IDR Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 10, 2016

S. Hares
Huawei

February 7, 2016

An Information Model for Basic Network Policy and Filter Rules
draft-hares-idr-flowspec-combo-00.txt

Abstract

BGP flow specification (RFC5575) describes the distribution of filters and actions that apply when packets are received on a router with the flow specification function turned on. If one considers the reception of the packet as an event, then BGP flow specification describes a set of minimalistic Event-Match Condition-Action policies. The initial set of policy (RFC5575 and RFC7674) for this policy includes 12 types of match filters encoded in the NLRI for two types of SAFIs (IP-only SAFI, 133; VPN SAFI, 134) for IPv4. The popularity of these flow specification filters in deployment for DoS and SDN/NFV has led to the requirement for more BGP flow specification match filters in the NLRI and more BGP flow specification actions.

This document provides rules for combining new flow specification packet ECA policies which support IPv6, L2, nvo03 and MPLS match filters, and new actions. This document also provides rules for the interaction of IDR Flow Specification policy (session ephemeral policy) with policy found in I2RS (reboot ephemeral policy), and policy found in ACLs and Policy routing (configuration policy).

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 August 10, 2016.

Table of Contents

1. Introduction

Section 1 of this draft contains an introduction to BGP flow specification [RFC5575] and drafts expanding the RFC5575 state. Section 2 contains the definitions related to this draft. Section 3 provides an overview of existing and proposed flow specification policy rules decribed in terms of packet event, packet match conditions, and actions (packet forwarding or packet match). The flow specification policies reviewed include policy in RFCs ([RFC5575], [RFC7674]), IDR WG documents ([I-D.ietf-idr-flow-spec-v6], [I-D.ietf-idr-flowspec-l2vpn]), and the following proposed IDR WG documents

- [I-D.eddy-idr-flowspec-packet-rate] (traffic limiting by packet rate),
- [I-D.eddy-idr-flowspec-exp] (Extensions for BGP security and others),
- [I-D.hao-idr-flowspec-nvo3] (flow specification for inner/outer nv03 forwarding),
- [I-D.hao-idr-flowspec-redirect-tunnel] (redirect to tunnel),
- [I-D.li-idr-flowspec-rpd] (Additions to BGP FlowSpecification in Attribute),
- [I-D.liang-idr-bgp-flowspec-label] MPLS label related filters and actions,
- [I-D.liang-idr-bgp-flowspec-time] Filters by time,
- [I-D.litkowski-idr-flowspec-interfaceset]Filters applied by order for Interface group, and
- [I-D.vandevelde-idr-flowspec-path-redirect]Filters applied to packet identifier,

Section 4 describes the default precedence order for BGP flow specification policy based on Flow Specification packet events, packet match conditions, and the packet match actions; and a extended

community action to be used for "ordering action". Initial validation rules requires the passing of a IPv4 route associated with the BGP Flow specification rules. Section 4 also provides proposes new rules for validating BGP Flow Specification routes based on the new technologies of BGP ROAs ([RFC6482], [RFC6483]) and BGPSEC protocol [I-D.ietf-sidr-bgpsec-protocol]. Section 5 expands this precedence order to specify how the current BGP Flow specification interacts with the following non-BGP Filter packet filter forwarding specifications:

- I2RS Filter-Based RIB ([I-D.kini-i2rs-fb-rib-info-model], [I-D.hares-i2rs-fb-rib-data-model]),
- Policy Routing (aka Filter RIB), and
- ACLs.

Section 6 suggests the benefits of creating a Flow Specification version 2 with a new NRLI encoding that can allow ordering of flow specification filters and actions. Section 8 describes changes for the proposed Flow Specification Yang Module ([I-D.wu-idr-flowspec-yang-cfg].

Section 9 discusses the security considerations for all the BGP Flow Specifications.

1.1. Overview of RFC5575

[RFC5575] describes the dissemination of flow specification rules via groups BGP Multi-Protocol NLRIs and BGP communities. A flow specification operates on packets received in a router when the flow specification feature is configured. The flow specification specifies match conditions for filters for packets received by a router and actions to do based on a match of those filters. If one considers the reception of a packet as an event, then a BGP flow specifications can be considered a set of minimalistic Event-Match Condition-Action policies (ECA policies). This set is minimalistic because there is only one event - the reception of a packet. BGP Flow specifications are BGP policy passed between peers.

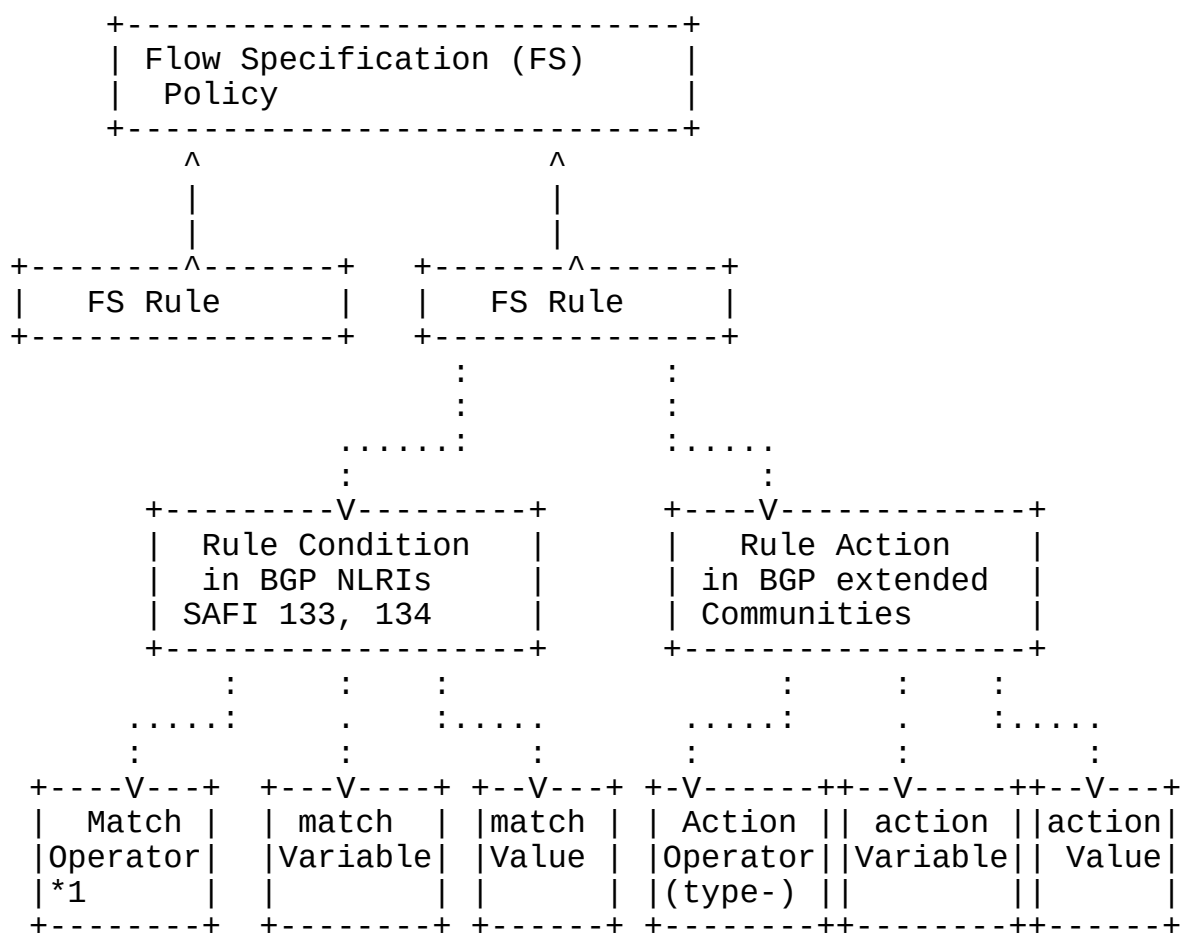
The BGP flow specification policy is specified in filters contained in the MP-BGP NLRIs and actions contained within BGP Extended communities. The BGP peer propagates the flow-specifications between domains in order to automate inter-domain coordination of traffic filtering. Two applications that are using this are: distributed denial of service attack suppression and traffic filtering in BGP/ MPLS VPN service. BGP. BGP flow specifications use SAFI 133 non-VPN flow specifications, and SAFI 134 for BGP VPN flow specificatinos.

