

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 140 2019

Cable Modem IPv4 and IPv6 eRouter Specification

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at <http://www.scte.org>.

All Rights Reserved
© Society of Cable Telecommunications Engineers, Inc. 2019
140 Philips Road
Exton, PA 19341

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

Contents

1	SCOPE	8
1.1	Introduction and Purpose.....	8
1.2	Requirements	8
2	REFERENCES	9
2.1	Normative References	9
2.1.1	<i>SCTE References</i>	<i>9</i>
2.1.2	<i>Standards from Other Organizations.....</i>	<i>9</i>
2.1.3	<i>Published Materials.....</i>	<i>12</i>
2.2	Informative References	12
2.2.1	<i>SCTE References</i>	<i>12</i>
2.2.2	<i>Standards from Other Organizations.....</i>	<i>12</i>
2.2.3	<i>Published Materials.....</i>	<i>13</i>
3	TERMS AND DEFINITIONS	14
4	ABBREVIATIONS AND ACRONYMS.....	16
5	THEORY OF OPERATION	19
5.1	eDOCSIS eRouter and TR-069 Architecture	21
5.2	eRouter Device Management.....	22
5.3	Service Discovery	22
5.3.1	<i>mDNS (multicast Domain Name System).....</i>	<i>22</i>
5.3.2	<i>UPnP (Universal Plug and Play)</i>	<i>23</i>
5.4	CER-ID (Customer Edge Router – Identification).....	24
6	EROUTER INITIALIZATION.....	26
6.1	Network Time Protocol	27
6.2	DNS Proxy Forwarding.....	28
7	IPv4 PROVISIONING.....	29
7.1	DHCPv4 Fields Used by the eRouter	30
7.2	eRouter Interface Addressing Using Link-ID	31
7.3	Router DHCPv4 Server Sub-element.....	32
7.3.1	<i>DHCPv4 Server Function Goals</i>	<i>32</i>
7.3.2	<i>DHCPv4 Server Function System Description.....</i>	<i>32</i>
7.3.3	<i>DHCPv4 Server Function Requirements</i>	<i>32</i>
7.4	Operator-Facing IPv4 Address Release Behavior	35
7.5	Customer-Facing IPv4 Address Release Behavior	35
8	OPERATOR-FACING IPv6 PROVISIONING	36
8.1	Obtain Link-Local Address	37
8.2	Perform Router Discovery.....	37
8.3	Obtain IPv6 Address and Other Configuration Parameters	37
8.4	Use of T1 and T2 Timers.....	40
8.5	Customer-Facing IPv6 Provisioning of CPE Devices	40
8.5.1	<i>Additional Customer-Facing IP Interfaces Enabled After Initial Provisioning</i>	<i>42</i>
8.5.2	<i>SLAAC Requirements for eRouter</i>	<i>43</i>
8.5.3	<i>DHCPv6 Requirements for eRouter.....</i>	<i>43</i>
8.5.4	<i>Prefix Changes.....</i>	<i>44</i>
8.6	Operator-Facing IPv6 Address Release Behavior	45
8.7	Customer-Facing IPv6 Address Release Behavior	45
8.8	CER-ID Requirements	45

9	IPv4 DATA FORWARDING AND NAPT OPERATION	47
9.1	Introduction	47
9.1.1	Assumptions	47
9.1.2	Overview.....	47
9.2	System Description	47
9.2.1	Overview.....	47
9.3	IPv4 Router.....	48
9.3.1	Dual IP Protocol and Link-ID Enabled Mode IPv4 Routing.....	50
9.4	NAPT	50
9.4.1	Dynamically Triggered NAPT Translations.....	51
9.4.2	Application Layer Gateways (ALGs).....	51
9.4.3	Multicast NAPT.....	52
9.5	ARP.....	52
9.6	IPv4 Multicast.....	52
9.6.1	IGMP Proxying	53
9.6.2	IPv4 Multicast Forwarding.....	54
9.6.3	IPv4 Multicast Forwarding Example.....	54
9.7	IPv4/IPv6 Co-existence Technologies.....	56
9.7.1	Dual-Stack Lite Operation	56
9.7.2	Mapping of Address and Port (MAP)	56
9.7.3	Packet Fragmentation.....	57
10	IPv6 DATA FORWARDING.....	59
10.1	Overview	59
10.2	System Description	60
10.3	IPv6 Multicast.....	61
10.3.1	MLD Proxying.....	62
10.3.2	IPv6 Group Membership Database	62
10.3.3	IPv6 Multicast Forwarding.....	63
10.3.4	IPv6 Multicast Forwarding Example.....	63
11	QUALITY OF SERVICE	66
11.1	Downstream Quality of Service Operation	66
11.2	Upstream Quality of Service Operation.....	66
12	EROUTER MANAGEMENT.....	67
12.1	eRouter SNMP Management Interface Requirements.....	67
12.2	eRouter TR-069 Management Interface Requirements	67
12.2.1	ACS Discovery.....	67
12.2.2	ACS Selection.....	67
12.2.3	Dynamic ACS Updates.....	68
12.2.4	TR-069 CWMP Control and Credentials	68
13	SECURITY	69
14	EROUTER TUNNEL MANAGEMENT AND CONFIGURATION.....	70
14.1	GRE Requirements.....	70
ANNEX A	SNMP MIB OBJECTS SUPPORTED BY THE EROUTER (NORMATIVE).....	71
A.1	eRouter Interface Numbering.....	71
A.2	eRouter ifTable Requirements	72
A.3	eRouter ipNetToPhysicalTable Requirements	74
A.4	CLAB-GRE-MIB.....	74
A.5	CLAB-GW-MIB	74
ANNEX B	CONFIGURATION OF EROUTER OPERATIONAL PARAMETERS (NORMATIVE).....	77

B.1	eRouter SNMP Configuration.....	77
B.1.1	eRouter SNMP Modes of Operation	77
B.1.2	eRouter SNMP Access Control Configuration	77
B.1.3	SNMPv1v2c Coexistence Configuration	77
B.2	SNMP Configuration of eRouter.....	82
B.3	eCM Proxy mechanism for configuration of eRouter.....	82
B.4	eRouter Configuration Encodings.....	83
B.4.1	eRouter TLV Processing	83
B.4.2	eRouter Initialization Mode Encoding.....	83
B.4.3	TR-069 Management Server.....	83
B.4.4	eRouter Initialization Mode Override.....	84
B.4.5	SNMPv1v2c Coexistence Configuration	85
B.4.6	SNMPv3 Access View Configuration.....	86
B.4.7	Vendor Specific Information	87
B.4.8	SNMP MIB Object.....	88
B.4.9	Topology Mode Encoding	88
B.4.10	Router Advertisement (RA) Transmission Interval	88
B.4.11	IP Multicast Configuration Server	89
B.4.12	Link-ID Control.....	89
B.5	SNMP Soft Reset	89
B.6	Provisioning and Operational Event Messages	90
ANNEX C	EROUTER INITIALIZATION MODE CONTROL INTERACTIONS (NORMATIVE).....	92
C.1	Assumptions	92
C.2	Invalid Cases.....	94
ANNEX D	TR-069 MANAGED OBJECTS REQUIREMENTS (NORMATIVE).....	95
D.1	Profiles from [TR-181].....	95
D.2	Extensions to TR-181 Profiles	98
D.3	Management Interface Protocols Requirements for GRE.....	98
ANNEX E	EXAMPLE: ROUTING WITH LINK ID (NORMATIVE)	101
E.1	IP MIB Route Example	102
ANNEX F	SECTION CATEGORIZING [RFC 6092] SIMPLE SECURITY RECOMMENDATIONS (NORMATIVE).....	103
F.1	Summary of Simple Security Requirements	103
F.2	Critical Recommendations.....	103
F.3	Important Recommendations	106
F.4	BCP Recommendations.....	107
F.5	Other RFC 6092 Recommendations.....	109
F.6	RFC 6092 Recommendations In Conflict With MSO Needs.....	110
ANNEX G	EROUTER GRE TUNNELING ARCHITECTURE (NORMATIVE)	111
G.1	Use Case for Data Traffic Flow for Both Private and Public SSIDs	112
G.1.1	Private Network Outbound From the LAN.....	113
G.1.2	Private Network Inbound From the WAN.....	113
G.1.3	Community WiFi User Outbound Via Public SSID	113
G.1.4	Community WiFi User Inbound Via Public SSID.....	113

Figures

Figure 4-1 - Logical Components of an eDOCSIS device with an IPv4 Protocol Enabled eRouter.....	19
Figure 4-2 - Logical Components of an eDOCSIS device with an IPv6 Protocol Enabled eRouter.....	19
Figure 4-3 - Logical Components of an eDOCSIS device with a Dual Protocol Enabled eRouter	20
Figure 4-4 - TR-069 Interface Model Applied to eDOCSIS eRouter	22
Figure 4-5 - mDNS Source IP and Payload Changes Going Through a Router	23
Figure 4-6 - UPnP General Architecture.....	24
Figure 4-7 - Example of a CER Demarcation Boundary	25
Figure 6-1 - IPv4 Provisioning Message Flow.....	29
Figure 6-2 - Example Deriving IPv4 Octets 2 and 3 from an IPv6 Prefix	32
Figure 7-1 - IPv6 Provisioning Message Flow.....	36
Figure 8-1 - eRouter IPv4 Forwarding Block Diagram	48
Figure 8-2 - eRouter IPv4 Multicast Forwarding Block Diagram	53
Figure 8-3 - IPv4 Multicast Forwarding Example.....	55
Figure 9-1 - eRouter IPv6 Forwarding Block Diagram	59
Figure 9-2 - eRouter IPv6 Multicast Forwarding Block Diagram	62
Figure 9-3 - IPv6 Multicast Forwarding Example.....	64
Figure E-1 - Example of Link-ID with Prefix Delegation – Topology Mode Favors Width	101
Figure G-1 - eRouter GRE Tunneling Architecture	111

