              A YANG Data Model for Dual-Stack Lite (DS-Lite)

Abstract

   This document defines a YANG module for the Dual-Stack Lite (DS-Lite)
   Address Family Transition Router (AFTR) and Basic Bridging BroadBand
   (B4) elements.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc8513.

Table of Contents

1. Introduction

   This document defines a data model for DS-Lite [RFC6333], using the
   YANG data modeling language [RFC7950]. Both the Address Family
   Transition Router (AFTR) and Basic Bridging BroadBand (B4) elements
   are covered by this specification.

   Figure 1 is a slight adaptation of Figure 1 from RFC 6333 and is
   provided here for the convenience of the reader.

```
                    +-----------+
                    |   Host    |
                    +-----+-----+
                          |192.0.2.1
                          |
                          |
                          |192.0.2.2
                 +--------|---------+
                 |        |         |
                 |   Home router    |
                 |+-------+-------+|
                 ||      B4       ||
                 |+-------+-------+|
                 +--------|||--------+
                          |||2001:db8:0:1::1
                          |||
                          |||<-IPv4-in-IPv6 Softwire
                          |||
                  -------|||-------
                 /       |||        \
                |   ISP core network  |
                 \       |||        /
                  -------|||-------
                          |||
                          |||2001:db8:0:2::1
                 +--------|||--------+
                 |       AFTR       |
                 |+-------+-------+|
                 ||  Concentrator  ||
                 |+-------+-------+|
                 |       |NAT|       |
                 |       +-+-+       |
                 +--------|---------+
                          |198.51.100.1
                          |
                  -------|--------
                 /        |         \
                |     Internet       |
                 \        |         /
                  -------|--------
                          |
                          |203.0.113.1
                    +-----+-----+
                    | IPv4 Host |
                    +-----------+
```
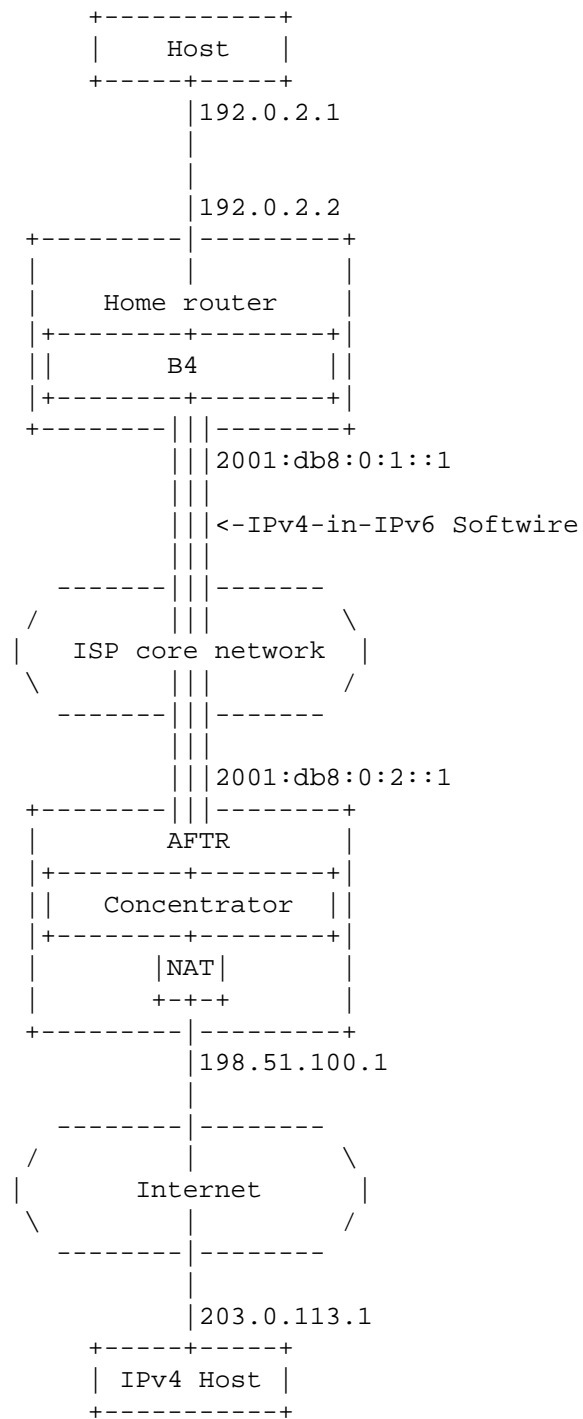
                Figure 1: DS-Lite Base Architecture