BGP Flow specification are validated based on:

a) originator of flow specification matching the originator of the best-match unicast route for the destination prefix embedded in the flow specification, and

b) no more specific unicast routes, when compared with flow destination prefix, that have been received from differenting neighboring AS than the best-match unicast route

Originator is specified by BGP originator path attribute or transport address of the BGP peer sending the BGP Flow specification. To support BGP flow specification, implementations are required to enforce the neighbor AS in the AS_PATH attribute is in the left-most position of AS_PATH.



*1 match operator for Types 3-12. Match operator supports pairs of matching operators.

Figure 1: BGP Flow Specification Policy

Match operators includes a sequence of match operations each with the form [op, value] where match can match values greater, lessthan, or equal to teh value. The sequence of match operators can be combined as logical AND or ORs.

1.2. Flow Specifications: Ephemeral or not?

BGP Flow specification does not indicate what happens to the flow specifications if a BGP peering session closes. [RFC5575] specifies a link to received "best-match" unicast routes, but does not provide any standard way of determining whether the flow specification sent by the BGP peer is kept after the BGP session closes. It is unclear whether BGP Flow specifications disappear when a BGP session closes (denoted as BGP session ephemeral), or disapppear when the BGP module’s hardware or software reboots (reboot ephemeral), or it is

kept like configuration state that survives a reboot. This document in section 5 proposes that BGP Flow Specification is by default considered BGP session ephemeral disappearing when the BGP Session closes, and processes a precedence between the different types of ephemeral state.

Why is this precedence needed?

[RFC5575] states that Flow specification takes advantage of the "ACL" feature (section 1), but it does not state how BGP Flow specification interacts with ACL features. NETCONF [RFC6241] or RESTCONF [I-D.ietf-netconf-restconf] can be used to set ACL configuration state using the [I-D.ietf-netmod-acl-model] yang data module.

[I-D.litkowski-idr-flowspec-interfaceset] proposes an action which defines that a specific ordering of BGP flow-specifications and ACLs interaction for a set of interfaces for the drop/forward actions (see section 5.2 for a review). Section 5.1 proposes a default precedence between different types of flow Specification and an action. Section 5.2 proposed an action which augments [I-D.litkowski-idr-flowspec-interfaceset] to set an alternate order of precedence of flow specification drafts.

I2RS Filter-Based RIB (FB-RIB) also specifies another way to do flow filtering per packet/frame being received ([I-D.kini-i2rs-fb-rib-info-model], [I-D.hares-i2rs-fb-rib-data-model]) using a packet filter event-match_condition-action policy (draft-hares-i2rs-pkt-eca-data-model). I2RS protocol allows a I2RS Client to talk to an I2RS Agent within a routing device ([I-D.ietf-i2rs-architecture]) to set ephemermal policy which is module ephemeral and box ephemeral. Similar to BGP flow specification, the I2RS Filter-Based RIBs focus on a minimalistic event-match_condition-action (ECA) policy with a single event - the reception of a packet/frame on by a routing device. The I2RS match_conditions examine frame/packet information (L1-L4, NV03, and SFC), and I2RS match_actions that modify packet/frame information. Figure 2 shows the structure of packet filtering ECA rules from draft-hares-i2rs-pkt-eca-data-model) used by I2RS Filter-Based RIB (FB-RIB). Note that these each rule has policy rule name, policy rule order number, and rule status.

Section 5 compares the filters and actions between BGP Flow Specification, I2RS Filter-Based RIB, Filter-RIB (aka Policy-Based Routing), and the ACL. The I2RS packet filter rules also allow the rule to be ordered and named. I2RS flow-based filters are ephemeral state [I-D.ietf-i2rs-ephemeral-state] are stored as ephemeral state which is lost upon a reboot.

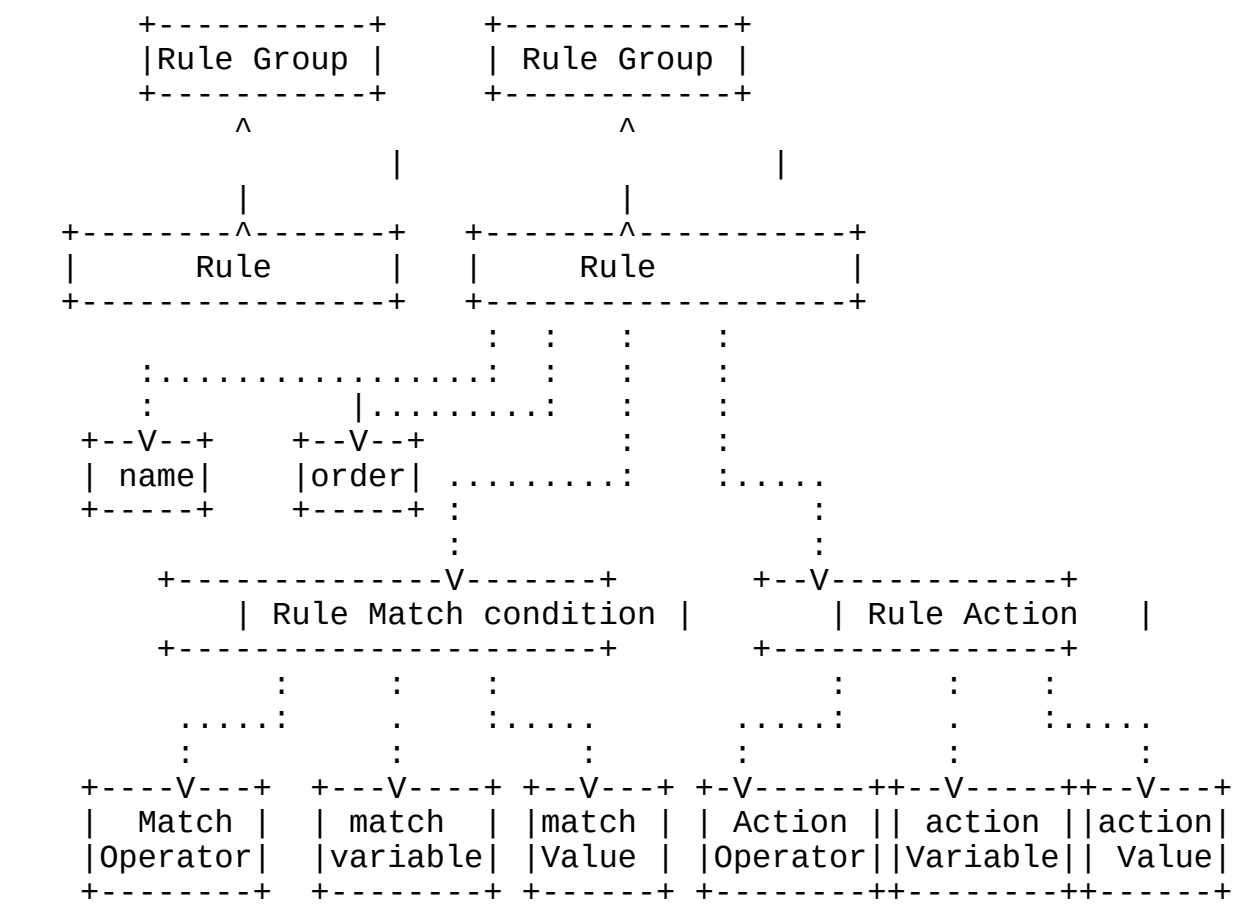


Figure 2: I2RS Filter-Based RIB Policy

1.3. BGP Flow Specification and logging

[RFC5575] specifies the Traffic Action Extended Community which specifies a Terminal (T) action flag and Sampling (S) flag. The sample flag indicates that "traffic sampling and logging" [is enabled] for a set of flow specifications in a BGP packet. the details of traffic sampling and logging are not specified in this standard. Logging and sampling provide valuable information to establish the impact of BGP Flow specification in order to automatic intra-AS DoS prevention or inter-AS automation of DOS or VPN traffic filters. [RFC5575] was written before the advent of yang modules that specify operational state [I-D.ietf-netmod-opstate-reqs]. [I-D.wu-idr-flowspec-yang-cfg] proposes a BGP Flow Specification Yang Data model with BGP Flow Specification configuration, operational state for BGP Flow specifications received from peers (BGP Session Ephemeral state), and statistics on the use of filters, actions, and dropped packets. Section 7 describes how the logging and notifications for BGP Flow specifications can be added to this yang module.

