Ospf Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2015

Q. Liang
J. You
N. Wu
Huawei

March 6, 2015

# OSPF Extensions for Flow Specification
# draft-liang-ospf-flowspec-extensions-03

## Abstract

This document discusses the use cases why OSPF (Open Shortest Path First) distributing flow specification (FlowSpec) routes is necessary. This document also defines a new OSPF FlowSpec Opaque Link State Advertisement (LSA) encoding format that can be used to distribute FlowSpec routes.

For the network only deploying IGP (Interior Gateway Protocol) (e.g. OSPF), it is expected to extend IGP to distribute FlowSpec routes. One advantage is to mitigate the impacts of Denial-of-Service (DoS) attacks.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 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 http://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 September 7, 2015.

Table of Contents



## 1. Introduction

[RFC5575] defines a new Border Gateway Protocol Network Layer Reachability Information (BGP NLRI) encoding format that can be used to distribute traffic flow specifications. One application of that

encoding format is to automate inter-domain coordination of traffic filtering, such as what is required in order to mitigate (distributed) denial-of-service attacks. [RFC5575] allows flow specifications received from an external autonomous system to be forwarded to a given BGP peer. However, in order to block the attack





traffic more effectively, it is better to distribute the BGP FlowSpec routes to the customer network, which is much closer to the attacker.

For the network only deploying IGP (e.g. OSPF), it is expected to extend IGP to distribute FlowSpec routes. This document discusses the use cases why OSPF distributing FlowSpec routes is necessary. This document also defines a new OSPF FlowSpec Opaque Link State Advertisement (LSA) [RFC5250] encoding format that can be used to distribute FlowSpec routes to the edge routers in the customer network. This mechanism can be used to mitigate the impacts of DoS attacks.

## 2. Terminology

This section contains definitions for terms used frequently throughout this document. However, many additional definitions can be found in [RFC5250] and [RFC5575].

Flow Specification (FlowSpec): A flow specification is an n-tuple consisting of several matching criteria that can be applied to IP traffic, including filters and actions. Each FlowSpec consists of a set of filters and a set of actions.

## 3. Use Cases for OSPF based FlowSpec Distribution

For the network only deploying IGP (e.g. OSPF), it is expected to extend IGP (OSPF in this document) to distribute FlowSpec routes, because when the FlowSpec routes are installed in the customer network, it would be closer to the attacker than when they are installed in the provider network. Consequently, the attack traffic could be blocked or the suspicious traffic could be limited to a low rate as early as possible.

The following sub-sections discuss the use cases for OSPF based FlowSpec routes distribution.

## 3.1. BGP/MPLS VPN

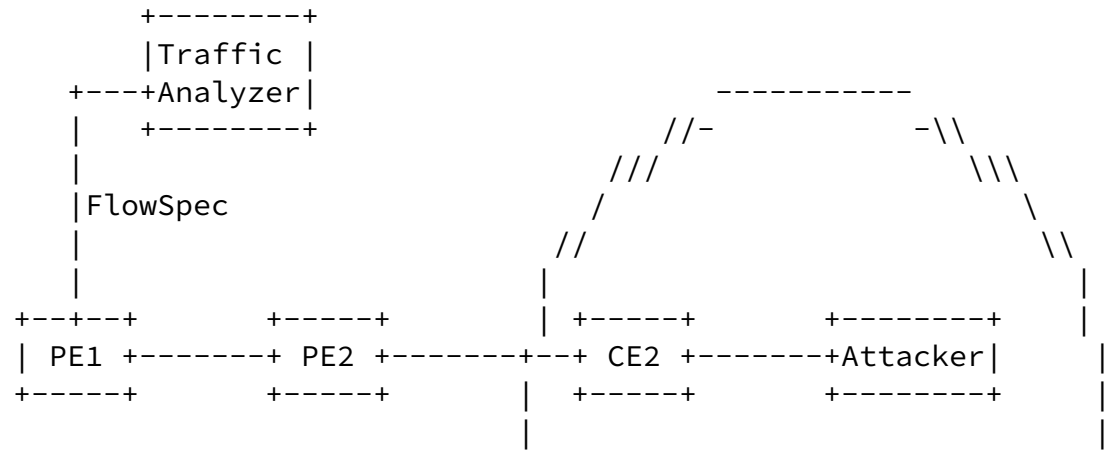
[RFC5575] defines a BGP NLRI encoding format to distribute traffic flow specifications in BGP deployed network. However in the BGP/MPLS VPN scenario, the IGP (e.g. IS-IS, OSPF) is used between PE (Provider Edge) and CE (Customer Edge) for many deployments. In order to distribute the FlowSpec routes to the customer network, the IGP needs to support the FlowSpec route distribution. The FlowSpec routes are usually generated by the traffic analyzer or the traffic policy center in the network. Depending on the location of the traffic analyzer deployment, two different distribution scenarios will be discussed below.