Tables

Table 5-1 - eRouter Modes	27
Table 6-1 - eRouter DHCP Retransmission Interval	29
Table 6-2 - DHCPv4 Server Options.....	34
Table 7-1 - eRouter Behavior.....	37
Table A-1 - eRouter Interface Numbering	71
Table A-2 - eRouter ifTable Row Entries.....	72
Table A-3 - eRouter ifTable Row Entries for Supported Interfaces	73
Table A-4 - eRouter ipNetToPhysicalTable Row Entries.....	74
Table A-5 - Gateway MIB Objects.....	74
Table B-1 - vacmViewTreeFamilyTable	77
Table B-2 - SNMPv1v2c Coexistence Configuration Mapping.....	78
Table B-3 - snmpCommunityTable.....	78
Table B-4 - snmpTargetAddrTable	79
Table B-5 - snmpTargetAddrExtTable	79
Table B-6 - vacmSecurityToGroupTable.....	80
Table B-7 - vacmAccessTable	80
Table B-8 - SNMPv3 Access View Configuration Encoding	81
Table B-9 - vacmViewTreeFamilyTable	82
Table B-10 - esafeErouterInitModeControl	82
Table C-1 - eRouter Initialization Behavior Based upon Mode Control Interactions.....	92
Table C-2 - Invalid Cases	94

Table D-1 - TR-181 Profiles for eRouter	95
Table D-2 - CableLabs Extensions to TR-181 Profiles for GRE.....	98
Table D-3 - GRE Data Model Objects.....	98
Table E-1 - Routing Table Example Based on Link ID Reference Examples in Figure E-1.....	102
Table F-1 - Critical Recommendations.....	103
Table F-2 - Important Recommendations	106
Table F-3 - BCP Recommendations.....	107
Table F-4 - Other 6092 Recommendations.....	109
Table F-5 - RFC 6092 Recommendations In Conflict With MSO Needs	110
Table G-1 - IF Indices and Row Instances for Data Objects Associated with GRE Tunneling.....	111

1 SCOPE

This standard was developed for the benefit of the cable industry, and includes contributions by operators and vendors from North America, Europe, and other regions.

The present document corresponds to and is the technical equivalent of the CableLabs [eRouter] specification.

1.1 Introduction and Purpose

This standard 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 an embedded 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 and among 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 standard.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this standard.
"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

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1.1 SCTE References

[eDOCSIS]	ANSI/SCTE 107 2017, Embedded Cable Modem Devices.
[MULPIv3.0]	ANSI/SCTE 135-2 2019, DOCSIS 3.0 Part 2: MAC and Upper Layer Protocols.
[OSSIV3.0]	ANSI/SCTE 135-4 2019, DOCSIS 3.0 Part 4: Operations Support Systems Interface.
[SECv3.0]	ANSI/SCTE 135-3 2019, DOCSIS 3.0 Part 3: Security Services.

2.1.2 Standards from Other Organizations

[CANN DHCP]	CableLabs DHCP Options Registry Specification, CL-SP-CANN-DHCP-Reg-I13-160317, March 17, 2016, Cable Television Laboratories, Inc.
[CLAB-GRE-MIB]	CableLabs Generic Route Encapsulation MIB, CLAB-GRE-MIB, http://www.cablelabs.com/MIBs/common/
[CLAB-GW-MIB]	Cablelabs Wi-Fi Gateway MIB, CLAB-GW-MIB, http://www.cablelabs.com/MIBs/common/
[ISO/IEC 29341]	Universal Plug and Play Architecture Version 1.1, September 12, 2011.
[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 1157]	IETF RFC 1157, Simple Network Management Protocol (SNMP), J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin, Simple Network Management Protocol (SNMP), May 1990.
[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 2710]	IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6, S. Deering, W. Fenner, B. Haberman, October 1999.
[RFC 2784]	IETF RFC 2784, Generic Routing Encapsulation (GRE), D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000.

- [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.
- [RFC 2863] IETF RFC 2863, The Interfaces Group MIB, K. McCloghrie, F. Kastenholz, June 2000.
- [RFC 2890] IETF RFC 2890, Key and Sequence Number Extensions to GRE, G. Dommety, September 2000.
- [RFC 3022] IETF RFC 3022, Traditional IP Network Address Translator (Traditional NAT), P. Srisuresh, K. Egevang, January 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, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), J. Case, D. Harrington, R. Presuhn, B. Wijnen, December 2002.
- [RFC 3413] IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications, D. Levi, P. Meyer, B. Stewart, December 2002
- [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, Transport Mappings for the Simple Network Management Protocol (SNMP), R. Presuhn, December 2002.
- [RFC 3419] IETF RFC 3419, Textual Conventions for Transport Addresses, M. Daniels, J. Schoenwaelder, December 2002.
- [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 4022] IETF RFC 4022, Management Information Base for the Transmission Control Protocol (TCP), R. Raghunarayan, March 2005
- [RFC 4075] IETF RFC 4075, Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6, V. Kalusivalingam, Cisco Systems, May 2005.
- [RFC 4113] IETF RFC 4113, Management Information Base for the User Datagram Protocol (UDP), B. Fenner, J. Flick, June 2005.
- [RFC 4191] IETF RFC 4191, Default Router Preferences and More-Specific Routes, R. Draves, D. Thaler, November 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 4292] IETF RFC 4292, IP Forwarding Table MIB, B. Haberman, April 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, Neighbor Discovery for IP Version 6 (IPv6), T. Narten, E. Nordmark, W. Simpson, H. Soliman, September 2007.
- [RFC 4862] IETF RFC 4862, IPv6 Stateless Address Autoconfiguration, S. Thomson, T. Narten, T. Jinmei, 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 5389] IETF RFC 5389, Session Traversal Utilities for NAT (STUN), J. Rosenberg, R. Mahy, P. Matthews, D. Wing, October 2008.
- [RFC 5494] IETF RFC 5494, IANA Allocation Guidelines for the Address Resolution Protocol (ARP), J. Arkko Ericsson, C. Pignataro, April 2009
- [RFC 5905] IETF RFC 5905, Network Time Protocol version 4: Protocol and Algorithms Specification, D. Mills, U. Delaware, J. Martin, Ed., J. Burbank, W. Kasch, June 2010.
- [RFC 5908] IETF RFC 5908, Network Time Protocol (NTP) Server Options for DHCPv6, R. Gayroud, B. Lourdelet, June 2010,
- [RFC 5942] IETF RFC 5942, IPv6 Subnet Model: The Relationship Between Links and Subnet Prefixes, H. Singh, W. Beebee, E. Nordmark, July 2010.
- [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 6298] IETF RFC 6298, Computing TCP's Retransmission Timer, V. Paxson, M. Allman, J. Chu, M. Sargent, June 2011
- [RFC 6333] IETF RFC 6333, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, A. Durand, R. Droms, J. Woodyatt, Y. Lee, August 2011.
- [RFC 6334] IETF RFC 6634, Dynamic Host-Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite, D. Hankins, T. Mrugalski, August 2011.
- [RFC 6540] IETF RFC 6540, IPv6 Support Required for All IP-Capable Nodes. W. George, C. Donley, C. Liljenstolpe, L. Howard, April 2012.
- [RFC 6633] IETF RFC 6633, Deprecation of ICMP Source Quench Messages, F. Gont, May 2012
- [RFC 6644] IETF RFC 6644, Rebind Capability in DHCPv6 Reconfigure Messages. D. Evans, R. Droms, S. Jiang, July 2012.
- [RFC 6762] IETF RFC 6762, Multicast DNS, S. Cheshire, M. Krochmal, Apple Inc., February 2013.