1.4. BGP Flow Specification and BGPSEC

[RFC5575] does not require BGP Flow specifications to be passed BGPSEC [I-D.ietf-sidr-bgpsec-protocol]. [RFC5575] states "as long as traffic filtering rules are restricted to match the corresponding unicast routing paths for relevant prefixes, the security characteristics of this protocol are equivalent to existing security properties of BGP unicast properties", and "where this is not the case, this would open the door to further denial of service attack" (section 10). [I-D.eddy-idr-flowspec-exp] suggests passing BGP Flow Specification in BGPSEC. Section 10 summarizes the security issues with the current [RFC5575] and the enhancements described in this draft, and discusses the proposed fixes that that [I-D.eddy-idr-flowspec-exp] provides.

2. Definitions

2.1. Definitions and Acronyms

NETCONF: The Network Configuration Protocol [RFC6241].

RESTconf - http programmatic protocol to access yang modules [I-D.ietf-netconf-restconf]

BGPSEC - secure BGP [I-D.ietf-sidr-bgpsec-protocol].

I2RS - Interface to Routing System [I-D.ietf-i2rs-architecture].

ephemeral - state which does not survive a particular event.

BGP Session ephemeral state - state which does not survive the loss of BGP peer,

Reboot ephemeral state - state which does not survive the reboot of a software module, or a hardware reboot.

configuration state - state which persist across a reboot of software module within a routing systsem or a reboot of a hardware routing device.

2.2. RFC 2119 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].

3. BGP Flow Specification Policy - Original and Expansions

3.1. Packet Reception Event

The reception of a packet is the event that causes the BGP policy to enact. By default the BGP Flow specification applies to all interfaces. This can be restricted by a BGP Flow Specification Action or policy local to a node running the BGP peer session.

The definition of a packet is not limited to a IP packet (IPv4 or IPv6) but also includes mpls packets, L2 frames (802.1Q), encapsulated packets (NVGRE or VXLAN or any other NV03 encapsulation).

The same definition of the event is utilized by the I2RS Filter-based RIBs ([I-D.kini-i2rs-fb-rib-info-model] and [I-D.hares-i2rs-fb-rib-data-model] and the Filter-Based RIBs (draft-hares-rtgwg-fb-rib-data-model), and ACL filters [I-D.ietf-netmod-acl-model].

These packet events are the standardized packet events. Additional packet events for vendors may augment these standards events.

3.2. BGP Flow Specification Match Filters

[RFC5575] defines match conditions for IPv4 to be carried with the NLRI format for 12 types of packet match events (see figure 3), and that all filters specified must be combined by a "AND". The proposed expansions to this filter list utilizing the Flow Specification NLRI are listed in figure 4. [I-D.li-idr-flowspec-rpd] proposed a BGP Attribute which contains additional flow specification filters, and actions. Figure 5 contains the match filters from this draft.

The proposals to expand flow specification beyond [RFC5575] filter specifications include:

- Matches for the inner-outer header for encapsulated traffic for being specified for the NV03 networks (MF-1, MF-2, MF-3) in [I-D.hao-idr-flowspec-nvo3],

- extended match filters carried in BGP attribute which includes time (MF-5) for enacting flow-specification filter rules ([I-D.li-idr-flowspec-rpd], [I-D.liang-idr-bgp-flowspec-time]).

One filter that seems obvious is the filter for the MPLS labels. However, no proposal includes this Match filter for MPLS.

The precedence order for the match filter rules was specified in [RFC5575] and expanded in [I-D.ietf-idr-flowspec-l2vpn]. The combined precedence is shown in figure 4.

Table 1: IDR WG BGP Flow Specification Match Filter

type#	Type Name	Match	Reference
1	Destination Prefix	IPv4 Prefix	RFC5575
		IPv6 Prefix	ietf-idr-flow-spec-v6
2	Source Prefix	IPv4 Prefix	RFC5575
		IPv6 Prefix	ietf-idr-flow-spec-v6
3	IP protocol	IPv4 Protocol number	RFC5575
3	Next Header	IPv6 protocol	ietf-idr-flow-spec-v6
4	Port (source or destination port)	Port number	RFC5575
			RFC5575
5	Source port	Port number	RFC5575
6	Destination port	Port number	RFC5575
7	ICMP type	ICMP type	RFC5575
8	ICMP code	ICMP code	RFC5575
9	TCP Flags	1 or 2 byte bitmask for TCP flags	RFC5575
			RFC5575
10	Packet length (for IP packet)	# of bytes	RFC5575
11	DSCP	IPv4 DSCP (6 bit mask)	RFC5575
			RFC5575
11	Traffic class	IPv6 traffic (8 bit mask)	ietf-idr-flow-spec-v6
12	IPv4 Fragment	4 bit mask	RFC5575
13	IPv6 Flow	20 bit flow	ietf-idr-flow-spec-v6
14	Ethernet type	2 bytes	ietf-idr-flowspec-l2vpn
15	Source MAC	MAC address	ietf-idr-flowspec-l2vpn
16	Destination MAC	MAC Address	ietf-idr-flowspec-l2vpn
17	DSAP in LLC	1 octet	ietf-idr-flowspec-l2vpn
18	SSAP in LLC	1 octet	ietf-idr-flowspec-l2vpn
19	LLC Control field	1 octet	ietf-idr-flowspec-l2vpn
20	SNAP	5 octets	ietf-idr-flowspec-l2vpn
21	VLAN ID	1 or 2 bytes	ietf-idr-flowspec-l2vpn
22	VLAN COS	3 bit COS	ietf-idr-flowspec-l2vpn
23	Inner VLAN ID	1 or 2 bytes	ietf-idr-flowspec-l2vpn
24	Inner VLAN COS	1 or 2 bytes	ietf-idr-flowspec-l2vpn

Figure 3

Table 2: Proposed BGP Flow Specification Match Condition Filters

type#	Type Name	Match	Reference
MF-1	Delimiter type (Encapsulation type VXLAN or NVGRE)	2 bytes	hao-idr-flowspec-nv03
MF-2	VNID (virtual network ID)	24 bit VN	hao-idr-flowspec-nv03
MF-3	Flow ID (NVGRE Flow ID)	8 bit flow ID	hoa-idr-flowspec-nv03
MF-4	MPLS LSP (label 20 bits, EXP (3 bits), S Bit TTL (8 bits)	TBD Label stack	not specified
MF-5	Interface (Group ID, intf id)	TBD	not specified

Figure 4

Table 3: Proposed BGP Flow Specifications Match in BGP Attribute

type#	Type Name	Match	Reference
MF-6	Time	??	liang-idr-bgp-flowspec -time
MF-7	Policy from IPv4 Neighbor	?? ??	li-idr-flowspec-rpd
MF-8	Policy from IPv6 Neighbor	?? ??	li-idr-flowspec-rpd
MF-9	Policy with ASpath	??	li-idr-flowspec-rpd