### 3.1.1. Traffic Analyzer Deployed in Provider Network

The traffic analyzer (also acting as the traffic policy center) could be deployed in the provider network as shown in Figure 1. If the traffic analyzer detects attack traffic from the customer network VPN1, it would generate the FlowSpec routes for preventing DoS attacks. The FlowSpec routes with a route distinguisher information corresponding to VPN1 are distributed from the traffic analyzer to the PE1 which the traffic analyzer is the attached to. If the traffic analyzer is also a BGP speaker, it can distribute the FlowSpec routes based on the BGP [RFC5575]. Then the PE1 distributes the FlowSpec routes further to the PE2. Finally, the FlowSpec routes need to be distributed from the PE2 to the CE2 based on OSPF, i.e. to the customer network VPN1. As the attacker is more likely in the customer network, if the FlowSpec routes installed on the CE2, it could mitigate the impacts of DoS attacks better.



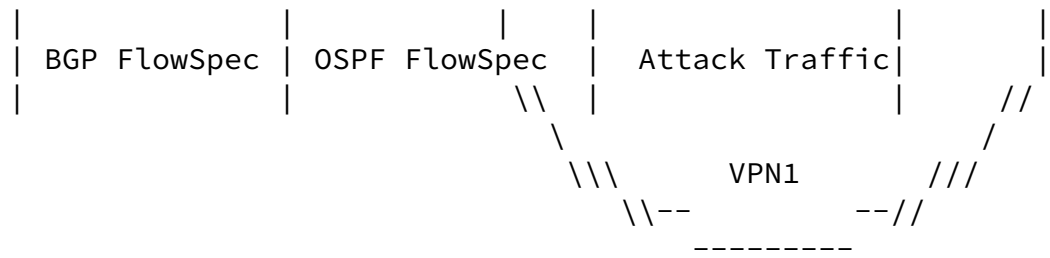



Figure 1: Traffic Analyzer deployed in Provider Network

### 3.1.2. Traffic Analyzer Deployed in Customer Network

The traffic analyzer (also acting as the traffic policy center) could be deployed in the customer network as shown in Figure 2. If the traffic analyzer detects attack traffic, it would generate FlowSpec routes for preventing DoS attacks. Then the FlowSpec routes would be distributed from the traffic analyzer to the CE1 based on OSPF or other policy protocol (e.g. RESTful API over HTTP). Further, the FlowSpec routes need to be distributed through the provider network





via the PE1/PE2 to the CE2, i.e. to the remote customer network VPN1 Site1. If the FlowSpec routes installed on the CE2, it could block the attack traffic as close to the source of the attack as possible.