- [RFC 6918] IETF RFC 6918, Formally Deprecating Some ICMPv4 Message Types, F. Gont, C. Pignataro, April 2013
- [RFC 7083] IETF RFC 7083, Modification to Default Values of SOL_MAX_RT and INF_MAX_RT, R. Droms, November 2013.
- [RFC 7084] IETF RFC 7084, Basic Requirements for IPv6 Customer Edge Routers, H. Singh, W. Beebe, C. Donley, B. Stark, November 2013.
- [RFC 7597] IETF RFC 7597, Mapping of Address and Port With Encapsulation (MAP-E), O. Troan, W. Dec, X. Li, C. Bao, S. Matsushima, T. Murakami, T. Taylor, July 2015.
- [RFC 7598] IETF RFC 7598, DHCPv6 Options for Configuration of Software Address and Port-Mapped Clients, T. Mrugalski, O. Troan, I. Farrer, S. Perreault, W. Dec, C. Bao, L. Yeh, X. Deng, July 2015.
- [RFC 7599] IETF RFC 7599, Mapping of Address and Port Using Translation (MAP-T), X. Li, C. Bao, W. Dec, O. Troan, S. Matsushima, T. Murakami, July 2015
- [TR-064] TR-064 LAN-Side DSL CPE Configuration Specification, May 2004, Broadband Forum Technical Report.
- [TR-069] TR-069 CPE WAN Management Protocol v1, Issue 1 Amendment 5, November 2013, 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-181] TR-181 Device Data Model for TR-069, Issue 2 Amendment 8, November 2013, Broadband Forum Technical Report.
- [WIFI-GW] Wi-Fi Requirements for Cable Modem Gateways, WR-SP-WiFi-GW-I05-150515, May 15, 2015, Cable Television Laboratories, Inc.

2.1.3 Published Materials

- No informative references are applicable.

2.2 Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

2.2.1 SCTE References

- No informative references are applicable.

2.2.2 Standards from Other Organizations

- No informative references are applicable.

- [MAP-TR] Mapping of Address and Port (MAP) Technical Report, CL-TR-MAP-V01-160630, June 30, 2016, Cable Television Laboratories, Inc.
- [MC-EMC] IP Multicast Controller-Client Interface Specification, OC-SP-MC-EMCI-102-160923, September 23, 2016, Cable Television Laboratories, Inc.
- [MR-230] TR-069 Deployment Scenarios, Issue 1, MR-230, August 2010, Broadband Forum Marketing Report.
- [RFC 793] IETF RFC 793/STD-7, Transmission Control Protocol, Postel, J., September 1981.

- [RFC 1323] IETF RFC 1323, TCP Extensions for High Performance, Jacobson, V., Braden, B., and D. Borman, May 1992.
- [RFC 2460] IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, Deering, S. and R. Hinden, December 1998.
- [RFC 3775] IETF RFC 3775, Mobility Support in IPv6, Johnson, D., Perkins, C., and J. Arkko, June 2004.
- [RFC 3828] IETF RFC 3828, The Lightweight User Datagram Protocol (UDP-Lite), Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., and G. Fairhurst, July 2004.
- [RFC 3879] IETF RFC 3859, Deprecating Site Local Addresses, C. Huitema, B. Carpenter, September 2004.
- [RFC 4007] IETF RFC 4007, IPv6 Scoped Address Architecture, Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, March 2005.
- [RFC 4193] IETF RFC 4193 Unique Local IPv6 Unicast Addresses. R. Hinden, B. Haberman, October 2005.
- [RFC 4302] IETF RFC 4302, IP Authentication Header, Kent, S., December 2005.
- [RFC 4303] IETF RFC 4303, IP Encapsulating Security Payload (ESP). S. Kent. December 2005.
- [RFC 4340] IETF RFC 4340, Datagram Congestion Control Protocol (DCCP), Kohler, E., Handley, M., and S. Floyd, March 2006.
- [RFC 4960] IETF RFC 4960, Stream Control Transmission Protocol, Stewart, R., September 2007.
- [RFC 5095] IETF RFC 5095, Deprecation of Type 0 Routing Headers in IPv6, Abley, J., Savola, P., and G. Neville-Neil, December 2007.
- [RFC 5156] IETF RFC 5156, Special-Use IPv6 Addresses, Blanchet, M., April 2008.
- [RFC 5201] IETF RFC 5201, Host Identity Protocol, Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, April 2008.
- [RFC 5382] IETF RFC 5382, NAT Behavioral Requirements for TCP, Guha, S., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, October 2008.
- [RFC 5625] IETF RFC 5625, DNS Proxy Implementation Guidelines, R. Bellis, August 2009.
- [RFC 5996] IETF RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, September 2010.
- [TR-106a5] TR-106 Data Model Template for TR-069-Enabled Devices, Issue 1, Amendment 5, November 2010, Broadband Forum Technical Report.
- [WIFI MGMT] Wi-Fi Provisioning Framework Specification, WR-SP-WiFi-MGMT-I07-160512, May 12, 2016, Cable Television Laboratories, Inc.
- [eRouter] IPv4 and IPv6 eRouter Specification, CM-SP-eRouter-I19-160923, September 23, 2016, Cable Television Laboratories, Inc.

2.2.3 Published Materials

- No informative references are applicable.

3 TERMS AND DEFINITIONS

This standard uses the following terms:

Customer Edge Router	The Customer Edge Router (CER) role provides specific services and forwarding capabilities necessary for establishing and maintaining the customer edge on the Operator-Facing Interface (WAN). In this role, Router application services such as DHCP, NAT and Packet Filtering Firewall are enabled.
Customer-Facing Interface	An eRouter interface used for connecting CPE devices. Defined in [RFC 7084] as a Local Area Network (LAN) Interface, the Customer-Facing Interface is represented by a physical port.
Customer-Facing IP Interface	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 7084], this is an IP LAN interface in which one or many physical ports are associated with an IP address.
Customer-Facing Logical Interface	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 7084], this is a LAN interface in which one or more physical ports are associated with a logical interface, such as a VLAN.
DNS Proxy Forwarding	A mechanism in which the DNS queries of the LAN clients are proxied by the eRouter before being transmitted to the service provider's DNS servers that the eRouter learned during DHCP.
Down Interface	An interface on a router that is further away from the ISP network than the 'Up' interface on that same router. See Up Interface.
eRouter	An eSAFE device that is implemented in conjunction with the DOCSIS embedded cable modem.
Hard Reset	Describes a full reset of the eDOCSIS device and its constituent eSAFE application elements (such as the eRouter) and embedded CM.
Internet Gateway Device	A remotely managed gateway device as defined in CPE WAN Management Protocol [TR-069].
Link ID	16 bits of both IPv4 and IPv6 addresses chosen to uniquely identify each "link" or LAN segment (Customer-Facing IP Interface) within the home network. Counting from the left, the Link ID includes bits 49 - 64 (fourth 16-bit block) in an IPv6 address and bits 9 - 24 (middle two octets) in an IPv4 address.
Multicast Subscription Database	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.
Operator-Facing Interface	The eRouter interface that is connected to the Embedded cable modem. As defined in [RFC 7084], this is a Wide Area Network (WAN) interface. In CPE WAN Management Protocol (CWMP) this is called an upstream interface.
Operator-Facing IP Interface	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 7084], this is a WAN interface.
Prefix	A common address component, which defines a portion of a network. The meanings of the terms Prefix and Subnet are interchangeable. The term Prefix is favored in this document. See also Prefix Delegation.

Prefix Delegation	Prefix Delegation is a form of IPv6 address assignment allowing the operator's DHCP server to delegate a prefix of a specific length, such as /56, to a customer's Router. The delegation of one or more prefixes allows the Router to further sub-divide and assign individual prefixes (which are /64 in length) to its interfaces and/or provide prefix sub-delegation to additional Routers within the customer's network. Prefix Delegation occurs only between the operator's DHCP server and a Router operating in the role of Customer Edge Router (CER). See also Customer Edge Router.
Reset	Describes a routine in which the operational state is interrupted by the instruction to shut down and restart. The term is synonymous with the terms re-initialization and reboot. The term can describe either a full device reset (a Hard Reset) or the re-initialization of an individual eSAFE's software application (a Soft Reset) and any associated routines necessary to notify connected clients or other nodes of the device becoming temporarily unavailable.
Service Discovery	A set of protocols and methods that are used to discover services that are made available by hosts and nodes within the customer network.
Soft Reset	Describes a reset operation in which the software layer of the eRouter eSAFE application is re-initialized without impacting other eSAFEs or the embedded CM within an eDOCSIS device.
Subnet	A portion of a network that shares a common address component. The meanings of the terms Prefix and Subnet are interchangeable. The term Prefix is favored in this document.
TR-069	Term used to refer to the CPE WAN Management Protocol suite defined in [TR-069].
TR-069 CPE	Term used to refer to the CPE managed using the CPE WAN Management Protocol suite defined in [TR-069].
Up Interface	A router interface that connects to another router that is closer to the ISP network. For example, the 'Up Interface' of an Internal router is the port used to connect to the CFI (down interface), of the eRouter. See Down Interface.