DS-Lite deployment considerations are discussed in [RFC6908].

This document follows the guidelines of [RFC8407], uses the common
YANG types defined in [RFC6991], and adopts the Network Management
Datastore Architecture (NMDA) [RFC8342].

1.1. Terminology

This document makes use of the terms defined in Section 3 of
[RFC6333].

The terminology for describing YANG data models is defined in
[RFC7950].

The meaning of the symbols in tree diagrams is defined in [RFC8340].

2. DS-Lite YANG Module: An Overview

As shown in Figure 1:

o The AFTR element is a combination of an IPv4-in-IPv6 tunnel and a
   NAPT function (Section 2.2 of [RFC3022]).

o The B4 element is an IPv4-in-IPv6 tunnel.

Therefore, the DS-Lite YANG module is designed to augment both the
Interfaces YANG module [RFC8343] and the NAT YANG module [RFC8512]
with DS-Lite-specific features.

The YANG "feature" statement is used to distinguish which of the
DS-Lite elements ('aftr' or 'b4') is relevant for a specific data
node.

Concretely, the DS-Lite YANG module (Figure 2) augments the
Interfaces YANG module with the following:

o An IPv6 address used by the tunnel endpoint (AFTR or B4) for
   sending and receiving IPv4-in-IPv6 packets (ipv6-address).

o An IPv4 address that is used by the tunnel endpoint (AFTR or B4)
   for troubleshooting purposes (ipv4-address).

o An IPv6 address used by a B4 element to reach its AFTR (aftr-
   ipv6-addr).

o The tunnel MTU used to avoid fragmentation (tunnel-mtu).

o   A policy to instruct the tunnel endpoint (AFTR or B4) whether it
    must preserve Differentiated Services Code Point (DSCP) marking
    when encapsulating/decapsulating packets (v6-v4-dscp-
    preservation).

In addition, the DS-Lite YANG module augments the NAT YANG module
(policy, in particular) with the following:

o   A policy to limit the number of DS-Lite softwires per subscriber
    (max-softwire-per-subscriber).

o   A policy to instruct the AFTR whether a state can be automatically
    migrated (state-migrate).

o   Further, in order to prevent a Denial of Service (DoS) by
    frequently changing the source IPv6 address, 'b4-address-change-
    limit' is used to rate-limit such changes.

o   An instruction to rewrite the TCP Maximum Segment Size (MSS)
    option (mss-clamping) to avoid TCP fragmentation.

Given that the NAPT table of the AFTR element is extended to include
the source IPv6 address of incoming packets, the DS-Lite YANG module
augments the NAPT44 mapping entry with the following:

o   b4-ipv6-address, which is used to record the source IPv6 address
    of a packet received from a B4 element. This IPv6 address is
    required to disambiguate between the overlapping IPv4 address
    space of subscribers.

o   The value of the Traffic Class field in the IPv6 header as
    received from a B4 element (v6-dscp): This information is used to
    preserve DSCP marking when encapsulating/decapsulating at the
    AFTR.

o   The IPv4 DSCP marking of the IPv4 packet received from a B4
    element (internal-v4-dscp): This information can be used by the
    AFTR for setting the DSCP of packets relayed to a B4 element.

o   The IPv4 DSCP marking as set by the AFTR in its external interface
    (external-v4-dscp): An AFTR can be instructed to preserve the same
    marking or to set it to another value when forwarding an IPv4
    packet destined to a remote IPv4 host.