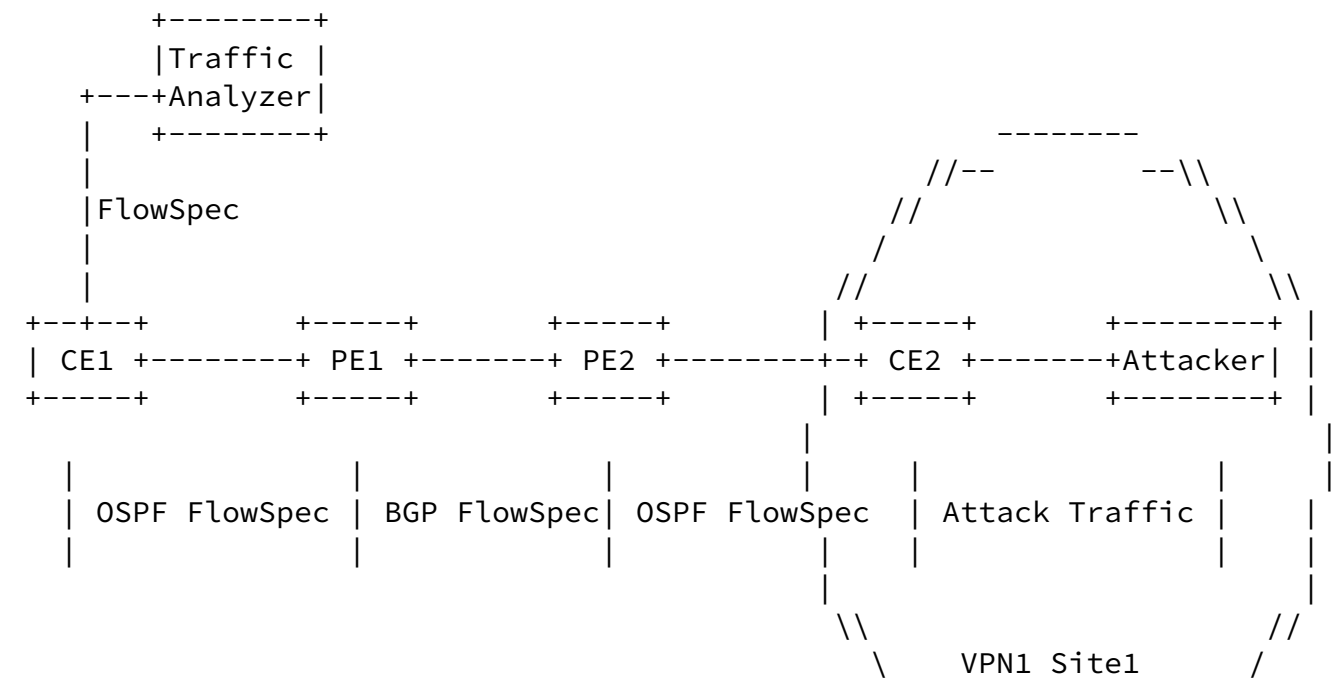


Figure 2: Traffic Analyzer deployed in Customer Network

### 3.1.3. Policy Configuration

The CE or PE could deploy local filtering policies to filter OSPF FlowSpec rules, for example, deploying a filtering policy to filter the incoming OSPF FlowSpec rules in order to drop illegal or invalid FlowSpec rules, or to filter the outcoming OSPF FlowSpec rules in order to prevent locally valid OSPF FlowSpec rules from dissemination outside.

The PE should configure FlowSpec importing policies to control importing action between BGP IP/VPN FlowSpec RIB and OSPF Instance FlowSpec RIB. Otherwise, the PE couldn't transform a BGP IP/VPN FlowSpec rule to an OSPF FlowSpec rule or transform an OSPF FlowSpec rule to a BGP IP/VPN FlowSpec rule.

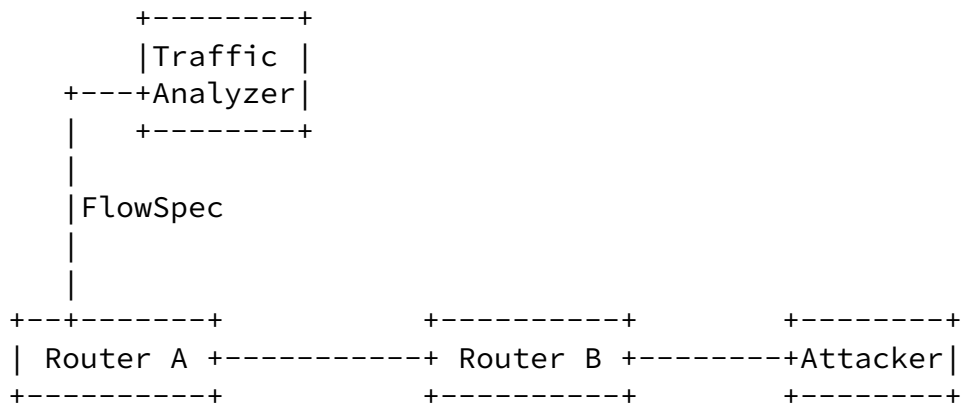
## 3.2. OSPF Campus Network

For the network not deploying BGP, for example, the campus network using OSPF, it is expected to extend OSPF to distribute FlowSpec routes as shown in Figure 3. In this kind of network, the traffic





analyzer could be deploy with a router, then the FlowSpec routes from the traffic analyzer need to be distributed to the other routers in this domain based on OSPF.



