LSR
Internet-Draft
Intended status: Standards Track
Expires: 10 July 2026

R. Chen
D. Zhao
ZTE Corporation
P. Psenak
K. Talaulikar
Cisco Systems
C. Lin
H3C

6 January 2026

OSPFv2 Anycast Property Advertisement
draft-ietf-lsr-anycast-flag-11

Abstract

An IP prefix may be configured as anycast and as such the same value can be advertised by multiple routers. It is useful for other routers to know that the advertisement is for an anycast prefix.

This document defines a new flag in the OSPFv2 Extended Prefix TLV Flags to advertise the anycast property. The document also specifies a companion YANG module for managing this function.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 July 2026.

Copyright Notice

Table of Contents

1. Introduction

An IP prefix may be configured as anycast and as such the same value can be advertised by multiple routers. It is useful for other routers to know that the advertisement is for an anycast prefix.

[RFC7684] defines OSPFv2 Opaque LSAs based on Type-Length-Value (TLV) tuples that can be used to associate additional attributes with prefixes or links. The OSPFv2 Extended Prefix TLV that is contained in the OSPFv2 Extended Prefix Opaque LSA is used to advertise additional attributes associated with a prefix.

Extensions related to the anycast property of prefixes have been specified for IS-IS [RFC9352] and OSPFv3 [RFC9513], even though those documents are related to Segment Routing over IPv6, the anycast property applies to any IP prefix advertisement. This document

defines a flag to advertise the anycast property for a prefix advertisement in OSPFv2 in the Flags field of the OSPFv2 Extended Prefix TLV Flags (section 2.1 of [RFC7684]). The document also specifies a companion YANG module for managing this function.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. OSPFv2 Anycast Property Advertisement

An IP prefix may be configured as anycast and it is useful for other routers to know that the advertisement is for an anycast prefix.

In the context of the flags defined in this document, the term ’set’ means the bit is set to 1, and the term ’clear’ means the bit is set to 0.

A flag is introduced in OSPFv2 Extended Prefix TLV Flags [RFC7684] to advertise the anycast property:

Value: TBD

Description: Anycast Flag (AC-flag)

The only meaning of the AC-flag is that the prefix is intended to be advertised by multiple nodes.

When a prefix is configured as anycast, the AC-flag MUST be set. Otherwise, this flag MUST be clear.

The AC-flag and the N-flag (section 2.1 of [RFC7684]) MUST NOT both be set. The reception of an advertisement with both the N-flag and AC-flag set MUST be considered a configuration anomaly, and N-flag MUST be ignored. Additionally, the detection of such a conflicting advertisement SHOULD be logged as an operational error(subject to rate-limiting).

The AC-flag MUST be preserved when the OSPFv2 Extended Prefix Opaque LSA is re-advertised into other areas.

The same prefix can be advertised by multiple routers, and that if at least one of them sets the AC-flag in its advertisement, the prefix is considered as anycast.

A prefix that is advertised by a single node and without an AC-flag is considered a node-specific prefix.

Anycast prefixes SHOULD be consistently managed throughout the network. Since an AC-flag set takes precedence in identifying anycast property, stale configurations should be strictly monitored.

3. BGP-LS Advertisement

[RFC9085] defines the Prefix Attribute Flags TLV for BGP-LS that carries prefix attribute flags information, and the Flags field of this TLV is interpreted according to OSPFv2 [RFC7684]. Thus the Flags field of the BGP-LS Prefix Attribute Flags TLV also conveys the anycast property introduced by this document.

4. YANG Data Model

YANG [RFC7950] is a data definition language used to define the contents of a conceptual data store that allows networked devices to be managed using NETCONF [RFC6241] or RESTCONF [RFC8040].

This section defines a YANG data model that can be used to manage the usage of OSPFv2 Anycast Property as defined in this document, which augments the OSPF YANG data model [RFC9129] and the YANG Data Model for Routing Management [RFC8349].

4.1. Tree for the YANG Data Model

This document uses the graphical representation of data models per [RFC8340].

