Final draft ETSI ES 204 049 V1.1.1 (2025-11)

ETSI STANDARD

Integrated broadband cable telecommunication networks (CABLE); Standalone router specification

Reference

DES/CABLE-0030

Keywords

CPE, IPCable, IPv4, IPv6, security

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This final draft ETSI Standard (ES) has been produced by ETSI Technical Committee Integrated broadband cable telecommunication networks (CABLE), and is now submitted for the ETSI Membership Approval Procedure.

Modal verbs terminology

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

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

1 Scope

The present document defines a core set of features that enables multiple subscriber devices to gain access to operator provided high-speed data service independently of the underlying access network. This core set of features allows for both IPv4- and IPv6-enabled devices to gain connectivity to the Internet. The core set of features defined in the present document 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.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

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

[1] CableLabs DHCP Options Registry Specification: "CL-SP-CANN-DHCP-Reg-I16-200715", July 15, 2020, Cable Television Laboratories, Inc.

[2] CableLabs Access Network Independent Device MIB: "CLAB-ANI-DEV-MIB".

[3] CableLabs Generic Route Encapsulation MIB: "CLAB-GRE-MIB".

[4] CableLabs Gateway MIB: "CLAB-GW-MIB".

[5] CableLabs Wireless MIB: "CLAB-WIFI-MIB".

[6] Federal Information Processing Standards Publication (FIPS PUB) 140-3: "Security, Requirements for Cryptographic Modules", March 2022.

[7] Federal Information Processing Standards Publication (FIPS PUB) 180-4: "Secure Hash Standard", August 2015.

[8] ISO/IEC 29341-1-1:2011: "Information technology -- UPnP Device Architecture -- Part 1-1: Universal Plug and Play Architecture Version 1.1", September 12, 2011.

[9] IETF RFC 792: "Internet Control Message Protocol", J. Postel, September 1981.

[10] IETF RFC 826: "An Ethernet Address Resolution Protocol", David C. Plummer, November, 1982.

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

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

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

[14] IETF RFC 1907: "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996.

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

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

[17] IETF RFC 2473: "Generic Packet Tunneling in IPv6 Specification", A. Conta, S. Deering, December 1998.

[18] IETF RFC 2710: "Multicast Listener Discovery (MLD) for IPv6", S. Deering, W. Fenner, B. Haberman, October 1999.

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

[20] IETF RFC 2827: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", P. Ferguson, D. Senie, May 2000.

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

[22] IETF RFC 2890: "Key and Sequence Number Extensions to GRE", G. Dommety, September 2000.

[23] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)", P. Srisuresh, K. Egevang, January 2001.

[24] 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. .

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

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

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

[28] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms, December 2003.

[29] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6, R. Droms", April 2004.

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

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

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

[33] IETF RFC 4191: "Default Router Preferences and More-Specific Routes", R. Draves, D. Thaler, November 2005.

[34] IETF RFC 4242: "Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", S. Venaas, T. Chown, B. Volz, November 2005.

[35] IETF RFC 4291: "IP Version 6 Addressing Architecture", R. Hinden, S. Deering, February 2006.

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

[37] IETF RFC 4293: "Management Information Base for the Internet Protocol (IP)", S. Routhier, (Editor), Bill Fenner, Brian Haberman, Dave Thaler, April 2006.

[38] IETF RFC 4301: "Security Architecture for the Internet Protocol", S. Kent, K. Seo, December 2005.

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1", T. Dierks, E. Rescorla, April 2006.

[40] IETF RFC 4347: "Datagram Transport Layer Security", E. Rescorla, N. Modadugu, April 2006.

[41] IETF RFC 4361: "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", T. Lemon, B. Sommerfeld, February 2006.

[42] 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.

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

[44] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration", S. Thomson, T. Narten, T. Jinmei, September 2007.

[45] IETF RFC 4884: "Extended ICMP to Support Multi-Part Messages", R. Bonica, D. Gan, D. Tappan, C. Pignataro, April 2007.

[46] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", T. Dierks, E. Rescorla, August 2008.

[47] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Hously, W. Polk, May 2008.

[48] IETF RFC 5389: "Session Traversal Utilities for NAT (STUN)", J. Rosenberg. R, Mahy, P. Matthews, D. Wing, October 2008.

[49] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification", D. Mills, J. Martin, J. Burbank, W. Kasch, June 2010.

[50] IETF RFC 5908: "Network Time Protocol (NTP) Server Options for DHCPv6", R. Gayroud, B. Lourdelet, June 2010.

[51] IETF RFC 5942: "IPv6 Subnet Model: The Relationship Between Links and Subnet Prefixes", H. Singh, W. Beebee, E. Nordmark, July 2010.

[52] IETF RFC 6092: "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", J. Woodyatt, Ed., January 2011.

[53] IETF RFC 6106: "IPv6 Router Advertisement Options for DNS Configuration", J. Jeong, S. Park, L. Beloeil, S. Madanapalli, November 2010.

[54] IETF RFC 6145: "IP/ICMP Translation Algorithm", X. Li, C. Bao, F. Baker, April 2011.

[55] IETF RFC 6333: "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", A. Durand, R. Droms, J. Woodyatt, Y. Lee, August 2011.

[56] IETF RFC 6334: "Dynamic Host-Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite", D. Hankins, T. Mrugalski, August 2011.

[57] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2", E. Rescorla, N. Modadugu, January 2012.

[58] IETF RFC 6540: "IPv6 Support Required for All IP-Capable Nodes", W. George, C. Donley, C. Liljenstolpe, L. Howard, April 2012.

[59] IETF RFC 6762: "Multicast DNS", S. Cheshire, M. Krochmal, Apple Inc., February 2013.

[60] IETF RFC 7083: "Modification to Default Values of SOL_MAX_RT and INF_MAX_RT, R. Droms", November 2013.

[61] IETF RFC 7084: "Basic Requirements for IPv6 Customer Edge Routers", H. Singh, W. Beebee, C. Donley, B. Stark, November 2013.

[62] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)", C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, October 2014.

[63] 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.

[64] 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.

[65] IETF RFC 2313: PKCS #1: RSA Encryption Version 1.5", March 1998.

[66] Broadband Forum Technical Report BBF TR-069: "CPE WAN Management Protocol v1: Issue 1 Amendment 6, Corrigendum 1: CPE WAN Management Protocol", June 2020.

[67] Broadband Forum Technical Report BBF TR-181: "Device Data Model for TR-069: Issue 2 Amendment 19 Corrigendum 1: Device Data Model for CWMP Endpoints and USP Agents", April 2025.

[68] ETSI ES 203 311-3: "Integrated broadband cable telecommunication networks (CABLE); Fourth generation transmission systems for interactive cable television services - IP cable modems; Part 3: MAC and upper layer protocols interface; DOCSIS® 3.1 [ANSI/SCTE 220-2 2016]", May 2019.

[69] ETSI ES 203 311-4: "Integrated broadband cable telecommunication networks (CABLE); Fourth generation transmission systems for interactive cable television services - IP cable modems; Part 4: Cable modem operations support system interface; DOCSIS® 3.1 [ANSI/SCTE 220-3 2016]", May 2019.

[70] ETSI ES 203 311-5: "Integrated broadband cable telecommunication networks (CABLE); Fourth generation transmission systems for interactive cable television services - IP cable modems; Part 5: Converged cable access platform operations support system interface; DOCSIS® 3.1 [ANSI/SCTE 220-4 2016]", May 2019.

[71] ETSI ES 203 311-6: "Integrated broadband cable telecommunication networks (CABLE); Fourth generation transmission systems for interactive cable television services - IP cable modems; Part 6: Security; DOCSIS® 3.1 [ANSI/SCTE 220-5 2016]", May 2019.

[72] Cable Television Laboratories Inc. WR-SP-WiFi-MGMT-I08-161213: "Wi-Fi Provisioning Framework Specification", December 13, 2016.

2.2 Informative references

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

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

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] BBF TR-069: "Deployment Scenarios Issue 1, MR-230", August 2010, Broadband Forum Marketing Report.

[i.2] IETF RFC 793/STD-7: "Transmission Control Protocol", J. Postel, September 1981.

[i.3] IETF RFC 1323: "TCP Extensions for High Performance", V. Jacobson, B. Braden, and D. Borman, May 1992.

[i.4] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification", S. Deering, and R. Hinden, December 1998.

[i.5] IETF RFC 3775: "Mobility Support in IPv6", D. Johnson, C. Perkins, and J. Arkko, June 2004.

[i.6] IETF RFC 3828: "The Lightweight User Datagram Protocol (UDP-Lite)", L-A. Larzon, M. Degermark, S. Pink, L-E. Jonsson, and G. Fairhurst, July 2004.

[i.7] IETF RFC 3879: "Deprecating Site Local Addresses", C. Huitema, B. Carpenter, September 2004.

[i.8] IETF RFC 4007: "IPv6 Scoped Address Architecture", S. Deering, B. Haberman, T. Jinmei, E. Nordmark, and B. Zill, March 2005.

[i.9] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses", R. Hinden, B. Haberman, October 2005.

[i.10] IETF RFC 4302: "IP Authentication Header", S. Kent, December 2005.

[i.11] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)", S. Kent, December 2005.

[i.12] IETF RFC 4340: "Datagram Congestion Control Protocol (DCCP)", E. Kohler, M. Handley, and S. Floyd, March 2006.

[i.13] IETF RFC 4960: "Stream Control Transmission Protocol, R. Stewart, September 2007.

[i.14] IETF RFC 5095: "Deprecation of Type 0 Routing Headers in IPv6", J. Abley, P. Savola, and G. Neville-Neil, December 2007.

[i.15] IETF RFC 5156: "Special-Use IPv6 Addresses", M. Blanchet, April 2008.

[i.16] IETF RFC 5201: "Host Identity Protocol", R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, April 2008.

[i.17] IETF RFC 5382: "NAT Behavioral Requirements for TCP", S. Guha, K. Biswas, B. Ford, S. Sivakumar, and P. Srisuresh, October 2008.

[i.18] IETF RFC 5996: "Internet Key Exchange Protocol Version 2 (IKEv2)", C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, September 2010.

[i.19] Broadband Forum Technical Report BBF TR-106: "Data Model Template for TR-069-Enabled Devices", Issue 1, Amendment 7", September 2013.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

access network demarcation device: access network endpoint CPE (e.g. DOCSIS CM or EPON ONU) that provides the interface(s) to the managed equipment in the customer's site

Best Current Practice (BCP): recommendation or numbered standard typically provided by the Internet Engineer Task Force (IETF)

Customer Edge Router (CER): CPE providing specific services and forwarding capabilities necessary for establishing and maintaining the customer edge on the operator-facing interface (WAN), thus, enabling sRouter application services such as DHCP, NAPT and packet filtering firewall are enabled

customer-facing interface: sRouter interface used for connecting CPE devices

NOTE: A customer-facing interface is defined in IETF RFC 7084 [61] as a Local Area Network (LAN) interface and is represented by a physical port.

customer-facing IP interface: sRouter interface in which one or many physical ports used for connecting CPE devices are associated with an IP address

NOTE 1: A customer-facing IP interface is defined in IETF RFC 7084 [61] as an IP LAN interface.

NOTE 2: A customer-facing IP interface is not necessarily mapped one-to-one with a customer-facing interface on the sRouter.

customer-facing logical interface: sRouter interface in which one or more physical ports used for connecting CPE devices are associated with a logical interface, such as a VLAN

NOTE 1: A customer-facing logical interface is defined in IETF RFC 7084 [61] as a LAN interface.

NOTE 2: A customer-facing logical interface is not necessarily mapped one-to-one with a customer-facing interface on the sRouter.

down interface: sRouter interface that is topologically further away from the operator's network than the up interface on that same router

hard reset: full reset of the device

Link-ID: 16 bits of both IPv4 and IPv6 addresses chosen to uniquely identify each link or LAN segment (on a customer-facing IP interface) within the home network

NOTE: 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: simple table of entries for the IPv4 or IPv6 Multicast Group Membership information maintained by the sRouter on respective interfaces

NOTE: Implementation details for storage of records are completely vendor-defined.

operator-facing interface: sRouter interface that is connected to the access network demarcation device such as a CM or ONU

NOTE: As defined in IETF RFC 7084 [61], this is a Wide Area Network (WAN) interface. In CPE WAN Management Protocol (CWMP) this is called an upstream interface.

operator-facing IP interface: sRouter IP interface that is provisioned with an IP address provided by the operator

NOTE: As defined in IETF RFC 7084 [61], this is a WAN interface.

prefix: common IPv4 address and IPv6 address component, which defines a portion of a network

NOTE: The meanings of the terms prefix and subnet are used interchangeably. The term prefix is favored in the present document.

Prefix Delegation (PD): 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

NOTE: 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).

reset: routine in which the operational state is interrupted by the instruction to shut down and restart

NOTE: The term is synonymous with the terms re-initialization and reboot.

Router Advertisement (RA): periodic message containing one or more of the following: prefix information including prefix lifetime, default router and other information

Router Information Option (RIO): encoding within the Router Advertisement containing next hop and default router information

Router Solicitation (RS): client message requesting the Router Advertisement

service discovery: set of protocols and methods that is used to discover services that are made available by hosts and nodes within the customer network

sRouter: standalone router conforming to the requirements in the present document intended to be network access independent with regard to provisioning and management

subnet: portion of a network that shares a common address component

NOTE: The meanings of the terms prefix and subnet are used interchangeably. The term prefix is favored in the present document.

TR-069: CPE WAN Management Protocol suite defined in BBF TR-069 [66]

TR-069 CPE: CPE managed using the CPE WAN Management Protocol suite defined in BBF TR-069 [66]

up interface: router interface that connects to another router that is closer to the ISP network

NOTE: For example, the up interface of an internal router is the port used to connect to the CFI (down interface) of the router.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACS	Auto-Configuration Server
AFTR	Address Family Translation Router
AH	Authentication Header
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
B4	Basic Bridging BroadBand
BCP	Best Current Practice
BMR	Basic Mapping Rule
BR	Border Relay
CER	Customer Edge Router
CER-ID	CER-IDentifier
CM	Cable Modem
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
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
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
GW	GateWay
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
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
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
NAPT	Network Address Port Translation
NAT	Network Address Translation
ND	Neighbor Discovery
NS	Neighbor Solicitation
NTPv4	Network Time Protocol version 4
OID	Object IDentifier
ONU	Optical Network Unit
ORCHIDv2	Overlay Routable Cryptographic Task IDentifiers version 2
ORO	Option Request Option (DHCP)
OUI	Organization Unique Identifier
PD	Prefix Delegation
PDU	Protocol Data Unit
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
sRouter	standalone Router
SSDP	Simple Service Delivery Protocol
TCP	Transmission Control Protocol
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

4 Theory of operation

4.1 General functions

The present document defines the following:

a) The provisioning of the IP-enabled modes of the sRouter.

b) The sRouter serving as a Customer Edge Router.

c) The provisioning of the CPE devices with IPv4 and IPv6 addressing.

d) IPv6 data forwarding, as well as IPv4 data forwarding with and without NAPT.

e) IP multicast traffic forwarding.

f) The preservation of IP QoS markings applied to IP data forwarded to and from the CPE devices.

g) GRE tunnel configuration and management.

h) Service discovery.

The present document defines requirements for an sRouter device with a single operator-facing IP interface and one or more customer-facing IP interfaces. The sRouter makes use of TR-069 [66] CWMP for its operator-facing management interface options for the provisioning and management of the sRouter. In addition, the present document defines configuration and monitoring via SNMP. However, SNMP configuration is distinguished from TR-069 [66] in that SNMP SET PDUs can only be sent after the sRouter has become operational.

The present document defines two methods that the sRouter uses to assign IP addresses to its customer-facing interfaces. These two methods include Link-ID and non-Link-ID addressing schemes. Both methods implement IPv4 addressing using IPv4 address ranges as defined in IETF RFC 1918 [15], but only the Link-ID method uses an algorithm to derive a unique IPv4 subnet to support multiple routers within the customer LAN. Link-ID provides a predictable IPv4 addressing scheme, where the IPv6 link bits obtained during IPv6 prefix acquisition are reflected in IPv4 octets 2 and 3, and enabling native IPv4 routing within the customer network. This functionality allows for routing across several routers without routing protocols or the encumbrance of two or more layers of 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 unless the sRouter is manually configured.

The primary functions provided by the sRouter defined by the present document include connecting multiple customer CPE devices to the operator's high-speed Internet service, and provides essential network application services to support the customer's LAN. The sRouter is delegated the responsibility of provisioning CPE devices in the customer's LAN, acting in the role of the Customer Edge Router (CER). Typical network services provided by the sRouter include DHCP, packet filtering firewall, and NAPT.

In addition, the sRouter is configured to support IPv4 only, IPv6 only and simultaneous IPv4/IPv6 operator-facing IP interfaces as defined in table 1. By default, the sRouter assumes Dual Protocol Enabled mode operation in the absence of explicit provisioning information to the contrary.

Table 1: IP-enabled modes

IP-enabled mode	Forwarding behavior
IPv4 Protocol Enabled mode	IPv4 route forwarding
IPv6 Protocol Enabled mode	IPv6 route forwarding
Dual IP Protocol Enabled mode	Both IPv4 and IPv6 route forwarding

4.2 Operational use cases

4.2.1 Introduction

Clause 4.2 describes the use cases for the sRouter when operating in a layer 3 forwarding mode. In each of the operational use cases, the following assumptions also apply:

- Community Wi-Fi™ support, provisioning and management of the public and private SSIDs.

4.2.2 sRouter as the Customer Edge Router (CER)

This use case is characterized by a single sRouter providing services and traffic forwarding within the customer's network core over a single, operator managed access network. A single sRouter operates as the Customer Edge Router, which provides GRE tunnel origination to the operator's Wi-Fi core for Community Wi-Fi services, Internet services, DHCP, packet filtering firewall and, depending on the specific IP-enabled mode, NAPT services. It is assumed that a single IA_PD is assigned by the operator with sufficient length to allow the router to assign prefixes to interfaces.

NOTE: Community Wi-Fi SSIDs are under the control of the operator's Wi-Fi core, not the sRouter.

Table 2: sRouter network roles

sRouter role in the network	Associated functions and services
Customer Edge Router (CER)	IPv4 services: • Layer 3 forwarding • NAPT • DHCPv4 • Packet filtering firewall • DNS forwarding IPv6 Services: • Layer 3 forwarding • DHCPv6 • DHCP-PD • Packet filtering firewall [52] • DNS forwarding Community Wi-Fi: • GRE tunnel origination and public/private SSID differentiation • Wi-Fi management functions, such as RADIUS AAA

4.3 TR-069 architecture

The present clause defines TR-069 [66] requirements for the sRouter management architecture.

The TR-069 [66] specification suite defines the Device 2.x data model in [67]. It refers to a CPE device management space for holding the device itself and root of other service specifications (e.g. VoIP, storage, and IPTV). See [i.1] for more details on TR-069 deployment scenarios. TR-069 is access network technology agnostic.

TR-069 [66] allows the transparent integration and management of access network technologies within the sRouter and CPE services by combining the components and their respective management data. Figure 1 is based on the "Simple Router Example (interfaces Visualized)" figure of [67]. In figure 1, the stack layers are seen as interfaces per [67], physical interfaces (e.g. Ethernet, SSID, Wi-Fi radio), bridges, and IP interfaces.

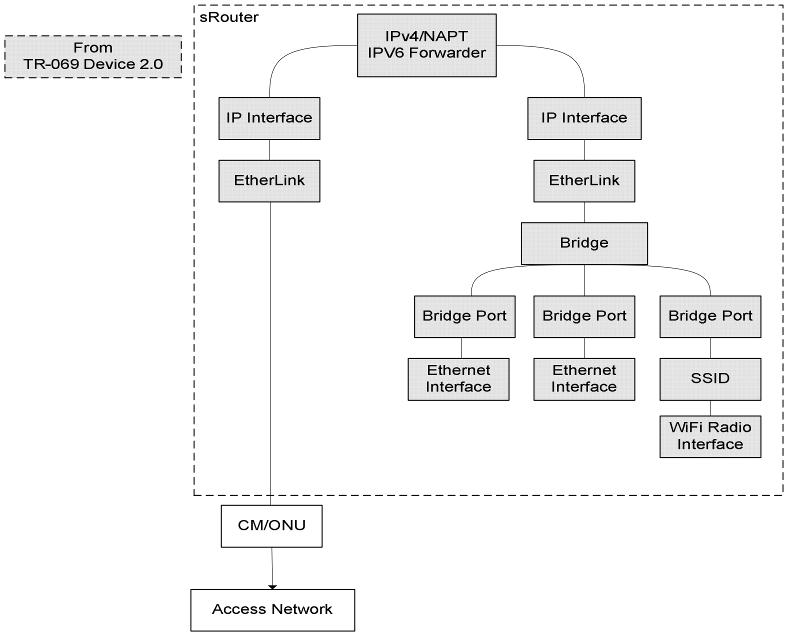


Figure 1: TR-069 interface model applied to sRouter

4.4 sRouter device management

The sRouter enables remote management by supporting TR-069 [66] and, optionally, SNMP.

4.5 Service discovery

4.5.1 Introduction

Service discovery will allow LAN-attached 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. For example, a network-based printer could be discovered by one or more service discovery techniques. The mDNS protocol as defined in IETF RFC 6762 [59] and UPnP as defined by the UPnP Forum and specified in ISO/IEC 29341-1-1 [8] are used for providing service discovery in the sRouter.

4.5.2 Multicast Domain Name System (mDNS)

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 but can be enhanced to provide service to multiple networks in the customer network. A method to relay announcements and queries/responses between different networks is therefore needed.

The sRouter takes an announcement, query or response packet from one link/subnet and relays it onto another link/subnet, but replaces the IP source address from the originating link/subnet with the sRouter'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 are removed before the packet is placed onto the new link/subnet.

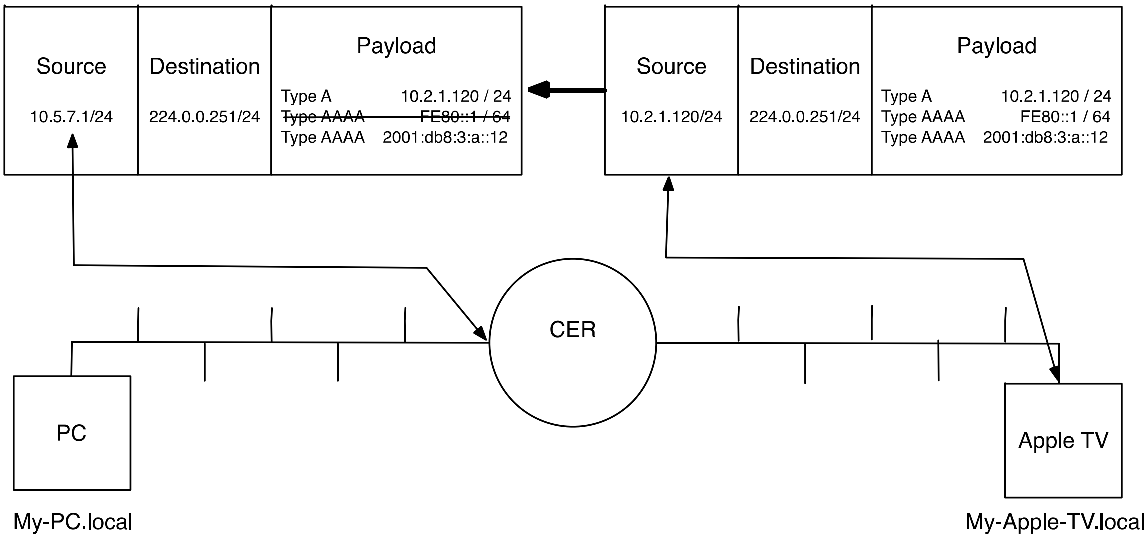


Figure 2: mDNS source IP and payload changes going through an sRouter

Hosts implementing the mDNS protocol may silently discard any frame with a source IP address that is not part of the receiver's network. When the sRouter receives a packet with an address that is not on the receiver's network, the sRouter shall replace the source address in the packet with the IP address of the sRouter'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 in figure 2 to multicast addresses (FF02::FB and 224.0.0.251).

The sRouter will not keep state information, but simply relays the packet and makes the appropriate changes to the IP source address and payload. The sRouter shall not forward or listen for announcement, query or response messages, for either IPv4 or IPv6, on the operator-facing interface.

4.5.3 Universal Plug and Play (UPnP)

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 the present clause 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.

UPnP forwards to multicast addresses (FF02::C, FF05::C, FF02::130 and 239.255.255.250) as shown in figure 3. The sRouter is expected to forward to the site scoped address only.

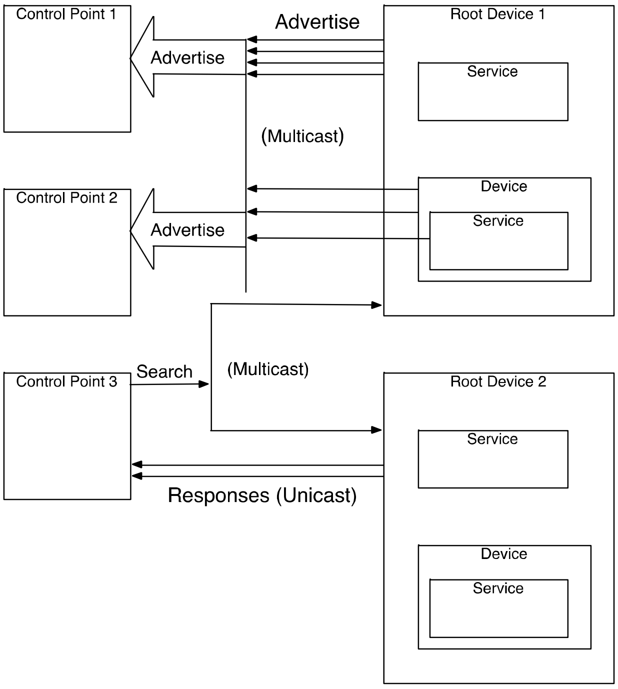


Figure 3: UPnP general architecture

The sRouter does not forward or listen for SSDP messages, over either IPv4 or IPv6, on the operator-facing interface. IPv6 support was added to annex A of ISO/IEC 29341-1-1 [8].