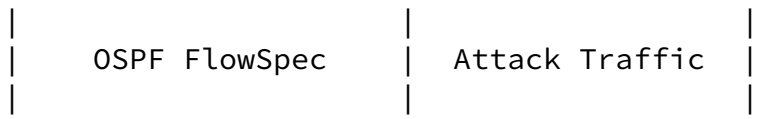



Figure 3: OSPF Campus Network

# 4. OSPF Extensions for FlowSpec Routes

## 4.1. FlowSpec LSA

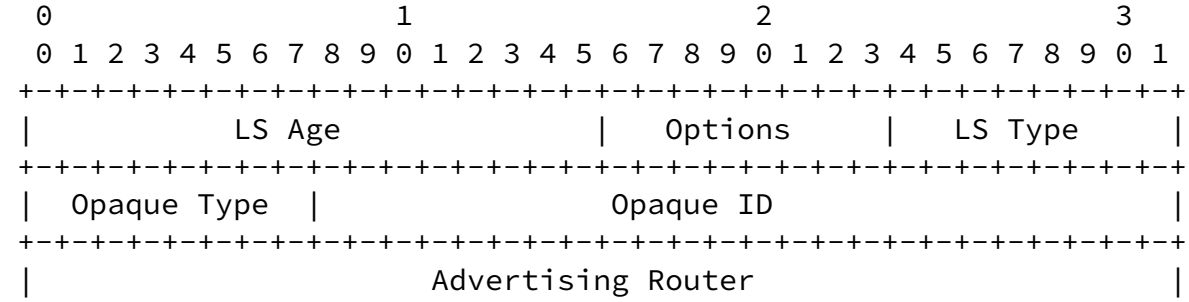
### 4.1.1. OSPFv2 FlowSpec Opaque LSA

This document defines a new OSPFv2 flow specification Opaque Link State Advertisement (LSA) encoding format that can be used to distribute traffic flow specifications. This new OSPF FlowSpec Opaque LSA is extended based on [RFC5250].

The OSPFv2 FlowSpec Opaque LSA is defined below in Figure 4:







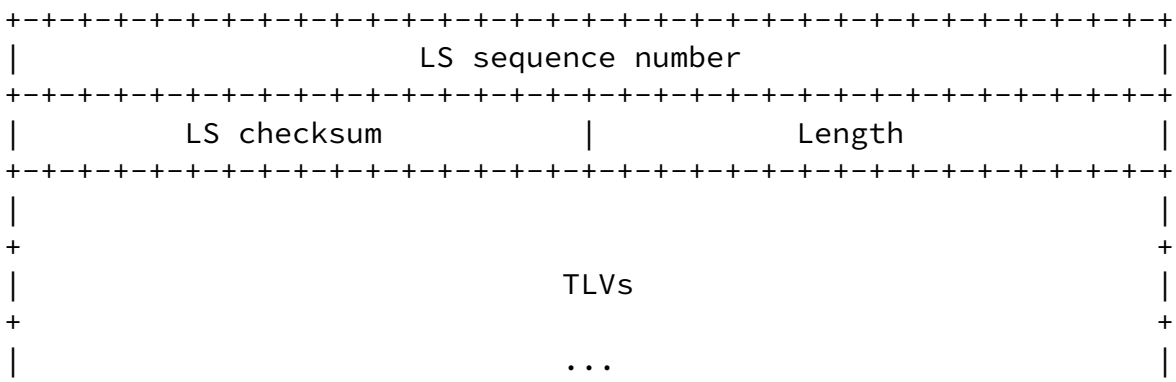



Figure 4: OSPFv2 FlowSpec Opaque LSA

LS age: the same as defined in [RFC2328].

Options: the same as defined in [RFC2328].

LS type: A type-11 Opaque-LSA SHOULD be originated since DoS attacks can happen at any place in one Autonomous System. At the same time, the originator MUST advertise itself as ASBR to satisfy the need for availability checking when inter-area propagating happened. Since the type-11 LSA has the same flooding scope as a type-5 LSA as stated in [RFC5250], it MUST NOT be flooded into stub areas or NSSAs (Not-So-Stubby Areas). When stub or NSSA areas are encountered in the scenario of flow spec, we may have to make our choice, either making peace with it and filtering the DoS traffic at ABRs or generating a new type-10 Opaque-LSA into stub/ NSSA areas, which may aggravate the burden of devices in that area.