Figure 5

```
Precedence logic for BGP Flow Specifications
 (RFC5575, draft-idr-bgp-flowspec-l2vpn)

flow-rule-cmp (a,b)
{
  comp1 = next_component(a);
  comp2 = next_component(b);
  while (comp1 || comp2) {
   // component_type returns infinity on end of list
   if (component_type(comp1) < component_type(comp2)) {
    return A_HAS_PRECEDENCE;
    }

   if (component_type(comp1) > component_type(comp2)) {
    return B_HAS_PRECEDENCE;
   }

   // IP values)
   if (component_type(comp1) == IP_DESTINATION || IP_SOURCE) {
      common = MIN(prefix_length(comp1),prefix_length(comp2));
          cmp = prefix_compare (comp1,comp2,common);
          // not equal, lowest value has precedence
          // equal, longest match has precedence;
   } else if (component_type (comp1) == MAC_DESTINATION ||
               MAC_SOURCE) {
                 common = MIN(MAC_address_length(comp1),
                              MAC_address_length(comp2));
                 cmp = MAC_Address_compare(comp1,comp2,common);
                 //not equal, lowest value has precedence
                 //equal, longest match has precedence
        } else {
        common = MIN(component_length(comp1),
                              component_length(comp2));
            cmp = memcmp(data(comp1), data(comp2), common);
                 //not equal, lowest value has precedence
                 //equal, longest string has precedence
    }
  }
}
```

Figure 6

3.3. BGP Flow Specification Actions

[RFC5575] also defines four actions which would be carried in BGP extended communities: traffic rate (in bytes), traffic action, redirect to IPv4 VPAN, and traffic marking. Traffic action has two bits Terminal bit (T) and Sample (S) bit. If the Terminal Bit is

set, the the node apply all filter rules based as defined by "AND" and precedence. If the terminal bit is clear, then the flow specification process is to stop. The Sample bit implies that the flow specification enables sampling and logging for this event.

Unfortunately, [RFC5575] was unclear about the "redirect to IP VPN action" and did not handle IPv6. [RFC7674] was written to clarify [RFC5575] by clearly specifying the 3 extended communities that "IPv4 VPN" needed to support AS 4 byte, and IPv4 address Routing Distinguishers (RDs). [I-D.ietf-idr-flow-spec-v6] was written to extend this work to IPv6 filters, and to include the IPv6 flow in the filter set as figure 5 shows.

Proposals to extend these standardized actions include:

- (FA1) [I-D.eddy-idr-flowspec-packet-rate] specifies a traffic rate limit by packets the number of packets forwarded,

- (FA2)[I-D.li-idr-flowspec-rpd] specifies an "R" bit for traffic action that allows a BGP Attribute to pass additional BGP Flowspecification match filters and actions,

- (FA3) [I-D.hao-idr-flowspec-redirect-tunnel] specifies a redirection to a tunnel specified in [I-D.rosen-idr-tunnel-encaps],

- (FA4)[I-D.ietf-idr-flowspec-l2vpn] specifie push, pop, or swap VLANs before forwarding,

- (FA5) [I-D.ietf-idr-flowspec-l2vpn] specifies the ability to replace TPIDs values with new values before forwarding,

- (FA6) [I-D.liang-idr-bgp-flowspec-label] specifies push/pop/swap on MPLS labels before forwarding,

- (FA7)[I-D.litkowski-idr-flowspec-interfaceset] which specifies that ACL filters plus BGP flow specification filters will determine the acceptance/drop of inbound packet, and the forwarding/drop of outbound packets.

Figure 8 shows these flow specifications.

[RFC5575] indicates that the actions specified in the document represent only the "subset of filtering actions that can be interpreted across the network". As additional standardized actions occur, the non-standard action will need to have a precedence below the standardized actions.

One the probems with adding the actions is that precedence has not been set for the actions.

Table 4: BGP Flow Specifications in RFC5575 and RFC7674

type#	Action name	action	Reference
0x8006	Traffic Rate (in bytes)	2 octet AS 4 octet float	RFC5575
0x8007	Traffic Action (S:Sample and log, T:last flowspec	6 octet bit mask:S,T bits	RFC5575
0x8008	Redirect (IP VPN) (RD: 2 octet AS, 4 octet value)	Route Target (6 octet)	RFC5575 and RFC7674
0x8108	Redirect (IP VPN) (RD: 4 octet IPv4 address, 2 byte value)	Route Target (6 octet)	RFC7674
0x8208	Redirect (IP VPN) (RC: 4 byte AS, 2 byte value)	Route Target	RFC7674

Figure 7

Table 5: Proposed Flow Specification Actions

type#	Action name	action	Reference
FA1	Traffic Rate (in packets)	2 octet AS 4 octet float	eddy-idr-flowspec-packet-rate
FA2	Extended Traffic Extension for R to take additional Flow specifications from BGP Flow spec Policy attribute	R bit P bit	li-idr-flowspec-rpd Alternate action procedures(this draft)
FA3	Redirect to tunnel (tunnel in BGP Attribute)	6 octets 1 bit flag (C=applies to copies only)	hao-idr-flowspec-redirect-to-tunnel
FA4	VLAN-action (push, pop, swap)	bitmask	idr-bgp-flowspec-l2vpn

FA5	TPID Action (NVGRE Flow ID)	6 octets	idr-bgp-flowspec-l2vpn
FA6	Label Action (push/pop/swap MPLS label uses Exp flag, TTL, Stack flag (S))	MPLS Tag, TTL(1 octet) S bit	liang-idr-bgp-flowspec-label-01
FA7	Alternate NLRI Validation (mask for support of RFC5755, ROA and bgpsec-protocol AS path) and L2MAC NRLI for IP Address	validation bit mask	eddy-idr-flowspec-exp (some functions)
FA8	for Interface set filter ACL + Flow specification rules	4 Byte AS 2 byte interface group ID	litkowski-idr-flowspec-interfaceset

Note: FA8 is really a filer plus an action:
FA8-filter: Restrict processing for filters to set of interfaces
FA8-Action: Forward only if: ACL + Flow-Specification filters suggest forwarding.

Figure 8

3.4. BGP Flow Specification Security

[RFC5575] requires BGP flow specification is not required to pass in BGPSEC [I-D.ietf-sidr-bgpsec-protocol]. [RFC5575] states "as long as traffic filtering rules are restricted to match the corresponding unicast routing paths for relevant prefixes, the security characteristics of this protocol are equivalent to existing security properties of BGP unicast properties", and "where this is not the case, this would open the door to further denial of service attack" (section 10).

[RFC5575] requires an extension of the BGP route selection procedures [RFC4271] in section 9.1.2 in order to validate the BGP flow specification NLRI. The BGP Flow Specification NLRI is valid if and only if:

- o "the originator of the flow specification matches the orginator of the the best-match unicast route for the destination prefix embedded in the flow specification",

- o "no more specific unicast routes" exist "when compared with the flow destination prefix", that have been received from a different neighboring AS than the best-match unicast route, which has been determined in step A".

This set of validation requirements also require that BGP implementations are required to enforce the AS_PATH attribute having the neighbor AS in the left-most position.

These validation steps required a unicast IPv4 or IPv6 route be transmitted with L2VPN ([I-D.ietf-idr-flowspec-l2vpn]) and the NV03 flow specifications [I-D.hao-idr-flowspec-nvo3] to validate the path. These specifications do not provide additional details on any additional validation needed for the L2VPN or NV03 Case.

Since [RFC5575] BGP Route Origin validation [RFC6482] has been standardized, and the BGPSEC protocol [I-D.ietf-sidr-bgpsec-protocol] has been developed. [I-D.eddy-idr-flowspec-exp] specifies cryptographic enhancements that include:

- o creating a BGP identifier (in BGP attribute or in BGPSEC signature),

- o Expanding BGPSEC coverage for Route Orgination Authorization (ROA) to cover the orignator of the BGP Flow specification for the BGP Flow specification SAFIs.