4 ABBREVIATIONS AND ACRONYMS

This standard uses the following abbreviations:

ACS	Auto-configuration Server
AFTR	Address Family Translation Router
AH	Authentication Header
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
B4	Basic-Bridging BroadBand
BCP	Best Current Practice
BMR	Basic Mapping Rule
BR	Border Relay
CER	Customer Edge Router
CER-ID	Customer Edge Router-Identification
CM	Cable Modem
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment (includes internal routers)
CWMP	CPE WAN Management Protocol
DAD	Duplicate Address Detection
DCCP	Datagram Congestion Control Protocol
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Service
DUID	DHCP unique identifier
DUID-EN	DUID Enterprise Number
DUID-LL	DUID Link Layer address
DUID-LLT	DUID Link Layer plus Time
EA	Embedded Address
EAE	Early Authentication and Encryption
eCM	embedded Cable Modem
eSAFE	Embedded Service/Application Functional Entity
ESP	Encapsulating Security Protocol
EUI	Extended Unique Identifier
FMR	Forwarding Mapping Rule
FTP	File Transfer Protocol
GNAP	Global Network Address Port

GRE	Generic Route Encapsulation
GUA	Global Unique Address
IA_NA	Identity Association for Non-temporary Addresses
IA_PD	Identity Association for Prefix Delegation
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identifier
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRT	Initial Retransmission Times
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAP-E	Mapping of Address and Port (Encapsulation)
MAP-T	Mapping of Address and Port (Translation)
mDNS	Multicast Domain Name System
MIB	Management Information Base
MLD	Multicast Listener Discovery
MoCA	Multimedia over Coax Alliance
MRC	Maximum Retransmission Count
MRD	Maximum Retransmission Duration
MRT	Maximum Retransmission Time
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAPT	Network Address Port Translation
NAT	Network Address Translation
ND	Neighbor Discovery
NTPv4	Network Time Protocol version 4
OID	Object ID
ORCHIDv2	Overlay Routable Cryptographic Task Identifiers version 2
ORO	Option Request Option (DHCP)

OUI	Organization Unique Identifier
PD	Prefix Delegation
PIO	Prefix Information Option
PNAP	Private Network Address Port
QoS	Quality of Service
RA	Router Advertisement
RD	Router Discovery
RFC	Request For Comment
RG	Residential Gateway
RIO	Router Information Option
RS	Router Solicitation
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
SLAAC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSDP	Simple Service Delivery Protocol
TCP	Transmission Control Protocol
TLV	Type/Length/Value
ToS	Type of Service
TTL	Time To Live
UDP	User Datagram Protocol
ULA	Unique Local Addresses
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WAN	Wide Area Network

5 THEORY OF OPERATION

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

This standard defines a set of features for an eRouter that is in one of three protocol enabled modes: IPv4 protocol enabled, IPv6 protocol enabled, or dual protocol enabled.

The figures below depict implementations of an eDOCSIS eRouter device in each of the three enabled modes.

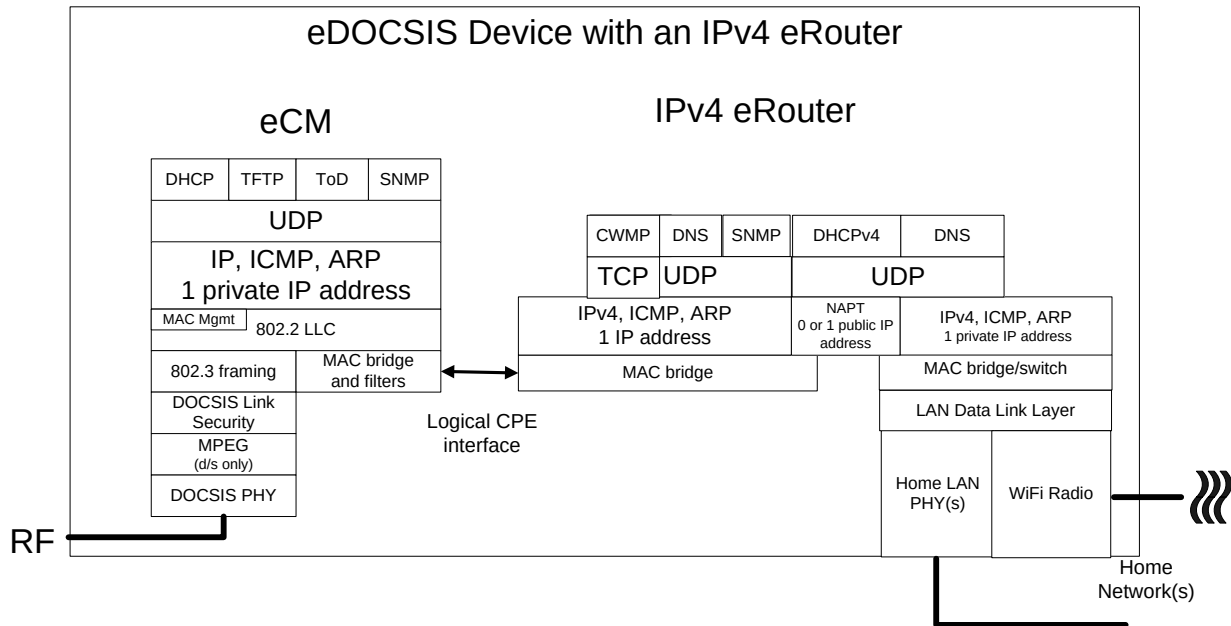


Figure 5-1 - Logical Components of an eDOCSIS device with an IPv4 Protocol Enabled eRouter

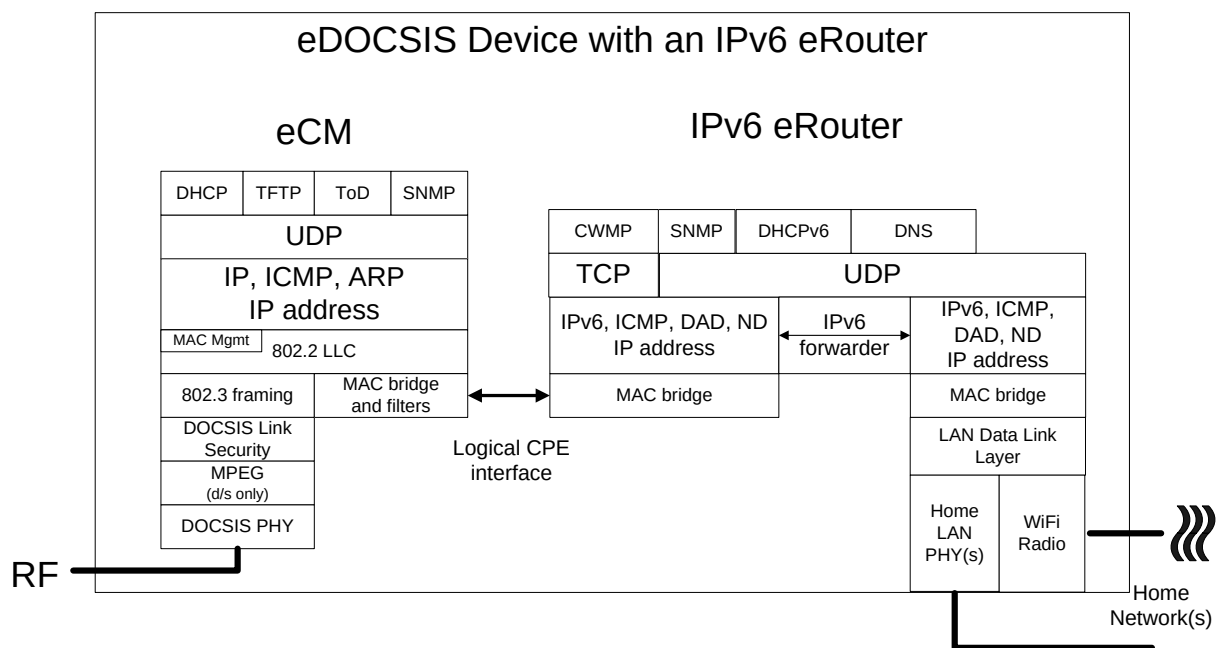


Figure 5-2 - Logical Components of an eDOCSIS device with an IPv6 Protocol Enabled eRouter

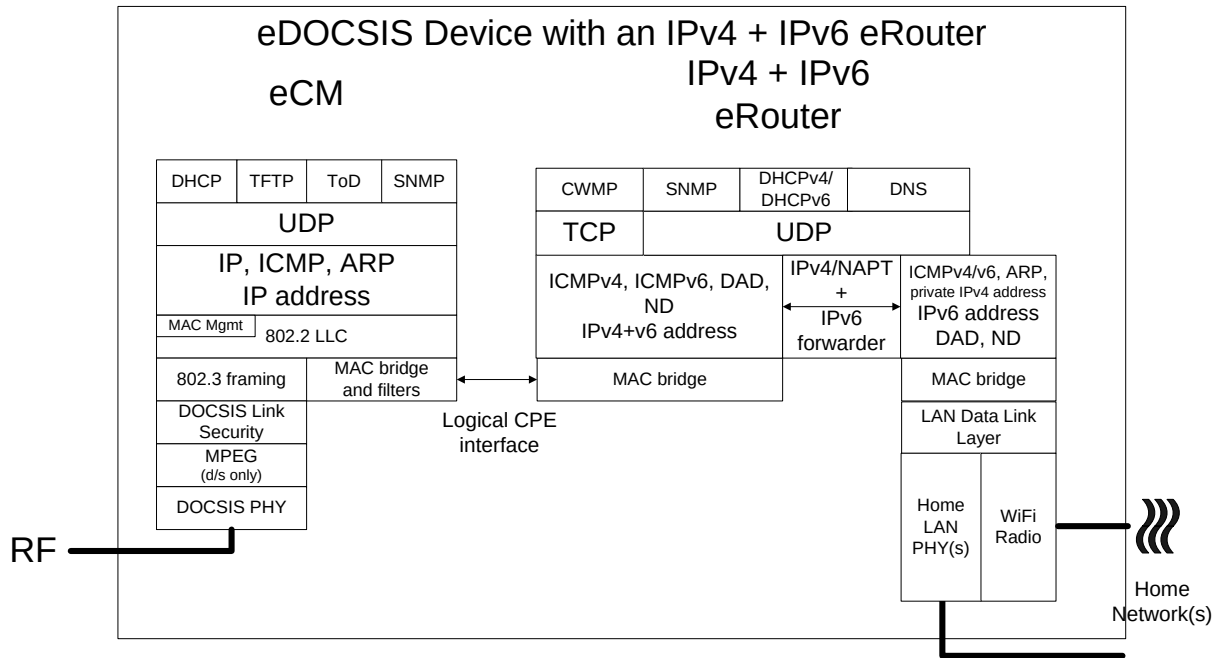


Figure 5-3 - Logical Components of an eDOCSIS device with a Dual Protocol Enabled eRouter

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 IP 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 IP Protocols are enabled, the eRouter allows provisioning of IPv4 CPEs, IPv6 CPEs, or both IPv4 and IPv6 CPEs simultaneously.