Opaque type: OSPF FlowSpec Opaque LSA (Type Code: TBD1).

Opaque ID: the same as defined in [RFC5250].

Advertising Router: the same as defined in [RFC2328].

LS sequence number: the same as defined in [RFC2328].

LS checksum: the same as defined in [RFC2328].





Length: the same as defined in [RFC2328].

TLVs: one or more TLVs MAY be included in a FlowSpec Opaque LSA to carry FlowSpec information.

The variable TLVs section consists of one or more nested Type/Length/Value (TLV) tuples. Nested TLVs are also referred to as sub-TLVs. The format of each TLV is shown in Figure 5:

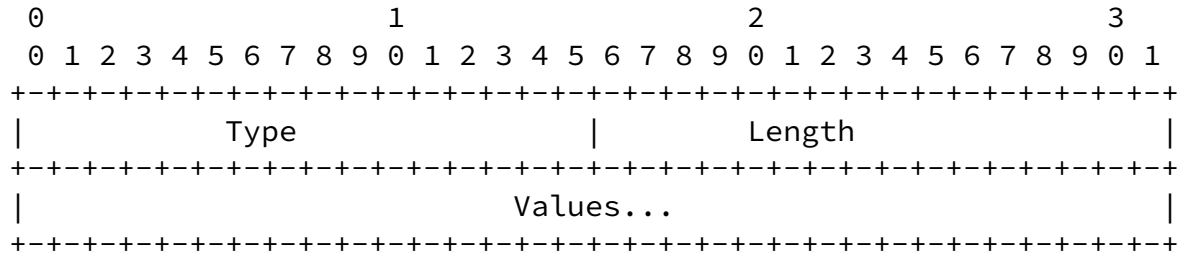



Figure 5: TLV Format

The Length field defines the length of the value portion in octets (thus a TLV with no value portion would have a length of 0). The TLV is padded to 4-octet alignment; padding is not included in the length field (so a 3-octet value would have a length of 3, but the total size of the TLV would be 8 octets). Nested TLVs are also 32-bit aligned. For example, a 1-byte value would have the length field set to 1, and 3 octets of padding would be added to the end of the value portion of the TLV.

FlowSpec Opaque LSA is Type-11 Opaque LSA which is not flooded into Stub and NSSA areas. As the traffic accessing a network segment outside Stub and NSSA areas would be aggregated to the ABR, FlowSpec rules could be executed on the ABR instead of disseminating them into Stub and NSSA areas.

### 4.1.2. OSPFv3 FlowSpec LSA

This document defines a new OSPFv3 flow specification LSA encoding format that can be used to distribute traffic flow specifications. This new OSPFv3 FlowSpec LSA is extended based on [RFC5340].

The OSPFv3 FlowSpec LSA is defined below in Figure 6:

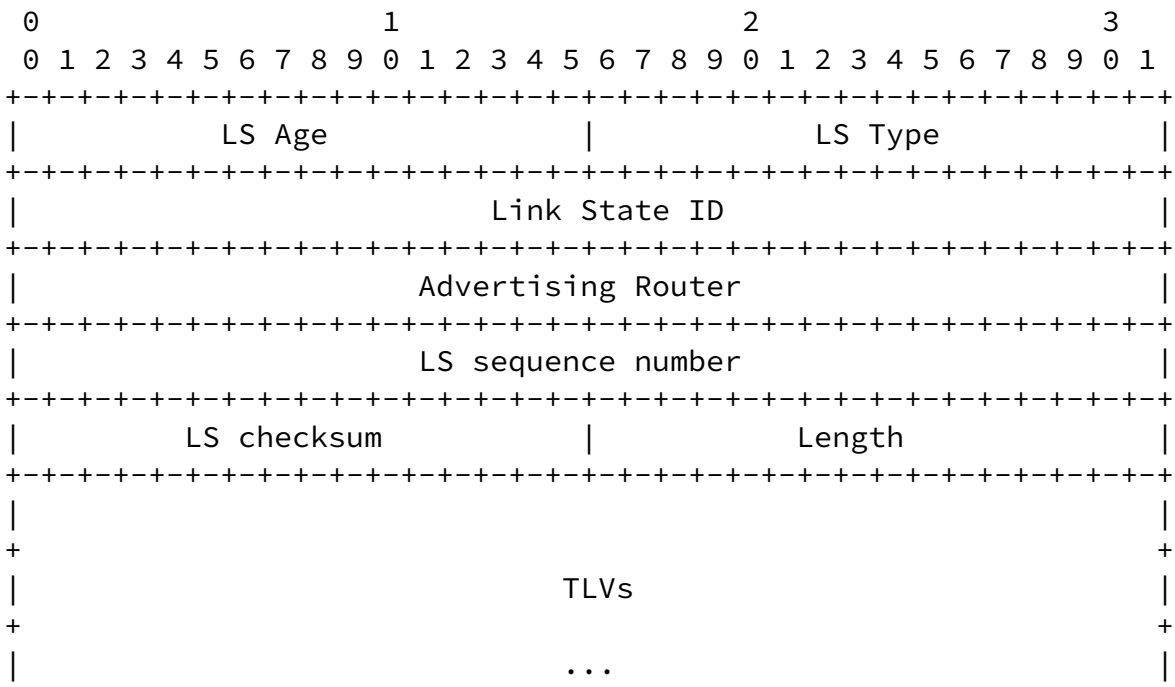



Figure 6: OSPFv3 FlowSpec LSA

LS age: the same as defined in [RFC5340].

LS type: the same as defined in [RFC5340]. The format of the LS type is as follows:

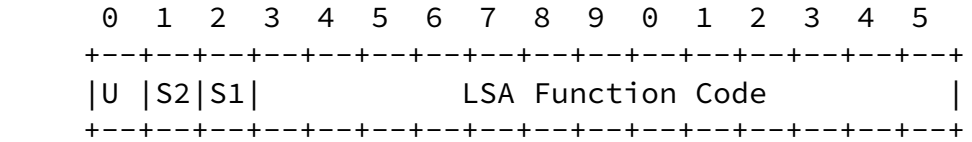



Figure 7: LSA Type

In this document, the U bit should be set indicating that the OSPFv3 FlowSpec LSA should be flooded even if it is not understood. For the area scope, S1 bit should be set and S2 should be 0. For the AS scope, the S1 bit should be 0 and S2 bit should be set. Meanwhile, A new LSA Function Code (TBD2) needs to be defined for OSPFv3 FlowSpec LSA. To facilitate inter-area reachability validation, any OSPFv3 router originating AS scoped LSAs is considered an AS Boundary Router (ASBR).

Link State ID: the same as defined in [RFC5340].

Advertising Router: the same as defined in [RFC5340].

LS sequence number: the same as defined in [RFC5340].





LS checksum: the same as defined in [RFC5340].

Length: the same as defined in [RFC5340].

TLVs: one or more TLVs MAY be included in a OSPFv3 FlowSpec LSA to carry FlowSpec information.

## 4.2. OSPF FlowSpec Filters TLV

The FlowSpec Opaque LSA carries one or more FlowSpec Filters TLVs and corresponding FlowSpec Action TLVs. OSPF FlowSpec Filters TLV is defined below in Figure 6.

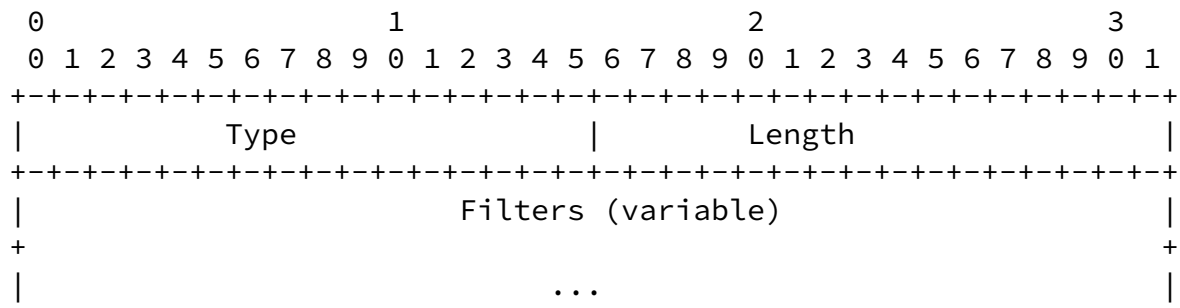



Figure 6: OSPF FlowSpec Filters TLV

Type: the TLV type (Type Code: TBD3)

Length: the size of the value field (typically in bytes)

Filters: the same as "flow-spec NLRI value" defined in [RFC5575].

