Support of address families in OSPFv3
draft-ietf-ospf-af-alt-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet Drafts are draft documents valid for a maximum of six months. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a "working draft" or "work in progress".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document describes a mechanism for supporting multiple address families in OSPFv3 using multiple instances. It maps an address family (AF) to an OSPFv3 instance using the Instance ID field in the OSPFv3 packet header. This approach is fairly simple and minimizes
extensions to OSPFv3 for supporting multiple AF’s.
1. Motivation

OSPFv3 has been defined to support IPv6 unicast AF. There is a need to carry other AFs in OSPFv3 such as multicast IPv6, unicast or multicast IPv4. This document introduces these other AFs in OSPFv3 by reserving Instance IDs and using one OSPFv3 instance for one AF.

2. Proposed Solution

Currently the entire Instance ID number space is used for IPv6 unicast. We propose to assign different ranges to different AF’s in order to support other AF’s in OSPFv3. Each AF will establish different adjacency, have different link state database and compute different shortest path tree. Additionally, the current LSAs that are defined to carry IPv6 unicast prefix can be used without any modification in different instances to carry different AF’s prefixes.

It should be noted that OSPFv3 is running on the top of IPv6 and uses IPv6 link local address for OSPFv3 control packet and next hop calculation. Therefore, it is required that IPv6 be enabled on a link, although the link may not be participating in IPv6 unicast AF.

3. Instance ID values for new AF’s

Instance ID zero is already used by default for IPv6 unicast AF. We define the following ranges for different AF’s. The first value of each range is considered as the default value for the corresponding AF.

<table>
<thead>
<tr>
<th>Instance ID</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>#31</td>
<td>IPv6 unicast AF</td>
</tr>
<tr>
<td>32</td>
<td>#63</td>
<td>IPv6 multicast AF</td>
</tr>
<tr>
<td>64</td>
<td>#95</td>
<td>IPv4 unicast AF</td>
</tr>
<tr>
<td>96</td>
<td>#127</td>
<td>IPv4 multicast AF</td>
</tr>
<tr>
<td>128</td>
<td>#255</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

4. New bit in Options field

A new bit is defined in the Options field for AF support.
AF-bit

When a router supports AF, it MUST set this bit in the Options field of Hello Packets, DD packets and LSAs.

5. Changes to the Hello processing

When a router does not support an AF but it is configured with an Instance ID in the same range, packets could be blackholed. This could happen due to misconfiguration or router downgrade to a previous code level. Blackholing is possible because the router which doesn’t support the AF can still be included in the SPF calculated path as long as it establishes adjacencies using the Instance ID corresponding to the AF. Note that router and network LSAs are AF independent.

In order to avoid the above situation, hello processing is changed in order to only establish adjacency with the routers that have the AF-bit set in their Options field.

Receiving Hello Packets is specified in section 3.2.2.1 of [Ref1]. The following check is added to Hello reception:

When a router participate in an AF (sets the AF-bit in Options field) it MUST discard Hello packets having the AF-bit clear in the Options field. The only exception is IPv6 unicast AF, where this check MUST NOT be done (to help backward compatibility).

6. Modification to some of the bits defined in [Ref1]

Some of the bits defined in OSPFv3 are relevant to IPv6 unicast AF, and are not needed in other AF’s. Some may be applicable only to a certain AF. Below is the list of changes to those bits:

- Options Field

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| | | | | | | | | | | | | | | | | |DC| R | N* | E* |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- V6-bit
The V6 bit is used in OSPFv3 to exclude a node from IPv6 unicast route calculation but allow it in the SPF calculation for other address families. Since Instance ID now denotes the AF explicitly, this bit is ignored in AF’s other than IPv6 unicast.
o MC-bit

This bit is not used in other AF’s introduced in this document.

o Prefix Options Field

```
  0 1 2 3 4 5 6 7
+---+---+---+---+---+---+---+
|   |   |   | P|* |LA|NU |
+---+---+---+---+---+---+
```

o MC bit in the Prefix Options field

This bit is not used in other AF’s introduced in this document.

o NU bit usage in the Prefix Options field

The NU bit must be clear in all unicast AF’s and it must be set in all multicast AF’s.

Note that all bits unused in a given AF could be redefined later.

7. Carrying Prefixes in new AF’s

Each Prefix defined in OSPFV3 has a prefix length field. This facilitate advertising prefixes of different lengths in different AF’s. The existing LSAs defined in OSPFV3 are used for this purpose and there is no need to define new LSAs.