Access Control List (ACL) and Quality-of-Service (QoS) policies
discussed in Section 2.5 of [RFC6908] are out of scope. A YANG
module for ACLs is documented in [ACL-YANG].

Likewise, considerations that are related to the Port Control
Protocol (PCP) and discussed in Section 8.5 of [RFC6333] are out of
scope. A YANG module for PCP is documented in [YANG-PCP].

The YANG module "ietf-dslite" has the following structure:

```
module: ietf-dslite
  augment /if:interfaces/if:interface:
    +--rw ipv6-address?             inet:ipv6-address
    +--rw ipv4-address?             inet:ipv4-address
    +--rw aftr-ipv6-addr?           inet:ipv6-address {b4}?
    +--rw tunnel-mtu?               uint16
    +--rw v6-v4-dscp-preservation?  boolean
  augment /nat:nat/nat:instances/nat:instance/nat:policy:
    +--rw max-softwires-per-subscriber?   uint8 {aftr}?
    +--rw state-migrate?                  boolean {aftr}?
    +--rw b4-address-change-limit?        uint32 {aftr}?
    +--rw mss-clamping {aftr}?
       +--rw enable?      boolean
       +--rw mss-value?   uint16
  augment /nat:nat/nat:instances/nat:instance
          /nat:mapping-table/nat:mapping-entry:
    +--rw b4-ipv6-address {aftr}?
    |  +--rw address?              inet:ipv6-address
    |  +--rw last-address-change?  yang:date-and-time
    +--rw v6-dscp?           inet:dscp {aftr}?
    +--rw internal-v4-dscp?  inet:dscp {aftr}?
    +--rw external-v4-dscp?  inet:dscp {aftr}?
  augment /nat:nat/nat:instances/nat:instance
          /nat:statistics/nat:mappings-statistics:
    +--ro active-softwires?   yang:gauge32 {aftr}?

  notifications:
    +---n b4-address-change-limit-policy-violation {aftr}?
       +--ro id           -> /nat:nat/instances/instance/id
       +--ro policy-id    -> /nat:nat/instances/instance/policy/id
       +--ro address      inet:ipv6-address
```

                   Figure 2: DS-Lite YANG Tree Diagram

Examples to illustrate the use of the "ietf-dslite" module are
provided in Appendices A and B.

3. DS-Lite YANG Module

   This module uses the tunnel interface identity defined in [RFC7224].

