Abstract

The OSPFv2 specifies an SPF algorithm that identifies transit vertices based on their adjacencies. Therefore, OSPFv2 does not have a mechanism to prevent traffic transiting a participating node if it is a transit vertex in the only existing or shortest path to the destination. The use of metrics to make the node undesirable can only help to repel traffic if an alternative better route exists. This document defines the Host-bit functionality to prevent other OSPFv2 routers from using the router for transit traffic in OSPFv2 routing domains. This document updates the [RFC2328] by assigning a new bit (Host-bit) in the OSPF Router-LSA bit registry. If the Host-bit is set, the calculation of the shortest-path tree for an area, as described in [RFC2328], is modified by including a new check to verify that transit vertices have the Host-bit clear.

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 November 20, 2019.
1. Introduction

The OSPFv2 specifies an SPF algorithm that identifies transit vertices based on their adjacencies. Therefore, OSPFv2 does not have a mechanism to prevent traffic transiting a participating node if it
is a transit vertex in the only existing or shortest path to the
destination. The use of metrics to make the node undesirable can
only help to repel traffic if an alternative better route exists.

This functionality is particularly useful for a number of use cases:

1. To isolate a router to avoid blackhole scenarios when there is a
   reload and possible long reconvergence times.

2. Closet Switches are usually not used for transit traffic but need
to participate in the topology.

3. Overloaded routers could use such a capability to repel traffic
   until they stabilize.

4. BGP Route reflectors known as virtual Route Reflectors (vRRs),
   that are not in the forwarding path but are in central locations
   such as data centers. Such Route Reflectors typically are used
   for route distribution and are not capable of forwarding transit
   traffic. However, they need to learn the OSPF topology to
   perform spf computation for optimal routes and reachability
   resolution for its clients
   [I-D.ietf-idr-bgp-optimal-route-reflection].

This document defines the Host-bit (H-Bit) functionality to prevent
other OSPFv2 routers from using the router for transit traffic in
OSPFv2 routing domains. This document updates the [RFC2328] by -
assigning the Host-bit in the OSPF Router-LSA bit registry - if the
host-bit is set then the calculation of the shortest-path tree for an
area, as described in section 16.1 of [RFC2328], is modified by
including a new check to verify that transit vertices DO NOT have the
host-bit set.

2. 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.

3. Host-bit Support

This document defines a new router-LSA bit known as the Host Bit or
the H-bit. An OSPFv2 router advertising a router-LSA with the H-bit
set indicates to other OSPFv2 routers in the area supporting the
functionality that it MUST NOT be used as a transit router (see
section 4).
If the host-bit is NOT set routers MUST act transit routers as described in [RFC2328] ensuring backward compatibility.

The Host Bit in router-LSA

<table>
<thead>
<tr>
<th>Host Bit in router-LSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>+-----------------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Bit H is the high-order bit of the OSPF as shown above. When set, an OSPFv2 router is a non-transit router and is incapable of forwarding transit traffic.
An OSPFv2 router originating a router-LSA with the H-bit set MUST advertise all its router links with a link cost of MaxLinkMetric [RFC6987]. This is to increase the applicability of the H-bit to partial deployments where it is the responsibility of the operator to ensure that OSPFv2 routers not supporting the H-bit do not install routes causing routing loops.

When the H-bit is set, an Area Border Router (ABR) MUST advertise a consistent H-bit setting in its self-originated router-LSAs for all attached areas. ONLY IPv4 prefixes associated with its local interfaces MAY be advertised in summary LSAs.

When the H-bit is set cannot act as an AS Boundary Router (ASBR), as non-local IPv4 prefixes, e.g., those exported from other routing protocols, MUST NOT be advertised in AS-external-LSAs.

4. SPF Modifications

The SPF calculation described in section 16.1 [RFC2328] will be modified to ensure that the routers originating router-LSAs with the H-bit set will not be used for transit traffic. Step 2 is modified as follows:

2) Call the vertex just added to the tree vertex V. Examine the LSA associated with vertex V. This is a lookup in the Area A’s link state database based on the Vertex ID. If this is a router-LSA, and the H-bit of the router-LSA is set, and vertex V is not the root, then the router should not be used for transit and step (3) should be executed immediately. If this is a router-LSA, and bit V of the router-LSA (see Section A.4.2) is set, set Area A’s TransitCapability to TRUE. In any case, each link described by the LSA gives the cost to an adjacent vertex. For each described link, (say it joins vertex V to vertex W):
5. Auto Discovery and Backward Compatibility

To avoid the possibility of any routing loops due to partial deployment, this document defines a OSPF Router Information (RI) LSA with a Router Functional Capability TLV that includes the following Router Functional Capability Bit:

<table>
<thead>
<tr>
<th>Bit</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Host Router Support capability</td>
</tr>
</tbody>
</table>

Auto Discovery via announcement of the Host Support Functional Capability ensures that the H-bit functionality and its associated SPF changes SHOULD only take effect if all the routers in a given OSPF area support this functionality.

Implementations are encouraged to provide a configuration parameter to manually override enforcement of the H-bit functionality in partial deployments where the topology guarantees that OSPFv2 routers not supporting the H-bit do not compute routes resulting in routing loops. More precisely, the advertisement of MaxLinkMetric for the router's non-local links will prevent OSPFv2 routers not supporting the H-bit from attempting to use it for transit traffic.

6. OSPF AS-External-LSAs/NSSA LSAs with Type 2 Metrics

When calculating the path to an OSPF AS-External-LSA or NSSA-LSA with a Type-2 metric, the advertised Type-2 metric is taken as more significant than the OSPF intra-area or inter-area path. Hence, advertising the links with MaxLinkMetric as specified in [RFC6987] does not discourage transit traffic when calculating AS external or NSSA routes. Consequently, OSPF routers implementing [RFC6987] or this specification should advertise a Type-2 metric of LSInfinity for any self-originated AS-External-LSAs or NSSA-LSAs in situations when the OSPF router is acting as a stub router [RFC6987] or implementing this specification.

7. IANA Considerations

IANA is requested to create the OSPF Router-LSA bit registry with the following assignments:
This document also defines a new Router Functional Capability [RFC7770] known as the Host Router Support Functional Capability. This document requests IANA to allocate the value of this capability from the Router Functional Capability Bits TLV.

8. Security Considerations

This document introduces no new security considerations beyond those already specified in [RFC6987], [RFC2328], and [RFC5340].

9. Acknowledgements

The authors would like to acknowledge Hasmit Grover for discovery of the limitation in [RFC6987], Acee Lindem, Abhay Roy, David Ward, Burjiz Pithawala and Michael Barnes for their comments.

10. References

10.1. Normative References


10.2. Informative References


Authors’ Addresses

Keyur Patel
Arrcus

Email: keyur@arrcus.com

Padma Pillay-Esnault
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: padma@huawei.com
Manish Bhardwaj  
Cisco Systems  
170 W. Tasman Drive  
San Jose, CA 95134  
USA  
Email: manbhard@cisco.com

Serpil Bayraktar  
Cisco Systems  
170 W. Tasman Drive  
San Jose, CA 95134  
USA  
Email: serpil@cisco.com