- o Covering the BGP Extended Communities with BGP signature.

This document describes the precedence of these BGP security features.

4. Precedence Ordering for BGP Flow specification

BGP Flow specification is session ephemeral state which will not persist when the BGP peer session closes. I2RS Filter-Based RIB is reboot ephemeral state which will not persist when the routing entity reboots. Policy RIB (aka Filter Forwarding RIB) and ACLs are configuration state which can persist over the reboot of a system.

4.1. New Validation Rules for BGP Flow Specification: Precedence with ROA

This precedence within BGP Session Ephemeral state depends on the preference associated with valid BGP Session flow specification NLRI received within a BGP State. Since [RFC5575] was published, additional mechanisms to validate originating prefixes with an AS with Prefix Orgin Validation (ROA), and the BGPSEC Secure Path have been standardized. The precedence of these mechanisms should be from BGP Security to ROA to [RFC5575]. The BGP peers determine that a BGP Flow specification is valid if and only if one of the following cases:

- If the BGP Flow Specification NLRI has a IPv4 or IPv6 address in destination address match filter and the following is true:
  - A BGP ROA has been received to validate the originator, and
  - the route is the best-match unicast route for the destination prefix embedded in the match filter; or
- If a BGP ROA has not been received that matches the IPv4 or IPv6 destination address in the destination filter, the match filter must abide by the [RFC5575] validation rules of:
  - The originator match of the flow specification matches the originator of the best-match unicast route for the destination prefix filter embedded in the flow specification", and
  - No more specific unicast routes exist when compared with the flow destination prefix that have been received from a different neighboring AS than the best-match unicast route, which has been determined in step A.

The best match is defined to be the longest-match NLRI with the highest preference.

4.2. Default Match Condition Filter Precedence Ordering

Match conditions depends on an "AND" of all rules within a Flow Specification policy. A Flow specification policy is defined by a sequence of BGP Flow specification NLRIs with filter-match rules. The sequence of Flow Specification rules are terminate Traffic Action with a T-Bit flag set to zero.

Match condition processing occurs in the following overall precedence:

1. IP Protocol (1-13),

2. NV03-matches (MF-1 to MF-3),

3. Other overlay matches (spring, SFC)

4. L2VPN matches (14-24),

5. MPLS matches (MF-4),

6. L2VPN matches (currently 14-24),

7. interfaces matches (MF-5),

8. time matches (MF-6), and

9. Non-Standardized (First-Come-First Serve(FCFS)) match conditions (see [RFC5575] section 11)

Table 6 in figure 9 shows the filter by filter precedence order. All flow specification filters combine as an "AND" of all filters. A re-ordering of match filters is only possible in the the proposed version 2 of BGP Flow specification.

Table 6: Flow Specification Match Filter Precedence Order

type#	Type Name	Match	Reference
1	Destination Prefix	IPv4 Prefix	RFC5575
		IPv6 Prefix	ietf-idr-flow-spec-v6
2	Source Prefix	IPv4 Prefix	RFC5575
		IPv6 Prefix	ietf-idr-flow-spec-v6
3	IP protocol	IPv4 Protocol number	RFC5575
3	Next Header	IPv6 protocol	ietf-idr-flow-spec-v6
4	Port (source or destination port)	Port number	RFC5575
			RFC5575
5	Source port	Port number	RFC5575
6	Destination port	Port number	RFC5575
7	ICMP type	ICMP type	RFC5575
8	ICMP code	ICMP code	RFC5575
9	TCP Flags	1 or 2 byte bitmask for TCP flags	RFC5575
			RFC5575
10	Packet length (for IP packet)	# of bytes	RFC5575
11	DSCP	IPv4 DSCP (6 bit mask)	RFC5575
			RFC5575

11	Traffic class	IPv6 traffic (8 bit mask)	ietf-idr-flow-spec-v6
12	IPv4 Fragment	4 bit mask	RFC5575
13	IPv6 Flow	20 bit flow	ietf-idr-flow-spec-v6
14 MF-1	Delimiter type (Encapsulation type VXLAN or NVGRE)	2 bytes	hao-idr-flowspec-nv03
15 MF-2	VNID (virtual network ID)	24 bit VN	hao-idr-flowspec-nv03
16 MF-3	Flow ID (NVGRE Flow ID)	8 bit flow ID	hoa-idr-flowspec-nv03
17	Segment ID		
18-25	Other packet ids above MPLS		
29 MF-4	MPLS LSP (label 20 bits, EXP (3 bits), S Bit TTL (8 bits)	TBD Label stack	not specified
30	Ethernet type	2 bytes	ietf-idr-flowspec-l2vpn
31	Source MAC	MAC address	ietf-idr-flowspec-l2vpn
32	Destination MAC	MAC Address	ietf-idr-flowspec-l2vpn
33	DSAP in LLC	1 octet	ietf-idr-flowspec-l2vpn
34	SSAP in LLC	1 octet	ietf-idr-flowspec-l2vpn
35	Control filed in LLC	1 octet	ietf-idr-flowspec-l2vpn
36	SNAP	5 octet	ietf-idr-flowspec-l2vpn
37	VLAN ID	1 or 2 bytes	ietf-idr-flowspec-l2vpn
38	VLAN COS	3 bit COS	ietf-idr-flowspec-l2vpn
39	Inner VLAN ID	1 or 2 bytes	ietf-idr-flowspec-l2vpn
40	Inner VLAN COS	1 or 2 bytes	ietf-idr-flowspec-l2vpn
41	Interface (Group ID, intf id)	TBD	not specified
42	Time		
65	FCFS matches		non-standard actions

Figure 9

4.3. Default Flow Specification Action Precedence and Incompatiabilites

Some BGP Flow Specification actions can conflict with other BGP Flow specification Actions. Table 7 in figure 10 shows the default precedence order and the potential conflicting actions. Existing

actions with conflicts denote the default action taken on conflicting actions.

Each flow specification that specifies a BGP action must create a "BGP Flow Specification Action Conflicts" section within the flow specification. In this section, the flow specification must point to this document indicating the precedence between actions, and indicate how the action handles the conflict. All Standards actions have precedence overall FCFS actions incoded in BGP Extended Communities.

R-Policy bit - Additional BGP Version 2 Flow specification has additional filters and policy in BGP Attribute X.

TP-Mod bit - make modifications to packet before sending to the IP-VPN via a tunnel,

R-Intf bit - process restrict to interface sets

Two bits are added to the Extended Traffic Action Flag so that the total flags are:

R - Additional Policy in a BGP Flow Specification version 2 NLRI, BGP attribute (or BGP wide communities).

Table 7 - Action Precedence and Conflicts between Actions

order	Action	Possible Conflicting Actions
FA7 1	Alternate NLRI Validation (mask for support of RFC5755, ROA and bgpsec-protocol AS path) and L2MAC NRLI for IP Address	none
2	Traffic Rate(0x8006) in bytes	Traffic rate in packets (FA1) Default Conflict action: Allow traffic monitoring by bytes and packets, but process byte rate limit checks first
3	Traffic Rate (FA1) in packets	traffic rate in bytes (0x8006) Default Conflict action: same as in Traffic Rate action conflict

4	Traffic Action (0x8007)	Extended Traffic action with "R-Policy" bit(FA2), "TN-P" bit, R-intf bit Default conflict action: Process Traffic Action, then Extended traffic action
5	Extended Traffic Action (FA2)	Traffic Action (0x8007) "R" bit(FA2), "TN-P" bit (above) R-Intf bit Default conflict action: Process Traffic action, then extended traffic action
6	Redirect to IP-VPN 0x8008: 2 byte AS RD 0x8108: 4 byte IP RD 0x8208: 4 byte AS RD	Redirect to IP Tunnel (FA3) VLAN-action (FA4), TPID-action (FA5) Label-action (FA6) interface set (FA7) Default Conflict action: Process forward to IP-VPN first and ignore other conflicting actions unless TN-Mod bit set in Extended action. If TN-Mod set then process the conflict actions which change the packet prior to forwarding the packet via tunnel to IP-VPN. If I bit set, process interface restriction’s narraowing of scope to certain interfaces before processing other options, and process interface restrictions implied in outboudn direction before sending packet. outbound policy before any other If "R" bit set use version 2 of BGP Flow Specification handling
7	Redirect to IP Tunnel (FA3)	Redirect to IP VPN (0x8008, 0x8108, 0x8208) VLAN-action (FA4), TPID-action (FA5),