  <CODE BEGINS> file "ietf-dslite@2019-01-10.yang"

```
module ietf-dslite {
 yang-version 1.1;
 namespace "urn:ietf:params:xml:ns:yang:ietf-dslite";
 prefix dslite;

 import ietf-inet-types {
   prefix inet;
   reference
     "Section 4 of RFC 6991";
 }
 import ietf-interfaces {
   prefix if;
   reference
     "RFC 8343: A YANG Data Model for Interface Management";
 }
 import iana-if-type {
   prefix ianaift;
   reference
     "RFC 7224: IANA Interface Type YANG Module";
 }
 import ietf-nat {
   prefix nat;
   reference
     "RFC 8512: A YANG Module for Network Address Translation (NAT)
               and Network Prefix Translation (NPT)";
 }
 import ietf-yang-types {
   prefix yang;
   reference
     "Section 3 of RFC 6991";
 }

 organization
   "IETF Softwire Working Group";
 contact
   "WG Web:   <https://datatracker.ietf.org/wg/softwire/>
    WG List:  <mailto:softwires@ietf.org>

    Editor:   Mohamed Boucadair
              <mailto:mohamed.boucadair@orange.com>
```

```
      Author:   Christian Jacquenet
                <mailto:christian.jacquenet@orange.com>

      Author:   Senthil Sivakumar
                <mailto:ssenthil@cisco.com>";

   description
     "This module is a YANG module for DS-Lite AFTR and B4
      implementations.

      Copyright (c) 2018 IETF Trust and the persons identified as
      authors of the code.  All rights reserved.

      Redistribution and use in source and binary forms, with or
      without modification, is permitted pursuant to, and subject
      to the license terms contained in, the Simplified BSD License
      set forth in Section 4.c of the IETF Trust's Legal Provisions
      Relating to IETF Documents
      (http://trustee.ietf.org/license-info).

      This version of this YANG module is part of RFC 8513; see
      the RFC itself for full legal notices.";

   revision 2019-01-10 {
     description
       "Initial revision.";
     reference
       "RFC 8513: A YANG Data Model for Dual-Stack Lite (DS-Lite)";
   }

   identity dslite {
     base ianaift:tunnel;
     description
       "DS-Lite tunnel.";
   }

   /*
    * Features
    */

   feature b4 {
     description
       "The B4 element is a function implemented on a dual-stack-capable
        node, either a directly connected device or Customer Premises
        Equipment (CPE), that creates a tunnel to an AFTR.";
     reference
       "Section 5 of RFC 6333";
   }
```

```
   feature aftr {
     description
       "An AFTR element is the combination of an IPv4-in-IPv6 tunnel
        endpoint and an IPv4-IPv4 NAT implemented on the same node.";
     reference
       "Section 6 of RFC 6333";
   }

   /*
    * Augments
    */

   augment "/if:interfaces/if:interface" {
     when 'derived-from(if:type, "dslite")';
     description
       "Augments Interface module with DS-Lite parameters.

        IANA interface types are maintained at this registry:
        <https://www.iana.org/assignments/ianaiftype-mib/>.

        tunnel (131),        -- Encapsulation interface";
     leaf ipv6-address {
       type inet:ipv6-address;
       description
         "IPv6 address of the local DS-Lite endpoint (AFTR or B4).";
       reference
         "RFC 6333: Dual-Stack Lite Broadband Deployments Following
                    IPv4 Exhaustion";
     }
     leaf ipv4-address {
       type inet:ipv4-address;
       description
         "IPv4 address of the local DS-Lite AFTR or B4.

          192.0.0.1 is reserved for the AFTR element, while
          192.0.0.0/29 is reserved for the B4 element.

          This address can be used to report ICMP problems and will
          appear in traceroute outputs.";
       reference
         "RFC 6333: Dual-Stack Lite Broadband Deployments Following
                    IPv4 Exhaustion";
     }
     leaf aftr-ipv6-addr {
       if-feature "b4";
       type inet:ipv6-address;
       description
         "Indicates the AFTR's IPv6 address to be used by a B4
```

```
          element.";
        reference
          "RFC 6333: Dual-Stack Lite Broadband Deployments Following
                     IPv4 Exhaustion";
      }
      leaf tunnel-mtu {
        type uint16;
        description
          "Configures a tunnel MTU.

           RFC 6908 specifies that since fragmentation and reassembly
           are not optimal, the operator should do everything possible
           to eliminate the need for them.  If the operator uses simple
           IPv4-in-IPv6 softwire, it is recommended that the MTU size
           of the IPv6 network between the B4 and the AFTR account
           for the additional overhead (40 bytes).";
        reference
          "RFC 6908: Deployment Considerations for Dual-Stack Lite";
      }
      leaf v6-v4-dscp-preservation {
        type boolean;
        description
          "Copies the DSCP value from the IPv6 header, and vice versa.

           According to Section 2.10 of RFC 6908, operators should
           use the uniform model by provisioning the network such
           that the AFTR/B4 copies the DSCP value in the IPv4 header
           to the Traffic Class field in the IPv6 header, after the
           IPv4-in-IPv6 encapsulation.";
        reference
          "Section 2.10 of RFC 6908";
      }
    }

    augment "/nat:nat/nat:instances/nat:instance/nat:policy" {
      when "derived-from-or-self(/nat:nat/nat:instances/nat:instance"
         + "/nat:type, 'nat:napt44')"
         + " and /nat:nat/nat:instances/nat:instance/"
         + "nat:per-interface-binding='dslite'";
      if-feature "aftr";
      description
        "Augments the NAPT44 module with AFTR parameters.";
      leaf max-softwires-per-subscriber {
        type uint8;
        default "1";
        description
          "Configures the maximum softwires per subscriber feature.
```