The following shows the tree diagram of the module:

```
module: ietf-ospf-anycast-flag

  augment /rt:routing/rt:control-plane-protocols
         /rt:control-plane-protocol/ospf:ospf/ospf:areas/ospf:area
        /ospf:interfaces/ospf:interface:
    +--rw anycast-flag?   boolean
```

4.2. YANG Data Model for OSPFv2 Anycast Property Advertisement

The following is the YANG module:

```
<CODE BEGINS> file "ietf-ospf-anycast-flag@2025-08-28.yang"
module ietf-ospf-anycast-flag {
  yang-version 1.1;
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-ospf-anycast-flag";
  prefix ospf-anycast-flag;

  import ietf-routing {
    prefix rt;
    reference
      "RFC 8349: A YANG Data Model for Routing
       Management (NMDA Version)";
  }
  import ietf-ospf {
    prefix ospf;
    reference
      "RFC 9129: YANG Data Model for the OSPF Protocol";
  }

  organization
    "IETF LSR - Link State Routing Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/lsr/>
     WG List:  <mailto:lsr@ietf.org>

     Author:   Ran Chen
               <mailto:chen.ran@zte.com.cn>
     Author:   Detao Zhao
               <mailto:zhao.detao@zte.com.cn>
     Author:   Peter Psenak
               <mailto:ppsenak@cisco.com>
     Author:   Ketan Talaulikar
               <mailto:ketant.ietf@gmail.com>
     Author:   Changwang Lin
               <mailto:linchangwang.04414@h3c.com>";

  description
    "This YANG module adds the support of managing an OSPFv2
     prefix as anycast.

     Copyright (c) 2025 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 Revised BSD License set
     forth in Section 4.c of the IETF Trust's Legal Provisions
     Relating to IETF Documents
```

```
        (https://trustee.ietf.org/license-info).

        All revisions of IETF and IANA published modules can
        be found at the YANG Parameters registry group
       (https://www.iana.org/assignments/yang-parameters);

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

     revision 2025-11-18 {
       description
         "Initial version";
       reference
         "RFC XXXX: OSPFv2 Anycast Property Advertisement";
     }

     identity ac-flag {
       base ospf:ospfv2-extended-prefix-flag;
       description
         "Indicates that the prefix is configured as anycast.";
     }

     augment "/rt:routing/rt:control-plane-protocols/"
           + "rt:control-plane-protocol/ospf:ospf/"
           + "ospf:areas/ospf:area/ospf:interfaces/ospf:interface" {
       when "derived-from(/rt:routing/rt:control-plane-protocols/"
          + "rt:control-plane-protocol/rt:type, 'ospf:ospfv2')" {
         description
           "This augments the OSPFv2 interface.";
       }
       description
         "This augments OSPFv2 interface with anycast
          property advertisement.";
       leaf anycast-flag {
         type boolean;
         default "false";
         description
           "Indicates that the prefix is an anycast address,
           if set to 1. It indicates a node-specific prefix
           if set to 0.";
       }
     }
   }
   <CODE ENDS>
```

5. IANA Considerations

This document requests allocation for the following registry.

5.1. OSPFv2 Extended Prefix TLV Flags Registry

This document requests the allocation of new value in the "OSPFv2 Extended Prefix TLV Flags" registry:

TBD:AC-flag (Anycast Flag).

5.2. OSPFv2 Anycast Flag YANG Module Registry

IANA is requested to register the following URI in the "ns" registry within the "IETF XML Registry" group ([RFC3688]):

URI: urn:ietf:params:xml:ns:yang:ietf-ospf-anycast-flag
Registrant Contact: The IESG.
XML: N/A, the requested URI is an XML namespace

IANA is requested to register the following YANG module in the "YANG Module Names" registry ([RFC6020]) within the "YANG Parameters" registry group.

name: ietf-ospf-anycast-flag
Maintained by IANA? N
namespace: urn:ietf:params:xml:ns:yang:ietf-ospf-anycast-flag
prefix: ospf-anycast-flag
reference: RFC XXXX

6. Security Considerations

6.1. Protocol Security Considerations

Procedures and protocol extensions defined in this document do not affect the OSPFv2 security model. See the "Security Considerations"section of [RFC7684] for a discussion of OSPFv2 security.

The newly introduced AC-flag, which MUST be either set or clear, introduces operational dependencies that impact the semantic validity of the advertised prefix. The correct semantic interpretation of the AC-flag relies on both router implementation support for the flag and accurate operator configuration of the anycast route. Consequently, receivers MUST consider the possibility of misconfiguration or inconsistent implementation when relying on the AC-flag for forwarding or security decisions.