This standard defines the core set of functions that are performed by the eRouter; however, in most implementations, vendors include additional features and functionality that enhance the eRouter device.

The standard defines: a) CPE provisioning with IPv4 and IPv6 addresses, b) IPv4 data forwarding with and without NAPT 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.

The eRouter specification defines two methods that an eRouter uses when assigning IP Addresses to Customer Facing Interfaces. The methods are Link-ID and non Link-ID. Both methods implement IPv4 addressing using RFC-1918 IPv4 address ranges, but in different ways.

The method, called Link-ID, provides a predictable IPv4 addressing scheme, where IPv6 link bits are reflected in IPv4 octets 2 and 3, and enabling native IPv4 routing within the home. This functionality allows for routing across multiple routers without the need for routing protocols or multiple routers running NAPT.

However, if Link-ID is not enabled or an IPv6 prefix is not available from which to generate a Link-ID, then IPv4 routing across multiple routers will not be possible without manual configuration.

One overall goal is that after a reset or reboot, CFI IPv4 addressing should follow the address scheme implemented by the eRouter before the reset/reboot event.

Another overall goal is to bring up the IPv4 LAN interfaces quickly after reboot/reset/power-cycle to provide some LAN functionality even if the OFI is non-operational for any reason.

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

This standard defines requirements for an eRouter device with a single Operator-Facing IP Interface. This standard defines requirements for an eRouter device with a single one or more Customer-Facing logical IP Interfaces that are not necessarily mapped one-to-one with the number of Customer-Facing ports on the eRouter.

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

5.1 eDOCSIS eRouter and TR-069 Architecture

This section defines TR-069 requirements for the eRouter management architecture, which are derived from the [eDOCSIS] specification.

The TR-069 specification suite defines the Device 2.x entity in [TR-181]. 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 [MULPIv3.0] and [eDOCSIS]. Only devices attached to the Customer-Facing Interfaces of a cable modem are termed CPEs in [MULPIv3.0] 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; that is, the eRouter eSAFE is considered to be a 'CPE' under both the DOCSIS and TR-069 definitions, whereas the eCM is not. However, in this specification the eSAFE term is used when referring to the eRouter.

The main differences between both architectures are:

- A TR-069 Device 2.x [TR-181] 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-181]. In Figure 5-4, the stack layers are seen as interfaces per [TR-181], physical interfaces (e.g., Ethernet, SSID, WiFi Radio), bridges, ports, Bridges, Ethernet Link 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.

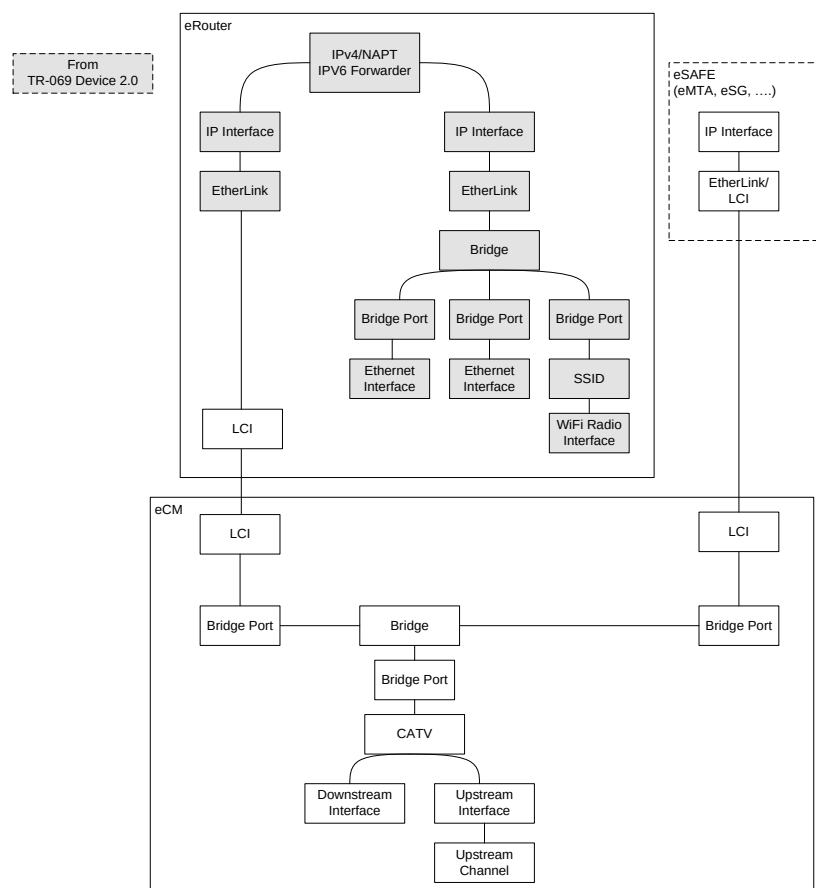


Figure 5-4 - TR-069 Interface Model Applied to eDOCSIS eRouter

5.2 eRouter Device Management

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.

eRouter eSAFEs can be modeled as a stack of interfaces, and, in the future, other eSAFEs might support TR-069 protocol. This standard 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 standard and within the scope of [eDOCSIS].

5.3 Service Discovery

Service discovery will allow devices with services to announce their presence and allow a query / response method for discovering and choosing a service from a list of possible candidates that provide that service. An example is a network-based printer, mDNS, as defined in [RFC 6762], and UPnP, as defined by the UPnP forum and specified in [ISO/IEC 29341] are used to implement Service Discovery in the eRouter.

5.3.1 mDNS (multicast Domain Name System)

The mDNS protocol provides both an announcement and a query / response mechanism to provide a list of devices that offer services on the home network. The mDNS protocol is link-scoped only but can be enhanced to provide service to multiple networks in the home. Therefore, a method to relay announcements and queries/responses between different networks is needed. The requirements to accomplish this are listed in the sections for IPv4 and IPv6 Service Discovery implementation.

The eRouter will take an announcement, query or response packet from one link/subnet and relay it onto another link/subnet but replace the IP source address from the originating link/subnet with the eRouter's egress IP address on the other link/subnet. Additionally, if the payload of the mDNS packet contains a link-local or Auto-IP resource record, those address records will be removed before the packet is placed onto the new link/subnet.

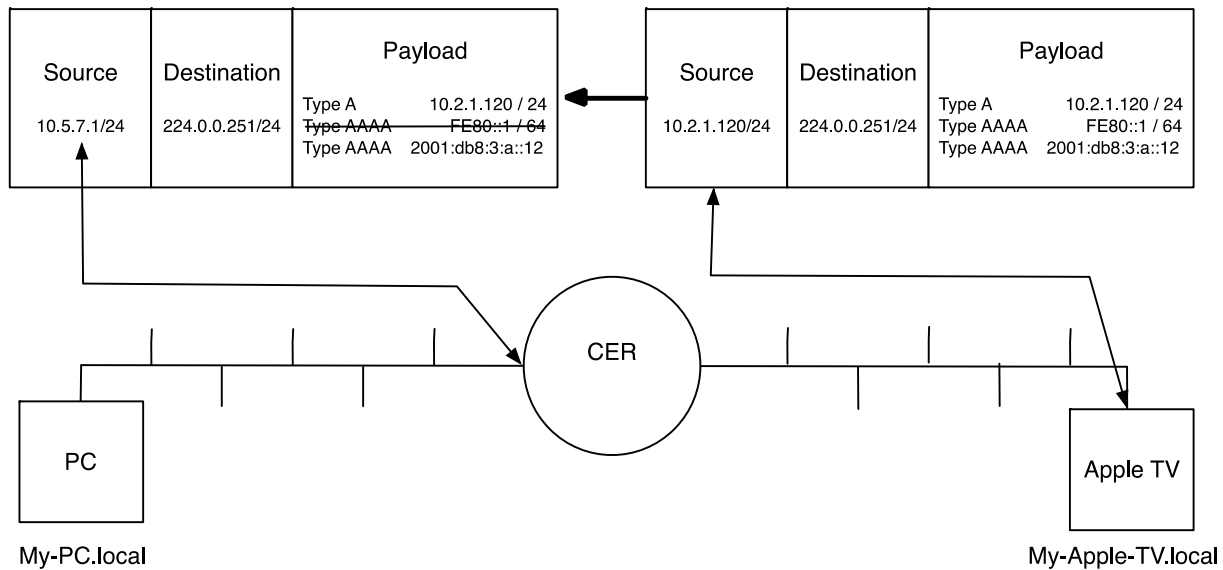


Figure 5-5 - mDNS Source IP and Payload Changes Going Through a Router

Hosts implementing the mDNS protocol might silently discard any frame with a source IP address that is not part of the receiver's network. When the eRouter receives a packet with an address that is not on the receiver's network, the eRouter **MUST** replace the source address in the packet with the IP address of the eRouter's egress interface to the receiver's network. This ensures that the packet is properly relayed to other hosts and not dropped by the host.

mDNS forwards as described above to multicast addresses (FF02::FB and 224.0.0.251).