```
        A subscriber is uniquely identified by means
        of a subscriber-mask (subscriber-mask-v6).

        This policy aims to prevent a misbehaving subscriber from
        mounting several DS-Lite softwires that would consume
        additional AFTR resources (e.g., get more external ports
        if the quota was enforced on a per-softwire basis and
        consume extra processing due to a large number of active
        softwires).";
    reference
      "Section 4 of RFC 7785";
  }
  leaf state-migrate {
    type boolean;
    default "true";
    description
      "State migration is enabled by default.

        In the event a new IPv6 address is assigned to the B4 element,
        the AFTR should migrate existing state to be bound to the new
        IPv6 address.  This operation ensures that traffic destined to
        the previous B4's IPv6 address will be redirected to the newer
        B4's IPv6 address.  The destination IPv6 address for tunneling
        return traffic from the AFTR should be the last seen as the
        B4's IPv6 source address from the user device (e.g., CPE).

        The AFTR uses the subscriber-mask-v6 to determine whether two
        IPv6 addresses belong to the same CPE (e.g., if the
        subscriber-mask-v6 is set to 56, the AFTR concludes that
        2001:db8:100:100::1 and 2001:db8:100:100::2 belong to the same
        CPE assigned with 2001:db8:100:100::/56).";
    reference
      "RFC 7785: Recommendations for Prefix Binding in the Context
                 of Softwire Dual-Stack Lite";
  }
  leaf b4-address-change-limit {
    type uint32;
    units "seconds";
    default "1800";
    description
      "Minimum number of seconds between a successive B4's IPv6
        address change from the same prefix.

        Changing the source B4's IPv6 address may be used as an attack
        vector.  Packets with a new B4's IPv6 address from the same
        prefix should be rate-limited.

        It is recommended that this rate limit be set to 30 minutes;
```

```
            other values can be set on a per-deployment basis.";
        reference
          "RFC 7785: Recommendations for Prefix Binding in the Context
                     of Softwire Dual-Stack Lite";
      }
      container mss-clamping {
        description
          "MSS rewriting configuration to avoid IPv6 fragmentation.";
        leaf enable {
          type boolean;
          description
            "Enable/disable MSS rewriting feature.";
        }
        leaf mss-value {
          type uint16;
          units "octets";
          description
            "Sets the MSS value to be used for MSS rewriting.";
        }
      }
    }

    augment "/nat:nat/nat:instances/nat:instance"
          + "/nat:mapping-table/nat:mapping-entry" {
      when "derived-from-or-self(/nat:nat/nat:instances/nat:instance"
         + "/nat:type, 'nat:napt44')"
         + "and /nat:nat/nat:instances/nat:instance"
         + "/nat:per-interface-binding='dslite'";
      if-feature "aftr";
      description
        "Augments the NAPT44 mapping table with DS-Lite specifics.";
      container b4-ipv6-address {
        description
          "Records the IPv6 address used by a B4 element and the last
           time that address changed.";
        leaf address {
          type inet:ipv6-address;
          description
            "Corresponds to the IPv6 address used by a B4 element.";
          reference
            "RFC 6333: Dual-Stack Lite Broadband Deployments Following
                       IPv4 Exhaustion";
        }
        leaf last-address-change {
          type yang:date-and-time;
          description
            "Records the last time that the address changed.";
        }
```

```
      }
      leaf v6-dscp {
        when "/if:interfaces/if:interface"
           + "/dslite:v6-v4-dscp-preservation = 'true'";
        type inet:dscp;
        description
          "DSCP value used at the softwire level (i.e., IPv6 header).";
      }
      leaf internal-v4-dscp {
        when "/if:interfaces/if:interface"
           + "/dslite:v6-v4-dscp-preservation = 'true'";
        type inet:dscp;
        description
          "DSCP value of the encapsulated IPv4 packet.";
      }
      leaf external-v4-dscp {
        when "/if:interfaces/if:interface"
           + "/dslite:v6-v4-dscp-preservation = 'true'";
        type inet:dscp;
        description
          "DSCP value of the translated IPv4 packet as marked by
           the AFTR.";
      }
    }

    augment "/nat:nat/nat:instances/nat:instance"
          + "/nat:statistics/nat:mappings-statistics" {
      if-feature "aftr";
      description
        "Indicates the number of active softwires.";
      leaf active-softwires {
        type yang:gauge32;
        description
          "The number of currently active softwires on the AFTR
           instance.";
      }
    }

    /*
     * Notifications
     */

    notification b4-address-change-limit-policy-violation {
      if-feature "aftr";
      description
        "Generates notifications when a B4 unsuccessfully attempts
         to change the IPv6 address in a time shorter than the value
         of b4-address-change-limit.
```

```
       Notifications are rate-limited (notify-interval).";
    leaf id {
      type leafref {
        path "/nat:nat/nat:instances/nat:instance/nat:id";
      }
      mandatory true;
      description
        "NAT instance identifier.";
    }
    leaf policy-id {
      type leafref {
        path "/nat:nat/nat:instances/nat:instance/nat:policy/nat:id";
      }
      mandatory true;
      description
        "Policy identifier.";
    }
    leaf address {
      type inet:ipv6-address;
      mandatory true;
      description
        "B4's IPv6 address.";
    }
  }
}

<CODE ENDS>
```