4.6 Customer Edge Router Identification (CER-ID)

An sRouter is situated at the edge of the customer network facing the operator's network, and acts as the demarcation point. When the sRouter is operating in this role, it is referred to as the CER. The CER-ID is used by routers to determine their role in the LAN, which may impact the services the router should enable. The CER-ID is passed from DHCP server to connected sRouters which then compare the information in the CER-ID and the sRouter's own WAN interface addressing to determine its role. The sRouter compares the IA_NA address assigned to its customer-facing IP interface to the assigned IA_PD on the customer-facing IP interface. If the two address scopes are derived from the same parent prefix, then the router determines that it is not the CER, but is a router operating within the interior of the LAN. For the purposes of the present document, the only role currently supported is the CER and is assumed regardless of the settings of the CER-ID or the absence of the CER-ID from the DHCP response.

4.7 IPv4 multicast NAPT

IPv4 multicast packets destined to multicast servers outside the customer's home network are a special case for NAPT and need special handling at the sRouter. One scenario where forwarding of IP multicast packets at the sRouter needs 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 sRouter is required to run at least one industry-standard multicast routing protocol to advertise the flows.

Since the sRouter supports IGMP proxy for IGMP v2 and IGMP v3, there is no reason to support a special translation for multicast packets in the sRouter for IGMP messages from private network addresses arriving on the customer-facing IP interface, as they are consumed by the sRouter and new IGMP messages are sent by the proxy agent from a public source network address on the operator-facing IP interface.

As there is no NAPT for IPv6 multicast traffic, the sRouter will forward MLD IPv6 multicast traffic that is not link- or site-scoped through the operator-facing interface that originates from LAN based devices.

5 sRouter initialization

5.1 General requirements

The sRouter operates in any one of three possible modes - IPv4 Protocol Enabled, IPv6 Protocol Enabled, or Dual IP Protocol Enabled, as summarized in table 3, and the sRouter shall support all three modes of operation. The sRouter shall default to Dual IP Protocol Enabled mode in conformance with IETF RFC 6540 [58].

The sRouter initializes, by default, in Dual IP Protocol Enabled mode. After initialization, the operator may change the mode to any of the possible modes (e.g. IPv4 Protocol Enabled, IPv6 Protocol Enabled) using either TR-069 [66] or SNMP.

The sRouter IP protocol mode shall persist across initializations.

When the sRouter is in IPv4 Protocol Enabled mode, the sRouter performs IPv4 provisioning as described in clause 6 and IPv4 data forwarding and NAPT according to clause 8. The sRouter operating in IPv4 Protocol Enabled mode does not perform any IPv6 provisioning. When the sRouter is in IPv4 Protocol Enabled mode, the sRouter shall not forward IPv6 traffic between the operator-facing interface and the customer-facing interfaces.

When the sRouter is in IPv6 Protocol Enabled mode, the sRouter performs IPv6 provisioning according to clause 7 and IPv6 data forwarding according to clause 9. The sRouter operating in IPv6 Protocol Enabled mode does not perform any IPv4 provisioning. When the sRouter is in IPv6 Protocol Enabled mode, the sRouter shall not forward IPv4 traffic between the operator-facing interface and the customer-facing interfaces.

When the sRouter is in Dual IP Protocol Enabled mode, the sRouter performs IPv4 provisioning as described in clause 6 and IPv6 provisioning according to clause 7. Once an sRouter in Dual IP Protocol Enabled mode acquires an IPv6 address and prefix per clause 7, the sRouter performs IPv6 data forwarding according to clause 9. An sRouter in Dual IP Protocol Enabled mode acquires an IPv4 address per clause 6 and then performs IPv4 data forwarding and NAPT according to clause 8.

When the sRouter is enabled in any of the IP protocol enabled modes, the sRouter shall forward IP traffic between the customer-facing interfaces, regardless of which IP protocol enabled mode is enabled.

Table 3 provides a summary of the sRouter behavior based upon the configured mode of operation as well as when it is disabled.

Table 3: Operator-facing sRouter modes

Mode	IPv4	IPv6
IPv4 Protocol Enabled	IPv4 provisioning (see clause 6). IPv4 data forwarding using NAPT (see clause 8).	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 (see clause 7). IPv6 data forwarding (see clause 9).
Dual IP Protocol Enabled	IPv4 provisioning (see clause 6). IPv4 data forwarding using NAPT (see clause 8).	IPv6 provisioning (see clause 7). IPv6 data forwarding (see clause 9).

5.2 Network Time Protocol (NTP)

Network Time Protocol version 4 (NTPv4) is used to provide time synchronization to the sRouter from one or more NTP servers. Such time synchronization is essential for correlating events in the sRouter's local log, and for providing accurate time for features that, while not explicitly defined in the sRouter specification, 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 or provide a specific date and time in the application's interface.

The sRouter implements the NTPv4 protocol client per IETF RFC 5905 [49] with the following exceptions:

- The sRouter shall act as a client per clause 2 of [49], Modes of Operation, using the operator-facing interface.
- The sRouter shall support a minimum of three NTP servers in the NTP server list.
- The sRouter may support the broadcast protocol mode of NTPv4 per clause 3 of [49], Protocol Modes, with the provision that a filtering mechanism is provided to prevent security vulnerabilities as described in clause 15 of [49].
- The sRouter may support dynamic server discovery via multicast or anycast mechanisms per clause 3.1 of [49], Dynamic Server Discovery.
- The sRouter shall support the client/server protocol mode per clause 3 of [49], Protocol Modes.

The sRouter implements the NTPv4 protocol server for LAN clients per [49] with the following exceptions:

- The sRouter shall populate the DHCP scopes defined for each customer-facing interface with the NTPv4 server information obtained from the operator-facing interface IP provisioning.

6 IPv4 provisioning

6.1 General requirements

The normative requirements of clause 6 are mandatory for an sRouter operating in IPv4 Protocol Enabled mode and/or in Dual IP Protocol Enabled mode as defined in clause 5.

The sRouter shall use DHCPv4 [16] 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 4.

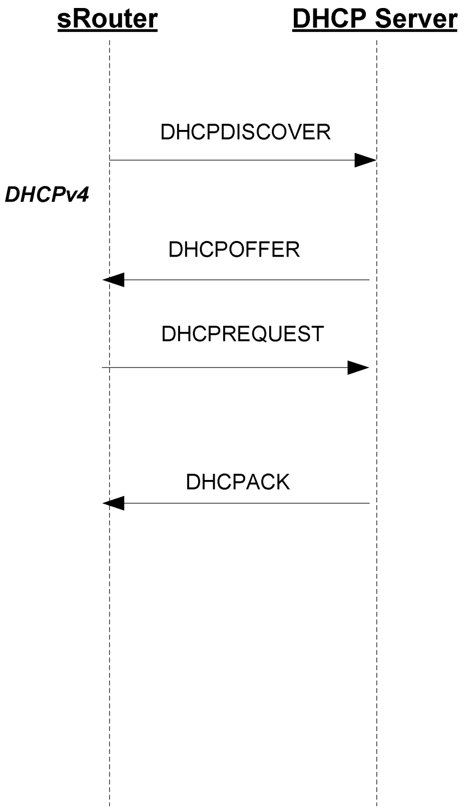


Figure 4: IPv4 provisioning message flow

The sRouter can 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 clause 6.3, the sRouter shall 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 sRouter shall retransmit the DHCPDISCOVER message.

The backoff values for the sRouter retransmission of DHCPDISCOVER messages should be chosen according to a uniform distribution between the minimum and maximum values as specified in table 4.

Table 4: sRouter DHCP retransmission interval

Backoff number	Minimum [s]	Maximum [s]
1	3	5
2	7	9
3	15	17
4	31	33
5	63	65

The sRouter should also implement a different retransmission strategy for the RENEWING and REBINDING states, as recommended in IETF RFC 2131 [16], which is based on one-half of the remaining lease time.

The sRouter shall limit the number of retransmissions of the DHCPDISCOVER and DHCPREQUEST messages to five or fewer. The sRouter shall 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 sRouter shall not forward IPv4 traffic if, at any time, it does not have an IPv4 address for its operator-facing interface.

The sRouter shall be able to accept a unicast response from the DHCP server/relay agent.

6.2 DHCPv4 fields used by the sRouter

The sRouter shall include the following fields in the DHCPDISCOVER and DHCPREQUEST messages:

- The hardware type (htype) shall be set to 1.
- The hardware length (hlen) shall be set to 6.
- The client hardware address (chaddr) shall be set to the 48-bit MAC address associated with the IPv4 operator-facing interface of the sRouter.
- The broadcast bit shall not be set.
- The client identifier option shall be included, using the format defined in IETF RFC 4361 [41].
- The parameter request list option shall be included.
- The following option codes (defined in IETF RFC 2473 [17] and IETF RFC 4361 [41]) shall 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 55 (Parameter Request List)
    - Option code 60 (Vendor Class Identifier) [sRouter 1.0]

The following fields are expected in the DHCPOFFER and DHCPACK messages returned to the sRouter. The sRouter shall configure itself with the listed fields from the DHCPACK:

- The IP address to be used by the sRouter (yiaddr) (critical).
- The IP address lease time (option 51) (critical).
- The server identifier (option 54) (critical).
- The subnet mask to be used by the sRouter (Subnet Mask, option 1) (critical).
- A list of addresses of one or more routers to be used for forwarding sRouter-originated IP traffic (Router Option, option 3) (critical).
- A list of DNS server addresses (critical).

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

If a critical field is missing or invalid in the DHCPACK received during initialization, the sRouter shall 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 sRouter shall 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 sRouter shall 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 sRouter shall 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 sRouter shall ignore the field if it is invalid and remain operational.

6.3 sRouter DHCPv4 server sub-element

6.3.1 Introduction

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 IETF RFC 2473 [17].

6.3.2 DHCPv4 server function goals

Goals for the DHCP server include the following:

- Assign network address leases to CPE devices according to IETF RFC 2131 [16].
- Assign private CPE addresses according to IETF RFC 1918 [15].
- Assign configuration information according to IETF RFC 2473 [17].

6.3.3 DHCPv4 server function system description

The sRouter 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.

6.3.4 DHCPv4 server function requirements

The sRouter shall include a DHCPv4 server compliant with IETF RFC 2131 [16].

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

- When the sRouter DHCP server assigns an active lease for an IP address to a CPE device, the server function of the sRouter shall remove that IP address from the pool of IP addresses available for assignment.
- The requirements in the present clause use an appropriate address space as defined in IETF RFC 1918 [15], and overrides the requirements in clause 7.10 when using IPv4 Protocol Enabled mode (not in Dual IP Protocol Enabled mode).
- The DHCP server function of the sRouter shall support the DHCP options indicated as mandatory in table 5.
- The DHCP server function of the sRouter shall 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 sRouter shall not deliver any DHCP option with null value to any CPE device.
- The DHCP server function of the sRouter should be operational independent of the sRouter operator-facing interface connectivity state.
- If the sRouter operator-facing interface is not successfully provisioned, the sRouter DHCP server function should assign a short lease time to CPE devices and may omit options it has not acquired.
- The DHCP server function of the sRouter shall assign private IP address space as defined in [15].
- The DHCP server function of the sRouter should log errors to a local event log.

Table 5: 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
4491.3	Option(s) acquired under CL_V4EROUTER_CONTAINER_OPTION from the operator

6.4 Operator-facing IPv4 address release behavior

There are a number of situations in which it is desirable for the sRouter 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 sRouter 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.

Whenever the sRouter is instructed to reset, the sRouter shall send a DHCP_RELEASE message [16] for the IPv4 public address assigned by the DHCPv4 server to the sRouter's operator-facing interface. The sRouter shall send the DHCP_RELEASE message [16] for the IPv4 public address assigned by DHCPv4 to the sRouter's operator-facing interface whenever the sRouter receives a DHCPv4 server renewal response that contains a different IPv4 address. The sRouter shall not wait for a confirmation of the receipt of the release by the DHCPv4 server in order to re-initialize.

6.5 Customer-facing IPv4 address release behavior

After initiating an administrative device reset in which the public address has been released, the sRouter 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 sRouter is enabled.

7 Operator-facing IPv6 provisioning

7.1 General requirements

If the sRouter is operating in either IPv6 Protocol Enabled mode or Dual IP Protocol Enabled mode as defined in clause 5, the sRouter shall use DHCPv6 [24] 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 5. The sRouter shall use DHCPv6 Prefix Delegation [27] in order to obtain an IPv6 prefix for the sRouter's customer-facing IP interfaces and any downstream Internal Routers (IRs) as well as any other parameters needed to establish IPv6 connectivity within the home or office network.

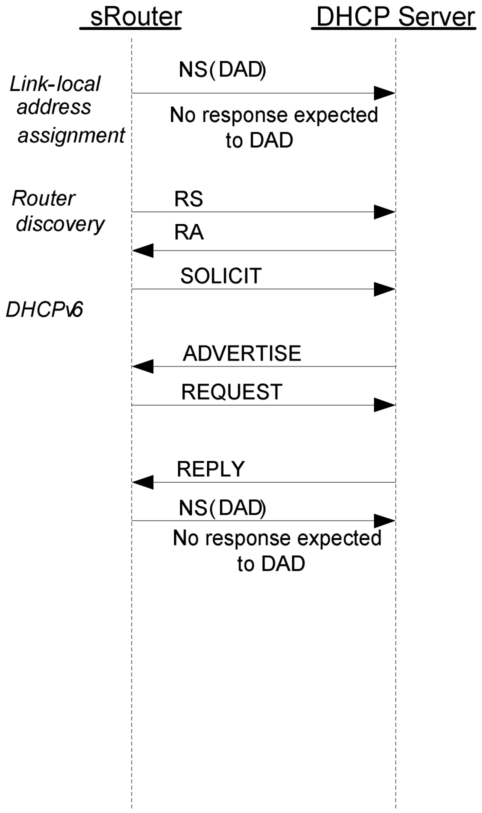


Figure 5: IPv6 provisioning message flow

The steps in figure 5 are described in clauses 7.2 to 7.10.

7.2 Obtain link-local address

The sRouter shall construct a link-local address for its operator-facing interface and each of its customer-facing interface(s) according to the procedure in clause 5.3 of IETF RFC 4862 [44]. The sRouter shall use the EUI-64 identifier as a link-local address for each of its interfaces as described in [35]. For each of its interfaces, the sRouter shall join the all-nodes multicast address and the solicited-node multicast address of the corresponding link-local address [18], [44]. The sRouter shall use Duplicate Address Detection (DAD) as described in clause 5.4 of IETF RFC 4862 [44] to confirm that the constructed link-local addresses are not already in use prior to sending any Router Solicitations on the interface. If the sRouter determines that the constructed link-local address is already in use, the sRouter shall terminate IPv6 operation on that interface.

7.3 Perform router discovery

The sRouter shall perform router discovery as specified in clause 6.3 of IETF RFC 4861 [43] on its operator-facing interface. The source address used in the Router Solicitation shall be the link-local address on the operator-facing interface. The sRouter identifies neighbouring routers and default routers from the received RAs.

7.4 Obtain IPv6 address and other configuration parameters

The sRouter shall examine the contents of RAs it receives on the operator-facing interface and obey the following rules:

- If the M bit is set to 1, the sRouter shall use stateful DHCPv6 to obtain its IA_NA IPv6 address and other configuration information (and ignore the A and O bits).

- If the M bit is set to 1, the sRouter shall use stateful DHCPv6 to obtain its IA_PD.

- If the M bit is set to 0, the sRouter shall not attempt to use DHCPv6 to obtain its IPv6 address and other configuration information.

- The sRouter shall not support SLAAC on its operator-facing interface.

If the sRouter receives an RA where the M bit is set to 0, then the sRouter considers provisioning to have failed. This is due to the prohibition of SLAAC address generation techniques on the operator-facing interface.

If an RA contains a prefix advertisement for an IPv6 network prefix on which the sRouter does not have an address and the M bit in the RA is set to 1, the sRouter shall use DHCPv6 to obtain its IPv6 address for its operator-facing interface and renew any current IA_PD lease(s).

Table 6 depicts sRouter behavior based on the values present in the M and O bits.

Table 6: sRouter behavior

M bit	O bit	Stateful DHCPv6	Stateless DHCPv6	Prefix Delegation
1	1	Yes	No	Yes
1	0	Yes	No	Yes

The sRouter shall follow the recommendations in clause 4 of IETF RFC 5942 [51], and in particular the handling of the L flag in the sRouter Advertisement Prefix Information option (PIO).

The sRouter shall act as a requesting router for the purposes of DHCPv6 Prefix Delegation [27]. DHCPv6 address assignment (IA_NA) and DHCPv6 Prefix Delegation (IA_PD) should be done as a single DHCPv6 session.

The sRouter sends a DHCPv6 Solicit message as described in clause 17.1.1 of IETF RFC 3315 [24]. The Solicit message shall include:

1) A Client Identifier option containing the DHCP Unique Identifier (DUID) for this sRouter (as specified by IETF RFC 3315 [24]), the DUID is to be formatted as follows:

    a) the sRouter shall use a DUID that is one of DUID-LL, DUID-EN or DUID-LLT type; and

    b) the sRouter shall use a DUID that is persistent across administrative reset or reboot following a loss of power per IETF RFC 7084 [61] W-6.

2) An IA_NA option to obtain its IPv6 address.

3) An IA_PD option (as specified in IETF RFC 3633 [27]) to obtain its delegated IPv6 prefix.

The Solicit message should also include the following:

4) A Reconfigure Accept option to indicate the sRouter is willing to accept Reconfigure messages.

5) An Options Request option, which includes the following options:

    - DNS Recursive Name Server option [28].

    - DNS Domain Search List option [28].

    - OPTION_SOL_MAX_RT (82) [60].

    - OPTION_NTP_SERVER (56) [50].

6) A vendor-specific option containing:

    - The 32-bit number 4491 (enterprise number).

    - A vendor-specific Option Request option CL_OPTION_ORO as defined in [1].

The sRouter shall include the DHCP options for the MAP-E or MAP-T container options in the DHCP Solicit and Request messages per clause 8.8.3.2.

The sRouter shall use the delegated prefix assigned by the most recent DHCPv6 operation even if the new prefix differs from a prefix that was previously assigned. This new prefix will overwrite any stored prefix information preserved across resets by the sRouter.

If the sRouter does not have a previously assigned delegated prefix, the sRouter shall indicate a non-zero prefix size as DHCPv6 hint information [27]. The sRouter shall 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 sRouter shall 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 sRouter should assign a single /64 for all customer-facing logical interfaces and log an error message.

Any packet received from the operator-facing interface by the sRouter with a destination address in the prefix(es) delegated to the sRouter but not in the set of prefix(es) assigned by the sRouter to the customer-facing interface shall be dropped. For example, if the delegated prefix is a /56 but only 12 /64 are in active use, the sRouter should discard all traffic destined to the 242 unused /64 prefixes. 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 sRouter resources.

The sRouter shall use the following values for retransmission of the Solicit message (see clause 14 of IETF RFC 3315 [24] 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 sRouter shall use the following value for the Max Solicit timeout value as per IETF RFC 7083 [60] in preference to any value shown in IETF RFC 3315 [24]:

- SOL_MAX_RT = 3 600 s

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 sRouter, or as configured by the administrator, to be sent to the sRouter. If any of the following options are absent from the Advertise message and the SOL_MAX_RT option is not present, the sRouter shall discard the message and wait for another Advertise message. If any of the following critical options are absent from the Reply message, the sRouter shall consider IPv6 provisioning to have failed, discard the Reply, and continue transmitting Solicit messages. In addition, the sRouter may log an event:

1) The IA_NA option containing the sRouter's IPv6 address;

2) The IA_PD option containing the delegated IPv6 prefix for use by the sRouter;

If the following non-critical options are absent from the Reply message, the sRouter may log an event:

3) Reconfigure Accept option;

4) The DNS Recursive Name Server option;

5) DHCP option 94 (MAP-E) or DHCP option 95 (MAP-T).

When the SOL_MAX_RT option is present in an Advertise message, or critical options are absent, the sRouter shall acquire the value of SOL_MAX_RT and use such value for future transmissions of Solicit messages. After the sRouter obtains an Advertise containing a new value for SOL_MAX_RT, it shall use the newly acquired value of SOL_MAX_RT for any subsequent Solicit transmissions. It is not necessary to preserve the value of SOL_MAX_RT across resets.

The sRouter may log an event if IPv6 provisioning has failed.

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

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

- 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, log the event in the local log, and re-initiate the DHCP process.

The sRouter shall support the Reconfigure Key Authentication Protocol as described in clause 21.5 of IETF RFC 3315 [24].

The sRouter shall 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 sRouter shall 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. The sRouter shall not forward any IPv6 traffic between its customer-facing interface and its operator-facing interface if it has not completed the delegated prefix acquisition process.

If DHCPv6 provisioning fails on the operator-facing interface for any reason, then the sRouter shall transmit a Router Advertisement on the customer-facing interface with the router lifetime equal to zero.

7.5 Use of T1 and T2 timers

The sRouter shall initiate the lease renewal process when timer Router-T1 expires. The sRouter shall initiate the lease rebinding process when timer Router-T2 expires. Timers Router-T1 and Router-T2 are called T1 and T2, respectively, in the DHCP specifications. If the DHCP server sends a value for Router-T1 to the sRouter in a DHCP message option, the sRouter shall use that value. If the DHCP server does not send a value for Router-T1, the sRouter shall set T1 to 0,5 times the duration of the lease [24]. If the DHCP server sends a value for Router-T2 to the sRouter in DHCP message options, the sRouter shall use that value. If the DHCP server does not send a value for Router-T2, the Router shall set Router-T2 to 0,875 times the duration of the lease [24].

7.6 Customer-facing IPv6 provisioning of CPE devices

7.6.1 Initial customer-facing IP interface provisioning

An sRouter that has no default routers on its operator-facing interface shall not send Router Advertisements to its customer-facing interfaces with router lifetime values other than zero. If an sRouter is serving as an advertising router (acting as the default router for the PD) and subsequently detects loss of connectivity on its operator-facing interface, it shall deprecate itself as an IPv6 default router on each of its customer-facing interfaces. The sRouter shall then transmit one or more Router Advertisement messages with the Router Lifetime field set to zero.

Per IETF RFC 7084 [61], whenever the sRouter detects loss of connectivity to the access network on the operator-facing interface the sRouter shall:

- Set both the router lifetime and the preferred lifetime to zero (0) in the Router Advertisement (RA) messages for each customer-facing interface that has been allocated a prefix from the delegated prefix that was provisioned on the sRouter operator-facing interface;
- Transmit one (1) or more Router Advertisement (RA) messages on the customer-facing interfaces that have been allocated prefixes from the delegated prefix that was provisioned on the sRouter operator-facing interface.

The sRouter may log an event associated with the change in link-state of the operator-facing interface.

The sRouter shall detect disruption of connectivity to the access network when the access network demarcation device (e.g. CM or ONU) loses its connection with the access network. How the sRouter determines the access network demarcation has lost its connection is implementation specific.

Upon detecting access network connectivity has been restored, the sRouter shall send a DHCPv6 Solicit message to the DHCP server by resetting the back off timer to its lowest value. Prompt transmission of DHCPv6 Solicit messages is essential to re-establishing local IPv6 networking and to allow the injection of the assigned PD into the CMTS's routing table. This insures rapid recovery after planned or unplanned outage events.

The sRouter shall divide the delegated prefix acquired from the IA_PD option per clause 7.4 during the provisioning process into several sub-prefixes to be used for its customer-facing IP interfaces and any downstream IRs.

By default, the sRouter shall divide the delegated prefix based on the provisioned prefix size and the configurable Topology mode (clause 7.4) as follows:

- If the provisioned IA_PD is smaller than a /56 (e.g. a /60) and the Topology mode is set to "favor depth", the sRouter shall divide the delegated prefix on two (2)-bit boundaries into four (4) sub-prefixes by default.
- If the provisioned IA_PD is smaller than a /56 (e.g. a /60) and the Topology mode is set to "favor width", the sRouter shall divide the delegated prefix on three (3)-bit boundaries into eight (8) sub-prefixes by default.
- If the provisioned IA_PD is a /56 or larger and the Topology mode is set to "favor depth", the sRouter shall divide the delegated prefix on three (3)-bit boundaries into eight (8) sub-prefixes by default.
- If the provisioned IA_PD is a /56 or larger and the Topology mode is set to "favor width", the sRouter shall divide the delegated prefix on four (4)-bit boundaries into sixteen (16) sub-prefixes by default.
- If the provisioned IA_PD is too small to divide in the manner described, the sRouter shall divide the delegated prefix into as many /64 sub-prefixes as possible and log an error message indicating the fault.