The eRouter will not keep state information, but simply relays the packet and make the appropriate changes to the IP source address and payload.

5.3.2 UPnP (Universal Plug and Play)

The UPnP architecture makes use of a number of protocols including IP, TCP, UDP, HTML, and XML to enable peer-to-peer networking and service discovery. Most of the protocols used by UPnP will function across network segments in the home network. The one exception and the focus of this section is the UPnP Device Discovery Protocol, which uses the Simple Service Discovery Protocol (SSDP). UPnP was designed to function in an unmanaged network environment by having UPnP controllers (control points) automatically discover UPnP devices. SSDP is used by UPnP controllers to search for UPnP devices and is also used by UPnP devices to announce themselves and their services to UPnP controllers.

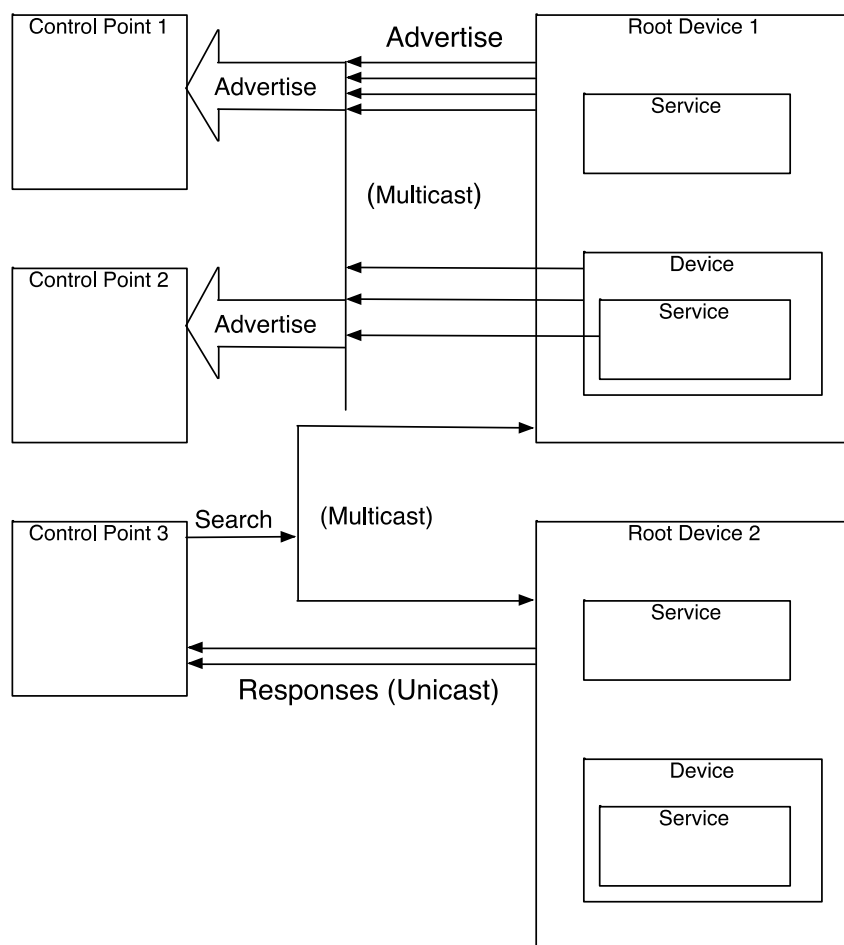


Figure 5-6 - UPnP General Architecture

UPnP forwards as described above to multicast addresses (FF02::C, FF05::C, FF02::130 and 239.255.255.250). eRouter is expected to forward to the site scoped address only.

The eRouter should not forward or listen for SSDP messages, for either IPv4 or IPv6, on the Operator Facing interface. IPv6 support was added to the [ISO/IEC 29341] in annex A.

5.4 CER-ID (Customer Edge Router – Identification)

A home network may contain one or more edge routers and one or more internal routers providing connectivity to home devices. An eRouter, by default, demarcates the edge of the customer network and provides a method to assist internal routers in determining which device(s) reside at the edge of the customer network using a DHCPv6 CER-ID option encoding. The CER-ID is a 128-bit string that is usually set to an IPv6 interface address that is reachable on the customer LAN, though other values can be set to establish the role of the edge router.

It is desirable to have services such as firewall functions and NAT/NAPT employed by the device(s) at the edge of the home network and not by other internal routers.

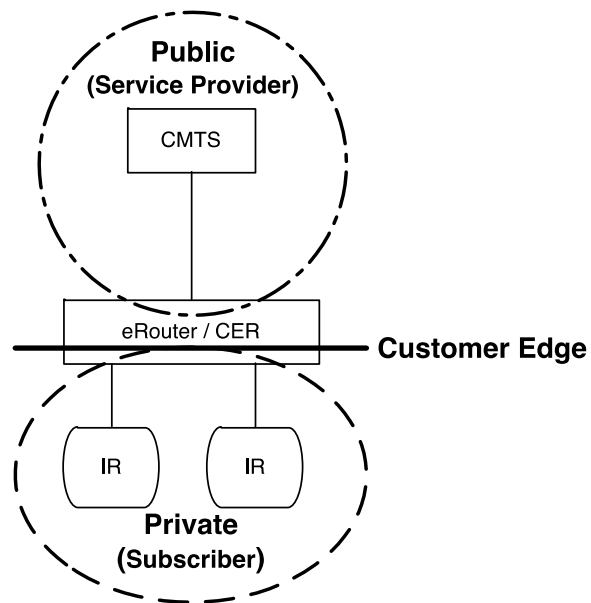


Figure 5-7 - Example of a CER Demarcation Boundary

6 eROUTER INITIALIZATION

The eRouter operates in any one of three possible modes – 'IPv4 Protocol Enabled', 'IPv6 Protocol Enabled', or 'Dual IP Protocol Enabled', as summarized in Table 6-1. The eRouter can also be set to 'Disabled', which turns the eRouter into a bridging device. The eRouter MUST support all three modes of operation, and the ability to be set to 'Disabled'. The eRouter MUST default to 'Dual IP Protocol Enabled' mode in conformance with [RFC 6540].

The eRouter Mode is controlled via the eRouter Initialization Mode Encoding, the eRouter Initialization Mode Override Encoding and the `esafeErouterInitModeControl` object, all defined in Annex B. Prior to its initialization, the eRouter is enabled or disabled through the eRouter Initialization and eRouter Initialization Mode Override encodings in the cable modem configuration file. The `esafeErouterInitModeControl` object is used to change (override) the eRouter Mode after eRouter initialization completes. The eRouter ignores the `esafeErouterInitModeControl` object if it is present in a DOCSIS cable modem configuration file.

There are two means of overriding the eRouter Initialization Mode Encoding, the eRouter Initialization Mode Override Encoding and the `esafeErouterInitModeControl` object.

The `esafeErouterInitModeControl` object is used to change the eRouter Mode after the eRouter has initialized. Whenever the value of `esafeErouterInitModeControl` is changed from the default of `honoreRouterInitMode(5)` via an SNMP SET, the eRouter MUST override the eRouter Initialization Mode encoding encapsulated in the eCM configuration file and use the value of the `esafeErouterInitModeControl`.

For an eRouter which has been set to 'Disabled', the eRouter Initialization Mode Override Encoding is used to force the eRouter to remain 'Disabled' and ignore the value of the eRouter Initialization Mode TLV. If the eRouter is 'Disabled' and the `esafeErouterInitModeControl` object is set to `honoreRouterInitMode(5)`, the eRouter MUST follow the eRouter Initialization Mode Override Encoding to determine whether it is to continue to remain 'Disabled' or whether it is to obey the eRouter Initialization Mode Encoding. If the eRouter is not 'Disabled' or the `esafeErouterInitModeControl` object is not set to `honoreRouterInitMode(5)`, the eRouter MUST ignore the eRouter Initialization Override Encoding.

The eRouter MUST evaluate Initialization Mode configuration controls in the following order of precedence:

1. The stored `esafeErouterInitModeControl` object written via an SNMP management station SET prior to a reset,
2. The eRouter Initialization Mode Override [TLV 202.3 in the cable modem configuration file],
3. eRouter Initialization Mode [TLV 202.1 in the cable modem configuration file].