6.2. YANG Security Considerations

This section is modeled after the template described in Section 3.7 of [I-D.ietf-netmod-rfc8407bis].

The "ietf-ospf-anycast-flag" YANG module defines data model that is designed to be accessed via YANG-based management protocols, such as NETCONF [RFC6241] and RESTCONF [RFC8040]. These protocols have to use a secure transport layer (e.g., SSH [RFC4252], TLS [RFC8446], and QUIC [RFC9000]) and have to use mutual authentication.

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.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes can be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. Specifically, the following subtrees and data nodes have particular sensitivities/vulnerabilities:

```
/ospf:ospf/ospf:areas/ospf:area/ospf:interfaces/ospf:interface/
ospf-anycast-flag:anycast-flag
```

As specified in Section 2, the AC-flag and the N-flag MUST NOT both be set to 1. An attacker or a misconfiguration that violates this rule creates a configuration anomaly. The handling of such anomalies is defined in Section 2. Modifications to these data nodes without proper protection could prevent interpreting the IPv4 prefix as anycast or node-specific.

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. Specifically, the following subtrees and data nodes have particular sensitivities/ vulnerabilities:

```
/ospf:ospf/ospf:areas/ospf:area/ospf:interfaces/ospf:interface/
ospf-anycast-flag:anycast-flag
```

Exposure of the OSPF link state database may be useful in mounting Denial-of-Service (DoS) attacks.

Unauthorized access to any data node of these subtrees can disclose the operational state information of the OSPF protocol on a device.

There are no particularly sensitive RPC or action operations.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

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

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC7684] Psenak, P., Gredler, H., Shakir, R., Henderickx, W., Tantsura, J., and A. Lindem, "OSPFv2 Prefix/Link Attribute Advertisement", RFC 7684, DOI 10.17487/RFC7684, November 2015, <https://www.rfc-editor.org/info/rfc7684>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

[RFC8349] Lhotka, L., Lindem, A., and Y. Qu, "A YANG Data Model for Routing Management (NMDA Version)", RFC 8349, DOI 10.17487/RFC8349, March 2018, <https://www.rfc-editor.org/info/rfc8349>.

[RFC9085] Previdi, S., Talaulikar, K., Ed., Filsfils, C., Gredler, H., and M. Chen, "Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing", RFC 9085, DOI 10.17487/RFC9085, August 2021, <https://www.rfc-editor.org/info/rfc9085>.

[RFC9129] Yeung, D., Qu, Y., Zhang, Z., Chen, I., and A. Lindem, "YANG Data Model for the OSPF Protocol", RFC 9129, DOI 10.17487/RFC9129, October 2022, <https://www.rfc-editor.org/info/rfc9129>.

7.2. Informative References

[I-D.ietf-netmod-rfc8407bis] Bierman, A., Boucadair, M., and Q. Wu, "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", Work in Progress, Internet-Draft, draft-ietf-netmod-rfc8407bis-28, 5 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-netmod-rfc8407bis-28>.

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/info/rfc4252>.

[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>.

[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>.

[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>.

[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>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC9352] Psenak, P., Ed., Filsfils, C., Bashandy, A., Decraene, B., and Z. Hu, "IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane", RFC 9352, DOI 10.17487/RFC9352, February 2023, <https://www.rfc-editor.org/info/rfc9352>.

[RFC9513] Li, Z., Hu, Z., Talaulikar, K., Ed., and P. Psenak, "OSPFv3 Extensions for Segment Routing over IPv6 (SRv6)", RFC 9513, DOI 10.17487/RFC9513, December 2023, <https://www.rfc-editor.org/info/rfc9513>.

Acknowledgements

The authors would like to thank Acee Lindem for aligning the terminology with existing OSPF documents and for editorial improvements.

Contributors

This document has the following contributor:

Yingzhen Qu
Futurewei Technologies
Email: yingzhen.ietf@gmail.com

Authors' Addresses

Ran Chen
ZTE Corporation
Nanjing
China
Email: chen.ran@zte.com.cn

Detao Zhao
ZTE Corporation
Nanjing
China
Email: zhao.detao@zte.com.cn

Peter Psenak
Cisco Systems
Email: ppsenak@cisco.com

Ketan Talaulikar
Cisco Systems

Email: ketant.ietf@gmail.com

Changwang Lin
H3C
Email: linchangwang.04414@h3c.com