4. Security Considerations

   The YANG module specified in this document defines a schema for data
   that is designed to be accessed via network management protocols such
   as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer
   is the secure transport layer, and the mandatory-to-implement secure
   transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer
   is HTTPS, and the mandatory-to-implement secure transport is TLS
   [RFC8446].

   The Network Configuration Access Control Model (NACM) [RFC8341]
   provides the means to restrict access for particular NETCONF or
   RESTCONF users to a preconfigured subset of all available NETCONF or
   RESTCONF protocol operations and content.

   All data nodes defined in the YANG module that can be created,
   modified, and deleted (i.e., config true, which is the default) are
   considered sensitive. Write operations (e.g., edit-config) applied
   to these data nodes without proper protection can negatively affect
   network operations. An attacker who is able to access the B4/AFTR
   can undertake various attacks, such as:

   o Setting the value of 'aftr-ipv6-addr' on the B4 to point to an
      illegitimate AFTR so that it can intercept all the traffic sent by
      a B4. Illegitimately intercepting users' traffic is an attack
      with severe implications on privacy.

   o Setting the MTU to a low value, which may increase the number of
      fragments ('tunnel-mtu' for both B4 and AFTR).

   o Setting 'max-softwire-per-subscriber' to an arbitrary high value,
      which will be exploited by a misbehaving user to grab more
      resources (by mounting as many softwires as required to get more
      external IP addresses/ports) or to perform a DoS on the AFTR by
      mounting a massive number of softwires.

   o Setting 'state-migrate' to 'false' on the AFTR. This action may
      lead to a service degradation for the users.

   o Setting 'b4-address-change-limit' to an arbitrary low value can
      ease DoS attacks based on frequent change of the B4 IPv6 address.

   o Setting 'v6-v4-dscp-preservation' to 'false" may lead to a service
      degradation if some policies are applied on the network based on
      the DSCP value.