The eRouter MUST persist its initialization mode across reinitializations. The eRouter MUST permit an SNMP SET to the `esafeErouterInitModeControl` object upon completing initialization via the TLV encodings.

When the eRouter is 'Disabled', the eRouter MUST NOT enable either IPv4 or IPv6 services or route IP between the Customer-Facing Interfaces and Operator-Facing Interfaces. When the eRouter is 'Disabled', it transparently bridges all traffic directly between its Customer-Facing Interfaces and its Operator-Facing Interface. When configured in this way, it will appear 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. When configured as 'Disabled', the eRouter specification becomes irrelevant – the interfaces become part of the cable modem. All behavior will occur according to the DOCSIS specifications.

When the eRouter is in 'IPv4 Protocol Enabled' mode, the eRouter performs IPv4 provisioning as described in Section 7 and IPv4 data forwarding and NAT according to Section 9. The eRouter operating in 'IPv4 Protocol Enabled' mode does not perform any IPv6 provisioning. When the eRouter is in 'IPv4 Protocol Enabled' mode, the eRouter MUST NOT forward IPv6 traffic between the Operator-Facing Interface and the Customer-Facing Interfaces.

When the eRouter is in 'IPv6 Protocol Enabled' mode, the eRouter performs IPv6 provisioning according to Section 8 and IPv6 data forwarding according to Section 10. The eRouter operating in 'IPv6 Protocol Enabled' mode does not perform any IPv4 provisioning. When the eRouter is in 'IPv6 Protocol Enabled' mode, the eRouter MUST NOT forward IPv4 traffic between the Operator-Facing Interface and the Customer-Facing Interfaces.

When the eRouter is in 'Dual IP Protocol Enabled' mode, the eRouter performs IPv4 provisioning as described in Section 7 and IPv6 provisioning according to Section 8. Once an eRouter in 'Dual IP Protocol Enabled' mode acquires an IPv4 address per Section 7, the eRouter performs IPv4 data forwarding and NAPT according to Section 9. Once an eRouter in 'Dual IP Protocol Enabled' mode acquires an IPv6 address and prefix per Section 8, the eRouter performs IPv6 data forwarding according to Section 10.

When the eRouter is enabled in any of the IP Protocol Enabled Modes, the eRouter **MUST** forward IP traffic between the Customer-Facing Interfaces, regardless of which IP Protocol Mode is enabled.

Table 6-1 provides a summary of the eRouter behavior based upon the configured mode of operation as well as when it is 'Disabled'.

Table 6-1 - eRouter Modes

Mode	IPv4	IPv6
Disabled	Disables the eRouter resulting in a bridge. No IPv4 provisioning. CM bridges all traffic per [MULPIv3.0] spec.	Disables the eRouter resulting in a bridge. No IPv6 provisioning. CM bridges all traffic per [MULPIv3.0] spec.
IPv4 Protocol Enabled	IPv4 Provisioning (Section 7). IPv4 data forwarding using NAPT (Section 9).	No IPv6 provisioning. No IPv6 data forwarding between Operator-Facing Interface and the Customer-Facing Interfaces.
IPv6 Protocol Enabled	No IPv4 provisioning. No IPv4 data forwarding between Operator-Facing Interface and the Customer-Facing Interfaces.	IPv6 Provisioning (Section 8). IPv6 data forwarding (Section 10).
Dual IP Protocol Enabled	IPv4 Provisioning (Section 7). IPv4 data forwarding using NAPT (Section 9).	IPv6 Provisioning (Section 8). IPv6 data forwarding (Section 10).

6.1 Network Time Protocol

Network Time Protocol version 4 is used to provide time synchronization to the eRouter from one or more master servers. Such time synchronization is essential for correlating events in the eRouter's local log, and for providing accurate time for features that while not explicitly defined in eRouter are commonplace in current implementations. These features and applications include content/parental controls, video content controls for such features as IP video and Digital Video Recorder, voice applications such as caller ID and voicemail notification and similar applications that rely on a standard time reference to perform specific actions.

If the eRouter supports NTPv4, its implementation will be guided by [RFC 5905] with the following exceptions:

- The eRouter **MUST** act as a client per section 2, Modes of Operation.
- The eRouter **MUST** support a minimum of three NTP servers in the NTP server list.
- The eRouter **MAY** act as a server for other clients per section 2, Modes of Operation.
- The eRouter **MUST** support the client/server protocol mode per section 3, Protocol Modes.
- The eRouter **MAY** support the broadcast protocol mode of NTPv4 per section 3, Protocol Modes, with the provision that a filtering mechanism is provided to prevent security vulnerabilities as described in section 15, Security Considerations.
- The eRouter **MAY** support dynamic server discovery via multicast or manycast mechanisms per section 3.1, Dynamic Server Discovery.
- The eRouter **MAY** support the SNTP protocol per section 14, Simple Network Time Protocol.

6.2 DNS Proxy Forwarding

DNS proxy forwarding functionality provides a means by which LAN clients using DHCP can obtain one or more of the eRouter's LAN addresses as the DNS server that will handle queries. The LAN of the eRouter is assumed to be dual stack for the purpose of the DNS proxy forwarding requirements.

The eRouter implements a DNS proxy forwarding agent that is controlled by a MIB object when the eRouter is in 'Dual Protocol Enabled' mode. An eRouter in 'IPv6 Protocol Enabled' mode will always provide DNS proxy forwarding, whereas an eRouter in 'IPv4 Protocol Enabled' mode will not provide DNS proxy forwarding as defined in this specification.

When operating in a 'Dual Protocol Enabled' mode, the DNS proxy forwarding agent performs transport layer re-encapsulation of IPv4 DNS queries for transmission across an IPv6 network when the MIB object 'dnsIpv6QueryForDualProtocolEnabled' is set to 'true'. The eRouter MUST NOT change the transport protocol (e.g., UDP, TCP) of the DNS query, nor modify the contents of the query consistent with the principles of transparency as described in [RFC 5625]. The default value of the MIB attribute 'dnsIpv6QueryForDualProtocolEnabled' is 'true.' The list below describes the DNS proxy forwarding requirements when the eRouter is in Dual Protocol Enabled mode and an IPv4 DNS query is targeted to an eRouter customer-facing interface:

- Whenever an eRouter has successfully completed DHCPv4 and DHCPv6 address acquisition, it MUST perform proxy forwarding of all IPv4 sourced DNS query types over the IPv4 protocol when the value of 'dnsIpv6QueryForDualProtocolEnabled' is set to 'false'. See Annex A.5.
- Whenever an eRouter has successfully completed DHCPv4 and DHCPv6 address acquisition, it MUST perform proxy forwarding of all IPv4 sourced DNS query types over the IPv6 protocol when the value of 'dnsIpv6QueryForDualProtocolEnabled' is set to 'true'. See Annex A.5.
- Whenever an eRouter receives an IPv4 sourced DNS query on its Customer Facing IP Interface, its DNS proxy forwarding agent MUST re-encapsulate and perform proxy forwarding of the IPv4 datagram containing the DNS query into an IPv6 datagram for transmission across the network when 'dnsIpv6QueryForDualProtocolEnabled' is set to 'true'.

The list below describes the DNS proxy forwarding requirements when the eRouter is in 'IPv6 Protocol Enabled' mode as follows.

- Whenever an eRouter has successfully completed DHCPv6 address acquisition, it MUST perform DNS proxy forwarding of all IPv4 sourced DNS query types over the IPv6 protocol regardless of the setting of the 'dnsIpv6QueryForDualProtocolEnabled' attribute. See Annex A.5.

For further information on DNS forwarding behaviors, please refer to [MAP-TR].

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 reached operational state, 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.

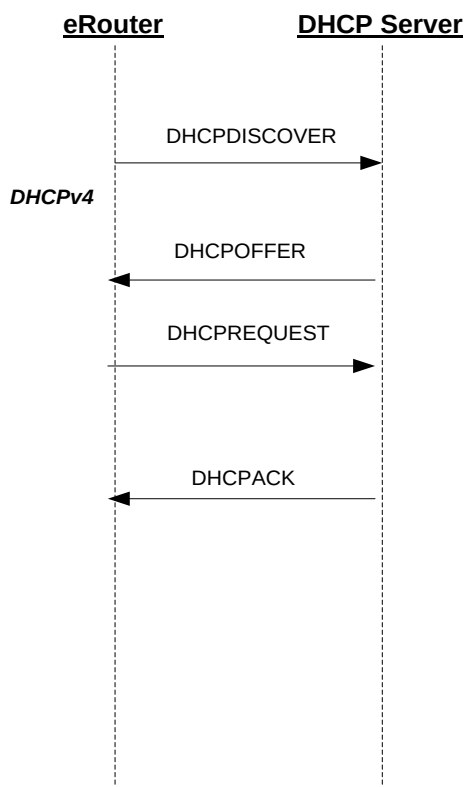


Figure 7-1 - IPv4 Provisioning Message Flow

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

Backoff Number	Minimum (sec.)	Maximum (sec.)
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.

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 42 Network Time Protocol Servers Option
 - Option code 60 (Vendor Class Identifier) [eRouter1.0]
 - Option code 43 (see [eDOCSIS])
 - Option code 55 (Parameter Request List)

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

- 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) (critical).