For example, if the sRouter set to "favor width" receives a /56 IA_PD during the provisioning process, the sRouter will split the /56 delegated prefix into sixteen /60 sub-prefixes for use within the home or office. In another scenario where an sRouter set to "favor depth" receives a /62 IA_PD during the provisioning process, it would split that /62 delegated prefix into four /64 prefixes for use within the home or office network.

The sRouter may support other methods of dividing the provisioned IA_PD; any such methods would have to be configured by the operator or its customer.

The sRouter shall generate and assign a /64 prefix for each customer-facing IP interface before sub-delegating any prefixes to downstream routers within the home.

The sRouter shall allocate these /64 interface prefixes starting from the numerically lowest sub-prefix generated from the division of the IA_PD (as described in the present clause). If the sub-prefix is too small to address all of the customer-facing IP interfaces, the sRouter shall allocate additional /64 interface prefixes from the next, numerically consecutive sub-prefix.

The sRouter may reserve additional /64 interface-prefixes for customer-facing logical interfaces that could be enabled in the future.

After all of the sRouter's customer-facing IP interfaces have been assigned a /64 prefix, the sRouter shall delegate sub-prefixes to directly attached downstream routers starting from the numerically highest sub-prefix and working down in reverse numerical order. The prefix assignment in reverse order allows for the flexibility of having a contiguous customer-facing IP interface prefix assignment for interfaces that may be enabled after the initial prefix assignment. This includes the most common use case of additional SSID interfaces that may be administratively disabled at the time the sRouter initializes that are later enabled.

If there are not enough sub-prefixes remaining to delegate to all downstream routers, the sRouter shall log an error message indicating the fault when the pool of available /64 prefixes has been exhausted.

For example, if there is an sRouter set to "favor depth" configured with two (2) customer-facing IP interfaces that receives a provisioned prefix of 3900:1234:5678:9ab0::/60, the prefix assignment would be as follows:

- customer-facing logical interface #1 would be assigned with the prefix: 3900:1234:5678:9ab0::/64
- customer-facing logical interface #2 would be assigned with the prefix: 3900:1234:5678:9ab1::/64

The sRouter would delegate sub-prefixes to the directly attached downstream routers starting first with the 3900:1234:5678:9abc::/62 sub-prefix, and next with 3900:1234:5678:9ab8::/62 sub-prefix, and so on.

If the provisioned prefix is too small to address all of its interfaces, the sRouter shall collapse the customer-facing IP interfaces into a single interface and assign a single /64, logging an error message indicating the fault. For example, if sRouter with eight (8) customer-facing (physical) interfaces receives a single /64 prefix during the provisioning process, the sRouter will be forced to bind all eight (8) interfaces into the lowest numbered, or primary LAN, creating a single flat network and a single customer-facing IP interface, regardless of the existing LAN or VLAN configuration(s).

The sRouter shall assign an IPv6 address from the /64 prefix allocated for each customer-facing IP interface. The sRouter should generate each customer-facing IP interface identifier using the Modified EUI-64 process as described per IETF RFC 4291 [35]. 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 clause 7.4 to create the 128-bit IPv6 interface identifier address.

This entire process can be illustrated in the following way:

1) The aggregate prefix is acquired per clause 7.4.

2) The sRouter breaks the aggregate prefix into sub-prefixes, based on the Topology mode in table C.3. If the aggregate prefix is not large enough, it is broken into as many /64 sub-prefixes as possible and an error message is logged.

3) The first of these sub-prefixes is further broken into /64 interface-prefixes for use one on each of the sRouter's customer-facing logical interfaces.

    a. If the sub-prefix is too small to number all customer-facing logical interfaces, the sRouter uses additional sub-prefixes as needed (in numerical order).

    b. If the aggregate prefix is too small to number all customer-facing logical interfaces, the sRouter collapses them into a single interface, assigns a single /64 to that interface, and logs an error message.

4) Each customer-facing IP interface is assigned an IP address from the corresponding interface-prefix.

5) The remaining sub-prefixes are delegated via DHCPv6 to directly connected downstream routers as needed, in reverse numerical order.

The sRouter shall support SLAAC [44] on all customer-facing interfaces. This requirement satisfies IP address allocation on the customer-facing interfaces for any host that does not implement a full DHCPv6 client.

The sRouter shall support a DHCPv6 server [24] on all customer-facing interfaces. This requirement provides the customer-facing interface with the ability to allocate IP addresses to hosts that implement a DHCPv6 client.

The sRouter shall support delegating sRouter behavior for the IA_PD option [27] on all customer-facing interfaces. This requirement provides the means to delegate sub-prefixes to routers within the customer's network from the aggregate, delegated prefix assigned by the operator to the sRouter.

The sRouter shall support Neighbor Discovery for IPv6 as defined in IETF RFC 4861 [43].

The sRouter shall advertise itself as a router for its delegated prefix(es) using the Route Information Option as specified in clause 2.3 of IETF RFC 4191 [33].

The sRouter's Router Advertisement (RA) transmission period shall be configurable from 3 seconds to 1 800 seconds for each customer-facing logical interface. This configuration flexibility is necessary to adapt to conditions for which the [44] defined default of a 120-second interval is inadequate. For example, when prefixes are changed and timely notification of such change is essential to maintaining network continuity.

The sRouter shall implement a 30-second Router Advertisement (RA) transmission interval by default for each of its customer-facing logical interfaces. If the prefix information contained in an RA changes, the sRouter shall immediately generate and transmit an updated RA.

7.6.2 Additional customer-facing IP interfaces enabled after initial provisioning

If an sRouter customer-facing IP interface is enabled after initial provisioning and the initial Prefix Delegation, the sRouter shall continue prefix assignment for this interface from the next available lowest numbered /64 prefix available. To illustrate using the same example as in clause 7.6.1, if an additional customer-facing IP interface is enabled after the initial prefix assignment, the sRouter would assign this interface with the prefix of 3900:1234:5678:9ab2::/64.

When the sRouter has used all of its sub-prefixes for any reason, the sRouter shall not enable any new customer-facing IP interfaces. When an attempt to enable a customer-facing IP interface fails because there are no available prefixes, the sRouter shall log an error message indicating the fault.

7.6.3 SLAAC requirements for sRouter

7.6.3.1 General requirements

SLAAC is required for hosts that do not implement a DHCPv6 client.

The /64 prefix length is required for the dynamic numbering of CPE devices using SLAAC [44]. The sRouter shall generate Router Advertisements (RA) on each customer-facing interface as per IETF RFC 4862 [44].

The sRouter shall include the following in its RA by default:

- A Prefix Information Option with a prefix derived from the prefix acquired under IA_PD in clause 7.4 and both the ICMPv6 options flags L-Bit (On-link) bit and A-Bit (Autonomous) bit set to 1.
- Preferred lifetimes in the Prefix Information Option set equal to or less than the preferred lifetime communicated in the IA_PD option received on the operator-facing interface. This requirement ensures prefix lifetime synchronization between the sRouter aggregate prefix and the prefix/es assigned to each customer-facing interface.

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

Once the sRouter has completed operator-facing DHCPv6 provisioning, it shall:

- Include DNS configuration option RDNSS in its RA messages as specified in IETF RFC 6106 [53].
- Include DNS configuration option DNSSL in its RA messages as specified in IETF RFC 6106 [53] if OPTION_DOMAIN_LIST (24) option is acquired via operator-facing DHCPv6 provisioning.
- Include the list of DNS servers specified in the OPTION_DNS_SERVERS (23).
- Include the list of domain names specified in the OPTION_DOMAIN_LIST (24) option, if acquired via operator-facing DHCPv6 provisioning.

7.6.3.2 Local configuration of SLAAC options

The sRouter may provide a mechanism for local configuration of SLAAC for CPE devices. If local configuration is used, the sRouter shall override the pass through of options received from the operator and provide the locally configured options to CPEs.

7.6.4 DHCPv6 server requirements for sRouter

7.6.4.1 General requirements

The sRouter shall provide a DHCPv6 server on customer-facing interfaces as described in:

- Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [24].
- Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 [29].

The sRouter DHCPv6 server shall support providing the following DHCPv6 options:

- DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [28].
- IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6 [27].
- Network Time Protocol (NTP) Configuration Option for DHCPv6 [50].
- Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [34].

The sRouter DHCPv6 server shall be able to manage at least one IA_NA for each client, and at least one address in each IA_NA.

The sRouter DHCPv6 server shall be able to manage at least one IA_PD for each client and at least one delegated prefix in each IA_PD. The sub-prefix delegated to the client is derived from the aggregate prefix delegated to the sRouter from the operator as described in clause 7.6.

The sRouter DHCPv6 server shall derive the preferred lifetimes for customer-facing IA_NA and IA_PD leases from the preferred lifetime acquired in the IA_PD on the operator-facing interface. The sRouter DHCPv6 messages sent on the customer-facing interface shall contain the lifetime value greater than zero and equal to or less than the IA_PD lifetime acquired on the operator-facing interface.

IA_NA and IA_PD T1 and T2 values are supplied to the customer-facing interface(s) in accordance with clause 22.4 of IETF RFC 3633 [24] and clause 9 of IETF RFC 3633 [27], respectively.

The sRouter shall generate Router Advertisements (RA) on each customer-facing IP interface as per IETF RFC 4862 [44]. The sRouter RA shall include the following by default:

- The M bit set to 1.
- The O bit set to 1.
- A Prefix Information Option with a prefix derived from the prefix acquired under IA_PD in clause 7.4 and both the ICMPv6 options flags L-Bit (On-link) bit and A-Bit (Autonomous) bit set to 1.
- The preferred lifetime in the Prefix Information Option set equal to the preferred lifetimes communicated in the IA_PD option on the operator-facing interface. This requirement ensures prefix lifetime synchronization between the sRouter aggregate prefix and the prefix(es) assigned to each customer-facing interface.

The settings in the RA will direct CPE devices to use DHCPv6 configuration for assigning their global IPv6 address. In most scenarios, an sRouter would make DHCPv6 services available concurrently with SLAAC in order to supply address and other information to hosts of varying capability. Hosts will be presented with a Router Advertisement that includes the M-bit set to indicate DHCPv6 operation in addition to the A-bit set to indicate SLAAC operation and the O-bit set to support stateless DHCPv6 clients.

NOTE: Recent testing shows operating systems will perform both DHCPv6 and SLAAC for address acquisition when the operating system includes a DHCP client and both methods of address acquisition are made available.

The sRouter shall be able to pass the following set of options received from the operator to the DHCPv6 server for configuration of CPEs.

- DNS Recursive Name Server option as specified in IETF RFC 3646 [28].
- DNS Domain Search List option as specified in IETF RFC 3646 [28].

The sRouter 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.

7.6.4.2 Local configuration of DHCPv6 options

The sRouter may provide a mechanism for local configuration of DHCPv6 options for CPE devices. If local configuration is used, the sRouter shall override the pass through of options received from the operator and provide the locally configured options to CPEs.

7.6.5 Prefix changes

An sRouter might receive a replacement prefix from the DHCP server (e.g. during a renewal operation on the operator-facing interface). Due to the global nature of IPv6 addressing of CPEs, the sRouter is to deprecate the previously acquired prefix and allocate addressing from the newly acquired prefix whenever this happens.

The sRouter shall perform CPE provisioning as per clause 7.6 immediately upon receiving a new prefix.

When an sRouter receives updated information for a currently assigned prefix, the sRouter shall immediately send Router Advertisements (RAs) with the updated prefix information and IPv6 DHCP RECONFIGURE (type 6, Rebind) on all customer-facing interfaces.

7.7 Operator-facing IPv6 address release behavior

There are a number of situations in which it is desirable for the sRouter 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 sRouter needs to be administratively reset (say for configuration change, software update or other reason) or a change to the IPv6 address during DHCPv6 renewal.

The sRouter shall release its lease information prior to an administratively imposed re-initialization of the access network demarcation device (e.g. CM or ONU) in order to prevent loss of the communications path with the DHCP server. The sRouter shall not wait for confirmation of receipt of the release by the DHCPv6 server in order to re-initialize.

The sRouter shall send a DHCP_RELEASE message [24] for the IPv6 IA_NA and IA_PD assigned by the DHCPv6 server to the sRouter's operator-facing interface for the following events:

- whenever the sRouter is instructed to reset;
- whenever the sRouter receives a DHCPv6 Reply message containing a different IPv6 prefix or IPv6 address;
- whenever the IA_PD is not renewed for any reason.

7.8 Customer-facing IPv6 address release behavior

After initiating an administrative device reset in which the IA_NA and IA_PD addresses have been released, the sRouter 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.

The sRouter shall send an ICMPv6 destination unreachable message (code 5) for packets forwarded to it that use an address from a prefix that has been deprecated.

After initiating a reset in which the operator-facing interface's IA_NA and IA_PD addresses have been released, the sRouter shall declare that it is no longer a default router by setting the Router Lifetime field to zero in the Router Advertisement.

7.9 CER-ID requirements

The sRouter shall assign the CER-ID value for each of its customer-facing IP interfaces for which an IPv6 prefix has been assigned by using the corresponding GUA (Global Unique Address) assigned to the customer-facing IP interface.

The sRouter shall include the DHCPv6 CL_CER_ID option [1] in Advertise or Reply messages containing an IA_PD.

If the IPv6 address of the sRouter's customer-facing IP interface that established the CER-ID changes for any reason, the sRouter shall assign a new value for CER-ID to be included in subsequent DHCPv6 messages.

7.10 Router interface addressing using Link-ID

The sRouter shall support Link-ID IPv4 address generation as defined in the present clause. The sRouter Link-ID feature can be enabled by the operator using TR-069 provisioning methods, see [67]. By default, the Link-ID feature shall be enabled on the sRouter.

The sRouter shall not persist Link-ID based IPv4 addressing across soft-reset or reboot. If soft-reset or reboot occurs, the sRouter waits for a valid IPv6 PD and provisioning instructions in order to enable Link-ID and generate IPv4 addresses using this algorithm. When sRouter 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 sRouter shall not modify Link-ID based IPv4 addressing. In other words, once Link-ID IPv4 addressing has been generated, the sRouter is expected to maintain this addressing until such time as the IPv6 PD changes or the sRouter is reset.

When operating in Dual IP Protocol Enabled mode and Link-ID is enabled, the sRouter shall 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 sRouter 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 sRouter 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 sRouter 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 NAPT when the sRouter is operating in Dual IP Protocol Enabled mode. Refer to figure 6 and annex G for further details.

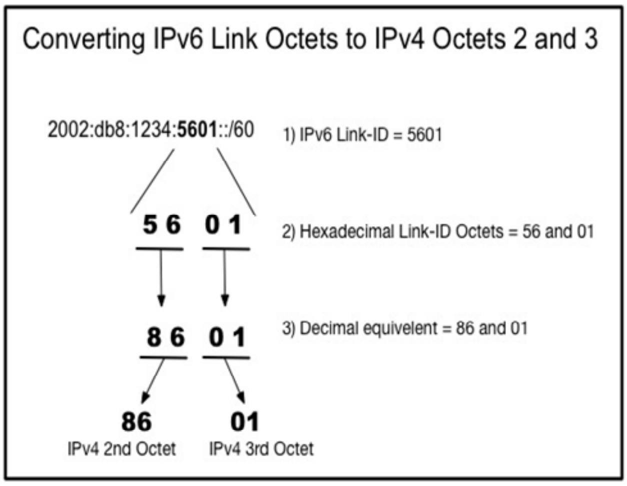

Converting IPv6 Link Octets to IPv4 Octets 2 and 3
2002:db8:1234:5601::/60
1) IPv6 Link-ID = 5601
5 6
0 1
2) Hexadecimal Link-ID Octets = 56 and 01
8 6
0 1
3) Decimal equivelent = 86 and 01
86
IPv4 2nd Octet
01
IPv4 3rd Octet

Figure 6: Example deriving IPv4 octets 2 and 3 from an IPv6 prefix

Using the Link-ID example in the present clause, 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 sRouter shall generate each unique /24 IPv4 prefix from one of the three blocks of address space reserved for private internets per IETF RFC 1918 [15].

8 IPv4 data forwarding and NAPT operation

8.1 Applicability

The normative requirements of clause 8 are mandatory for an sRouter that implements the IPv4 Protocol Enabled mode and/or the Dual IP Protocol Enabled mode.

8.2 Introduction

8.2.1 Assumptions

For the requirements in clause 8 the following is assumed:

- There is only a single operator-facing IP interface on the sRouter.

- At least one globally-routable IPv4 address is available to the sRouter's operator-facing IP interface.
- The operator-facing IP interface is Ethernet encapsulated.
- The customer-facing IP interface is Ethernet encapsulated.

8.2.2 Overview

IPv4 forwarding in the sRouter 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 of its interface or to its internal stack.

Packet handling in the sRouter 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 sRouter provides a mechanism for converting IPv4 network addresses to Ethernet MAC addresses on both customer-facing IP interfaces and the operator-facing IP interface.

8.3 System description

Some sRouters may have multiple customer ports that are connected to the same logical IP router interface. One scenario would be when the sRouter has an 802.11 wireless port and an 802.3 Ethernet port on the single customer-facing logical IP interface. The text in the present clause uses the term customer-facing IP interface to refer to a single customer-facing logical IP router interface connected to the sRouter that is not necessarily mapped one-to-one with the number of customer-facing ports on the sRouter. This text documents the behavior of a single customer-facing IP interface, though it is possible that an sRouter could have multiple customer-facing IP interfaces.

Packets need to be processed by each of the three sub-elements in a very specific order (see figure 7). 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 sRouter first attempts to route the packet through the IPv4 Router sub-element. If the IPv4 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-facing interface. If the IPv4 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 IPv4 Router sub-element. Once the NAPT has been performed on the packet, it is then sent to the IPv4 Router sub-element. If the IPv4 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 IPv4 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 sRouter from the operator network unless it is destined for a subnet known to the customer-facing IP interface.

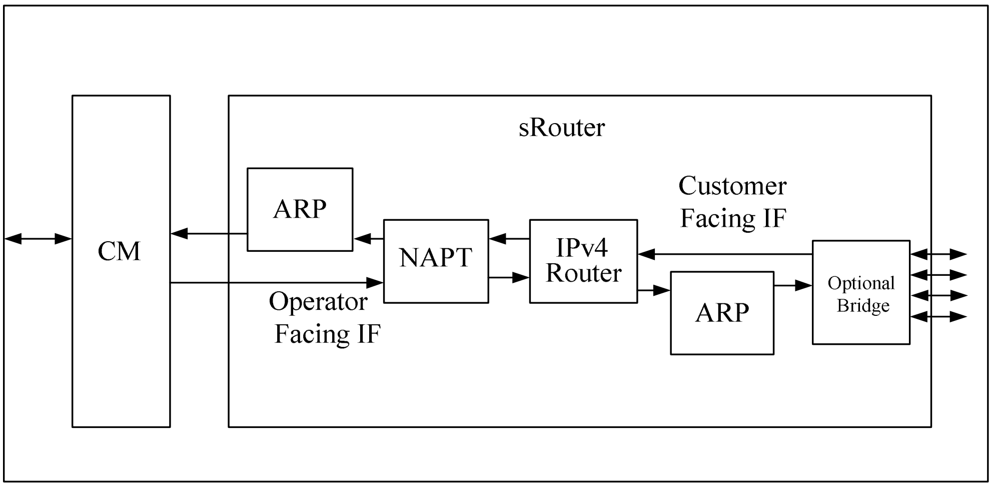


Figure 7: sRouter IPv4 forwarding block diagram

8.4 IPv4 Router sub-element

When the sRouter'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 sRouter may validate the IPv4 header in accordance with clause 5.2.2 of IETF RFC 1812 [12]. As defined in clause 5.3.1 of IETF RFC 1812 [12], the sRouter shall 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 sRouter's local IP stack for processing shall not decrement the TTL. Once the IPv4 header has been validated, the sRouter processes the destination IPv4 address of the packet. If the destination IPv4 address matches the sRouter's public address assigned to its operator-facing IP interface, the sRouter sends the packet to its local IP stack for processing. If the destination IPv4 address does not match this address, the sRouter 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 "not on-link", and the next-hop to use for ARP purposes is the address of the internal router. Discovering other routers on customer-facing IP interfaces, aside from knowledge derived via the use of Link-ID when operating in Dual IP Protocol Enabled mode as specified in clause 7.10, is vendor-specific. If the sRouter cannot determine the next-hop of the IPv4 destination, then it shall drop the packet.

When the sRouter's IPv4 Router sub-element receives a packet from its customer-facing IP interface, it validates the IPv4 header in the packet. The sRouter may validate the IPv4 header in accordance with clause 5.2.2 of [12]. As defined in clause 5.3.1 of [12], the sRouter shall 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 sRouter's local IP stack for processing shall not decrement the TTL. Once the IPv4 header has been validated, the sRouter processes the destination IPv4 address of the packet. If the destination IPv4 address matches one of the private addresses assigned to the sRouter, it sends the packet to its local IP stack for processing. If the destination IPv4 address does not match one of these addresses, the sRouter 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 sRouter 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 "not on-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 sRouter's default, learned via DHCP (see clause 6.3), 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 sRouter. If the sRouter cannot determine the next-hop of the IPv4 destination address, it shall drop the packet.

Regardless of whether the packet was received from the customer-facing IP interface or the operator-facing IP interface, the sRouter shall generate an appropriate ICMP error message as described in IETF RFC 792 [9] 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 clause 5.3.7 of IETF RFC 1812 [12]
- 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 sRouter's IPv4 Router sub-element shall process and/or generate the following ICMPv4 messages when appropriate:

0	Echo Reply	[9]
3	Destination Unreachable	[9]
11	Time Exceeded	[9]

NOTE: It is considered inappropriate for the sRouter's IPv4 Router sub-element to generate ICMPv4 Destination Unreachable messages on the operator-facing interface.

The sRouter shall have at least one MAC address for its operator-facing IP interface and one MAC address for its customer-facing IP interface. The sRouter shall share these source MAC addresses for IPv4 and IPv6. The sRouter shall 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 sRouter shall 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 sRouter shall forward broadcast packets received on either interface only to the sRouter's IP stack. The sRouter shall not forward broadcast packets received on either interface to any interface other than the sRouter's IP stack.

8.5 NAPT sub-element

8.5.1 General requirements

The sRouter shall implement a NAPT function compliant with traditional Network Address Port Translation (NAPT) as specified in clause 2.2 of IETF RFC 3022 [23]. Per IETF RFC 3022 [23], 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 IETF RFC 3022 [23], 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 clause 8.5 uses the term public address(es) to refer to the addresses reachable by the sRouter on its operator-facing IP interface, assuming that they are globally-unique registered addresses. Note that an IP address that the sRouter views as globally unique, may be private to the operator's network. However, from the sRouter'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 sRouter and not discussed in the present document. 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 sRouter shall use any of the private IPv4 network addresses described in IETF RFC 1918 [15] for its customer-facing IP interface.

The sRouter shall 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 clause 8.5.2.

For packets that traverse the NAPT function, the sRouter shall 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 sRouter does not implement a symmetric Network Address Translation (NAT) as defined in IETF RFC 5389 [48].

The sRouter shall 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. Therefore, the sRouter shall not create NAPT translations to allow connectivity between CPEs that live on the customer-facing IP interface.

In clause 8.5, 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.

8.5.2 Dynamically triggered NAPT translation

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 sRouter creates a mapping of source PNAP to GNAP and simultaneously creates a mapping of destination GNAP to PNAP for the return packets. The sRouter 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 sRouter intercepts the reply and changes the previously inserted GNAP fields (now destination) back to the original PNAP values.

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

8.5.3 Application Layer Gateways (ALGs)

8.5.3.1 Introduction

Many applications are hampered by NAPT 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 NAPT, 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 NAPT causes problems is when applications exchange address/port information to establish new connections, creating interdependencies that NAPT cannot know about. Clause 8.5.3 describes specific ALGs required by the sRouter.

8.5.3.2 ICMP error message ALG

ICMP error messages are required for the well-known trace-route network debugging tool to work across the sRouter. This ALG is described in detail in clause 4.3 of IETF RFC 3022 [23]. The ICMP error message ALG shall be implemented by the sRouter. Briefly stated, the sRouter shall 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 NAPT sub-element.

8.5.3.3 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 NAPT 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 clause 4.4 of IETF RFC 3022 [23]. The FTP ALG shall be implemented by the sRouter.

8.6 ARP sub-element

The ARP function in the sRouter is defined and shall be compliant with the following:

- An Ethernet Address Resolution Protocol [10].
- Requirements for IP Version 4 Routers in clause 3.3.2 of IETF RFC 1812 [12].
- Requirements for Internet Hosts in clause 2.3.2 of IETF RFC 1122 [11].

If the corresponding IPv4 network address is found in the table, its corresponding Ethernet address shall be used as the Ethernet destination address of the packet. If the corresponding IPv4 network address is not found, the sRouter shall start the ARP protocol in hopes that it will learn the IPv4 network address to Ethernet address association. The sRouter shall use its own MAC address, as described in clause 8.4, as the source MAC address and source hardware address of all ARP packets.

The sRouter dynamically creates ARP translations based on receiving ARP requests and/or replies for any of its IPv4 network addresses.

ARP entries maintained by the sRouter need careful examination before being aged out of the table. Both voice and video applications present negative subjectively noticeable impacts when ARP entries are removed during a session. Several different ways to age ARP entries are suggested in clause 2.3.2.1 of IETF RFC 1122 [11]. The sRouter 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.

8.7 IPv4 multicast

8.7.1 Introduction

The sRouter 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 sRouter forwards IPv4 multicast packets downstream based on the information learned at each customer-facing interface.

