet (ARRIS), Chris Donley (CableLabs), and Kirk Erichsen (Time Warner Cable) for their work on developing the QoS functionality. We thank Deepak Kharbanda (CableLabs) who led the IPv6 Focus Team that developed this specification. And finally, many thanks go out to all the active members of the IPv6 Focus Team who contributed to this specification.

## Appendix II Revision History

### II.1 The following ECN was incorporated into CM-SP-eRouter-I02-070223:

| ECN Identifier      | Accepted Date | Title of EC                |
|---------------------|---------------|----------------------------|
| eRouter-N-06.0352-1 | 1/10/2007     | eRouter Multicast Examples |

### II.2 The following ECN was incorporated into CM-SP-eRouter-I03-070518:

| ECN Identifier      | Accepted Date | Title of EC                                  |
|---------------------|---------------|--|
| eRouter-N-06.0396-1 | 3/14/2007     | IPv6 Provision of CPE Devices Clarifications |

### II.3 The following ECN was incorporated into CM-SP-eRouter-I04-100611:

| ECN Identifier      | Accepted Date | Title of EC        |
|---------------------|---------------|--------------------|
| eRouter-N-09-0877-2 | 12/30/2009    | IPv6 Router Update |

### II.4 The following ECN was incorporated into CM-SP-eRouter-I05-110210:

| ECN Identifier      | Accepted Date | Title of EC                                     |
|---------------------|---------------|---|
| eRouter-N-10.0974-2 | 01/05/2011    | eRouter Lease Renewal for IPv6 Prefix stability |

### II.5 The following ECN was incorporated into CM-SP-eRouter-I06-110623:

| ECN Identifier      | Accepted Date | Title of EC                                   |
|---------------------|---------------|---|
| eRouter-N-11.0991-1 | 05/04/2011    | Clarification to ICMP Destination Unreachable |

### II.6 The following ECNs were incorporated into CM-SP-eRouter-I07-111117:

| ECN Identifier      | Accepted Date | Title of EC                                   |
|---------------------|---------------|---|
| eRouter-N-11.1014-3 | 10/19/2011    | Adding TR-069 support for eRouter             |
| eRouter-N-11.1015-2 | 10/19/2011    | Update from RFC 6204 and address DHCP release |

---