			Label action (FA6),
			interface set (FA7)
			Default Conflict actions:
			Refer to processing in redirect
			IP-VPN tunnel
8	VLAN action (FM4)		Redirect to IP-VPN (0x8008,
			0x8108, 0x8208),
			Redirect to tunnel (FA3),
			VLAN-action (FA4),
			TPID-action (FA5),
			Label action (FA6),
			interface set (FA7)
			Default Conflict actions:
			Refer to processing in redirect
			IP-VPN tunnel
9	TPID action (FM5)		Redirect to IP-VPN (0x8008,
			0x8108, 0x8208),
			Redirect to tunnel (FA3),
			VLAN-action (FA4),
			TPID-action (FA5),
			Label action (FA6),
			interface set (FA7)
			Default Conflict actions:
			Refer to processing in redirect
			IP-VPN tunnel
10	Label Action (FM6)		Redirect to IP-VPN (0x8008,
			0x8108, 0x8208),
			Redirect to tunnel (FA3),
			VLAN-action (FA4),
			TPID-action (FA5),
			Label action (FA6),
			interface set (FA7)
			Default Conflict actions:
			Refer to processing in redirect
			IP-VPN tunnel
11	interface Set (FM8a)		Redirect to IP-VPN (0x8008,
			0x8108, 0x8208),
			Redirect to tunnel (FA3),
			VLAN-action (FA4),
			TPID-action (FA5),

			Label action (FA6),
			Default Conflict actions:
			Refer to processing in redirect
			IP-VPN tunnel
12	Filter precedence (FM8b) [proposed]		reorder default filter precedence 0 = BGP Flow-Spec only 1 = ACL + BGP Flow-Spec 2 = I2RS FB-RIB + BGP FS 3 = ACL + I2RS FB-FIB + BGP FS 4 = Config FB-RIB + BGP FS 5 = ACL + config FB-RIB + BGP FS 6 = Config FB-RIB + I2RS FB-RIB + BGP FS 7 = ACL + config FB-FIB + I2RS
13-63			Reserved for other standards actions
65+	FCFS actions		FCFS Actions

Figure 9

4.4. FCFS Flow Specification Match Condition Filter Interaction

[RFC5575] allowed for non-IETF standardized Flow Specification filters and extended community actions. The beginning order of precedence for non-IETF standardized FCFS BGP Flow specification match filters is 65. The network management yang modules SHOULD store the BGP Flow Specification match type byte for both IETF Standardized BGP Flow Specification Match Filters, FCFS BGP BGP Flow Specification Match filters.

4.5. FCFS Extended Communities with BGP Flow Specification Actions

[RFC7153]allows for FCFS (First Come First Serve) allocation of BGP transitive types. If an action is specified in the FCFS registry, the default precedence is after all standardized BGP Flow Specification actions(action 65+). The BGP Flow Specification Yang models should store the Extended Community value for the FCFS based Flow Specification action. If the precedence ordering has been changed by the FCFS, this should be stored in the configuration of BGP Flow Specification and in the operational state.

4.6. Ordering Filters and Actions

There are the following ways to get ordered filters and actions:

- add an attribute with ordered match filters and ordered actions as [I-D.li-idr-flowspec-rpd],
- Add an NLRI with filters and ordered actions,
- add an NLRI with ordered filters and use Wide Communities [I-D.ietf-idr-wide-bgp-communities] to get ordered actions

4.6.1. Additions to Attribute approach

To get ordered an ordered match field in [I-D.li-idr-flowspec-rpd] the following additions would need to be made for the match field format:

- Match order field

match type [bit 1 - deny/permit]
0-permit, 1 -deny

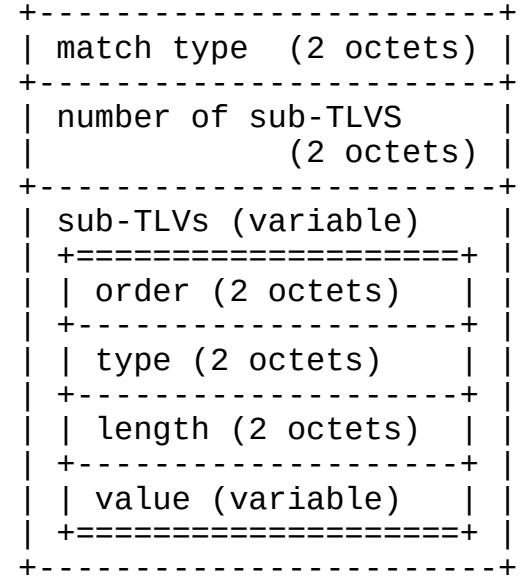


figure 10 - match field revision

The action field would be expanded to include an action order field (2 octets) as follows:

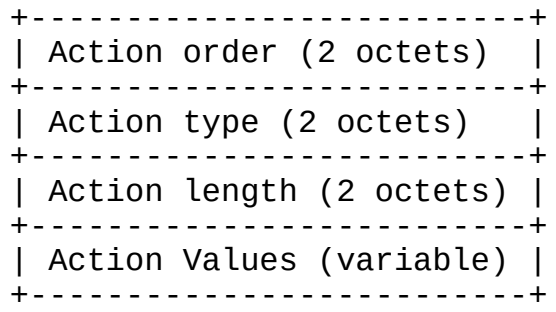


figure 11 - Action field revision

4.6.2. NLRI and Wide Community

The new BGP NLRI would have the following format to order filters:

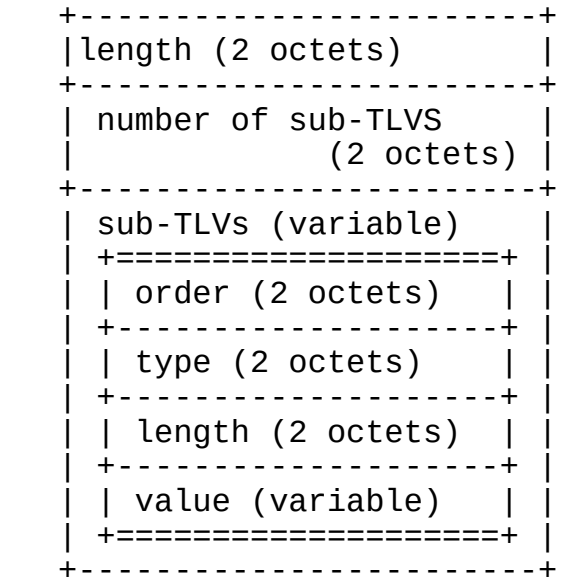
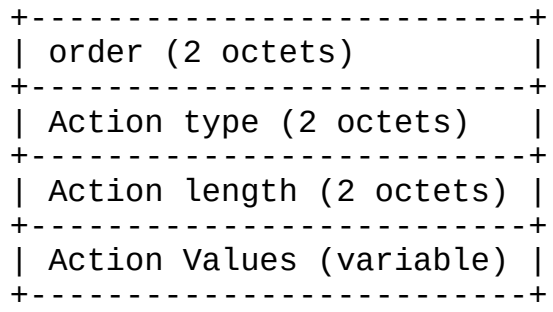


Figure 12 - NRLI revision

The BGP Wide community would need to have an atom (TBD) that indicates BGP Flow Specification actions. The atom would have the following information within it:



Wide Community Atom
figure 13

5. Precedence among Routing Functions

5.1. Precedence ordering Multiple Routing Filtering policy

This precedence for flow policy amoung routing functions SHOULD go from the most dynamic overwriting the the least dynamic. The order from dynamic to least is:

1. BGP Session flow specification ephemeral state with action based ephemeral state that specified interactions according to interface specification (FA8a and FA8b) from [I-D.litkowski-idr-flowspec-interfaceset],

2. BGP Flow specification Session ephemeral state,

3. I2RS reboot ephemeral state,

4. Filter-Based RIB (aka Policy RIB configuration State) (hares-rtgwg-fb-rib-data-model),

5. ACL configuration state [I-D.ietf-netmod-acl-model],

6. routing-config configuration state [I-D.ietf-netmod-routing-cfg],

7. interface addresses [RFC7223].