The sRouter 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 sRouter generates, terminates, and processes IGMP messages according to IGMPv3 requirements. For example, the version of IGMP used on the operator network or the local area network will be defined locally at each network. The sRouter may send IGMPv2 reports on the operator-facing interface while generating IGMPv3 queries on customer-facing interfaces.

The following elements define the sRouter IPv4 multicast behavior (also shown in figure 8):

- An IGMPv3 Group Member that implements the group member part of IGMPv3 [25] on the operator-facing interface.
- An IGMPv3 Router that implements the router portion of IGMPv3 [25] 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.

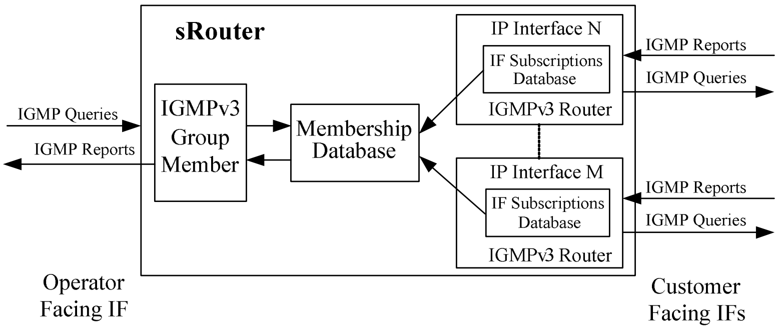


Figure 8: sRouter IPv4 multicast forwarding block diagram

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.

8.7.2 IGMP proxying

8.7.2.1 General requirements

The sRouter maintains the multicast reception state of CPEs on each customer-facing interface in the interface's multicast subscription database. The sRouter 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 sRouter in the form of IGMP Report messages transmitted by CPEs. The sRouter shall implement the router portion of IGMPv3 [25] on each customer-facing interface. The sRouter shall 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 sRouter. The sRouter shall always act as an IGMP querier on its customer-facing interfaces.

On the operator-facing interface, the sRouter shall implement the group member portion of IGMPv3 [25]. The sRouter shall merge the multicast reception state of connected CPEs into an IPv4 group membership database as described in clause 9.6.1.1 of IETF RFC 3376 [25]. The sRouter shall use the IPv4 group membership database as multicast reception interface state per clause 3.2 of IETF RFC 3376 [25], on the operator-facing interface. Thus, when the composition of the group membership database changes, the sRouter reports the change with an unsolicited report sent on the operator-facing interface. When queried by an upstream multicast router, the sRouter also responds with information from the group membership database.

The sRouter shall not perform the router portion of IGMPv3 on the operator-facing interface.

8.7.2.2 IPv4 group membership database

The sRouter's group membership database is formed by merging the multicast reception state records of customer-facing interfaces. In compliance with IETF RFC 3376 [25], the sRouter 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 sRouter keeps an IPv4 group membership database with records of the form:

> (multicast address, filter mode, source list)

The sRouter 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 sRouter shall abide by the following process to merge all customer-facing interface records for the group into one group membership database record:

- First, the sRouter 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 sRouter 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 clause 3.2 of IETF RFC 3376 [25].

8.7.2.3 IPv4 multicast forwarding

8.7.2.3.1 General requirements

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 sRouter shall 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 sRouter shall not replicate an IPv4 multicast session on a customer-facing interface if no CPE device connected to the interface has joined the session.

The sRouter shall 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 sRouter shall not forward IGMP messages received on any IP interface onto another IP interface.

The sRouter shall forward IPv4 local-scope multicast packets (239.255.0.0/16) to all customer-facing interfaces within the same customer-facing IP interface except the customer-facing interface from which they were received.

Except for IGMP packets and IPv4 administratively scoped (239.0.0.0/8) packets, the sRouter shall forward all IPv4 multicast traffic received on customer-facing interfaces onto the operator-facing interface.

8.7.2.3.2 IPv4 multicast forwarding example

The sRouter 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 sRouter (e.g. the CMTS) supports and is configured to operate in IGMPv3 mode, and thus the sRouter works in IGMPv3 mode on the operator-facing interface.

The setup is shown in figure 9.

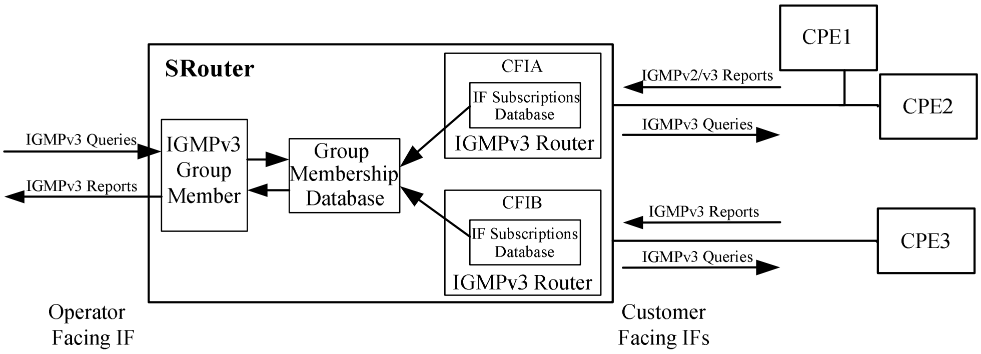


Figure 9: IPv4 multicast forwarding example

The CPEs send reports as follows:

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 sRouter multicast reception state at each customer-facing interface is the following:

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 sRouter'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 sRouter uses the information in group membership database as multicast reception state at the operator-facing interface. For example, in response to an IGMPv3 general query, the sRouter sends an IGMPv3 report for the two records shown.

Assuming that the CMTS is transmitting downstream four multicast streams, the sRouter forwards them as follows:

Stream #	Multicast address	Source address	sRouter forwards on interface	
			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

8.8 IPv4/IPv6 coexistence technologies

8.8.1 Introduction

Even as operators migrate customers from IPv4 to IPv6 addressing and deploy IPv6 more widely in their networks, 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 or CE products, 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 specific groups of subscribers behind a single IPv4 address, or encapsulating or translating IPv4 into IPv6. Clause 8.8 describes several technologies that solve the problem of IPv4/IPv6 coexistence for service providers.

8.8.2 Dual-Stack Lite operation

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) tunnelling and NAT. More specifically, Dual-Stack Lite encapsulates IPv4 traffic inside an IPv6 tunnel and sends it to an operator NAT device.

When Dual-Stack Lite is enabled, the sRouter acquires an IPv6 address on its operator-facing interface and learns the address of the operator NAT device via DHCPv6. It encapsulates IPv4 traffic inside IPv6 sourced from its operator-facing interface and destined for the operator NAT device.

To facilitate IPv4 extension over an IPv6 network, the sRouter may support Dual-Stack Lite.

If the sRouter supports Dual-Stack Lite, it shall support Dual-Stack Lite B4 functionality as specified in clause 5 of IETF RFC 6333 [55] with the exception of clause 5.3 in IETF RFC 6333 [55].

Requirements in clause 5.3 of IETF RFC 6333 [55] are replaced by the following requirements.

The provisioning of DS Lite shall be according to IETF RFC 6334 [56], and request option code 64 (OPTION_AFTR_NAME) for the AFTR tunnel FQDN endpoint name.

8.8.3 Mapping of Address and Port (MAP)

8.8.3.1 General requirements

Mapping of Address and Port (MAP) provides a mechanism for IPv4 network domains to communicate with IPv4 network domains over an IPv6-only network. This is particularly useful for operators that have made significant progress in deploying IPv6 in their networks but are challenged in supporting IPv4-only devices within the subscriber's home network.

An operator can use MAP to share IPv4 addresses among multiple customers or operate on a many-to-one or one-to-one basis. MAP Border Relays interpret a defined sequence of bits in the customer's assigned IPv6 prefix, the Embedded Address (EA), to support stateless operation.

MAP defines two types of transport modes: MAP-E and MAP-T. MAP-E uses encapsulation as specified in IETF RFC 2473 [17] as a mechanism for converting the IPv4 packet within an IPv6 header. MAP-T uses stateless translation as defined by IETF RFC 6145 [54] to translate the IPv4 header into an IPv6 header.

The sRouter shall support MAP-E as defined in IETF RFC 7597 [63]. The sRouter shall support MAP-T as defined in IETF RFC 7599 [64].

The sRouter shall support configuration of MAP-E or MAP-T functionality via DHCP options as defined in IETF RFC 7599 [64]. The sRouter is not required to support configuration of both MAP-E and MAP-T simultaneously. In a typical MAP deployment scenario, a MAP CE installs an IPv4 default route that directs non-local traffic through an IPv6 encapsulation or translation process so it may be forwarded on to a MAP BR. The resulting forwarding behavior follows a hub and spoke model, where a MAP CE will send all default route matching IPv4 destinations through the BR. In this mode of operation, MAP traffic between MAP CEs that belong to the same MAP domain shall traverse the BR. In mesh mode, traffic may be forwarded between MAP CEs without an intervening BR.

The sRouter shall support mesh mode operation between MAP CEs:

- The sRouter shall support the use of a Basic Mapping Rule (BMR) as a Forwarding Mapping Rule (FMR).
- The sRouter should support the explicit provisioning of FMR.

If the F-flag in an S46 Rule option is set, the sRouter shall enable mesh mode for the applicable BMR.

8.8.3.2 MAP-E or MAP-T configuration via DHCP

The sRouter that provisions MAP-E or MAP-T through DHCPv6 option encodings shall issue one (1) Option Request Option (ORO) (option 6) with the appropriate container option as defined in IETF RFC 7599 [64]:

- Softwire46 MAP-E Container option (IANA DHCPv6 option 94) in clause 5.1 of IETF RFC 7599 [64].
- Softwire46 MAP-T Container option (IANA DHCPv6 option 95) in clause 5.2 of IETF RFC 7599 [64].

Each MAP transport has particular option codes that are embedded in the applicable container option as defined in IETF RFC 7599 [64]. These option codes shall not be requested in the DHCPv6 ORO option encoding.

For MAP-E configuration, the sRouter shall accept the following parameters per IETF RFC 7599 [64] at a minimum to support MAP-E:

- S46 Rule option (IANA DHCPv6 option 89);
- S46 BR option (IANA DHCPv6 option 90);
- S46 Port Parameters option (IANA option 93).

For MAP-T configuration, the sRouter shall accept the following minimum parameters per IETF RFC 7599 [64] in order to support MAP-T:

- S46 Rule option (IANA DHCPv6 option 89);
- S46 DMR option (IANA DHCPv6 option 91);
- S46 Port Parameters option (IANA option 93).

8.8.4 Fragmentation

Packet fragmentation is necessary when an IPv4 packet enters the tunnel and the original packet size exceeds the negotiated tunnel MTU. The original IPv4 packet is handled as follows:

1) If in the original IPv4 packet header the DF (Don't Fragment) flag is SET, the sRouter shall discard the packet, and it shall return an ICMP message with type = 3 (unreachable), code = 4 (fragmentation needed and Don't Fragment was set). The next hop MTU field shall be set to the size of the tunnel MTU by the sRouter.

2) If in the original IPv4 packet header the DF (Don't Fragment) flag is CLEAR, the sRouter shall perform fragmentation of any IPv4 packet that will exceed the negotiated tunnel MTU. The sRouter may fragment in one of two ways:

   a. Via clause 5.3 of IETF RFC 6333 [55] where the original IPv4 packet is encapsulated into the IPv6 payload before fragmentation.

   b. Via alternative method where the original IPv4 packet is fragmented first and then each fragment is placed into a separate IPv6 packet.

3) In the sRouter, the method of fragmentation (a or b) shall be configurable.

The sRouter shall support TCP MSS clamping for IPv4 packets and shall overwrite the TCP MSS with a value supported by the negotiated tunnel MTU.

9 IPv6 data forwarding

9.1 Applicability and assumptions

The normative requirements of clause 9 are mandatory for an sRouter that implements the IPv6 Protocol Enabled mode and/or the Dual IP Protocol Enabled mode as defined in clause 5.

The following assumptions apply:

- There is only a single operator-facing IP interface on the sRouter.
- There is typically a single customer-facing IP interface on the sRouter.
- The operator-facing IP interface is Ethernet encapsulated.
- The customer-facing IP interface is Ethernet encapsulated.
- The sRouter advertises itself as a router (using ND) on all customer-facing interfaces so clients and routers learn about the sRouter. The sRouter does not send Router Advertisements on its operator-facing interface.

9.2 Overview

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

The Neighbor Discovery (ND) protocol is required on the sRouter. 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 sRouter to advertise its presence, host configuration parameters, routes, and on-link preferences.

Figure 10 shows a block diagram of the sRouter 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 Router and Neighbor Discovery blocks are closely intertwined and, therefore, are discussed together under the same clause.

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

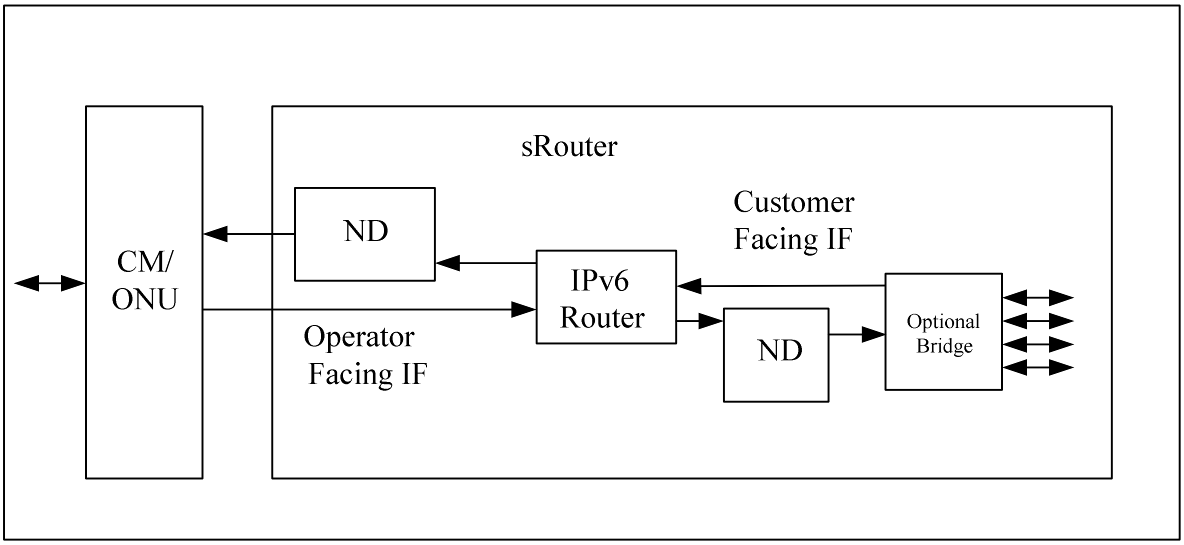


Figure 10: sRouter IPv6 forwarding block diagram

9.3 System description

Except when noted, the ND function in the sRouter shall comply with the Neighbor Discovery for IPv6 specification [43]. Per IETF RFC 4861 [43], ND is used "to determine the link-layer addresses for neighbours known to reside on attached links and to quickly purge cached values that become invalid".

Several clauses of IETF RFC 4861 [43] do not apply to the SRouter. These clauses include:

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

The sRouter shall support the Router Solicitation, Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement messages per IETF RFC 4861 [43].

The sRouter receives a packet and checks the destination address of the packet. If the destination IPv6 address matches the address assigned to the sRouter's IP interface, the sRouter forwards the packet to its local IP stack for processing. If the destination IPv6 address does not match the sRouter's address, the sRouter 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 prefixes assigned to the IP interfaces on which the sRouter is communicating. 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 the address of the packet does not match, the destination is considered remote or "not on-link", and the next-hop to use for ND purposes is the address of the intermediate router. If there is no intermediate router, the sRouter shall immediately drop the packet.

The typical scenario for packets routed to the operator-facing IP interface is that the next-hop router will be the sRouter's default router address, learned via Router Advertisement [24], from the service provider's network. Discovering other routers, aside from the CMTS (or routing delegate if the CMTS/OLT 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 sRouter. If the sRouter cannot determine the next-hop of the IPv6 destination address, then it shall immediately drop the packet.

Once a next-hop is determined, the sRouter's neighbour 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 neighbour to return its link-layer address in a Neighbor Advertisement. The neighbour cache entry is then updated with this link-layer address, and the sRouter then forwards the packet to the link-layer address contained in this cache entry. If an error occurs at any point in the process, the sRouter discards the packet. Regardless of whether the packet was received from the customer-facing IP interface or the operator-facing IP interface, the sRouter shall generate an appropriate ICMP error message as described in IETF RFC 4884 [45] 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 item (e) of clause 2.4 of IETF RFC 4884 [45]).
- The packet is destined for a link-layer multicast address.
- The source IPv6 address of the packet does not uniquely identify a single node as explained in detail in item € of clause 2.4 of IETF RFC 4884 [45].

The sRouter shall process and/or generate the following ICMPv6 messages when appropriate:

1	Destination Unreachable	[42]
3	Time Exceeded	[42]
129	Echo Reply	[42]
130	Multicast Listener Query	[30]
131	Multicast Listener Report	[30]
132	Multicast Listener Done	[30]
133	Router Solicitation	[43]
134	Router Advertisement	[43]
135	Neighbor Solicitation	[43]
136	Neighbor Advertisement	[43]
143	Version 2 Multicast Listener Report	[30]

NOTE: It is considered inappropriate for the sRouter to generate ICMPv6 Destination Unreachable messages on the operator-facing interface.

The IPv6 CE router shall implement ICMPv6 according to IETF RFC 4443 [42].

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

The sRouter is also responsible for reinserting the Ethernet header of IPv6 packets. The sRouter 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 clause 7.4). The sRouter shall 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 sRouter shall 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 IETF RFC 4861 [43], the sRouter uses the MAC address of the next-hop address learned via Neighbor Discovery as the destination MAC address for the IPv6 packet.

The sRouter shall forward link-local multicast packets received on either interface only to the sRouter's IP stack. The sRouter shall not forward link-local multicast packets received on either interface to any interface other than the sRouter's IP stack.

By default, an sRouter shall not initiate any IPv4 or IPv6 dynamic routing protocols on its operator-facing interface.

9.4 IPv6 multicast

9.4.1 General requirements

The sRouter 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 sRouter forwards IPv6 multicast packets downstream based upon the information learned at each customer-facing interface. The sRouter shall support the forwarding of Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) IP multicast streams.

The sRouter 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 sRouter generates, terminates, and processes MLD messages according to MLDv2 requirements. For example, the version of MLD used on the operator network or the local area network will be defined locally at each network. The sRouter may send MLDv1 reports on the operator-facing interface while generating MLDv2 queries on customer-facing interfaces.

The following elements define the sRouter IPv6 multicast behavior (also shown in figure 11):

- an MLDv2 Multicast Listener that implements the multicast listener part of MLDv2 [30] on the operator-facing interface;
- an MLDv2 Router that implements the router part of MLDv2 [30] 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 11.

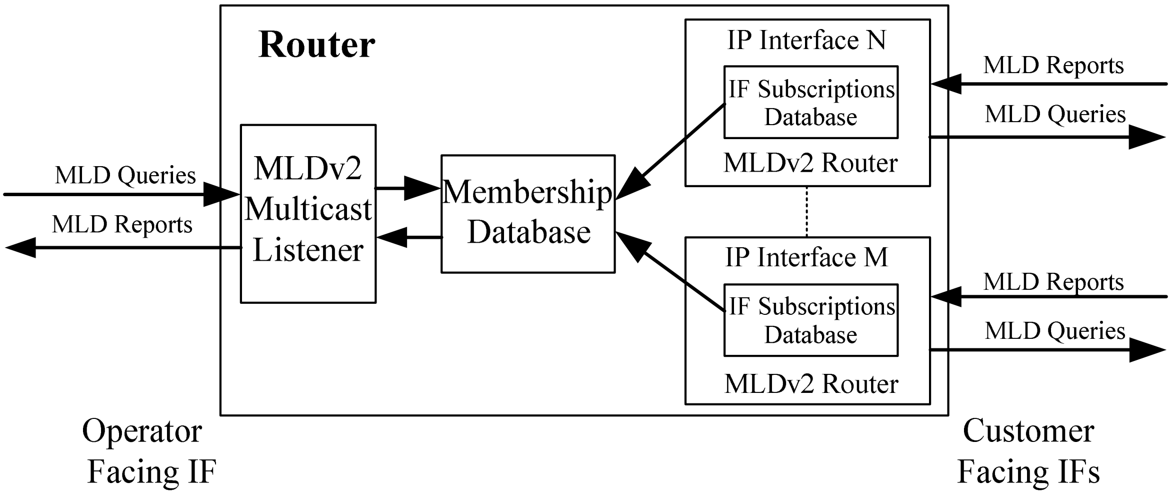


Figure 11: sRouter IPv6 multicast forwarding block diagram

9.4.2 MLD proxying

The sRouter maintains the multicast reception state of CPEs on each customer-facing interface in the interface's multicast subscription database. The sRouter 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 sRouter in the form of MLD Report messages transmitted by CPEs. The sRouter shall implement the router portion of the MLDv2 protocol [30] on each customer-facing interface. The sRouter shall 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 sRouter. The sRouter shall always act as an MLD querier on its customer-facing interfaces.

On the operator-facing interface, the sRouter shall implement the multicast listener portion of the MLDv2 protocol [30]. The sRouter shall merge the multicast reception state of connected CPEs into an IPv6 group membership database as described in clause 9.4.3. The sRouter shall use the membership database as multicast reception interface state per clause 4.2 of IETF RFC 3810 [30] for the operator-facing interface. Thus, when the composition of the IPv6 multicast membership database changes, the sRouter reports the change with an unsolicited report sent on the operator-facing interface. When queried by an upstream multicast router, the sRouter also responds with information from the membership database.

The sRouter shall not perform the router portion of MLDv2 on the operator-facing interface.

9.4.3 IPv6 group membership database

The sRouter's group membership database is formed by merging the multicast reception state records of customer-facing interfaces. In compliance with IETF RFC 3810 [30], the sRouter 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 sRouter keeps an IPv6 group membership database with records of the form:

- (multicast address, filter mode, source list)

The sRouter 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 sRouter shall abide by the following process to merge all customer interface records for the group into one group membership database record:

- First, the sRouter 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 sRouter 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 clause 4.2 of IETF RFC 3810 [30].

9.4.4 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 sRouter shall 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 sRouter shall not replicate an IPv6 multicast session on a customer-facing interface if no CPE device connected to the interface has joined the session.

In compliance with IPv6 link-scope packet forwarding rules, the sRouter shall not forward MLD messages received on an IP interface onto another IP interface. Also, the sRouter shall not forward link-scoped IPv6 multicast packets received on an IP interface onto another IP interface.

The sRouter shall forward site-scoped IPv6 multicast packets to all customer-facing interfaces within the same customer-facing IP interface except the customer-facing interface from which they were received.

The sRouter shall forward all non-link-scoped and non-site-scoped (e.g. not addressed to FF02::/16 or FF05::/16) IPv6 multicast traffic received on customer-facing interfaces onto the operator-facing interface. Operator control of multicast traffic forwarding onto the operator network, if desired, can be done through the implementation of filters at the demarcation device.

9.4.5 IPv6 multicast forwarding example

The sRouter 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 sRouter (e.g. the CMTS) supports and is configured to operate in MLDv2 mode, and thus the sRouter works in MLDv2 mode on the operator-facing interface.

The setup is shown in figure 12.

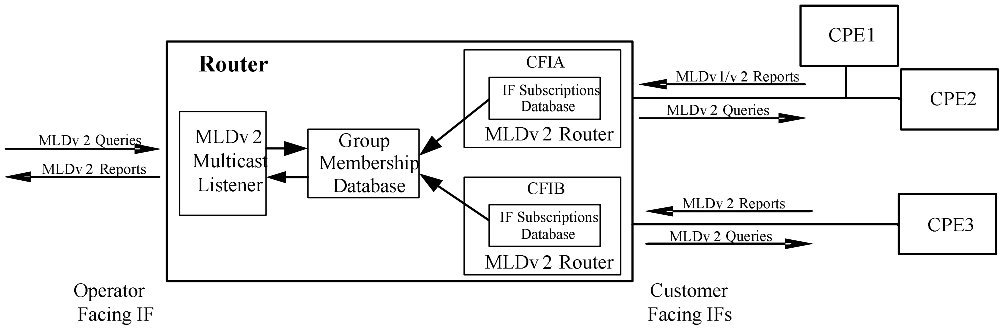


Figure 12: IPv6 multicast forwarding example

The CPEs send reports as follows:

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 sRouter multicast reception state at each customer-facing interface is the following:

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 sRouter merges the multicast reception state of connected CPEs into the group membership database as follows:

Multicast address	Filter mode	Source address
FF1E::100	EXCLUDE	Null
FF1E::128	EXCLUDE	Null

The sRouter 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 sRouter sends an MLDv2 report for the two records shown.

Assuming that the CMTS is transmitting four multicast streams downstream, the sRouter forwards them as follows:

Stream #	Multicast address	Source address	sRouter forwards on interface	
			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

10 Quality of Service (QoS)

10.1 General requirements

QoS on the sRouter is optional. The sRouter should support layer 2 and layer 3 QoS as defined in clause 10. The QoS functionality described in clause 10 allows the operator to selectively provide a level of differentiation among the various data streams destined for CPE behind the sRouter. Typical applications could include Internet Protocol TeleVision (IPTV) services and other enhanced data services, though it is anticipated that overall packet counts will still be dominated by largely undifferentiated best-effort data traffic.

