Link State Routing
Internet-Draft
Intended status: Standards Track
Expires: 8 September 2022

A. Retana
L. Han
Futurewei Technologies, Inc.

7 March 2022

OSPF Monitor Node
draft-retana-lsr-ospf-monitor-node-00

Abstract

This document specifies mechanisms that allow a node to monitor an OSPF network actively without influencing the topology or affecting its stability.

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 8 September 2022.

Table of Contents

1. Introduction

Monitoring the control plane activity in a network is essential to designing and maintaining a robust and stable network. Passive (listen- only) devices deployed in broadcast or non-broadcast multi-access (NBMA) networks have typically satisfied the need. However, passive devices depend on more than two routers being present in the network and are not visible to the network operator -- anyone can listen.

An alternative implementation, primarily used in point-to-point interfaces, or in cases where the listening device is the only other node on the interface, is to participate fully in the protocol: create a full adjacency with the closest router, participate in designated router (DR) election, etc. The node is now visible in the network, can advertise control plane information, and any changes in its status are flooded throughout the network. Many link state advertisements (LSA) or state changes can cause instability in the network, and additional configuration is usually needed to avoid the device becoming a transit node.

This document specifies mechanisms that allow a node to monitor OSPF activity without influencing the topology or affecting its stability while being fully adjacent and known to the network operator. These nodes are referred to as a Monitor Node. Two such mechanisms are introduced:

Section 3 describes a local implementation to be used in the case where the Monitor Node is the only other router on an interface.

Section 4 specifies signaling in the Hello message for a node to communicate its intention to become a Monitor Node.

The mechanisms presented apply to both OSPFv2 [RFC2328] and OSPFv3 [RFC5340]. The term OSPF is used to refer to both versions.

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. Router Interface Parameters

This document defines the following router interface configurable parameters:

DoNotAdvertiseLink
: Indicates whether or not the link is advertised on the local router-LSA. If set to "enabled," the router MUST NOT include a corresponding interface description in its router-LSA. The router MUST NOT originate other LSAs related to the link or its addresses. Enabling this interface parameter overrides the setting of LinkLSASuppression [RFC5340].

DoNotRequestAndIgnoreLSAs
: Indicates whether or not the router should request and use LSAs from other routers on this interface. If set to "enabled," the router MUST consider its Link state request list empty. Also, the router MUST consider the LS age of any received LSA to be equal to MaxAge and process it according to Section 13 of [RFC2328].

3. Monitoring Interface

By using the interface parameters specified in Section 2, a router can treat all neighbors on the interface as Monitor Nodes. To do so, DoNotAdvertiseLink and DoNotRequestAndIgnoreLSAs SHOULD be configured simultaneously. If either parameter is configured on a broadcast or NBMA interface, the router MUST NOT participate in the Designated Router (DR) selection process.

Enabling DoNotAdvertiseLink by itself results in any LSAs originated by the Monitor Node not being resolved in the routing table.

If only DoNotRequestAndIgnoreLSAs is enabled, the router MUST treat the link as a stub network. Note that the neighbor information (corresponding to the Monitor Node) is not advertised.

4. The Monitor Node Option

This document defines a new Option in the Extended Options and Flags (EOF) Link-Local Signaling (LLS) TLV [RFC5613]. The new option is called Monitor (M-bit) and has a value of TBD.

When set, the M-bit indicates that the originating router is a Monitor Node. Other routers on the same link MUST:

* Consider the Monitor Node ineligible for the DR selection process.

* Consider its Link state request list empty with respect to the Monitor Node.

* Consider the LS age of any LSA received from the Monitor Node is equal to MaxAge.

If the Monitor Node is one of only two routers on an interface, the other router MUST NOT include a corresponding interface description in its router-LSA. Furthermore, other LSAs related to the link or its addresses MUST NOT be originated. This situation overrides the setting of LinkLSASuppression.

5. Operational Considerations

The use of the monitoring interface (Section 3) applies to all other routers on the same interface. While the Monitor Node option (Section 4) applies to only the router signaling the M-bit. Network administrators should use the Monitor Node option in transit interfaces where one router is a Monitor Node.

If the Monitor Node is the only other router on an interface, the link information can be advertised (as a stub link) if only DoNotRequestAndIgnoreLSAs is enabled.

The deployment of the Monitoring Interface (Section 3) requires that only the non-Monitor Node supports this specification. On the other hand, the Monitor Node Option (Section 4) requires all nodes on the interface to support the functionality. If support is not present in all the routers on the link, the Monitor Node will be eligible to be a DR, and its information may be flooded through the network.

6. Acknowledgements

TBD

7. IANA Considerations

IANA is requested to allocate a value (TBD) from the "LLS Type 1 Extended Options and Flags" registry for the M-bit (Section 4).

8. Security Considerations

The security considerations documented in [RFC2328], [RFC5340], and [RFC5613] apply to this extension.

This document defines a new type of node, called a Monitor Node, intended only to receive information from its neighbors and not send any. If the LSAs from the Monitor Node are not ignored, they will be flooded throughout the network. A rouge Monitor Node may advertise LSAs with an Advertising Router field that doesn't correspond to its router ID. This type of vulnerability is not new, but it is already present in the base specification.

Even though it is expected that the local network operator deploys any Monitor Node, authentication mechanisms such as those specified in [RFC5709], [RFC7474], [RFC4552], or [RFC7166] SHOULD be used.

9. References

9.1. 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>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008, <https://www.rfc-editor.org/info/rfc5340>.

[RFC5613] Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "OSPF Link-Local Signaling", RFC 5613, DOI 10.17487/RFC5613, August 2009, <https://www.rfc-editor.org/info/rfc5613>.

[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>.

9.2. Informative References

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, DOI 10.17487/RFC4552, June 2006, <https://www.rfc-editor.org/info/rfc4552>.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, DOI 10.17487/RFC5709, October 2009, <https://www.rfc-editor.org/info/rfc5709>.

[RFC7166] Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", RFC 7166, DOI 10.17487/RFC7166, March 2014, <https://www.rfc-editor.org/info/rfc7166>.

[RFC7474] Bhatia, M., Hartman, S., Zhang, D., and A. Lindem, Ed., "Security Extension for OSPFv2 When Using Manual Key Management", RFC 7474, DOI 10.17487/RFC7474, April 2015, <https://www.rfc-editor.org/info/rfc7474>.

Authors' Addresses

Alvaro Retana
Futurewei Technologies, Inc.
2330 Central Expressway
Santa Clara, CA 95050
United States of America
Email: aretana@futurewei.com

Lin Han
Futurewei Technologies, Inc.
2330 Central Expressway
Santa Clara, CA 95050
United States of America
Email: lin.han@futurewei.com