   Additional security considerations are discussed in [RFC8512].

   Security considerations related to DS-Lite are discussed in
   [RFC6333].

5. IANA Considerations

   IANA has registered the following URI in the "ns" subregistry within
   the "IETF XML Registry" [RFC3688]:

           URI: urn:ietf:params:xml:ns:yang:ietf-dslite
           Registrant Contact: The IESG.
           XML: N/A; the requested URI is an XML namespace.

   IANA has registered the following YANG module in the "YANG Module
   Names" subregistry [RFC7950] within the "YANG Parameters" registry.

           name: ietf-dslite
           namespace: urn:ietf:params:xml:ns:yang:ietf-dslite
           prefix: dslite
           reference: RFC 8513

6. References

6.1. Normative References

   [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688,
              DOI 10.17487/RFC3688, January 2004,
              <https://www.rfc-editor.org/info/rfc3688>.

   [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed.,
              and A. Bierman, Ed., "Network Configuration Protocol
              (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011,
              <https://www.rfc-editor.org/info/rfc6241>.

   [RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure
              Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011,
              <https://www.rfc-editor.org/info/rfc6242>.

   [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
              Stack Lite Broadband Deployments Following IPv4
              Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011,
              <https://www.rfc-editor.org/info/rfc6333>.

   [RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types",
              RFC 6991, DOI 10.17487/RFC6991, July 2013,
              <https://www.rfc-editor.org/info/rfc6991>.

   [RFC7224] Bjorklund, M., "IANA Interface Type YANG Module",
              RFC 7224, DOI 10.17487/RFC7224, May 2014,
              <https://www.rfc-editor.org/info/rfc7224>.

   [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language",
              RFC 7950, DOI 10.17487/RFC7950, August 2016,
              <https://www.rfc-editor.org/info/rfc7950>.

   [RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF
              Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017,
              <https://www.rfc-editor.org/info/rfc8040>.

   [RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration
              Access Control Model", STD 91, RFC 8341,
              DOI 10.17487/RFC8341, March 2018,
              <https://www.rfc-editor.org/info/rfc8341>.

   [RFC8343] Bjorklund, M., "A YANG Data Model for Interface
              Management", RFC 8343, DOI 10.17487/RFC8343, March 2018,
              <https://www.rfc-editor.org/info/rfc8343>.

   [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol
              Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018,
              <https://www.rfc-editor.org/info/rfc8446>.

   [RFC8512] Boucadair, M., Ed., Sivakumar, S., Jacquenet, C.,
              Vinapamula, S., and Q. Wu, "A YANG Module for Network
              Address Translation (NAT) and Network Prefix Translation
              (NPT)", RFC 8512, DOI 10.17487/RFC8512, January 2019,
              <https://www.rfc-editor.org/info/rfc8512>.

6.2. Informative References

   [ACL-YANG] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair,
              "Network Access Control List (ACL) YANG Data Model", Work
              in Progress, draft-ietf-netmod-acl-model-21, November
              2018.

   [RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network
              Address Translator (Traditional NAT)", RFC 3022,
              DOI 10.17487/RFC3022, January 2001,
              <https://www.rfc-editor.org/info/rfc3022>.

   [RFC6908] Lee, Y., Maglione, R., Williams, C., Jacquenet, C., and
              M. Boucadair, "Deployment Considerations for Dual-Stack
              Lite", RFC 6908, DOI 10.17487/RFC6908, March 2013,
              <https://www.rfc-editor.org/info/rfc6908>.

   [RFC7785] Vinapamula, S. and M. Boucadair, "Recommendations for
              Prefix Binding in the Context of Softwire Dual-Stack
              Lite", RFC 7785, DOI 10.17487/RFC7785, February 2016,
              <https://www.rfc-editor.org/info/rfc7785>.

   [RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams",
              BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018,
              <https://www.rfc-editor.org/info/rfc8340>.