If the sRouter supports QoS, the sRouter shall manage the forwarding of IP packets based on the values marked in the IPv4 ToS byte or IPv6 Traffic Class field. This is because layer 2 (e.g. 802.1p/q Ethernet) headers will be removed as the packets traverse the sRouter.

10.2 Downstream QoS operation

The present clause deals with the requirements regarding traffic going to CPEs, through the sRouter, from the access network.

If the sRouter supports QoS, the sRouter shall provide two or more queues on each customer-facing interface for traffic going to CPEs. The sRouter may provide a configuration mechanism to map ToS/Traffic Class field values to the various queues. As a default setting, the sRouter might use the most significant bit of the ToS/Traffic Class field to determine queue mappings.

10.3 Upstream QoS operation

The present clause deals with traffic coming from the CPEs attached to the sRouter to the access network.

For the purposes of applying QoS to upstream traffic sourced from CPE devices, the interface between the sRouter and the access network demarcation device is considered to be of infinite bandwidth and thus no congestion, control, priority, nor reservation of bandwidth resources should be expected to occur on this interface. Thus, the sRouter does not need to provide any queues in the upstream direction. The sRouter may provide a configuration mechanism to determine whether the sRouter allows CPE devices to pass QoS-tagged packets with the IP ToS/Traffic Class field intact, or whether the sRouter resets the IP ToS/Traffic Class field to 0. The sRouter 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 sRouter may support additional QoS mechanisms to prioritize upstream traffic based on ingress interface.

11 sRouter management

11.1 General requirements

The sRouter allows the implementation of different management interfaces as described in clause 11. Management interfaces in the present document refer to the protocols, data models, and semantic representation of the data exchange to perform the conventional management functions in the device.

The sRouter shall support TR-069 [66] from the operator-facing management interface.

The router may support SNMP for remote management capability. If the router supports SNMP, then it shall support SNMPv2 as specified in IETF RFC 1901 [13] and IETF RFC 1907 [14].

User management from the customer-facing interface is vendor-specific. Remote management of the sRouter (from the operator-facing interface) by the customer is outside of the scope of the present document.

11.2 sRouter TR-069 management interface requirements

The sRouter TR-069 management interface requirements are listed in annex C.

11.3 sRouter SNMP management interface requirements

11.3.1 Introduction

The sRouter SNMP management interface is configured using the TR-069 [66] management interface. BBF TR-181 [67] is extended to provision basic SNMP agent functions as listed in [72].

11.3.2 ACS discovery

11.3.2.1 Introduction

The sRouter performs initial ACS discovery via the mechanisms specified in clause 11.3.2.

11.3.2.2 TR-069 management server DHCP requirements

The sRouter shall follow the DHCP requirements in TR-069 [66] for the initial ACS discovery with the possible exception of using any vendor-specific DHCP options mentioned in the present document.

11.3.3 ACS selection

The sRouter shall use TR-069 Management Server URL DHCP option as the initial ACS URL. If the TR-069 Management Server URL is not present in the DHCP Offer/Response, the sRouter shall not communicate with any ACS.

11.3.4 Dynamic ACS updates

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

11.3.5 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 procedures specified in TR-069 [66].

The parameter Device.ManagementServer.URL is delivered via DHCP.

12 Security

12.1 Introduction

sRouter security is important in order to provide a reliable service to subscribers and to protect their traffic as well as the operator's network from attacks. The security requirements in clause 12 cover traffic filtering, the management interface, software update, secure boot, the data plane and community Wi-Fi.

12.2 Traffic filtering

It is considered a best practice to filter obviously malicious traffic (e.g. spoofed packets, "Martian" addresses, etc.). Thus, the sRouter ought to support basic stateless egress and ingress filters. The sRouter 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 the present document. Filters should be remotely configurable by the operator. All provided filters shall be able to be remotely enabled or disabled by the operator. While implementation is left to vendors, filters should allow protection of both the sRouter and traffic passing through the sRouter.

The sRouter shall enable a stateful firewall by default. In particular, the sRouter should support functionality sufficient for implementing the set of recommendations in clause 4 of IETF RFC 5908 [52]. The sRouter shall support ingress filtering in accordance with IETF RFC 2827 [20]. Management and configuration of the stateful firewall may be by either or both the operator or the end user; however, the firewall should be remotely configurable by the operator. All features of the firewall shall be able to be remotely enabled or disabled by the operator. Implementation method of the firewall by vendors is beyond the scope of the present document.

IETF RFC 6092 [52] contains 50 "*Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service.*" Not all of these recommendations are applicable to operator networks. Of the applicable recommendations, not all are needed immediately. In order to ensure that vendors are able to implement "simple security" support in sRouter devices, annex D categorizes the recommendations into five requirement categories:

- Critical - Critical to network connectivity. Include in initial release.
- Important - Failure to implement could open subscribers to infosec attack.
- BCP - Security best practice/nice to have but not critical.
- Other - Operators have indicated ambivalence to this category of recommendations.
- Conflict - Recommendation conflicts with operator needs and requires modification or should not be implemented.

The local user should not be able to filter or block traffic necessary for the network operator to manage the sRouter.

12.3 Management security on the operator-facing interface

12.3.1 General requirements

The management connection on the operator-facing interface uses TR-069 and may use SNMP. The operator can secure the TR-069 interface by using an HTTPS URL for the Auto-Configuration Server (ACS). The sRouter shall establish a TLS connection with the ACS when an HTTPS URL is provided in the TR-069 Management Server URL DHCP option. When TLS is being used, the sRouter shall not accept or respond to TR-069 messages outside of the TLS connection. The sRouter shall support TLS 1.1 [39] and TLS 1.2 [46]. The sRouter may support other TLS versions. When SNMP is used, the sRouter shall establish a DTLS connection with the SNMP manager if a secure URI is provided during SNMP management interface configuration. When DTLS is being used, the sRouter shall not accept or respond to SNMP messages outside of the DTLS connection. The sRouter shall support DTLS 1.0 [40] and DTLS 1.2 [57]. It may also support other DTLS versions.

When using TLS or DTLS, the sRouter shall communicate its capabilities to the ACS or SNMP manager as specified in appendix E of TLS 1.2 [46], allowing the servers to choose the version of protocol to use.

During the initial TLS message exchange, the server and client negotiate the security algorithms for key exchange, traffic encryption and traffic integrity using cipher suites. The client indicates what cipher suites it supports, and the server selects which cipher suite will be used to secure the TLS connection. The sRouter shall support the following cipher suites defined in TLS 1.2 [46] when using TLS or DTLS:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

The sRouter may support additional cipher suites.

Digital certificate PKI credentials are used to authenticate both ends of the TLS or DTLS connection. The sRouter shall use the digital certificate PKI defined in annex F when establishing a secure TLS or DTLS management connection with the headend.

The root CA certificate of the PKI is used as a trust anchor in both the headend management server and the sRouter for validating received certificates. The root CA certificate can be acquired by requesting it from the CA managing the PKI. The operator installs the root CA certificate as a trust anchor in its management server(s). The sRouter shall have the root CA certificate installed as a trust anchor for validating certificates received from headend management servers.

A certificate with a unique identifier is installed in the management server(s) and in each sRouter device along with its corresponding private key and issuing intermediate CA certificate. The operator is responsible for acquiring certificates for its management servers and the manufacturer is responsible for acquiring sRouter device certificates to be installed during the manufacturing process. The sRouter shall have a device certificate, its corresponding private key, and issuing CA certificate installed. When mutual authentication is performed, the server and sRouter exchange certificates (server/device certificate and issuing intermediate CA certificate).

12.3.2 Management server authentication

When an sRouter receives certificates from the management server during TLS or DTLS authentication it shall perform the following validation checks:

1) Verify that the server certificate chains to the root CA certificate trust anchor using Basic Path Validation procedures defined in the X.509 PKI certificate standard [47].

2) Verify that the host portion of the ACS URL or SNMP manager URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the server certificate.

3) Verify the server certificate and issuing intermediate CA certificate are not revoked by checking the corresponding CRL of the issuing CAs.

To perform certificate revocation, the sRouter shall support CRLs as defined in the X.509 PKI certificate standard [47]. During manufacture the sRouter shall have the latest CRLs from the issuing CA of the server certificate and the intermediate CA certificate installed. When the current date/time is greater than the CRL's nextUpdate time, the sRouter shall attempt to download a new CRL using the URL provided in the Issuing Distribution Point extension of the CRL. If the attempt to download a new CRL is unsuccessful, the sRouter shall continue to use the current CRL.

Before accepting a new CRL, the sRouter shall verify its signature using the CA certificate identified in the current CRL's AIA extension. If the sRouter does not have the CA certificate, it shall download it using the URL provided in the current CRL's AIA extension. If the sRouter is unable to verify the new CRL's signature, it shall reject the new CRL and continue using the current CRL.

If the attempt to download a new CRL or verify a new CRL's signature is unsuccessful, the sRouter shall log an error, and retry the CRL download using the Session Retry Policy defined in BBF TR-069 [66]. If the sRouter is unable to establish a successful TLS or DTLS connection with the management server, it shall retry the connection using the Session Retry Policy defined in BBF TR-069 [66] and reset itself after the fifth retry count.

12.3.3 sRouter authentication

To support certificate-based mutual authentication, operators need to configure their management servers to request client certificates during TLS or DTLS certificate exchange. Management servers should validate sRouter device/client certificates using a similar method as defined in clause 12.3.2. The sRouter shall send its device certificate and issuing intermediate CA certificate to the management server during the TLS and DTLS authentication process when requested.

12.4 Secure software update

12.4.1 Introduction

The main steps for sRouter secure software update involve downloading software from the file server, installation, and software verification each time it is loaded into memory for execution during boot up. Clause 12.4 covers software download and secure boot.

12.4.2 Secure software download

12.4.2.1 Introduction

There are two methods used for secure software download: TR-069 and DOCSIS SNMP.

12.4.2.2 TR-069 secure download

TR-069 uses HTTP to download a software image from a file server. The download is triggered by the operator sending a Download RPC message to the sRouter. The operator can secure the download connection by using an HTTPS URL in the Download RPC message. If an HTTPS URL is provided in the TR-069 Download RPC message, the sRouter shall establish a TLS connection with the file server before downloading the software image.

Mutual authentication of the HTTPS download connection uses digital certificate PKI credentials and could use a username/password credential. The certificate PKI is defined in annex F. The sRouter shall use the digital certificate PKI defined in annex F when establishing an HTTPS connection with the download file server and performing server or client certificate authentication.

The root CA certificate of the PKI is used as a trust anchor in both the headend file server and the sRouter for validating received certificates. This is the same root CA certificate as used with securing the management connection in clause 12.3. The root CA certificate can be acquired by requesting it from the CA managing the PKI. The sRouter shall have the root CA certificate installed as a trust anchor for validating certificates received from the headend file server.

For sRouter authentication a device certificate or username/password credential can be used. If a device certificate is being used, the root CA certificate should be installed on the file server as a trust anchor for validating received sRouter device certificates. If a username/password credential is used, the file server should have access to the authorized username/password so it can be used to verify the username/password received from the sRouter.

A certificate with a unique identifier is installed in the file server along with its corresponding private key and issuing intermediate CA certificate. The operator is responsible for acquiring the certificates for the file server. When a client certificate is used for sRouter authentication, the sRouter device certificate used in securing the management connection can also be used for securing the software download connection. To enable sRouter authentication using a device certificate, the operator should configure their file server to request a client certificate when establishing an HTTPS connection. When the sRouter receives a client certificate request during HTTPS authentication, it shall send its device certificate and issuing intermediate CA certificate to the file download server.

When an sRouter receives certificates from the file server during HTTPS authentication, it shall perform the following validation checks:

1) Verify that the server certificate chains to the root CA certificate trust anchor using Basic Path Validation procedures defined in the X.509 PKI certificate standard [47].

2) Verify that the host portion of the Download RPC URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the server certificate.

3) Verify the server certificate and issuing intermediate CA certificate are not revoked. First check using an OCSP request to the OCSP URL in the certificate's AIA extension. If there is no response from the OCSP responder, then the sRouter checks the latest version of the CRL list it has stored. Additional sRouter certificate revocation support requirements are defined in clause 12.3.

When device certificates are used for sRouter authentication, the file server should validate them using a similar method as defined in clause 12.3.

After the sRouter has downloaded the new software image, it shall verify that it is compatible with the sRouter using a vendor-specific method before replacing the current image with the new image.

The image may be signed using the method defined in ETSI ES 203 311-6 [71] using code verification certificates (CVCs) issued from the PKI defined in annex F (same as DOCSIS 3.1 new PKI). If TR-069 image signature verification is enabled via the management interface, the sRouter shall validate the image signature as defined in the Code Verification Requirements clause of ETSI ES 203 311-6 [71] with the PKI defined in annex F when using the TR-069 download method. If TR-069 image signature verification is disabled and the image has been signed, the sRouter may ignore the image signature.

12.4.2.3 SNMP initiated secure software download

The SNMP initiated secure software download mechanism for the sRouter is based on the DOCSIS secure software download method defined in DOCSIS 3.1 [68], [69], [70] and [71]. The software image is signed using a Code Verification Certificate (CVC) and downloaded using TFTP from a file server. The sRouter then validates the signature on the image before replacing the current image. If SNMP management is supported by the sRouter, the DOCSIS SNMP secure software download mechanism defined in the present clause shall also be supported unless specified otherwise using the certificate PKI defined in annex F (same as the DOCSIS 3.1 new PKI). From a DOCSIS specification perspective, secure software download is considered already enabled and will trigger a download when the appropriate MIBs are set. The configuration file CVC to enable secure software download does not apply.

12.4.3 Secure boot

To help prevent attackers from hacking the sRouter device and replacing the software image with an unauthorized version, a method to secure the boot image is needed to verify that the image loaded into memory for execution during the boot process is authorized and valid. During the boot process, the sRouter should verify the software image is authorized before loading it into memory for execution using a hardware protected mechanism; the attacker cannot simply reflash the non-volatile memory in order to bypass the secure boot process. The sRouter should hardware-protect any keys used to verify the image. Details of the secure boot mechanism are left to vendor implementation detail.

12.5 Physical protection of keys in the sRouter

The sRouter shall store the Device Certificate private key in a manner that deters unauthorized disclosure and modification. Also, the sRouter should prevent debugger tools from reading the Device Certificate private key in production devices by restricting or blocking physical access to memory containing this key. The sRouter shall protect trust anchor public keys used for validating certificate chains and image signatures against unauthorized changes.

The sRouter shall meet security requirements as specified in FIPS PUB 140-3 [6] for all instances of private and public permanent key storage.

The sRouter shall meet Security Level 1 [6]. Security Level 1 requires minimal physical protection through the use of production-grade enclosures. The reader should refer to the cited document for the formal requirements; however, a summary of those requirements is provided in the present clause.

Under the classification of "physical embodiments" of cryptographic modules in FIPS PUB 140-3 [6], sRouter devices are "multiple-chip stand-alone cryptographic modules." For multiple-chip stand-alone modules, the following Security Level 1 requirements are specified in FIPS PUB 140-3 [6]:

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

12.6 Private data plane security on operator-facing interface

The operator-facing data plane carries in-home subscriber Internet traffic between the sRouter and the headend. Traffic may be unsecured (e.g. HTTP) or secured (e.g. HTTPS) by applications embedded in the sRouter or the subscriber's end devices. In cases where there is a reasonable threat of man-in-the-middle attacks, this traffic, or at least the unsecured traffic, should be secured using a protocol such as IPsec since it is applied lower in the protocol stack, including but not limited to transport protocols such as UDP and TCP IP traffic.

12.7 Community Wi-Fi security

When an sRouter supports community Wi-Fi traffic from roaming subscribers, it may be vulnerable to man-in-the-middle (MitM) attacks. A community Wi-Fi open SSID has no traffic protection over the wireless link, so subscribers should use application-specific security to protect sensitive or confidential information between the mobile device and the application server. This would include securing the connection to the authentication portal using HTTPS. Some operators may provide VPN applications to protect traffic.

For community Wi-Fi secure SSIDs, traffic is protected over the wireless link, but a MitM vulnerability can still exist at the modem where bridging of access network security and the Ethernet link occurs. It is important to properly secure community Wi-Fi secure SSID traffic, since roaming subscribers will assume their traffic is protected over the operator's network. This includes RADIUS traffic between the AP and AAA server. After successful authentication, the AAA server sends the Pairwise Master Key (PMK) to the AP for establishing a secure WPA2 connection with the mobile device. This PMK needs to be protected.

If GRE security is enabled via the management interface, the sRouter shall establish a secure DTLS 1.2 connection with the headend GRE concentrator to secure community Wi-Fi tunnelled traffic. Digital certificate PKI credentials are used to authenticate both ends of the DTLS connection. The certificate PKI requirements defined for securing the management interface also apply when securing the GRE concentrator connection. The sRouter shall use the certificate PKI requirements in clause 12.3 for securing the GRE tunnel, except that it verifies that the host portion of the GRE concentrator URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the server certificate. The sRouter device certificate is used for both management and GRE interface client authentication.

If AAA server security is enabled and connection to a AAA server has been configured via the management interface, the sRouter shall establish a secure DTLS 1.2 connection with the AAA server to protect transmission of the PMK. The certificate PKI requirements defined for securing the management interface also apply when securing the AAA server connection. The sRouter shall use the certificate PKI requirements in clause 12.3 for securing the AAA server connection, except that it verifies that the host portion of the AAA server URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the server certificate. The sRouter device certificate is used for both management and AAA server interface client authentication.

12.8 IPsec

The sRouter may utilize an IPsec tunnel or an IPsec encrypted GRE tunnel to protect traffic on the operator-facing interface. This traffic includes SNMP management traffic as well as AAA management traffic (RADIUS, TACACS) and GRE traffic for Community Wi-Fi applications. TR-069 management traffic is not included because it is protected by TLS as defined in clause 12.3. The sRouter IPsec architecture consists of an IPsec Gateway located in the service provider's headend that terminates IPsec tunnels from sRouter devices. An example architecture is provided in figure 13.

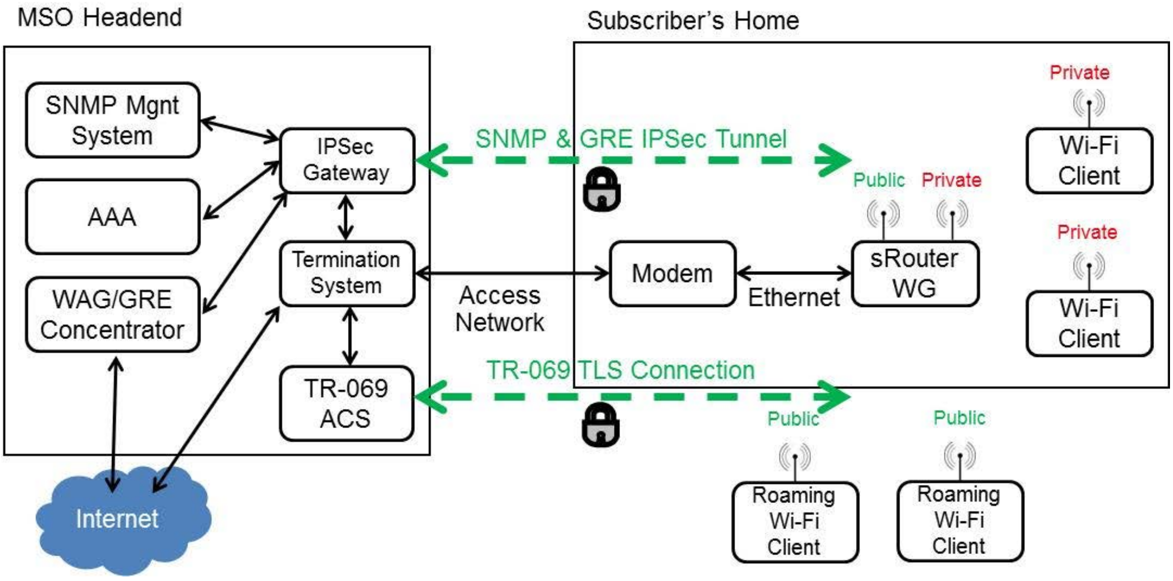


Figure 13: Example IPsec architecture

If the sRouter supports IPsec for securing traffic on the operator-facing interface, it shall implement the following requirements:

- If the sRouter is configured to enable the IPsec tunnel via the TR-069 management interface, it will establish an IPsec tunnel with the IPsec Gateway having the indicated domain name. The sRouter is required to support IPsec as defined in IETF RFC 4301 [38].

- IKEv2 is used to provide mutual authentication and key exchange between the IPsec Gateway and the sRouter using the certificate PKI defined in annex F. The sRouter is required to support IKEv2 defined in IETF RFC 7296 [62]. The sRouter will initiate an IKEv2 message exchange with the IPsec Gateway and use the certificate PKI defined in annex F for endpoint authentication purposes.

- The sRouter is required to validate certificates received from the IPsec Gateway using the Management Server Authentication steps defined in clause 12.3.2, except that it verifies the IPsec Gateway domain name value of the TR-069 management configuration matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the gateway certificate.

- During IKEv2 certificate exchange, the sRouter will send its device certificate and issuing intermediate CA certificate to the IPsec Gateway.

- The sRouter will use IPsec tunnel mode with an ESP header to secure packets.

- The sRouter is required to support the following cipher suites:

  - Data encryption - AES 128 CVC, AES 256 CBC

  - Message integrity - HMAC-SHA1-96, HMAC-SHA2-256-128

  - Pseudo-random function for key generation - HMAC-SHA1, HMAC-SHA2-256

- The sRouter is required to use the IPsec tunnel for sending & receiving SNMP, AAA, and GRE traffic. The IPsec tunnel can also be used for other traffic, e.g. the private data plane. The sRouter is required to ignore any SNMP, AAA, or GRE traffic received outside of the IPsec tunnel.

- If the sRouter is unable to establish a successful IPsec connection with the IPsec Gateway, it is required to retry the connection using the Session Retry Policy defined in BBF TR-069 [66] and reset itself after the fifth retry count.

13 Tunnel management and configuration

13.1 GRE requirements

Some of the applications envisioned for the sRouter rely upon the tunnelling of traffic between the customer's service location and the operator's network core. For example, a community Wi-Fi application that utilizes one or more SSIDs to provide public Wi-Fi could be configured to tunnel its traffic to a central concentrator within the operator's network core. While multiple tunnelling protocols and techniques exist, Generic Route Encapsulation (GRE) tunnelling as specified in IETF RFC 2784 [19] and IETF RFC 2890 [22] has become the prevalent method for conveying traffic to the operator's core. In order to support the management and configuration of these GRE tunnels, the present document defines both SNMP-based MIBs and BBF TR-181 [67] data model elements. The SNMP MIB defined referenced in the present document originated from the data model profiles for GRE tunnels specified in BBF TR-181 [67].

An sRouter that implements GRE over IPv4 shall support [19].

An sRouter that implements GRE over IPv6 shall support [22].

The sRouter shall support the BBF TR-181 [67]GRE data model elements found in BBF TR-181 [67].

An sRouter that supports GRE tunnelling and SNMP shall support [3].

When the sRouter is provisioned via the GRE tunnelling MIB in clause A.4, it shall permit the index of the Wi-Fi SSID to be set to the index numbers defined in clause A.1.

When the sRouter is provisioned via the GRE tunnelling profile in BBF TR-181 [67], it shall permit the index of the Wi-Fi SSID to be set to the index numbers defined in clause A.2.

Annex A (normative): SNMP MIB objects supported by the sRouter

A.1 General requirements

The present annex defines the SNMP MIBs that the sRouter is required to implement if SNMPv2c is supported.

The sRouter shall support the following MIB objects:

- Access Network Independent Device MIB [2];
- The System Group [26];
- The SNMP Group [26];
- The ifGeneralInformationGroup, the linkUpDownNotificationsGroup, and one of (ifFixedLengthGroup, ifHCFixedLengthGroup, ifPacketGroup, ifHCPacketGroup, ifVHCPacketGroup) [21];
- All mandatory groups of ipMIBCompliance2 in the IP-MIB [37];
- All mandatory groups of ipForwardReadOnlyCompliance in the IP-Forward-MIB [36];
- All mandatory groups of udpMIBCompliance2 in the UDP-MIB [32];
- All mandatory groups of tcpMIBCompliance2 in the TCP-MIB [31].

A.2 sRouter interface numbering

The sRouter shall 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. The sRouter shall use an ifIndex number in accordance with table A.1 for any additional customer-facing interfaces.

Table A.1: sRouter interface numbering

Interface	Type
1	Access network interface (sRouter operator-facing interface)
2 - 4	Reserved
5 - 15	Ethernet interfaces
16 - 31	Reserved
32 - 39	USB interfaces
40 - 47	MoCA interfaces
48 - 199	Reserved
200 - 299	Customer-facing IP interfaces
300 - 399	Operator-facing IP interfaces
400 - 499	GRE tunnel interfaces
1xxyy	Wi-Fi and SSID interfaces (where xx corresponds to the Wi-Fi radio interface (0 - 99), and yy corresponds to the SSID logical interface for Wi-Fi radio xx with yy in the range 1 - 99)
500 - 599	Additional sRouter CPE interfaces
600 - 699	sRouter internal interfaces (optional)

sRouter devices that include one or more Wi-Fi radios shall follow the interface numbering and naming conventions specified in clause 6.2.1 of [72].