## 4.3. OSPF FlowSpec Action TLV

There are one or more FlowSpec Action TLVs associated with a FlowSpec Filters TLV. Meanwhile, different FlowSpec Filters TLV could have the same FlowSpec Action TLV/s. The following OSPF FlowSpec action TLVs except Redirect are the same as defined in [RFC5575].

Redirect: 2-byte IPv4 or 16-byte IPv6 address. This IP address may correspond to a tunnel, i.e. the redirect allows the traffic to be

redirected to a real next hop or egress interface by looking up the RIB based on the IP address.





Table 1: Traffic Filtering Actions in [RFC5575]

| type | FlowSpec Action | encoding |
|---|---|---|
| 0x8006 | traffic-rate | 2-byte as#, 4-byte float |
| 0x8007 | traffic-action | bitmask |
| 0x8008 | redirect | 4/16-byte IPv4/v6 address |
| 0x8009 | traffic-marking | DSCP value |

## 4.4. Capability Advertisement

OSPF routers may use Router Information (RI) LSA [RFC4970] for OSPF features advertisement and discovery. The FlowSpec route requires an additional capability for the OSPF router. This capability needs to be advertised to other routers in an AS. This FlowSpec capability could be advertised in a RI Opaque LSA [RFC4970].

The format of the OSPF Router Informational Capabilities TLV within the body of an RI LSA is defined as follows:

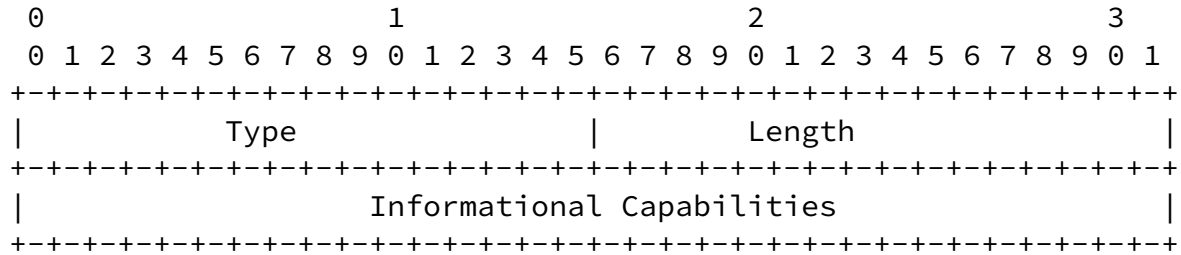


Figure 4: OSPF RI Capabilities TLV

The following informational capability bits are assigned:

| Bit | Capabilities |
|---|---|
| TBD4 | OSPF FlowSpec |
| 7-31 | Unassigned (Standards Action) |

## 5. IANA Considerations

This document defines a new OSPFv2 Opaque LSA, i.e. OSPFv2 FlowSpec Opaque LSA (Type Code: TBD1), which is used to distribute traffic flow specifications.





This document defines a new OSPFv3 LSA, i.e. OSPFv3 FlowSpec LSA (LSA Function Code: TBD2), which is used to distribute traffic flow specifications.

This document defines OSPF FlowSpec Filters TLV (Type Code: TBD3), which is used to describe the filters.

This document defines a new FlowSpec capability which need to be advertised in an RI Opaque LSA. A new informational capability bit needs to be assigned for OSPF FlowSpec feature (FlowSpec Bit: TBD4).

## 6. Security considerations

This extension to OSPF does not change the underlying security issues inherent in the existing OSPF. Implementations must assure that malformed TLV and Sub-TLV permutations do not result in errors which cause hard OSPF failures.

## 7. Acknowledgement

TBD.

## 8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, February 2006.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

[RFC4970] Lindem, A., Shen, N., Vasseur, JP., Aggarwal, R., and S. Shaffer, "Extensions to OSPF for Advertising Optional Router Capabilities", RFC 4970, July 2007.

[RFC5250] Berger, L., Bryskin, I., Zinin, A., and R. Coltun, "The OSPF Opaque LSA Option", RFC 5250, July 2008.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.





[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, August 2009.

Authors' Addresses

Qiandeng Liang
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, 210012
China

Email: liuweihang@huawei.com

Jianjie You
Huawei
101 Software Avenue, Yuhuatai District

Nanjing,  210012
China

Email: youjianjie@huawei.com

Nan Wu
Huawei

Email: eric.wu@huawei.com