   [RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K.,
              and R. Wilton, "Network Management Datastore Architecture
              (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018,
              <https://www.rfc-editor.org/info/rfc8342>.

   [RFC8407] Bierman, A., "Guidelines for Authors and Reviewers of
              Documents Containing YANG Data Models", BCP 216, RFC 8407,
              DOI 10.17487/RFC8407, October 2018,
              <https://www.rfc-editor.org/info/rfc8407>.

   [YANG-PCP] Boucadair, M., Jacquenet, C., Sivakumar, S., and
              S. Vinapamula, "YANG Modules for the Port Control Protocol
              (PCP)", Work in Progress, draft-boucadair-pcp-yang-05,
              October 2017.

Appendix A. B4 Example

   The following example shows a B4 element (2001:db8:0:1::1) that is
   configured with an AFTR element (2001:db8:0:2::1). The B4 element is
   also instructed to preserve the DSCP marking.

   <interfaces>
     <interface>
       <name>myB4</name>
       <type>dslite:dslite</type>
       <enabled>true</enabled>
       <dslite:ipv6-address>
         2001:db8:0:1::1
       </dslite:ipv6-address>
       <dslite:aftr-ipv6-addr>
         2001:db8:0:2::1
       </dslite:aftr-ipv6-addr>
       <dslite:v6-v4-dscp-preservation>
         true
       </dslite:v6-v4-dscp-preservation>
     </interface>
   </interfaces>

Appendix B. AFTR Examples

   The following example shows an AFTR that is reachable at
   2001:db8:0:2::1. Also, this XML snippet indicates that the AFTR is
   provided with an IPv4 address (192.0.0.1) to be used for
   troubleshooting purposes such as reporting problems to B4s.

   Note that a subscriber is identified by a subscriber-mask [RFC7785]
   that can be configured by means of [RFC8512].

   <interfaces>
     <interface>
       <name>myAFTR</name>
       <type>dslite:dslite</type>
       <enabled>true</enabled>
       <dslite:ipv6-address>2001:db8:0:2::1</dslite:ipv6-address>
       <dslite:ipv4-address>192.0.0.1</dslite:ipv4-address>
     </interface>
   </interfaces>

   The following shows an XML excerpt depicting a dynamic UDP mapping
   entry maintained by a DS-Lite AFTR for a packet received from the B4
   element introduced in Appendix A. Concretely, this UDP packet
   received with a source IPv6 address (2001:db8:0:1::1), a source IPv4
   address (192.0.2.1), and a source port number (1568) is translated

into a UDP packet having a source IPv4 address (198.51.100.1) and
source port number (15000). The remaining lifetime of this mapping
is 300 seconds.

```
<mapping-entry>
  <index>15</index>
  <type>
    dynamic-explicit
  </type>
  <transport-protocol>
    17
  </transport-protocol>
  <dslite:b4-ipv6-address>
    <dslite:address>
      2001:db8:0:1::1
    </dslite:address>
  </dslite:b4-ipv6-address>
  <internal-src-address>
    192.0.2.1
  </internal-src-address>
  <internal-src-port>
    <start-port-number>
      1568
    </start-port-number>
  </internal-src-port>
  <external-src-address>
    198.51.100.1
  </external-src-address>
  <external-src-port>
    <start-port-number>
      15000
    </start-port-number>
  </external-src-port>
  <lifetime>
    300
  </lifetime>
</mapping-entry>
```

Acknowledgements

Authors' Addresses

   Mohamed Boucadair
   Orange
   Rennes 35000
   France

   Email: mohamed.boucadair@orange.com

   Christian Jacquenet
   Orange
   Rennes 35000
   France

   Email: christian.jacquenet@orange.com

   Senthil Sivakumar
   Cisco Systems
   7100-8 Kit Creek Road
   Research Triangle Park, North Carolina 27709
   United States of America

   Phone: +1-919-392-5158
   Email: ssenthil@cisco.com