A.3 sRouter ifTable requirements

The sRouter shall implement the row entry specified in table A.2 for the ifTable as specified in IETF RFC 2863 [21].

Table A.2: sRouter ifTable row entries

ifTable [21]	Row entry
ifIndex	1
ifDescr	sRouter operator-facing interface
ifType	other(1)
ifMtu	0
ifSpeed	0
ifPhysAddress	sRouter MAC address
ifAdminStatus	up(1)
ifOperStatus	up(1)
ifLastChange	per [21]
ifInOctets	0
ifInNUCastPkts	deprecated
ifInDiscards	0
ifInErrors	0
ifUnknownProtos	0
ifOutOctets	0
ifOutUCastPkts	0
ifOutNUCastPkts	deprecated
ifOutDiscards	0
ifOutErrors	0
ifOutQlen	deprecated
ifSpecific	deprecated

Additionally, for all interfaces supported the sRouter shall use the values contained in table A.3 for the referenced objects in the ifTable. This includes modifications to the MAX-ACCESS for specific objects, which differs from IETF RFC 2863 [21] in some cases.

Table A.3: sRouter ifTable row entries for supported interfaces

ifTable object	Ethernet	USB	MoCA	CFI IP	OFI IP	GRE	Wi-Fi	SSID
ifIndex	5 - 15	30 - 39	40 - 47	200 - 299	300 - 399	400 - 499	per clause A.2	per clause A.2
ifDescr	-	-	-	-	-	-	-	-
ifType	ethernetCsmacd	usb	moca	ipForward	ipForward	tunnel	ieee80211(71)	ieee80211(71)
ifMtu	-	-	-	-	-	-	-	-
ifSpeed	-	-	-	-	-	-	-	-
ifPhysAddress	Ethernet physical address	USB physical address	MoCA physical address	CFI IP MAC address	OFI IP MAC address	MAC associated with tunnel endpoint	empty string	SSID physical address
ifAdminStatus	per [21]	per [21]	per [21]	per [21] implemented as read-only	per [21] implemented as read-only	per [21] implemented as read-only	per [21]	per [21]
ifOperStatus	per [21]	per [21]	per [21]	per [21]	per [21]	per [21]	per [21]	per [21]
ifLastChange	unspecified	unspecified	unspecified	unspecified	unspecified	unspecified	unspecified	unspecified
ifInOctets	-	-	-	-	-	-	-	-
ifInNUCastPkts	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated
ifInDiscards	-	-	-	-	-	-	-	-
ifInErrors	-	-	-	-	-	-	-	-
ifUnknownProtos	-	-	-	-	-	-	-	-
ifOutOctets	-	-	-	-	-	-	-	-
ifOutUCastPkts	-	-	-	-	-	-	-	-
ifOutNUCastPkts	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated
ifOutDiscards	-	-	-	-	-	-	-	-
ifOutErrors	-	-	-	-	-	-	-	-
ifOutQlen	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated
ifSpecific	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated	deprecated

A.4 sRouter ipNetToPhysicalTable requirements

The sRouter shall implement the row entry specified in table A.4 for the ipNetToPhysicalTable as specified in IETF RFC 4293 [37].

Table A.4: sRouter ipNetToPhysicalTable row entries

ipNetToPhysicalTable [37]	sRouter device
ipNetToPhysicalIfIndex	1
ipNetToPhysicalNetAddressType	ipv4(1) or ipv6(2)
ipNetToPhysicalNetAddress	sRouter IP address
ipNetToPhysicalPhysAddress	sRouter MAC address
ipNetToPhysicalLastUpdated	per [37]
ipNetToPhysicalType	static(4)
ipNetToPhysicalState	per [37]
ipNetToPhysicalRowStatus	active

A.5 CLAB-GRE-MIB

An sRouter that implements GRE tunnelling shall support the GRE MIB [3].

A.6 CLAB-GW-MIB

The Gateway MIB module was derived from the data models specified in BBF TR-181 [67] and includes management objects for MAP-E and MAP-T. It is specified in [4].

A.7 CLAB-WIFI-MIB

If an sRouter supports an IEEE 802.11 interface and implements SNMP, the sRouter shall support the Wi-Fi MIB [5].

A.8 CLAB-ANI-DEV-MIB

An sRouter that implements SNMP shall support the access network independent device MIB [2].

Annex B (normative): Provisioning and operational event messages

This list of the following locally logged event messages will facilitate resolution of issues. Access to the event log is vendor implementation specific.

Device	Error code	Event ID	Severity	Intf	Event message text	Variables	Message counter	Time stamp
sRouter	H10.1	72001001	Informational		OFI - DHCPv4 - provisioning complete	NA	NA	<time>
sRouter	H10.2	72001002	Informational		OFI - DHCPv6 - provisioning complete	NA	NA	<time>
sRouter	H10.3	72001003	Critical		OFI - DHCPv4 - provisioning; x retries attempted; last attempt at <time>	NA	<count>	<time>
sRouter	H10.4	72001004	Critical		OFI - DHCPv6 - provisioning; x retries attempted; last attempt at <time>	NA	<count>	<time>
sRouter	H10.5	72001005	Critical		OFI - ICMPv6 - no RA message received in response to RS	NA	<count>	<time>
sRouter	H10.6	72001006	Critical		OFI - ICMPv6 - RA not properly configured for DHCPv6 (M = 0)	NA	NA	<time>
sRouter	H10.7	72001007	Critical		OFI - ICMPv6 - link local DAD issue; duplicate IP address detected	NA	NA	<time>
sRouter	H10.8	72001008	Critical		OFI - DHCPv4 - no Offer / Ack message received	NA	<count>	<time>
sRouter	H10.9	72001009	Critical		OFI - DHCPv6 - no Advertise / Reply message received	NA	<count>	<time>
sRouter	H10.10	72001010	Critical		OFI - DHCPv4 - required DHCP option missing	<option #>	NA	<time>
sRouter	H10.11	72001011	Critical		OFI - DHCPv6 - required DHCP option missing	<option #>	NA	<time>
sRouter	H10.12	72001012	Critical		OFI - DHCPv4 - bad value in required DHCP option	<option #>	NA	<time>
sRouter	H10.13	72001013	Critical		OFI - DHCPv6 - bad value in required DHCP option	<option #>	NA	<time>
sRouter	H10.14	72001014	Critical		OFI - DHCPv4 - provisioning failed; no address available	NA	NA	<time>
sRouter	H10.15	72001015	Critical		OFI - DHCPv6 - provisioning failed; no prefix available	NA	NA	<time>
sRouter	H10.16	72001016	Critical		OFI - DHCPv6 - GUA DAD issue; duplicate IP address detected	NA	NA	<time>
sRouter	H10.17	72001017	Critical		OFI - DHCPv4 - failure to renew address	NA	<count>	<time>
sRouter	H10.18	72001018	Critical		OFI - DHCPv6 - failure to renew prefix	NA	<count>	<time>
sRouter	H10.19	72001019	Critical		OFI - DHCPv4 - failure to renew lease	NA	<count>	<time>
sRouter	H10.20	72001020	Informational		OFI - DHCPv4 - IP address released	NA	NA	<time>
sRouter	H10.21	72001021	Informational		OFI - DHCPv6 - IP address released	NA	NA	<time>
sRouter	H20.1	72002001	Critical		CFI - LAN Provisioning - no prefix available for sRouter interface(s)	<interface #>	NA	<time>

Device	Error code	Event ID	Severity	Intf	Event message text	Variables	Message counter	Time stamp
sRouter	H20.2	72002002	Critical		CFI - LAN Provisioning DHCPv6-PD - no prefix available; subdelegation	NA	Client ID (duid)	<time>
sRouter	H20.3	72002003	Informational		CFI - LAN Provisioning DHCPv6-PD - PD allocation mode set to width	NA	NA	<time>
sRouter	H20.4	72002004	Informational		CFI - LAN Provisioning DHCPv6-PD - PD allocation mode set to depth	NA	NA	<time>
sRouter	H20.5	72002005	Informational		CFI - LAN Provisioning DHCPv6-PD - PD hint of length 'X' received	X = [Null], Range [48 - 64]	Client ID (duid)	<time>
sRouter	H20.6	72002006	Alert		CFI - LAN Provisioning DHCPv6-PD - allocated prefix size X less than requested prefix Y; subdelegation	X, Y	Client ID (duid)	<time>
sRouter	H20.7	72002007	Critical		CFI - LAN Provisioning DHCPv6 - no client addresses available	NA	Client ID (duid)	<time>
sRouter	H20.8	72002008	Critical		CFI - Link Local DAD - duplicate IP address detected	NA	Client ID (duid)	<time>
sRouter	H20.9	72002009	Critical		CFI - GUA DAD - duplicate IP address detected	NA	Client ID (duid)	<time>
sRouter	H20.10	72002010	Critical		CFI - DHCPv6 - reconfigure failure	NA	Client ID (duid)	<time>
sRouter	H20.11	72002011	Critical		CFI - LAN Provisioning DHCPv4 - no Address available	NA	NA	<time>
sRouter	H20.12	72002012	Informational		CFI - LAN Provisioning DHCPv4 - IP address conflict	NA	CHADDR	<time>
sRouter	H30.1	72003001	Informational		sRouter administratively disabled	NA	NA	<time>
sRouter	H30.2	72003002	Informational		sRouter enabled as IPv4 Only	NA	NA	<time>
sRouter	H30.3	72003003	Informational		sRouter enabled as IPv6 Only	NA	NA	<time>
sRouter	H30.4	72003004	Informational		sRouter enabled as Dual Stack	NA	NA	<time>

Annex C (normative): TR-069 managed objects

C.1 General requirements

The sRouter shall support the objects associated with the profiles and components listed in the present annex. See BBF TR-069 [66] for information about components and profiles.

C.2 Profiles from TR-181

Table C.1: TR-181 profiles for sRouter

Profile	Requirement	Notes
Download:1	may	
DownloadTCP:1	may	
Upload:1	may	
UploadTCP:1	may	
UDPEcho:1	may	
UDPEchoPlus:1	may	
SupportedDataModel:1	shall	
SupportedDataModel:2	shall	
MemoryStatus:1	may	
ProcessStatus:1	may	
TempStatus:1	may	
TempStatusAdv:1	may	
TempStatusAdv:2	may	
AutonXferComplPolicy:1	may	
User:1	shall	
UPnPDev:1	shall	support data model, other specs to detail UPnP functional requirements
UPnPDiscBasic:1	shall	support data model, other specs to detail UPnP functional requirements
UPnPDiscAdv:1	may	
UPnPDiscAdv:2	may	
SelfTestDiag:1	may	
NSLookupDiag:1	may	
SimpleFirewall:1	shall	
AdvancedFirewall:1	shall	
USBHostsBasic:1	may	
USBHostsAdv:1	may	
PeriodicStatsBase:1	may	
PeriodicStatsAdv:1	may	
DownloadAnnounce:1	may	
DownloadQuery:1	may	
Baseline:3	shall	
Optical:1	shall if interface supported	
EthernetRMONStats:1	may	
Ghn:1	shall if interface supported	
DNSRelay:1	may	
Routing:1	shall	
Routing:2	shall	
IPv6Routing:1	shall	
IPinterface:2	shall	
IPv6interface:1	shall	
VLANTermination:1	shall	
EthernetLink:1	shall	
Bridge:1	shall	
VLANBridge:1	shall	
BridgeFilter:2	shall	

Profile	Requirement	Notes
BridgeFilterL3L4Filter:1	may	
Ethernetinterface:1	shall	
Ethernetinterface:2	may	
ProviderBridge:1	may	
ProviderBridgeQoS:1	may	
LLDPBaseline:1	may	
LLDPRemOrgDeInfo:1	may	
GREBasic:1	shall	
GREAdv:1	shall	
MAPBasic:1	shall	
MAPAdv:1	shall	
HPNA:1	shall if interface supported	
HPNADiagnostics:1	shall if interface supported	
HPNAQoS:1	shall if interface supported	
HomePlug:1	shall if interface supported	
MoCA:1	shall if interface supported	
UPA:1	shall if interface supported	
UPDiagnostics:1	shall if interface supported	
WiFiRadio:1	per [72]	
WiFiSSID:1	per[72]	
WiFiAccessPoint:1	per [72]	
WiFiEndPoint:1	per [72]	
USBinterface:1	shall if interface supported	
USBPort:1	shall if interface supported	
NAT:1	shall	
QoS:2	may	
QoSDynamicFlow:1	may	
QoSStats:1	may	
NeighborDiscovery:1	shall	
RouterAdvertisement:1	shall	
IPv6rd:1	may	
DSLite:1	may	
Hosts:2	shall	
GatewayInfo:1	shall	
DeviceAssociation:1	shall	
UDPConnReq:1	may	
CaptivePortal:1	may	
Time:1	may	
IEEE8021xAuthentication:1	per [72]	
IPPing:1	may	
TraceRoute:1	may	
DHCPv4Client:1	shall	
DHCPv4Server:1	shall	
DHCPv4CondServing:1	may	
DHCPv4Relay:1	shall not	
DHCPv4ServerClientInfo:1	shall	
DHCPv6Client:1	shall	
DHCPv6ClientServerIdentity:1	shall	
DHCPv6Server:1	shall	
DHCPv6ServerAdv:1	may	
DHCPv6ServerClientInfo:1	shall	
Processors:1	may	
VendorLogFiles:1	may	
DUStateChngComplPolicy:1	may	
SM_ExecEnvs:1	may	
SM_DeployAndExecUnits:1	may	
SM_Baseline:1	may	
Location:1	may	
FaultMgmtSupportedAlarms:1	may	
FaultMgmtActive:1	may	
FaultMgmtHistory:1	may	
FaultMgmtExpedited:1	may	
FaultMgmtQueued:1	may	
BulkDataColl:1	may	

Profile	Requirement	Notes
BullDataReports:1	may	
BulkDataJSONEncoding:1	may	
BulkDataCSVEncoding:1	may	
BulkDataHTTP:1	may	
BulkDataFileTransfser:1	may	
BulkDataStreaming:1	may	
IPsec:1	may	
IPsecAdv:1	may	
DNS_SD:1	shall	
StandbyPolicy:1	may	
XMPPBasic:1	may	
XMPPConnReq:1	may	
XMPPAdvanced:1	may	
XMPPReconnect:1	may	
UDPEchoDiag:1	may	
ServerSelectionDiag:1	may	
InformParameters:1	may	
IEEE1905Device:1	shall if interface supported	
IEEE1905TopologyMetric:1	shall if interface supported	
IEEE1905TopologyNeighbor:1	shall if interface supported	
IEEE1905TopologyHigherLayer	shall if interface supported	
IEEE1905Power:1	shall if interface supported	
IEEE1905interfaceSelection:1	shall if interface supported	
IEEE1905LinkMetric:1	shall if interface supported	
IEEE1905NetworkTopology:1	shall if interface supported	
Device.PCP	may	shall if DS Lite is implemented

C.3 Extensions to TR-181 profiles

C.3.1 GRE tunnelling extensions

The following are the extensions to the profiles defined in BBF TR-181 [67] for GRE tunnelling.

Table C.2: Extensions to TR-181 profiles for GRE

Attribute name	Type	Access	Type constraints	Units	Default
KeepAliveCount	unsignedInt	W			3
KeepAliveInterval	unsignedInt	W		seconds	60
KeepAliveFailureInterval	unsignedInt	W		seconds	300
KeepAliveRecoverInterval	unsignedInt	W		seconds	43200

MSSClampingValue	unsignedInt	W	Disabled(0)
			Clamped(1)
			Clamping Size(>1)
					0

ConcentratorServiceName	unsignedInt	W		FQDN	
RemoteEndpointConnectivityState	string(256)	RW			

An sRouter that implements GRE and TR-069 [66] shall support the data objects in table C.2.

The GRE data object descriptions are as follows:

- KeepAliveCount - Number of keep-alive messages sent in a burst at regular intervals.
- KeepAliveInterval - Interval in seconds between keep-alive message bursts.
- KeepAliveFailureInterval - Time (in seconds) to wait after all available GRE concentrators fail to respond, before retrying the first GRE concentrator address.

- KeepAliveRecoverInterval - Time (in seconds) to remain on a secondary GRE concentrator, with clients connected, before retrying primary GRE concentrator. A value of 0 means no limit. Setting to a small non-zero value will cause an immediate switch from a secondary GRE concentrator back to the primary.

- MSSClampingValue - Specifies whether TCP MSS clamping is enabled on the tunnel. 0 disables clamping. 1 clamps the MSS depending on the interface MTU. A value > 1 will be used as clamping size.

- ConcentratorServiceName - FQDN of GRE tunnel concentrator / GW service. If this is set, then a DNS query of type SRV will be used for discovering the FQDN of remote endpoints on a GRE tunnel.

- RemoteEndpointConnectivityState - Comma-separated list (up to 4 items) of strings. Each item corresponds to one item in the RemoteEndpoints list, and contains one of the following strings: Reachable indicates that the corresponding remote endpoint is responding to any configured KeepAlive messages; Unreachable indicates that the remote endpoint has failed to adequately respond to the most recent KeepAlive attempt; NotInUse indicates that the remote endpoint has not been used.

C.3.2 sRouter extensions

The following are the extensions to the Device.Routing.sRouter object defined in BBF TR-181 [67].

Table 7: Extensions to TR-181 profiles for sRouter

Attribute Name	Type	Access	Type Constraints	Units	Default

TopologyMode	boolean	R	depth(0)
			width(1)		

LinkIDEnable	boolean	R	disable(0)
			enabled(1)
					1

An sRouter shall support the data objects in table C.3.

C.4 Management interface protocol requirements for GRE

Table C.4 shows the mapping between the objects in the TR-181 data model and the SNMP MIB objects for GRE. Extension objects are included for completeness. An sRouter shall support the data objects in table C.4.

Table 8: GRE data model objects

TR-181 object model	SNMP MIB object	Requirement
Device.GRE.		
TunnelNumberOfEntries	clabGRETunnelNumberOfEntries	Mandatory
FilterNumberOfEntries	clabGREFilterNumberOfEntries	Mandatory
Device.GRE.Tunnel.{i}.		
Enable	clabGRETunnelEnable	Mandatory
Status	clabGRETunnelStatus	Mandatory
Alias	clabGRETunnelAlias	Mandatory
RemoteEndpoints	clabGRETunnelRemoteEndpoints	Mandatory
KeepAlivePolicy	clabGRETunnelKeepAlivePolicy	Mandatory
KeepAliveTimeout	clabGRETunnelKeepAliveTimeout	Mandatory
KeepAliveThreshold	clabGRETunnelKeepAliveThreshold	Mandatory
DeliveryHeaderProtocol	clabGRETunnelDeliveryHeaderProtocol	Mandatory
DefaultDSCPMark	clabGRETunnelDefaultDscpMark	Mandatory
ConnectedRemoteEndpoint	clabGRETunnelConnectedRemoteEndpoint	Mandatory
InterfaceNumberOfEntries	clabGRETunnelInterfaceNumberOfEntries	Mandatory
X_CABLELABS_COM_KeepAliveCount	clabGRETunnelKeepAliveCount	Mandatory
X_CABLELABS_COM_KeepAliveInterval	clabGRETunnelKeepAliveInterval	Mandatory
X_CABLELABS_COM_KeepAliveFailureInterval	clabGRETunnelKeepAliveFailureInterval	Mandatory
X_CABLELABS_COM_KeepAliveRecoverInterval	clabGRETunnelKeepAliveRecoverInterval	Mandatory
X_CABLELABS_COM_MSSClampingValue	clabGRETunnelTcpMssClamping	Mandatory
X_CABLELABS_COM_ConcentratorServiceName	clabGRETunnelConcentratorServiceName	Mandatory

TR-181 object model	SNMP MIB object	Requirement
X_CABLELABS_COM_RemoteEndpointConnectivityState	clabGRETunnnelRemoteEndpointConnectivityState	Mandatory
Device.GRE.Tunnel.{i}.Stats.		
KeepAliveSent	clabGRETunnelStatsKeepAliveSent	Mandatory
KeepAliveReceived	clabGRETunnelStatsKeepAliveReceived	Mandatory
BytesSent	clabGRETunnelStatsBytesSent	Mandatory
BytesReceived	clabGRETunnelStatsBytesReceived	Mandatory
PacketsSent	clabGRETunnelStatsPacketsSent	Mandatory
PacketsReceived	clabGRETunnelStatsPacketsReceived	Mandatory
ErrorsSent	clabGRETunnelStatsErrorsSent	Mandatory
ErrorsReceived	clabGRETunnelStatsErrorsReceived	Mandatory
Device.GRE.Tunnel.{i}.Interface.{i}.		
Enable	clabGRETunnelInterfaceEnable	Mandatory
Status	clabGRETunnelInterfaceStatus	Mandatory
Alias	clabGRETunnelInterfaceAlias	Mandatory
Name	clabGRETunnelInterfaceName	Mandatory
LastChange	clabGRETunnelInterfaceLastChange	Mandatory
LowerLayers	clabGRETunnelInterfaceLowerLayers	Mandatory
ProtocolIdOverride	clabGRETunnelInterfaceProtocolIdOverride	Mandatory
UseChecksum	clabGRETunnelInterfaceUseChecksum	Mandatory
KeyIdentifierGenerationPolicy	clabGRETunnelInterfaceKeyIdentifierGenerationPolicy	Mandatory
KeyIdentifier	clabGRETunnelInterfaceKeyIdentifier	Mandatory
UseSequenceNumber	clabGRETunnelInterfaceUseSequenceNumber	Mandatory
Device.GRE.Tunnel.{i}.Interface.{i}.Stats.		
BytesSent	clabGRETunnelInterfaceStatsBytesSent	Mandatory
BytesReceived	clabGRETunnelInterfaceStatsBytesReceived	Mandatory
PacketsSent	clabGRETunnelInterfaceStatsPacketsSent	Mandatory
PacketsReceived	clabGRETunnelInterfaceStatsPacketsReceived	Mandatory
ErrorsSent	clabGRETunnelInterfaceStatsErrorsSent	Mandatory
ErrorsReceived	clabGRETunnelInterfaceStatsErrorsReceived	Mandatory
DiscardChecksumReceived	clabGRETunnelInterfaceStatsDiscardChecksumReceived	Mandatory
DiscardSequenceNumberReceived	clabGRETunnelInterfaceStatsDiscardSequenceNumberReceived	Mandatory
Device.GRE.Filter.{i}.		
Enable	clabGREFilterEnable	Mandatory
Status	clabGREFilterStatus	Mandatory
Order	clabGREFilterOrder	Mandatory
Alias	clabGREFilterAlias	Mandatory
Interface	clabGREFilterInterface	Mandatory
AllInterfaces	clabGREFilterAllInterfaces	Mandatory
VLANIDCheck	clabGREFilterVlanIdCheck	Mandatory
VLANIDExclude	clabGREFilterVlanIdExclude	Mandatory
DSCPMarkPolicy	clabGREFilterDscpMarkPolicy	Mandatory

Annex D (normative): Simple security recommendations

D.1 Introduction

The present annex categorizes the recommendations from IETF RFC 6092 [52] into recommendations for sRouter devices. While IETF RFC 6092 [52] provides a good foundation for the development of a stateful inspection packet filtering firewall, it is not without omission and not all of its recommendations conform with best practices for operator networks. Additionally, in the context of integrated broadband cable telecommunication networks, several security mechanisms have been developed that supersede those provided in the recommendations. Where conflicts or recommendations other than those supplied by the RFC occur, they are called out explicitly.

D.2 Summary of simple security recommendations

The present clause provides a quick reference to the recommendations specified in IETF RFC 6092 [52] required by sRouter.

Critical - see table D.1
REC-3, REC-4, REC-5, REC-7, REC-10, REC-12, REC-14, REC-16, REC-18, REC-19, REC-21, REC-22, REC-23, REC-24, REC-25, REC-31, REC-32, REC-35, REC-36, REC-37, MSO-REC.

Important - see table D.2
REC-1, REC-2, REC-6, REC-8, REC-9, REC-11, REC-17, REC-33, REC-47.

BCP - see table D.3
REC-15, REC-20, REC-26, REC-27, REC-28, REC-29, REC-30, REC-38, REC-40, REC-41, REC-42, REC-43, REC-44, REC-45, REC-46, REC-48.

Other - see table D.4
REC-13, REC-49, REC-50.

Conflict - see table D.5
REC-34, REC-39.

D.3 Critical recommendations

The sRouter shall support [52] on the operator-facing interface. The following recommendations specified in IETF RFC 6092 [52] are critical to network connectivity and are to be included in all sRouter devices. All requirements in the present clause should be deemed mandatory as noted. These recommendations are in compliance with security requirements for the sRouter as the highest priority for development and testing.

Table D.1: Critical recommendations

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-3	Packets bearing source and/or destination addresses forbidden to appear in the outer headers of packets transmitted over the public Internet shall not be forwarded. In particular, site-local addresses are deprecated by [i.7], and [i.15] explicitly forbids the use of addresses with IPv4-Mapped, IPv4-Compatible, Documentation and ORCHID prefixes.	This would be the equivalent of an IPv6 bogon / martians list. Due to the CPU / memory resources of the devices and the fact that once deployed, it will not likely be changed, this would not include unallocated IPv6 space as it might on the backbone.
REC-4	Packets bearing deprecated extension headers prior to their first upper layer protocol header should not be forwarded or transmitted on any interface. In particular, all packets with routing extension header type 0 [i.4] preceding the first upper layer protocol header shall not be forwarded. (See [i.14] for additional background.)	

