draft-litkowski-idr-flowspec-interfaceset
IETF 90 - Toronto

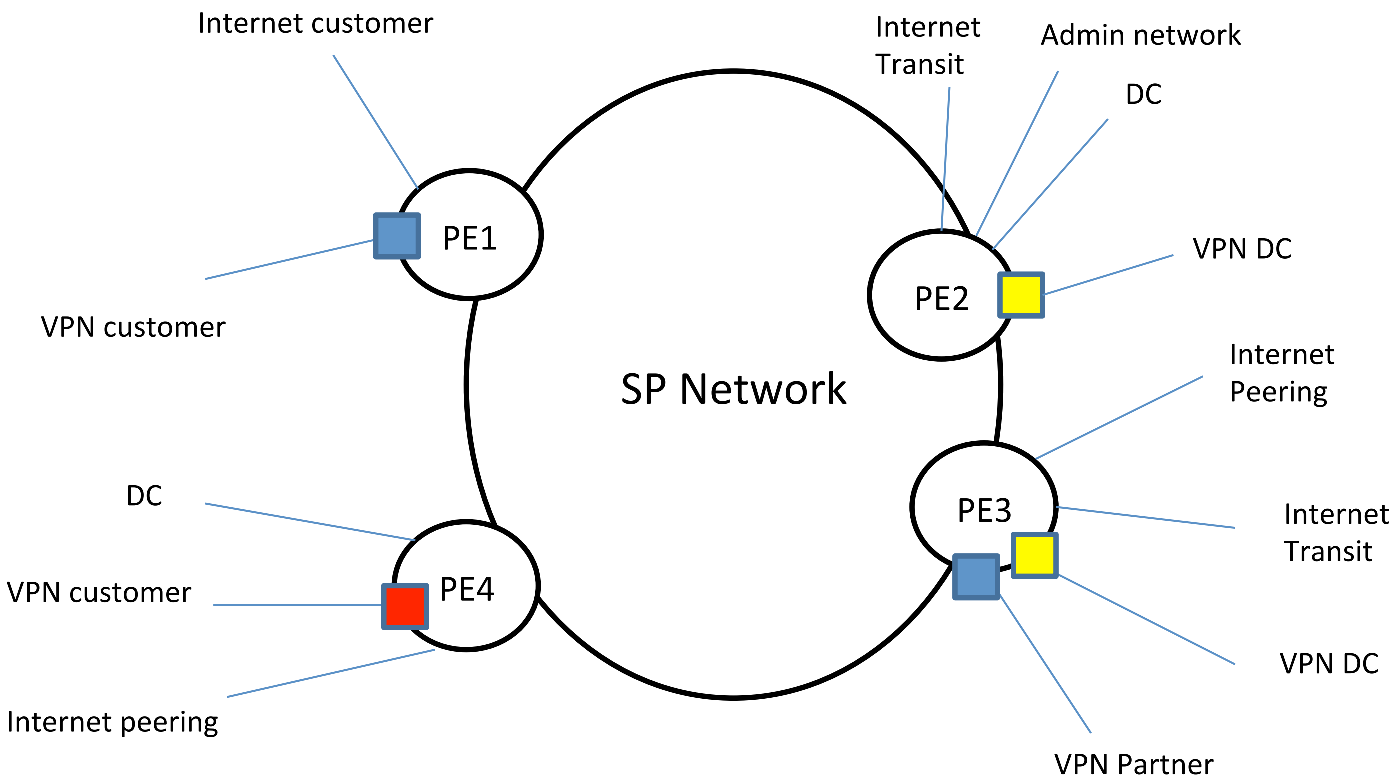
S. Litkowski, Orange

A. Simpson, ALU

K. Patel, Cisco

J. Haas, Juniper

Problem statement



Multiple outside connections in the network

How to deploy specific Flowspec rules on a specific set of interfaces ?

Use cases

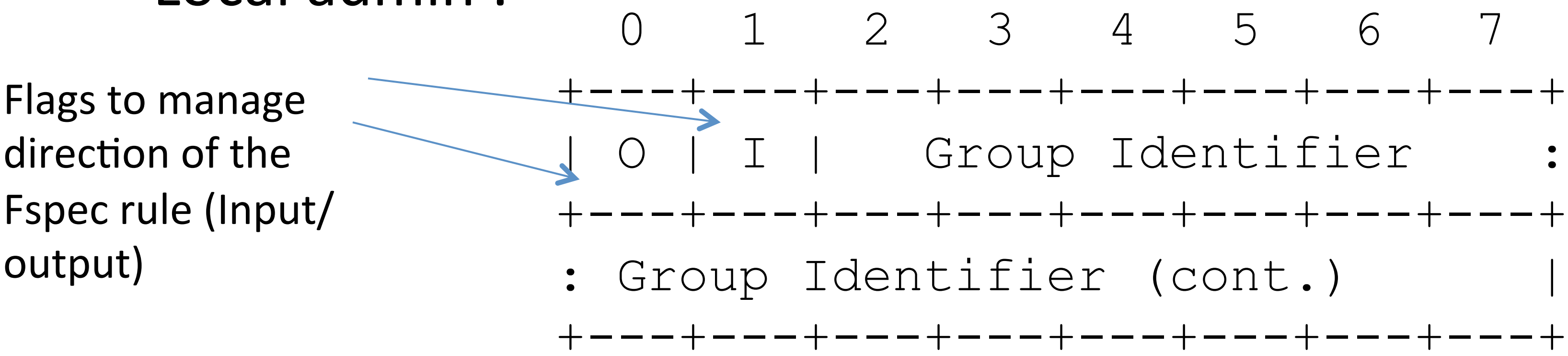
- Specific filtering for DDoS prevention :
  - Maintain rate-limiting rules (NTP, DNS …) on ISP connections based on interface BW