The filtering process for a packet received should attempt to match the more dynamic policy prior to matching a less dynamic policy.

This standardized order may be modified by local configuration policy on Flow Specification filtering precedence, but if it does the BGP FlowSpecification Yang Model show indicate the current precedence.

5.2. Precedence for re-ordering Match Policy

Actions that change interact between levels of policy need to be defined in terms of policy actions in BGP Flow Specification. For example [I-D.litkowski-idr-flowspec-interfaceset] provides a definition of the following combination of filter rules between ACLs and BGP flow Specifications:

1. Forward if both ACL forward and BGP Flow Specification Forward

2. Drop if either ACL drops or BGP Flow Specification drops.

6. Flow Specification Version 2 - to be or not to be

Pro - for version 2

The current version 1 of the Flow Specification does not have ordering of packet ECA policy rules, flow specification filters, or flow specification actions other than the default precedence. Current implementations of BGP flow specification are finding this lack of ordering to cause operational difficulties.

Con - for version 2

Version 2 must be coded. It can either be a BGP attribute with the policy rules (NLRI filters and actions) inside such as described in [I-D.li-idr-flowspec-rpd] or it can be a combination of a new BGP Flow Specification version 2 NLRI + Wide Community actions (with ordering).

(Additional comments will be added here)

7. Flow Specification Yang models

The Flow Specification Yang models are expressing the same policy as the Filter-Based RIB Yang modules for I2RS and configuration. Aligning these three yang data models should improve the management of the different levels of filter-based forwarding (BGP Session ephemeral, I2RS reboot ephemeral, config filter-based forwarding).

This section compares BGP Flow Specification yang model in [I-D.wu-idr-flowspec-yang-cfg] and the I2RS FB-RIB data model is described in [I-D.hares-i2rs-fb-rib-data-model] which uses the packet reception ECA policy data model found in [I-D.hares-i2rs-pkt-eca-data-model]. A comparison of the policy structures is given in table 8, and the operation status model is given in table 9.

The packet reception ECA policy data model is also used to describe configured packet reception filter RIBs which (aka Policy Routing) described in (draft-hares-rtgwg-fb-rib-00.txt).

Table 8 - comparison of Yang Data models

component	BGP Flow Spec Yang	I2RS FB-RIB + Packet-ECA Yang
Policy	flowspec-policy*	group* [group-name]
+-name	[policy-name]	
+-vrf	+-rw vrf-name	+-rw vrf-name
+-AFI	+-rw address-family	+-rw address-famil
+-rules	+-rw flowspec-rule*	+-rw group-rule-list
	[rule-name]	[rule-name]
+-rule-name	+-rw rule-name	+-rw rule-name
+-rule-order	+-rw traffic-filters	+-rw rule-order
	+-rw traffic-actions	+-rw eca-rules
		[order-id rule-name]
		+-rw installer
		+-rw eca-matches
		+-rw eca-qos-actions
		+-rw eca-fwd-actions

figure 14 - Comparison of Yang modules (Config state)

Note:The Yang "traffic-filters" found are the same as eca-matches found in [I-D.wu-idr-flowspec-yang-cfg] are the same filters found in [I-D.hares-i2rs-pkt-eca-data-model]. The "traffic actions" found in [I-D.wu-idr-flowspec-yang-cfg] can be broken into modify actions and forwarding actions as [I-D.hares-i2rs-pkt-eca-data-model] does.

Table 9 - comparison of Yang operational state

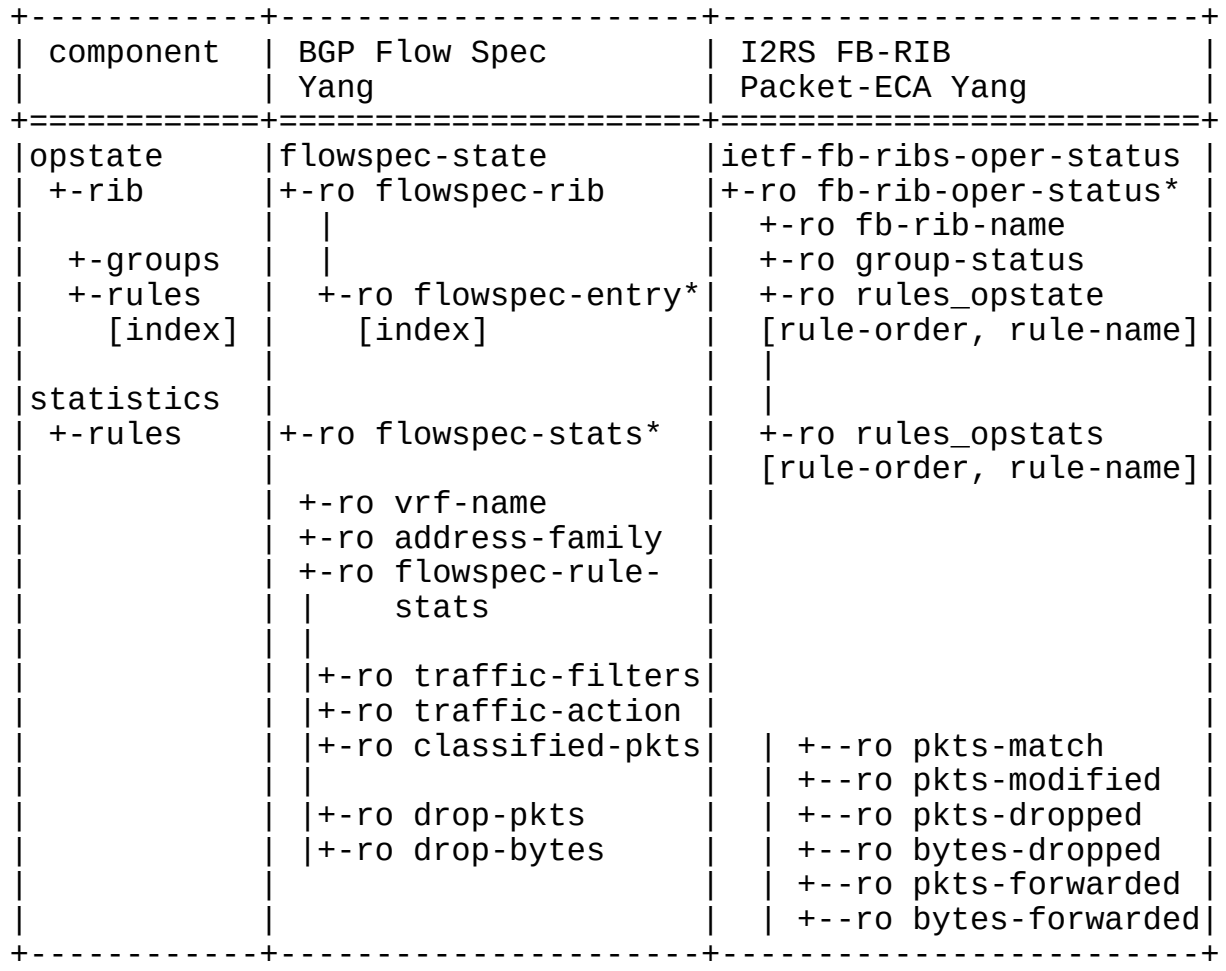


figure 15 - Comparison of Yang Models (Operation State)

8. IANA Considerations

This section complies with [RFC7153]

TBD. There are a lot of assignments which will be filled in after the initial review of the technology.