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-5	Outbound packets shall not be forwarded if the source address in their outer IPv6 header does not have a unicast prefix assigned for use by globally reachable nodes on the interior network.	uRPF like behavior
REC-7	By default, packets with unique local source and/or destination addresses [i.9] should not be forwarded to or from the exterior network.	Unique Local Addresses (ULA) can be forwarded between LAN interfaces on a customer premises router but as defined, should not exit the WAN interface. It is expected that ISP networks will not carry routes for ULA address blocks so traffic will be dropped anyway.
REC-10	IPv6 gateways shall forward ICMPv6 Destination Unreachable and Packet Too Big messages containing IP headers that match generic upper layer transport state records.	If not, an MTU size mismatch can prevent connectivity, causing IPv6 sessions to fail. Conversely, if there is no state table entry, drop the packets.
REC-12	Filter state records for generic upper-layer transport protocols shall not be deleted or recycled until an idle timer not less than two minutes has expired without having forwarded a packet matching the state in some configurable amount of time. By default, the idle timer for such state records is five minutes.	If the timers are less than 2-5 minutes, many VPN tunnels break because the keep alive timer is often set to 360 seconds.
REC-14	A state record for a UDP flow where both source and destination ports are outside the well-known port range (ports 0-1023) shall not expire in less than two minutes of idle time. The value of the UDP state record idle timer may be configurable. The default is five minutes.	See REC-12 except this applies to low ports instead of high ports.
REC-16	A state record for a UDP flow shall be refreshed when a packet is forwarded from the interior to the exterior, and it may be refreshed when a packet is forwarded in the reverse direction.	
REC-18	If a gateway forwards a UDP flow, it shall also forward ICMPv6 Destination Unreachable and Packet Too Big messages containing UDP headers that match the flow state record.	Avoiding breaking path MTU discovery.
REC-19	Receipt of any sort of ICMPv6 message shall not terminate the state record for a UDP flow.	If not supported, this could be employed in a DoS/DDoS attack against a CPE device by causing UDP sessions to close simply by receiving unsolicited ICMP reply messages.
REC-21	In their default operating mode, IPv6 gateways shall not prohibit the forwarding of packets, to and from legitimate node addresses, with destination extension headers of type Authentication Header (AH) [i.10] in their outer IP extension header chain.	This requirement applies only to IPv6 packets. IPv4 IPsec AH packets should continue to be blocked from the Internet to internal hosts by default.
REC-22	In their default operating mode, IPv6 gateways shall not prohibit the forwarding of packets, to and from legitimate node addresses, with an upper layer protocol of type Encapsulating Security Payload (ESP) [i.11] in their outer IP extension header chain.	This requirement applies only to IPv6 packets. Hosts sufficient to support IPv6 should support rejecting unrequested AH/ESP packets by any hosts within the LAN/WAN. IPv4 IPsec AH packets should continue to be blocked from the Internet to internal hosts by default.
REC-23	If a gateway forwards an ESP flow, it shall also forward (in the reverse direction) ICMPv6 Destination Unreachable and Packet Too Big messages containing ESP headers that match the flow state record.	
REC-24	In their default operating mode, IPv6 gateways shall not prohibit the forwarding of any UDP packets, to and from legitimate node addresses, with a destination port of 500, i.e. the port reserved by IANA for the Internet Key Exchange (IKE) Protocol [i.18].	Blocking will likely break common L3 VPN (IPsec) connectivity. The IPsec IKE service listening on UDP/500 will not respond if it does not have a corresponding IPsec policy configured. As a result, leaving UDP/500 open could expose hosts to attack but could not be used in a reflection attack. IPv4 UDP/500 packets should continue to be blocked from the Internet to internal hosts by default.

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-25	In all operating modes, IPv6 gateways should use filter state records for Encapsulating Security Payload (ESP) [i.11] that are indexable by a 3-tuple comprising the interior node address, the exterior node address, and the ESP protocol identifier. In particular, the IPv4/NAT method of indexing state records also by Security Parameters Index (SPI) should not be used. Likewise, any mechanism that depends on detection of Internet Key Exchange (IKE) [i.18] initiations should not be used.	ESP protocol identifier interactions may preclude more than one tunnel per endpoint.
REC-31	All valid sequences of TCP packets (defined in [i.2]) shall be forwarded for outbound flows and explicitly permitted inbound flows. In particular, both the normal TCP 3-way handshake mode of operation and the simultaneous-open mode of operation shall be supported.	
REC-32	The TCP window invariant shall not be enforced on flows for which the filter did not detect whether the window-scale option (see [i.3]) was sent in the 3-way handshake or simultaneous-open.	Fast start support. May be more difficult for vendors, but could be necessary for high-latency connections.
REC-35	If a gateway cannot determine whether the endpoints of a TCP flow are active, then it may abandon the state record if it has been idle for some time. In such cases, the value of the established flow idle-timeout shall not be less than two hours four minutes as discussed in [i.17]. The value of the transitory flow idle-timeout shall not be less than four minutes. The value of the idle-timeouts may be configurable by the network administrator.	
REC-36	If a gateway forwards a TCP flow, it shall also forward ICMPv6 Destination Unreachable and Packet Too Big messages containing TCP headers that match the flow state record.	Path MTU discovery and accessibility necessary for connectivity.
REC-37	Receipt of any sort of ICMPv6 message shall not terminate the state record for a TCP flow.	This will prevent DoS against router due to unsolicited ICMPv6 messages.
MSO-REC	By default an IGW shall deny any protocol received on the WAN (operator-facing) interface not specifically allowed by configuration with the following exceptions: DHCP, ND, ICMP and established TCP and UDP flows.	This recommendation is not found in [52] but support is required in sRouter devices.

D.4 Important recommendations

Failure to implement these recommendations specified in IETF RFC 6092 [52] could expose subscribers to infosec attacks. All sRouter implementations should support the list in the present clause as security requirements. The requirements in the present clause should be developed and tested after all critical requirements (clause D.3) are satisfied.

Table D.2: Important recommendations

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-1	Packets bearing in their outer IPv6 headers multicast source addresses shall not be forwarded or transmitted on any interface.	
REC-2	Packets which bear in their outer IPv6 headers multicast destination addresses of equal or narrower scope (see IPv6 Scoped Address Architecture [i.8]) than the configured scope boundary level of the gateway shall not be forwarded in any direction. The default scope boundary level should be organization-local scope, and it should be configurable by the network administrator.	
REC-6	Inbound packets shall not be forwarded if the source address in their outer IPv6 header has a global unicast prefix assigned for use by globally reachable nodes on the interior network.	Anti-spoofing.
REC-8	By default, inbound DNS queries received on exterior interfaces shall not be processed by any integrated DNS resolving server.	Prevents DNS reflection attacks. It will also prevent subscribers from hosting a DNS server behind a router by default.

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-9	Inbound DHCPv6 discovery packets [24] received on exterior interfaces shall not be processed by any integrated DHCPv6 server or relay agent.	Prevent recon scans (work around for vast IPv6 address space).
REC-11	If application transparency is most important, then a stateful packet filter should have endpoint independent filter behavior for generic upper layer transport protocols. If a more stringent filtering behavior is most important, then a filter should have address dependent filtering behavior. The filtering behavior may be an option configurable by the network administrator, and it may be independent of the filtering behavior for other protocols. Filtering behavior should be endpoint independent by default in gateways intended for provisioning without service provider management.	For example, this would support allowing all http but reduces ability to block access to specific http websites since the solution uses the same port on the external interface. Since most gateways are not managed, that blocking is unlikely unless the device is subscribed to a reputation like service.
REC-17	If application transparency is most important, then a stateful packet filter should have endpoint-independent filtering behavior for UDP. If a more stringent filtering behavior is most important, then a filter should have address-dependent filtering behavior. The filtering behavior may be an option configurable by the network administrator, and it may be independent of the filtering behavior for TCP and other protocols. Filtering behavior should be endpoint independent by default in gateways intended for provisioning without service provider management.	Similar to the REC-11 requirement but specific to UDP.
REC-33	If application transparency is most important, then a stateful packet filter should have endpoint-independent filtering behavior for TCP. If a more stringent filtering behavior is most important, then a filter should have address-dependent filtering behavior. The filtering behavior may be an option configurable by the network administrator, and it may be independent of the filtering behavior for UDP and other protocols. Filtering behavior should be endpoint independent by default in gateways intended for provisioning without service provider management.	Similar to the REC-11 requirement but specific to TCP.
REC-47	Valid sequences of packets bearing Shim6 payload extension headers in their outer IP extension header chains shall be forwarded for all outbound and explicitly permitted flows. The content of the Shim6 payload extension header may be ignored for the purpose of state tracking.	

D.5 BCP recommendations

The following recommendations specified in IETF RFC 6092 [52] are security best practices but are not critical to network communication. They may be supported as security requirements by sRouter devices, but are not deemed mandatory. These requirements should only be developed and tested after all requirements listed as critical (clause D.3) and important (clause D.4) have been implemented.

Table D.3: BCP recommendations

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-15	A state record for a UDP flow where one or both of the source and destination ports are in the well-known port range (ports 0-1023) may expire after a period of idle time shorter than two minutes to facilitate the operation of the IANA-registered service assigned to the port in question.	This supports SIP, SKINNY, FTP or other parsers typically found in firewalls. By watching the control traffic, they can close a session early.
REC-20	UDP-Lite flows [i.6] should be handled in the same way as UDP flows, except that the upper layer transport protocol identifier for UDP-Lite is not the same as UDP; therefore, UDP packets shall not match UDP-Lite state records, and vice versa.	UDP-Lite is an uncommon protocol and further implications may exist.

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-26	In their default operating mode, IPv6 gateways shall not prohibit the forwarding of packets, to and from legitimate node addresses, with destination extension headers of type Host Identity Protocol (HIP) [i.16] in their outer IP extension header chain.	Not currently a significant protocol, category approaches experimental.
REC-27	The state records for flows initiated by outbound packets that bear a Home Address destination option [i.5] are distinguished by the addition of the home address of the flow as well as the interior care-of address. IPv6 gateways shall not prohibit the forwarding of any inbound packets bearing type 2 routing headers, which otherwise match a flow state record, and where A) the address in the destination field of the IPv6 header matches the interior care-of address of the flow, and B) the Home Address field in the Type 2 routing header matches the home address of the flow.	This will be needed to support IPv6 mobility but its use case in home is not clear at this time.
REC-28	Valid sequences of Mobility Header [i.5] packets shall be forwarded for all outbound and explicitly permitted inbound Mobility Header flows.	
REC-29	If a gateway forwards a Mobility Header [i.5] flow, then it shall also forward, in both directions, the IPv4 and IPv6 packets that are encapsulated in IPv6 associated with the tunnel between the home agent and the correspondent node.	
REC-30	If a gateway forwards a Mobility Header [i.5] flow, then it shall also forward (in the reverse direction) ICMPv6 Destination Unreachable and Packet Too Big messages containing any headers that match the associated flow state records.	
REC-38	All valid sequences of SCTP packets (defined in [i.13]) shall be forwarded for outbound associations and explicitly permitted inbound associations. In particular, both the normal SCTP association establishment and the simultaneous-open mode of operation shall be supported.	If not implemented in first phase, SCTP should be dropped until this feature is implemented. Any unknown / unimplemented protocol shall be dropped.
REC-40	If a gateway cannot determine whether the endpoints of an SCTP association are active, then it may abandon the state record if it has been idle for some time. In such cases, the value of the established association idle-timeout shall not be less than two hours four minutes. The value of the transitory association idle-timeout shall not be less than four minutes. The value of the idle-timeouts may be configurable by the network administrator.	
REC-41	If a gateway forwards an SCTP association, it shall also forward ICMPv6 Destination Unreachable and Packet Too Big messages containing SCTP headers that match the association state record.	
REC-42	Receipt of any sort of ICMPv6 message shall not terminate the state record for an SCTP association.	
REC-43	All valid sequences of DCCP packets (defined in [i.12]) shall be forwarded for all flows to exterior servers, and for any flows to interior servers with explicitly permitted service codes.	
REC-44	A gateway may abandon a DCCP state record if it has been idle for some time. In such cases, the value of the open flow idle-timeout shall not be less than two hours four minutes. The value of the transitory flow idle-timeout shall not be less than eight minutes. The value of the idle-timeouts may be configurable by the network administrator.	
REC-45	If an Internet gateway forwards a DCCP flow, it shall also forward ICMPv6 Destination Unreachable and Packet Too Big messages containing DCCP headers that match the flow state record.	
REC-46	Receipt of any sort of ICMPv6 message shall not terminate the state record for a DCCP flow.	
REC-48	Internet gateways with IPv6 simple security capabilities should implement a protocol to permit applications to solicit inbound traffic without advance knowledge of the addresses of exterior nodes with which they expect to communicate.	UPnP like functionality, but the protocol to do this reliably and the need to do this may not exist.

D.6 Other recommendations

The following recommendations specified in IETF RFC 6092 [52] are not explicitly requirements for sRouter devices at this time. However, operator consensus was reached for the incorporation of these requirements into sRouter to supplement and extend what is present in IETF RFC 6092 [52]. These requirements should only be implemented after all other requirements have been satisfied.

Table D.4: Other recommendations

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-13	Residential IPv6 gateways should provide a convenient means to update their firmware securely, for the installation of security patches and other manufacturer-recommended changes.	This requirement applies more to home routers owned by subscribers.
REC-49	Internet gateways with IPv6 simple security capabilities shall provide an easily selected configuration option that permits a transparent mode of operation that forwards all unsolicited flows regardless of forwarding direction, i.e. not to use the IPv6 simple security capabilities of the gateway. The transparent mode of operation may be the default configuration.	The ability to turn off the firewall will probably be a requested feature but use case is still unclear as to who should be able to do this and when. The firewall shall be on by default.
REC-50	By default, subscriber-managed residential gateways shall not offer management application services to the exterior network.	Common management application services that need to be controlled include http (tcp/80), https (tcp/443), ssh (tcp/22), telnet (tcp/23) and snmp (udp161/162). As a default setting, it is important these be disabled to prevent blocking. Unclear impact to the operator's ability to manage CPE devices like the integrated home gateway router. All externally facing management application services support authentication and require changing of all default credentials. All externally facing management application services also support restricting access to trusted IP blocks via an ACL. ACL(s) block both IPv4 and IPv6 by default unless explicitly allowed.

D.7 Recommendations in conflict with operator needs

The remaining recommendations from IETF RFC 6092 [52] have been found to conflict with existing or proposed operator requirements and should not be included in sRouter devices without explicit operator approved modifications to render them useful. Such requirements should be interpreted to be shall not to avoid conflicts with operator security policies.

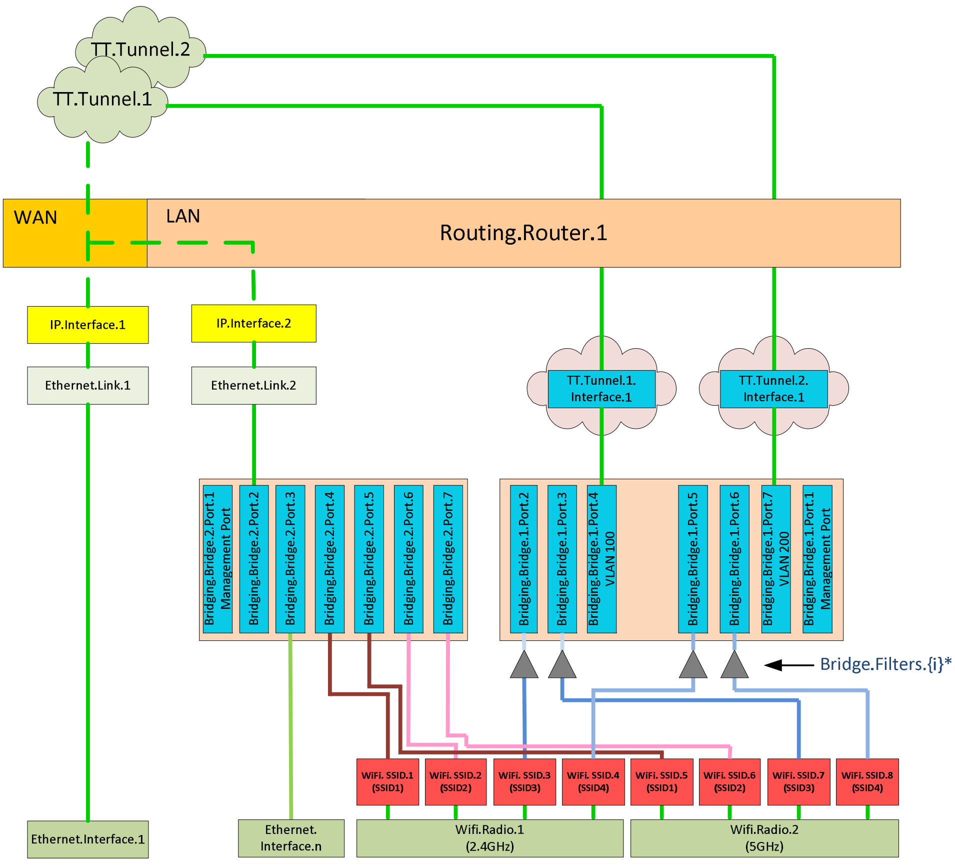
Table D.5: Recommendations in conflict with operator needs

REC #	IETF RFC 6092 [52] recommendation	Comments
REC-34	By default, a gateway shall respond with an ICMPv6 Destination Unreachable error code 1 (Communication with destination administratively prohibited), to any unsolicited inbound SYN packet after waiting at least 6 seconds without first forwarding the associated outbound SYN or SYN/ACK from the interior peer.	Preference would be to silently drop unsolicited packets from external sources rather than generate ICMPv6 Destination Unreachable due to administratively prohibited packets.
REC-39	By default, a gateway shall respond with an ICMPv6 Destination Unreachable error code 1 (Communication with destination administratively prohibited) to any unsolicited inbound INIT packet after waiting at least 6 seconds without first forwarding the associated outbound INIT from the interior peer.	Similar to SYN dropping / errors. Prefer to silently drop instead of sending ICMPv6 for DDoS protection and bounce attack protection.

Annex E (normative): sRouter GRE tunnelling architecture

E.1 Introduction

Figure E.1 depicts a GRE forwarding model using one tunnel interface. It is included here to depict the data objects and indexing for mapping the interface, bridge ports and SSID when packets traverse the tunnel. The diagram differentiates between traffic via a private and public SSID. The configuration applies whether the configuration mechanism is SNMP or TR-069. For the purposes of this use case, it is presumed that provisioning of private and public SSIDs on the sRouter has already been completed. Data objects required for provisioning of the sRouter for private and public SSIDs are discussed elsewhere in the present document. It is also presumed that SSIDs 1 and 2 are public and SSIDs 3 and 4 are private.



*Note: Classify and assign VLAN Tags for traffic separation.

Figure E.1: sRouter GRE tunnelling architecture

Figure E.1 depicts the physical and logical interfaces, bridges and SSIDs that are referenced in table E.1.

Table E.1: IF indices and row instances for data objects associated with GRE tunnelling

Row / instance	Higher layer interface	if index	Lower layer	if index
1	IP.Interface.1	300	Ethernet.Link.1	
2	Ethernet.Link.1		Ethernet.Interface.1	1
3	IP.Interface.2	200	Ethernet.Link.2	
4	Ethernet.Link.2		Bridging.Bridge.1.Port.4	

Row / instance	Higher layer interface	if index	Lower layer	if index
5	Bridging.Bridge.1.Port.1		Bridging.Bridge.1.Port.2, Bridging.Bridge.1.Port.3, Bridging.Bridge.1.Port.4, Bridging.Bridge.1.Port.5, Bridging.Bridge.1.Port.6	
6	Bridging.Bridge.1.Port.2		Ethernet.Interface.2	
7	Bridging.Bridge.1.Port.3		WiFi.SSID.1 SSID1	10001
8	Bridging.Bridge.1.Port.4		WiFi.SSID.5 SSID1	10101
9	Bridging.Bridge.1.Port.5		WiFi.SSID.2 SSID2	10002
10	Bridging.Bridge.1.Port.6		WiFi.SSID.6 SSID2	10102
11	Bridging.Bridge.2.Port.1		Bridging.Bridge.2.Port.2, Bridging.Bridge.2.Port.3, Bridging.Bridge.2.Port.4, Bridging.Bridge.2.Port.5, Bridging.Bridge.2.Port.6, Bridging.Bridge.2.Port.7	
12	Bridging.Bridge.2.Port.2		WiFi.SSID.3 SSID3	10003
13	Bridging.Bridge.2.Port.3		WiFi.SSID.7 SSID3	10103
14	Bridging.Bridge.2.Port.5		WiFi.SSID.4 SSID4	10004
15	Bridging.Bridge.2.Port.6		WiFi.SSID.8 SSID4	10104
16	Bridging.Bridge.2.Port.4		TT.Tunnel.1.Interface.1	400
17	Bridging.Bridge.2.Port.7		TT.Tunnel.2.Interface.1	401
17	WiFi.SSID.1 WiFi.SSID.3 WiFi.SSID.5 WiFi.SSID.7	10001 10003 10101 10103	WiFi.Radio.1	10000
18	WiFi.SSID.2 WiFi.SSID.4 WiFi.SSID.6 WiFi.SSID.8	10002 10004 10102 10104	WiFi.Radio.2	10100
19	WiFi.Radio.1	10000		
20	WiFi.Radio.2	10100		

E.2 Use case for data traffic flow for both private and public SSIDs

E.2.1 General requirements

An sRouter that supports both private and public SSIDs shall manage the private and public traffic separately. The following narrative describes how the private and public traffic traverses the physical and logical interfaces supported by the sRouter. There are four scenarios that will be described: private network outbound from the LAN, private network inbound from the WAN, public traffic outbound from a user on a public SSID, public traffic inbound to a user on a public SSID. Each of these traffic flows is described in clause E.2.2 to clause E.2.5, respectively.

E.2.2 Private network outbound from LAN

In this scenario, a user on the private network is connected via a private SSID and is attempting to connect to an outside network via the sRouter WAN interface. The following is an example of how the data traffic would flow.

E.2.3 Private network inbound from WAN

In this scenario, traffic associated with a private SSID is routed through the sRouter WAN interface. The following is an example of how the data would flow from the operator network through the Internet gateway to the private Wi-Fi end-user device.

Traffic enters via Ethernet.Interface.1 and Ethernet.Link.1 to IP.Interface.1 (sRouter WAN interface). From here, it is routed to IP.Interface.2 (sRouter LAN interface) and to Ethernet.Link.2. Traffic is then directed to a logical bridge (Bridging.Bridge.2.Port.1) and bridged to the private SSID (WiFi.SSID.1) where it is passed to the private user via the WiFi.Radio.1.

Similarly, any other private LAN traffic (such as Ethernet, MoCA, etc.) would travel through the same logical bridge, sRouter, etc., as the private wireless traffic. The only difference is the customer-facing network interface type.

E.2.4 Community Wi-Fi user outbound via public SSID

A public user connects via WiFi.Radio.2 and associates with WiFi.SSID.7. The traffic enters a logical bridge (Bridging.Bridge.1.Port.3) and is switched to another port within the bridge (Bridging.Bridge.1.Port.7). All ingress traffic is classified based on provider provisioned packet and/or port criteria. In this example, any ingress traffic via SSID3 will be tagged with an IEEE 802.1q service tag VLAN ID 200 and bridged to the appropriate egress port. The egress port is logically connected to the GRE tunnel interface (TT.Tunnel.1.Interface.1) that, in turn, is mapped to a tunnel instance (TT.Tunnel.1). The tunnel endpoint is the sRouter WAN interface (IP.Interface.1). Traffic exits the sRouter via Ethernet.Link.1 and Ethernet.interface.1 (operator-facing interface).

NOTE: This example describes a single tunnel interface for a single user. However, there can be multiple users on a single tunnel interface, or multiple interfaces, depending upon a service operator's preference for managing traffic or vendor implementation. Such differentiation of traffic management is out of scope for this use case.

E.2.5 Community Wi-Fi user inbound via public SSID

IEEE 802.1q service frames tagged with VLAN ID 200 and destined for the Community Wi-Fi end-user enters the gateway via the operator-facing interface and is passed to the Ethernet.Interface.1 and Ethernet.Link.1 to IP.Interface.1 (sRouter WAN interface). It is then placed on the tunnel (TT.Tunnel.1) and mapped to the logical tunnel interface (TT.Tunnel.1.Interface.1). Traffic then ingresses to the logical bridge (Bridging.Bridge.1.Port.7) and switched to (Bridging.Bridge.1.Port.3) where the VLAN tag is stripped and the frame is bridged to the public SSID (WiFi.SSID.7). Traffic is then transmitted to the user device using WiFi.Radio.2.

Annex F (normative): sRouter certificate public key infrastructure

F.1 General requirements

The sRouter security architecture uses an X.509 digital certificate Public Key Infrastructure (PKI) [47] for authenticating endpoints on secure connections. This annex defines the PKI hierarchy, certificate profiles and CRL profiles that are used. CableLabs manages the PKI. All Certification Authority (CA) certificates are hosted by CableLabs or an authorized trusted third party.

NOTE: Intermediate CA certificate Subject DN attributes can change due to maintenance/management of the PKI, which would also cause the Issuer DN attributes to change of end entity certificates. Operators contact CableLabs to acquire management/provisioning server certificates (TR-069 ACS, SNMP, file server, GRE concentrator). sRouter vendors/manufacturers contact CableLabs to acquire sRouter device certificates.