NOTE: The eRouter is not required to use more than one router IP address for forwarding.

- 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] (non-critical).

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

If a non-critical field is missing or invalid in the DHCPACK 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 DHCPACK 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 DHCPDISCOVER.

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

7.2 eRouter Interface Addressing Using Link-ID

The eRouter MUST support Link-ID IPv4 address generation as defined below. The eRouter Link-ID feature can be enabled by the operator using CM configuration file encapsulation of TLV 202.13 or TR-069 provisioning methods, see Annex B.4.12. By default, the Link-ID feature is disabled on the eRouter.

The eRouter MUST NOT persist Link-ID based IPv4 addressing across soft-reset or reboot. If soft-reset or reboot occurs, the eRouter waits for a valid IPv6 PD and provisioning instructions in order to enable Link-ID and generate IPv4 addresses using this algorithm. When eRouter is in dual IP protocol enabled mode and Link-ID is enabled, if there is a temporary loss of connectivity between the Operator-Facing Interface and the CMTS, then the eRouter MUST NOT modify Link-ID based IPv4 addressing. In other words, once Link-ID IPv4 addressing has been generated, the eRouter is expected to maintain this addressing until such time as the IPv6 PD changes or the eRouter is reset.

When operating in 'Dual IP Protocol Enabled' mode and Link-ID is enabled, the eRouter MUST generate a unique /24 prefix for each Customer-Facing IP Interface using the 10.0.0.0/8 aggregate prefix and the Link ID generated from the appropriate IPv6 prefix assigned to the Customer-Facing IP Interface.

A unique IPv4 prefix is created using two steps:

1. Use the decimal value 10 for the first octet,
2. Convert IPv6 Link octets to their decimal equivalents for IPv4 octets 2 and 3.

Step #2 is explained in both the following text and diagram. For example, if an eRouter assigns IPv6 prefix 2001:db8:1234:5601::/64 to a Customer-Facing IP Interface, the Link ID for that interface will be hex 5601(bits 49-64 of the IPv6 prefix). The eRouter will use this Link ID to construct the second and third octets of its /24 IPv4 prefix. The second octet for this example is decimal 86 (equivalent of 0x56, the first octet of the Link ID), and the third octet is decimal 1 (equivalent of 0x01, the second octet of the Link ID). Thus, in this example, the eRouter will assign an IPv4 prefix of 10.86.0.0/24 to the Customer-Facing IP interface. These requirements enable native routing of IPv4 without the need for a routing protocol or NAT when the eRouter is operating in Dual IP Protocol Enabled mode. Refer to the Figure 7-2 below and Annex E for further details.

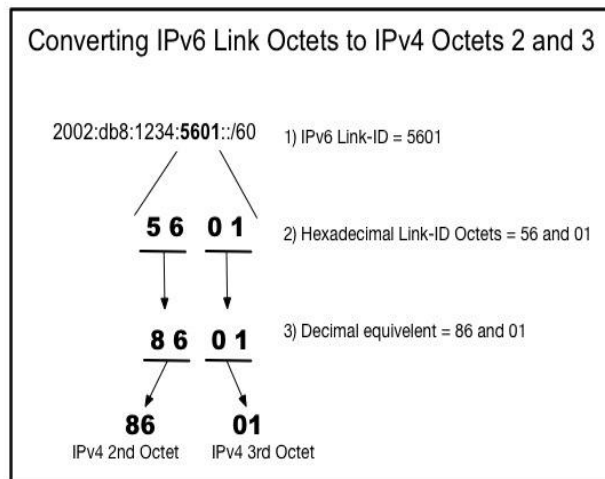


Figure 7-2 - Example Deriving IPv4 Octets 2 and 3 from an IPv6 Prefix

Using the above Link-ID example, the IPv6 address of 2001:db8:1234:5601::1/64 results in a corresponding IPv4 address of 10.86.1.1/24.

When operating in IPv4 Protocol Enabled mode or when operating in 'Dual IP Protocol Enabled' mode with Link-ID disabled, the eRouter MUST generate each unique /24 IPv4 prefix from one of the three blocks of address space reserved for private internets per [RFC 1918].

7.3 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].

7.3.1 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].

7.3.2 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.

7.3.3 DHCPv4 Server Function Requirements

eRouter Operator Facing Interface Provisioned Prefix: 2001:db8:1234:5600::/56

Customer-Facing IP Interface br(0)
 IPv6 Prefix: 2001:db8:1234:5600::/64

```
Link ID Conversion: 56 00 -> 86 00
IPv4 Network: 10.86.0.0/24 Gateway: 10.86.0.1
```

```
Customer-Facing IP Interface br(1)
IPv6 Prefix: 2001:db8:1234:5600::/64
Link ID Conversion: 56 00 -> 86 00
IPv4 Network: 10.86.1.0/24 Gateway: 10.86.1.1
```

```
Customer-Facing IP Interface br(2)
IPv6 Prefix: 2001:db8:1234:5601::/64
Link ID Conversion: 56 01 -> 86 01
IPv4 Network: 10.86.1.0/24 Gateway: 10.86.1.1
```

```
Customer-Facing IP Interface br(3)
IPv6 Prefix: 2001:db8:1234:5601::/64
Link ID Conversion: 56 01 -> 86 01
IPv4 Network: 10.86.1.0/24 Gateway: 10.86.1.1
```

```
Topology Mode Encoding: Favor Width
Calculated on 3-Bit Boundary
Calculated subdelegation prefix length: /59
Number /59 available for prefix sub-delegation: 7
-- Sub-delegated prefix: 2001:db8:1234:5620::/59
-- Sub-delegated prefix: 2001:db8:1234:5640::/59
-- Sub-delegated prefix: 2001:db8:1234:5660::/59
-- Sub-delegated prefix: 2001:db8:1234:5680::/59
-- Sub-delegated prefix: 2001:db8:1234:56a0::/59
-- Sub-delegated prefix: 2001:db8:1234:56c0::/59
-- Sub-delegated prefix: 2001:db8:1234:56e0::/59
```

Sub-delegation:

The CER in this example has (4) Customer Facing IP Interfaces - represented below as br(0) -> br(3).

Assume there are (4) IRs with one attached to each of those Customer Facing IP Interfaces of the CER.

Further assume each IR is assigned an IPv6: IA_NA and IA_PD and IPv4 address in the following way by the CER.

```
IR(0) on br(0) is assigned via DHCPv6 IA_NA = 2001:db8:1234:9a00::100 and IA_PD =
2001:db8:1234:9a20::/59 and via DHCPv4 IP Address = 10.154.0.100
IR(1) on br(1) is assigned via DHCPv6 IA_NA = 2001:db8:1234:9a01::100 and IA_PD =
2001:db8:1234:9a40::/59 and via DHCPv4 IP Address = 10.154.1.100
IR(2) on br(2) is assigned via DHCPv6 IA_NA = 2001:db8:1234:9a02::100 and IA_PD =
2001:db8:1234:9a60::/59 and via DHCPv4 IP Address = 10.154.2.100
IR(3) on br(3) is assigned via DHCPv6 IA_NA = 2001:db8:1234:9a03::100 and IA_PD =
2001:db8:1234:9a80::/59 and via DHCPv4 IP Address = 10.154.3.100
```

Route Table:

Network Destination	Next Hop	Interface

2001:db8:1234:9a20::/59	2001:db8:1234:9a00::100	br(0)
10.154.32.0/19	10.154.0.100	br(0)
2001:db8:1234:9a40::/59	2001:db8:1234:9a01::100	br(1)
10.154.64.0/19	10.154.1.100	br(1)
2001:db8:1234:9a60::/59	2001:db8:1234:9a02::100	br(2)
10.154.96.0/19	10.154.2.100	br(2)
2001:db8:1234:9a80::/59	2001:db8:1234:9a03::100	br(3)
10.154.128.0/19	10.154.3.100	br(3)

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 requirements in this section use an appropriate address space as defined in [RFC 1918], and overrides the requirements in Section 9.3.1 when using IPv4-only mode (not Dual-Stack)
- 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.
- Whenever the eRouter is in 'Dual IP Protocol Enabled' mode and the value of 'dnsIpv6QueryForDualProtocolEnabled' attribute is 'true', the eRouter's DHCP server function MUST replace the DNS server IP(s) obtained from the Service Provider's DHCP server with one or more of the eRouter's Customer-Facing IP interface addresses. The eRouter provides the DNS server list consisting of one or more of its Customer-Facing IPv4 addresses to connected clients using DHCP in order to perform DNS proxy forwarding on behalf of LAN clients. See Section 6.2.
- Whenever the eRouter is in 'Dual IP Protocol Enabled' mode and the value of 'dnsIpv6QueryForDualProtocolEnabled' attribute is 'false', the eRouter's DHCP server function provides the DNS server IP(s) obtained from the Service Provider's DHCP server to the DHCP clients on the Customer-Facing Interface as defined in this specification.

Table 7-2 - DHCPv4 Server Options

Option Number	Option Function
0	Pad
255	End
1	Subnet Mask
3	Router Option
6	Domain Name Server
42	Network Time Protocol Servers Option
50	Requested IP Address
51	IP Address Lease Time
54	Server Identifier
55	Parameter Request List