8. Next hop for IPv4 unicast and multicast AF’s

OSPFV3 runs on the top of IPv6 and uses IPv6 link local addresses for OSPFV3 control packets and next hop calculations. Although IPv6 link local addresses could be used as next hops for IPv4 address families, it is desirable to have IPv4 next hop addresses. For example, in IPv4 multicast having the nexthop address the same as the PIM neighbor address (IPv4 address) makes it easier to know to which upstream neighbor to send a PIM join when doing a RPF lookup for a source. It is also easier for troubleshooting purposes to have a next hop with the same semantics as the AF.
In order to achieve this, the link’s IPv4 address will be advertised in the "link local address" field of the IPv4 instance’s Link-LSA. This address is placed in the first 32 bit of "link local address" field and used for IPv4 next hop calculations.
We call direct interface address (DIA) the address that is reachable directly via the link provided that a layer 3 to layer 2 mapping is available. Note that there is no explicit need for the IPv4 link addresses to be on the same subnet. An implementation should resolve layer 3 to layer 2 mappings via ARP or ND for a DIA even if the IPv4 address is not on the same subnet as the router’s interface IP address.

9. OSPFv3 over IPv4

Although OSPFv3 is defined to run over IPv6, it is possible to run OSPFv3 over IPv4 and making IPv4 address-family, IPv6 independent. This is achieved by using IPv4 for OSPFv3 control packet with the same protocol number 89 as OSPFv2. The version in the OSPF packet allows to distinguish between OSPFv2 and OSPFv3.

We define a parameter in interface data structure called V4TransProtocol. V4TransProtocol flag can have two values: Enabled or Disabled, the default value being Disabled.

when set to Enabled OSPFv3 use IPv4 as transport protocol
When set to Disabled OSPFv3 use IPv6 as transport protocol

Note that this parameter can only be enabled in IPv4 address family (see section 3 for instance id range).

10. Virtual Link (VL)

When OSPFv3 is running over IPv4 there is no special requirement for VL to be operational since OSPFv3 control packet are sent over IPv4. However note that all routers within the area should run over IPv4 or provided that there is a contiguous path between the virtual link end point that run over IPv4.

When OSPFv3 is running over IPv6, the control packet sent for virtual link are IPv6 packets and may traverse multiples hops therefore there must be a global IPv6 address associated with the virtual link so that the control packet is forwarded correctly by the intermediate hops between VL end points. Although this requirement can be satisfied in IPv6 unicast AF, this will not function in other AF as there cannot be a multihop forwarding based on global IPv6 address or such a path may not exist. Therefore virtual link are not currently supported in other AF’s.
11. Backward compatibility issues

Each new AF will have their corresponding Instance ID and can operate with the existing non-capable routers in IPv6 unicast topology. Further, when a non-capable router uses an Instance ID which is reserved for a given AF, since the non-capable router will not have the AF-bit set in the Hello an adjacency will not be established with an AF capable router. Therefore, there are no backward compatibility issues. AF’s can be gradually deployed without disturbing networks with current non-capable routers.

12. Address-family design Considerations

This section describes the rationale for adopting the multiple instance ID approach for supporting multiple address families in OSPFv3. As described earlier, OSPFv3 is designed to support multiple instances. Hence mapping an instance to an address family doesn’t introduce new mechanisms in the protocol. It minimizes the protocol extensions required and it simplifies the implementation. The presence of a separate link state database per address family is also easier to debug and operate. Additionally, it doesn’t change the existing instance, area and interface based configuration model in most OSPF implementations.

13. Security Considerations

The technique described in this document does not introduce any new security issues to the OSPFv3 protocol.

14. References

15. Authors address

Sina Mirtorabi                          Acee Lindem
Cisco Systems                           Redback Networks
170 W. Tasman Dr.                       102 Carric Bend Court
San Jose, CA 95134                      Cary, NC 27519
Email: sina@cisco.com                   Email: acee@redback.com

Abhay Roy                               Quaizar Vohra
Cisco Systems                           Juniper Networks
170 W. Tasman Dr.                       1194 North Mathilda Ave.
San Jose, CA 95134                      Sunnyvale, CA 94089
Email: akr@cisco.com                    Email: qv@juniper.net

Michael Barnes                          Rahul Aggarwal
Cisco Systems                           Juniper Networks
170 W. Tasman Dr.                       1194 North Mathilda Ave.
San Jose, CA 95134                      Sunnyvale, CA 94089
Email: mjbarnes@cisco.com               Email: rahul@juniper.net