The profile tables contain extension criticality settings, which are defined in IETF RFC 5280 [47] as follows:

"*A certificate-using system shall reject the certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process. A non-critical extension may be ignored if it is not recognized, but shall be processed if it is recognized.*"

This definition also applies to CRLs. The present annex requires implementations to support critical extensions listed in the profile tables. Support of non-critical extensions is optional unless stated otherwise in the present document.

The sRouter PKI hierarchy is shown in figure F.1.

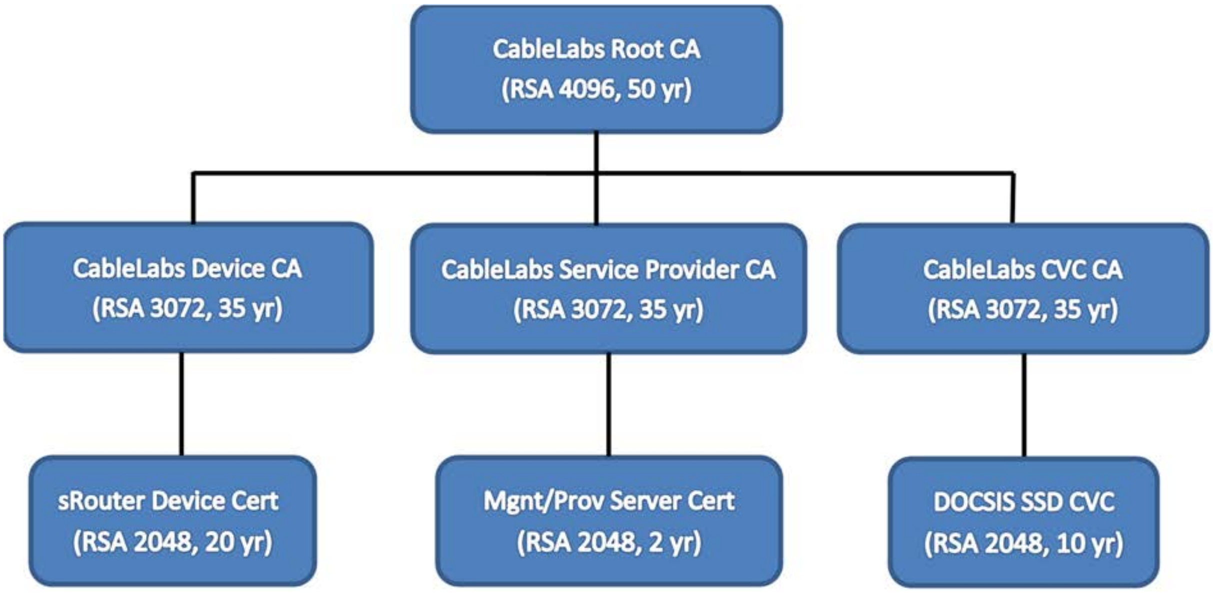


Figure F.1: Certificate hierarchy

To help simplify and consolidate certificates, the root and intermediate CA certificates are shared with other technologies (e.g. DOCSIS 3.1). End-entity certificates may also be shared with other technologies when serving the same function and having the same profile. For example, if a vendor has a Certificate Requesting Account (CRA) for DOCSIS 3.1 CM device certificates, it may be possible to use the same CRA for issuing sRouter device certificates. Code Verification Certificates (CVCs) are used with DOCSIS SNMP secure software download. CVCs already issued and used for DOCSIS may also be used for signing sRouter images and download using the DOCSIS SNMP method.

All certificates and CRLs described in this annex are signed with the RSA signature algorithm using SHA-256 as the hash function. The RSA signature algorithm is described in PKCS #1 [65]; SHA-256 is described in (FIPS PUB) 180-4 [7].

F.2 CableLabs Root CA certificate

Table F.1: CableLabs Root CA certificate

Attribute name		Settings		
Version		v3		
Serial number		Unique positive integer assigned by the CA		

Issuer DN		c=US
		o=CableLabs
		ou=Root CA01
		cn=CableLabs Root Certification Authority		

Subject DN		c=US
		o=CableLabs
		ou=Root CA01
		cn=CableLabs Root Certification Authority		

Validity period		50 years		
Public key algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		4 096 bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	***Criticality***	**Value**
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA

F.3 CableLabs Device CA certificate

Table F.2: CableLabs Device CA certificate

<table>
<tr><th colspan="2">Attribute name</th><th colspan="3">Settings</th></tr>
<tr><td colspan="2">Version</td><td colspan="3">v3</td></tr>
<tr><td colspan="2">Serial number</td><td colspan="3">Unique positive integer assigned by the CA</td></tr>
<tr><td colspan="2">Issuer DN</td><td colspan="3">c=US
o=CableLabs
ou=Root CA01
cn=CableLabs Root Certification Authority</td></tr>
<tr><td colspan="2">Subject DN</td><td colspan="3">c=US
o=CableLabs
ou=Device CA01
cn=CableLabs Device Certification Authority</td></tr>
<tr><td colspan="2">Validity period</td><td colspan="3">35 years</td></tr>
<tr><td colspan="2">Public key algorithm</td><td colspan="3">Sha256WithRSAEncryption (1 2 840 113549 1 1 11)</td></tr>
<tr><td colspan="2">Keysize</td><td colspan="3">3 072 bits</td></tr>
<tr><td colspan="2">Parameters</td><td colspan="3">NULL</td></tr>
<tr><td><b>Standard Extensions</b></td><td><b>OID</b></td><td><b>Include</b></td><td><b>Criticality</b></td><td><b>Value</b></td></tr>
<tr><td>keyUsage</td><td>{id-ce 15}</td><td>X</td><td>TRUE</td><td></td></tr>
<tr><td>keyCertSign</td><td></td><td></td><td></td><td>Set</td></tr>
<tr><td>cRLSign</td><td></td><td></td><td></td><td>Set</td></tr>
<tr><td>basicConstraints</td><td>{id-ce 19}</td><td>X</td><td>TRUE</td><td></td></tr>
<tr><td>cA</td><td></td><td></td><td></td><td>Set</td></tr>
<tr><td>pathLenConstraint</td><td></td><td></td><td></td><td>0</td></tr>
<tr><td>subjectKeyIdentifier</td><td>{id-ce 14}</td><td>X</td><td>FALSE</td><td></td></tr>
<tr><td>keyIdentifier</td><td></td><td></td><td></td><td>Calculated per Method 1</td></tr>
<tr><td>authorityKeyIdentifier</td><td>{id-ce 35}</td><td>X</td><td>FALSE</td><td></td></tr>
<tr><td>keyIdentifier</td><td></td><td></td><td></td><td>Calculated per Method 1</td></tr>
<tr><td>subjectAltName</td><td>{id-ce 17}</td><td>O</td><td>FALSE</td><td></td></tr>
<tr><td>directoryName</td><td></td><td></td><td></td><td>Set by the issuing CA for online CAs</td></tr>
</table>

F.4 sRouter device certificate

Table F.3: sRouter device certificate

<table>
<tr><th colspan="2">Attribute name</th><th colspan="3">Settings</th></tr>
<tr><td colspan="2">Version</td><td colspan="3">v3</td></tr>
<tr><td colspan="2">Serial number</td><td colspan="3">Unique positive integer assigned by the CA</td></tr>
<tr><td colspan="2">Issuer DN</td><td colspan="3">c=US
o=CableLabs
ou=Device CA01
cn=CableLabs Device Certification Authority</td></tr>
<tr><td colspan="2">Subject DN</td><td colspan="3">c=<Country of manufacturer>
o=<Company name>
ou=<Manufacturing location>
cn=<MAC address></td></tr>
<tr><td colspan="2">Validity period</td><td colspan="3">20 years</td></tr>
<tr><td colspan="2">Public key algorithm</td><td colspan="3">Sha256WithRSAEncryption (1 2 840 113549 1 1 11)</td></tr>
<tr><td colspan="2">Keysize</td><td colspan="3">2 048 bits</td></tr>
<tr><td colspan="2">Parameters</td><td colspan="3">NULL</td></tr>
<tr><td><b>Standard Extensions</b></td><td><b>OID</b></td><td><b>Include</b></td><td><b>Criticality</b></td><td><b>Value</b></td></tr>
<tr><td>keyUsage</td><td>{id-ce 15}</td><td>X</td><td>TRUE</td><td></td></tr>
<tr><td>digitalSignature</td><td></td><td></td><td></td><td>Set</td></tr>
<tr><td>keyEncipherment</td><td></td><td></td><td></td><td>Set</td></tr>
<tr><td>authorityKeyIdentifier</td><td>{id-ce 35}</td><td>X</td><td>FALSE</td><td></td></tr>
<tr><td>keyIdentifier</td><td></td><td></td><td></td><td>Calculated per Method 1</td></tr>
</table>

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

- <Country of manufacturer>: two-letter country code;
- <Company name>: name that identifies the company;
- <Manufacturing location>: name that identifies the location of manufacture;
- <MAC address>: MAC address of the sRouter.

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

F.5 CableLabs Service Provider CA certificate

Table F.4: CableLabs Device CA certificate

Attribute name		**Settings**		
Version		v3		
Serial number		Unique positive integer assigned by the CA		

Issuer DN		c=US
		o=CableLabs
		ou=Root CA01
		cn=CableLabs Root Certification Authority		

Subject DN		c=US
		o=CableLabs
		ou=Service Provider CA01
		cn=CableLabs Service Provider Certification Authority		

Validity period		35 years		
Public key algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		3 072 bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				0
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA for online Cas
authorityInfoAccess	{id-pe 1}	X	FALSE	Contains a single accessDescription with an OCSP accessMethod and responder accessLocation HTTP URI.

F.6 Management/provisioning server certificate

Table F.5: Management/provisioning server certificate

Attribute name		**Settings**		
Version		v3		
Serial number		Unique positive integer assigned by the CA		

Issuer DN		c=US
		o=CableLabs
		ou=Service Provider CA01
		cn=CableLabs Service Provider Certification Authority		

Subject DN		c=<Country>
		o=<Company name>
		cn=<Server FQDN>		

Validity period		5 years		
Public key algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2 048 bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	**Criticality**	***Value***
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	X	FALSE	
dNSName				<server FQDN>
authorityInfoAccess	{id-pe 1}	X	FALSE	Contains a single accessDescription with an OCSP accessMethod and responder accessLocation HTTP URI.

F.7 CableLabs DOCSIS CVC CA certificate

Table F.6: CableLabs DOCSIS CVC CA certificate

Attribute name		**Settings**		
Version		v3		
Serial number		Unique positive integer assigned by the CA		

Issuer DN		c=US
		o=CableLabs
		ou=Root CA01
		cn=CableLabs Root Certification Authority		

Subject DN		c=US
		o=CableLabs
		ou=CVC CA01
		cn=CableLabs CVC Certification Authority		

Validity period		35 years		
Public key algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		3 072 bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				0
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	

Attribute name		Settings		
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA for online CAs

F.8 Code Verification Certificate

Table F.7: Code Verification Certificate

Attribute name		Settings		
Version		v3		
Serial number		Unique positive integer assigned by the CA		

Issuer DN		c=US
		o=CableLabs
		ou=CVC CA01
		cn=CableLabs CVC Certification Authority		

Subject DN		c=<Country of manufacturer>
		o=<Company name>
		cn=Code Verification Certificate		

Validity period		Up to 10 years		
Public key algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2 048 bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	**Criticality**	**Value**
extKeyUsage	{id-ce 37}	X	TRUE	
codeSigning				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1

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

- <Country of manufacturer>: two-letter country code;
- <Company name>: name that identifies the company.

Co-signer CVCs will have a unique numeric value for the <Company Name>, which is assigned by the CA. The value is a printable string of eight hexadecimal digits. Each hexadecimal digit in the name is chosen from the ranges 0x30 to 0x39 or 0x41 to 0x46. The string 0x3030303030303030 is not assigned.

When a CVC is renewed, the organization name and validity start time of the old CVC will be used for the new CVC. The validity end time will be extended 10 years.

F.9 Certificate Revocation List (CRL)

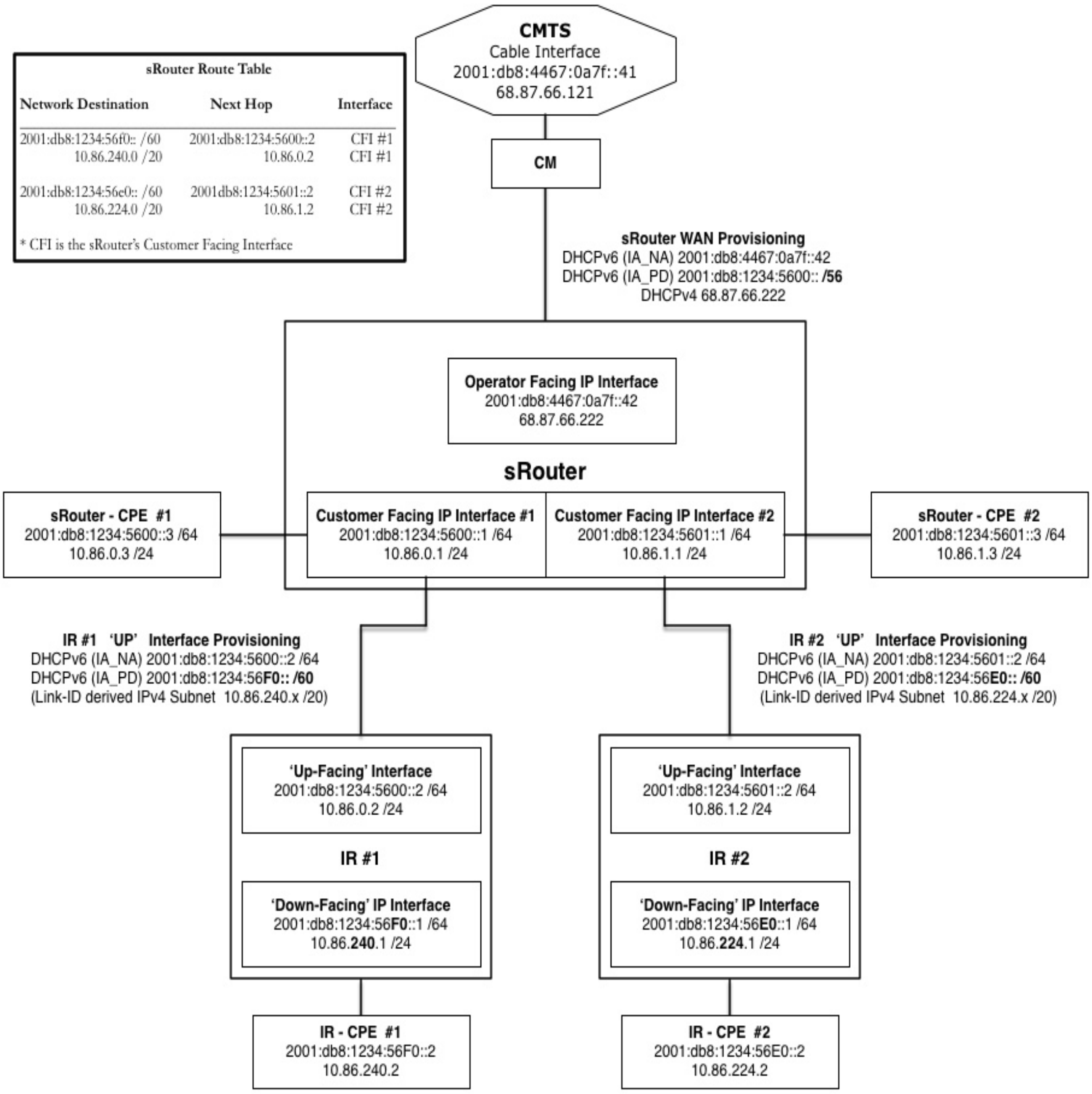
Table F.8: Certificate Revocation List

Attribute name		Settings		
Signature algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Issuer DN		<Subject DN of issuing CA>		
This update time		Time CRL was signed		
Next update time		1 month after time CRL was signed		
List of revoked certificates				
Extensions	**OID**	**Include**	**Criticality**	**Value**
issuingDistributionPoint	{id-ce 28}	X	TRUE	
distributionPoint				
generalName				HTTP URI to current CRL
authorityInformationAccess	{id-pe 1}	X	FALSE	
accessMethod				Id-ad-caIssuers
accessLocation				HTTP URI to signing CA certificate

Annex G (informative):
Example routing with Link-ID

G.1 Scenario

This annex provides example IP addressing and routing using Link-ID as described throughout the present document. The intention is to provide a reference example to aid in the proper application of Link-ID for consistent multi-router packet forwarding without a routing protocol. In this example, an sRouter is provisioned with a /56 IPv6 prefix and four (4) customer-facing IP interfaces:



sRouter Route Table

Network Destination	Next Hop	Interface
2001:db8:1234:56f0:: /60	2001:db8:1234:5600::2	CFI #1
10.86.240.0 /20	10.86.0.2	CFI #1
2001:db8:1234:56e0:: /60	2001db8:1234:5601::2	CFI #2
10.86.224.0 /20	10.86.1.2	CFI #2

* CFI is the sRouter's Customer Facing Interface

CMTS
Cable Interface
2001:db8:4467:0a7f::41
68.87.66.121
CM
sRouter WAN Provisioning
DHCPv6 (IA_NA) 2001:db8:4467:0a7f::42
DHCPv6 (IA_PD) 2001:db8:1234:5600:: /56
DHCPv4 68.87.66.222
Operator Facing IP Interface
2001:db8:4467:0a7f::42
68.87.66.222
sRouter
sRouter - CPE #1
2001:db8:1234:5600::3 /64
10.86.0.3 /24
Customer Facing IP Interface #1
2001:db8:1234:5600::1 /64
10.86.0.1 /24
Customer Facing IP Interface #2
2001:db8:1234:5601::1 /64
10.86.1.1 /24
sRouter - CPE #2
2001:db8:1234:5601::3 /64
10.86.1.3 /24
IR #1 'UP' Interface Provisioning
DHCPv6 (IA_NA) 2001:db8:1234:5600::2 /64
DHCPv6 (IA_PD) 2001:db8:1234:56F0:: /60
(Link-ID derived IPv4 Subnet 10.86.240.x /20)
IR #2 'UP' Interface Provisioning
DHCPv6 (IA_NA) 2001:db8:1234:5601::2 /64
DHCPv6 (IA_PD) 2001:db8:1234:56E0:: /60
(Link-ID derived IPv4 Subnet 10.86.224.x /20)
'Up-Facing' Interface
2001:db8:1234:5600::2 /64
10.86.0.2 /24
IR #1
'Down-Facing' IP Interface
2001:db8:1234:56F0::1 /64
10.86.240.1 /24
'Up-Facing' Interface
2001:db8:1234:5601::2 /64
10.86.1.2 /24
IR #2
'Down-Facing' IP Interface
2001:db8:1234:56E0::1 /64
10.86.224.1 /24
IR - CPE #1
2001:db8:1234:56F0::2
10.86.240.2
IR - CPE #2
2001:db8:1234:56E0::2
10.86.224.2

Figure G.1: Example of Link-ID with Prefix Delegation (topology mode favors width)

```
sRouter operator-facing interface provisioned prefix: 2001:db8:1234:5600::/56

customer-facing IP interface int(0)
     IPv6 prefix:         2001:db8:1234:5600::/64
     Link-ID conversion:  56 00 -> 86 00
     IPv4 network:        10.86.0.0/24
     IPv4 gateway:        10.86.0.1

customer-facing IP interface int(1)
     IPv6 prefix:         2001:db8:1234:5600::/64
     Link-ID conversion:  56 00 -> 86 00
     IPv4 network:        10.86.1.0/24
     IPv4 gateway:        10.86.1.1

customer-facing IP interface int(2)
     IPv6 prefix:         2001:db8:1234:5601::/64
     Link-ID conversion:  56 01 -> 86 01
     IPv4 network:        10.86.1.0/24
     IPv4 gateway:        10.86.1.1

customer-facing IP interface int(3)
     IPv6 prefix:         2001:db8:1234:5601::/64
     Link-ID conversion:  56 01 -> 86 01
     IPv4 network:        10.86.1.0/24
     IPv4 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 as int(0) -> int(3).
Assume there are (4) IRs with one attached to each of those customer-facing IP interfaces.
Further assume each IR is assigned an IPv6 IA_NA and IA_PD and IPv4 address in the following way.


IR(0) on int(0) is  assigned via DHCPv6
    IA_NA =  2001:db8:1234:9a00::100 and
    IA_PD = 2001:db8:1234:9a20::/59 and via DHCPv4
    IPv4 address = 10.154.0.100
IR(1) on int(1) is  assigned via DHCPv6
    IA_NA =  2001:db8:1234:9a01::100 and
    IA_PD = 2001:db8:1234:9a40::/59 and via DHCPv4
    IPv4 address = 10.154.1.100
IR(2) on int(2) is  assigned via DHCPv6
    IA_NA =  2001:db8:1234:9a02::100 and
    IA_PD = 2001:db8:1234:9a60::/59 and via DHCPv4
    IPv4 address = 10.154.2.100
IR(3) on int(3) is  assigned via DHCPv6
    IA_NA =  2001:db8:1234:9a03::100 and
    IA_PD = 2001:db8:1234:9a80::/59 and via DHCPv4
    IPv4 address = 10.154.3.100

Route table:

Network destination           Next hop                    Interface
-------------------------------------------------------------------------------
2001:db8:1234:9a20::/59       2001:db8:1234:9a00::100     int(0)
10.154.32.0/19                10.154.0.100                int(0)
2001:db8:1234:9a40::/59       2001:db8:1234:9a01::100     int(1)
10.154.64.0/19                10.154.1.100                int(1)
2001:db8:1234:9a60::/59       2001:db8:1234:9a02::100     int(2)
10.154.96.0/19                10.154.2.100                int(2)
2001:db8:1234:9a80::/59       2001:db8:1234:9a03::100     int(3)
10.154.128.0/19               10.154.3.100                int(3)
```

G.2 IP MIB sRouter example

Table G.1 details a routing table example based on the Link-ID reference example in figure G.1.

Table G.1: Routing table example

Route description	DestType	Dest	PfxLen	Policy	NextHop Type	NextHop	ifIndex	RouteType	Metric	RowStatus
Link-ID IR#1 IPv4 CPE network route	ipv4 (1)	10.86.240.0	20	-	ipv4 (1)	10.86.0.2	CFI#1 ifIndex	remote(4)	-	active(5)
Link-ID IR#1 IPv6 CPE network route	ipv6 (2)	2001:db8:1234:56f0::	60	-	ipv6 (2)	Link-Local of IR #1 'Up Facing' interface	CFI#1 ifIndex	remote(4)	-	active(5)
Link-ID IR#2 IPv4 CPE Network route	ipv4 (1)	10.86.224.0	20	-	ipv4 (1)	10.86.1.2	CFI#2 ifIndex	remote(4)	-	active(5)
Link-ID IR#2 IPv6 CPE network route	ipv6 (2)	2001:db8:1234:56e0::	60	-	ipv6 (2)	Link-Local of IR #2 'Up Facing' interface	CFI#2 ifIndex	remote(4)	-	active(5)
Customer-facing #1 IPv6 CPE network route	ipv6 (2)	2001:db8:1234:5600::	64	-	ipv6 (2)	Link-Local of CFI #1	CFI#1 ifIndex	remote(4)	-	active(5)
Customer-facing #2 IPv6 CPE network route	ipv6 (2)	2001:db8:1234:5601::	64	-	ipv6 (2)	Link-Local of CFI #2	CFI#2 ifIndex	remote(4)	-	active(5)
Operator-facing IPv4 interface host route	ipv4 (1)	68.87.66.222	32	-	ipv4 (1)	-	OFI ifIndex	local (3)	-	active(5)
Customer-facing #1 IPv4 interface host route	ipv4 (1)	10.86.0.1	32	-	ipv4 (1)	-	CFI#1 ifIndex	local (3)	-	active(5)
Customer-facing #2 IPv4 interface host route	ipv4 (1)	10.86.1.1	32	-	ipv4 (1)	-	CFI#2 ifIndex	local (3)	-	active(5)
Operator-facing IPv6 interface host route	ipv6 (2)	2001:db8:4467:0a7f::42	128	-	ipv6 (2)	-	OFI ifIndex	local (3)	-	active(5)
Customer-facing #1 IPv6 interface host route	ipv6 (2)	2001:db8:1234:5600::1	128	-	ipv6 (2)	-	CFI#1 ifIndex	local (3)	-	active(5)
Customer-facing #2 IPv6 interface host route	ipv6 (2)	2001:db8:1234:5601::1	128	-	ipv6 (2)	-	CFI#2 ifIndex	local (3)	-	active(5)
sRouter IPv4 default route	ipv4 (1)	0.0.0.0	0	-	ipv4 (1)	68.87.66.121	OFI ifIndex	remote (4)	-	active(5)
sRouter IPv6 default route	ipv6 (2)	::/0	0	-	ipv6 (2)	Link-Local of CMTS Cable interface	OFI ifIndex	remote (4)	-	active(5)

Annex I (informative): Change history

Date	Version	Information about changes
June 2024	v0.0.1	Initial draft agreed at CABLE #35 based on CL-SP-sRouter-I03
June 2025	v0.0.2	Stable draft agreed at CABLE #39
September 2025	v0.0.3	Final draft agreed at CABLE #40

History

Document history		
V1.1.1	November 2025	Membership Approval Procedure MV 20260118: 2025-11-19 to 2026-01-19