9. Security Considerations

The new BGP Validation described in section 4.1 with the ROA improves on [RFC5575] security by improving the validation of the originating AS having permissions to send Flow specifcation for a prefix. The validation of the path attributes and/or path requires the BGPSEC [I-D.ietf-sidr-bgpsec-protocol]. [I-D.eddy-idr-flowspec-exp] contains suggestions on how to implement this with flow specification, but at this time the authors consider the technology

described in [I-D.eddy-idr-flowspec-exp] so this draft does not suggest mandating it. However, it encourages the develop of such work that pairs BGP Flow Specification with BGPSEC protocol. When this work matures, this specification or BGP Flow Specification version 2 should implement it.

10. References

10.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <http://www.rfc-editor.org/info/rfc4271>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <http://www.rfc-editor.org/info/rfc4360>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <http://www.rfc-editor.org/info/rfc4760>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <http://www.rfc-editor.org/info/rfc5575>.

[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, <http://www.rfc-editor.org/info/rfc6241>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <http://www.rfc-editor.org/info/rfc6482>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <http://www.rfc-editor.org/info/rfc6483>.

[RFC7153] Rosen, E. and Y. Rekhter, "IANA Registries for BGP Extended Communities", RFC 7153, DOI 10.17487/RFC7153, March 2014, <http://www.rfc-editor.org/info/rfc7153>.

[RFC7223] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 7223, DOI 10.17487/RFC7223, May 2014, <http://www.rfc-editor.org/info/rfc7223>.

[RFC7674] Haas, J., Ed., "Clarification of the Flowspec Redirect Extended Community", RFC 7674, DOI 10.17487/RFC7674, October 2015, <http://www.rfc-editor.org/info/rfc7674>.

10.2. Informative References

[I-D.eddy-idr-flowspec-exp]
Eddy, W., Dailey, J., and G. Clark, "Experimental BGP Flow Specification Extensions", draft-eddy-idr-flowspec-exp-00 (work in progress), August 2015.

[I-D.eddy-idr-flowspec-packet-rate]
Eddy, W., Dailey, J., and G. Clark, "BGP Flow Specification Packet-Rate Action", draft-eddy-idr-flowspec-packet-rate-00 (work in progress), November 2015.

[I-D.hao-idr-flowspec-nvo3]
Weiguo, H., Zhuang, S., Li, Z., and R. Gu, "Dissemination of Flow Specification Rules for NVO3", draft-hao-idr-flowspec-nvo3-03 (work in progress), December 2015.

[I-D.hao-idr-flowspec-redirect-tunnel]
Weiguo, H., Li, Z., and L. Yong, "BGP Flow-Spec Redirect to Tunnel action", draft-hao-idr-flowspec-redirect-tunnel-00 (work in progress), October 2015.

[I-D.hares-i2rs-fb-rib-data-model]
Hares, S., Kini, S., Dunbar, L., Ghanwani, A., Krishnan, R., Bogdanovic, D., Tantsura, J., and R. White, "Filter-Based RIB Data Model", draft-hares-i2rs-fb-rib-data-model-01 (work in progress), January 2016.

[I-D.hares-i2rs-pkt-eca-data-model]
Hares, S., Wu, Q., and R. White, "Filter-Based Packet Forwarding ECA Policy", draft-hares-i2rs-pkt-eca-data-model-00 (work in progress), January 2016.

[I-D.ietf-i2rs-architecture]
Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", draft-ietf-i2rs-architecture-12 (work in progress), December 2015.

[I-D.ietf-i2rs-ephemeral-state]
Haas, J. and S. Hares, "I2RS Ephemeral State Requirements", draft-ietf-i2rs-ephemeral-state-02 (work in progress), September 2015.

[I-D.ietf-idr-flow-spec-v6]
Raszuk, R., Pithawala, B., McPherson, D., and A. Andy, "Dissemination of Flow Specification Rules for IPv6", draft-ietf-idr-flow-spec-v6-06 (work in progress), November 2014.

[I-D.ietf-idr-flowspec-l2vpn]
Weiguo, H., Litkowski, S., and S. Zhuang, "Dissemination of Flow Specification Rules for L2 VPN", draft-ietf-idr-flowspec-l2vpn-03 (work in progress), November 2015.

[I-D.ietf-idr-wide-bgp-communities]
Raszuk, R., Haas, J., Lange, A., Amante, S., Decraene, B., Jakma, P., and R. Steenbergen, "Wide BGP Communities Attribute", draft-ietf-idr-wide-bgp-communities-01 (work in progress), November 2015.

[I-D.ietf-netconf-restconf]
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-09 (work in progress), December 2015.

[I-D.ietf-netmod-acl-model]
Bogdanovic, D., Koushik, K., Huang, L., and D. Blair, "Network Access Control List (ACL) YANG Data Model", draft-ietf-netmod-acl-model-06 (work in progress), December 2015.

[I-D.ietf-netmod-opstate-reqs]
Watsen, K. and T. Nadeau, "Terminology and Requirements for Enhanced Handling of Operational State", draft-ietf-netmod-opstate-reqs-04 (work in progress), January 2016.

[I-D.ietf-netmod-routing-cfg]
Lhotka, L. and A. Lindem, "A YANG Data Model for Routing Management", draft-ietf-netmod-routing-cfg-20 (work in progress), October 2015.

[I-D.ietf-sidr-bgpsec-protocol]
Lepinski, M., "BGPsec Protocol Specification", draft-ietf-sidr-bgpsec-protocol-14 (work in progress), December 2015.

[I-D.kini-i2rs-fb-rib-info-model]
Kini, S., Hares, S., Dunbar, L., Ghanwani, A., Krishnan, R., Bogdanovic, D., Tantsura, J., and R. White, "Filter-Based RIB Information Model", draft-kini-i2rs-fb-rib-info-model-02 (work in progress), October 2015.

[I-D.li-idr-flowspec-rpd]
Li, Z., Ou, L., Luo, Y., Lu, S., Zhuang, S., and N. Wu, "BGP FlowSpec Extensions for Routing Policy Distribution (RPD)", draft-li-idr-flowspec-rpd-01 (work in progress), October 2015.

[I-D.liang-idr-bgp-flowspec-label]
You, J., Raszuk, R., and d. danma@cisco.com, "Carrying Label Information for BGP FlowSpec", draft-liang-idr-bgp-flowspec-label-01 (work in progress), September 2015.

[I-D.liang-idr-bgp-flowspec-time]
You, J. and S. Zhuang, "BGP FlowSpec with Time Constraints", draft-liang-idr-bgp-flowspec-time-00 (work in progress), October 2015.

[I-D.litkowski-idr-flowspec-interfaceset]
Litkowski, S., Simpson, A., Patel, K., and J. Haas, "Applying BGP flowspec rules on a specific interface set", draft-litkowski-idr-flowspec-interfaceset-03 (work in progress), December 2015.

[I-D.rosen-idr-tunnel-encaps]
Rosen, E., Patel, K., and G. Velde, "Using the BGP Tunnel Encapsulation Attribute without the BGP Encapsulation SAFI", draft-rosen-idr-tunnel-encaps-03 (work in progress), August 2015.

[I-D.vandevelde-idr-flowspec-path-redirect]
Velde, G., Henderickx, W., and K. Patel, "Flowspec Indirection-id Redirect", draft-vandevelde-idr-flowspec-path-redirect-01 (work in progress), January 2016.

[I-D.wu-idr-flowspec-yang-cfg]
Wu, N., Zhuang, S., and A. Choudhary, "A YANG Data Model for Flow Specification", draft-wu-idr-flowspec-yang-cfg-02 (work in progress), October 2015.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

Author's Address

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com