- Infrastructure ACL management
  - Complete management of infra ACL : all the ACL is maintained through a list of Fspec rules. Each interface type has its own Fspec rule set.

  - Quick update of CLI based ACLs (security alert …)

interface-set extended community

- Transitive 4-B AS-specific extended community
  - Global admin : ASN of the originating router
  - Local admin :

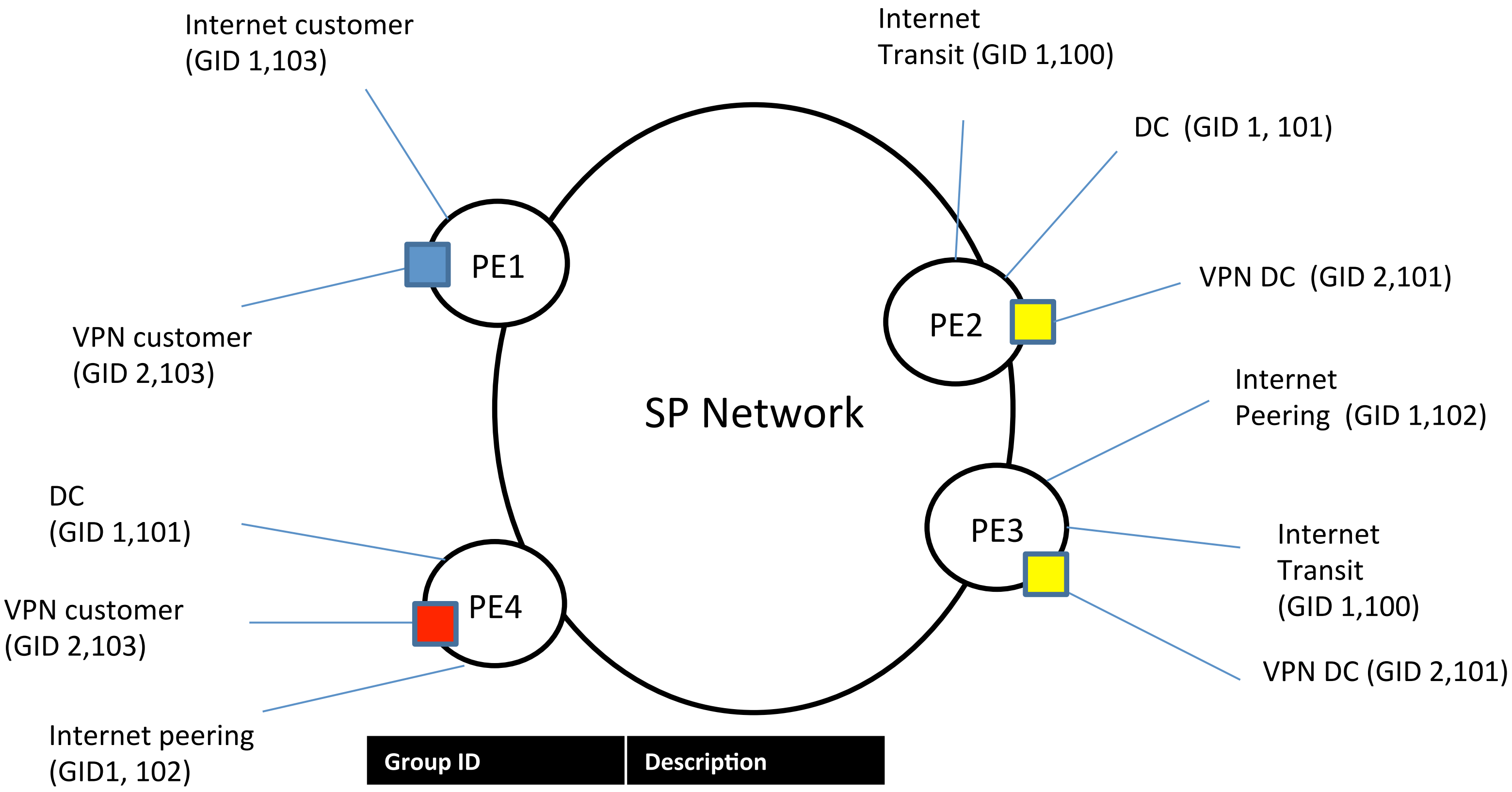


Flags to manage direction of the Fspec rule (Input/ output)

```
   0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| O | I |   Group Identifier    :
+---+---+---+---+---+---+---+---+
: Group Identifier (cont.)      |
+---+---+---+---+---+---+---+---+
```

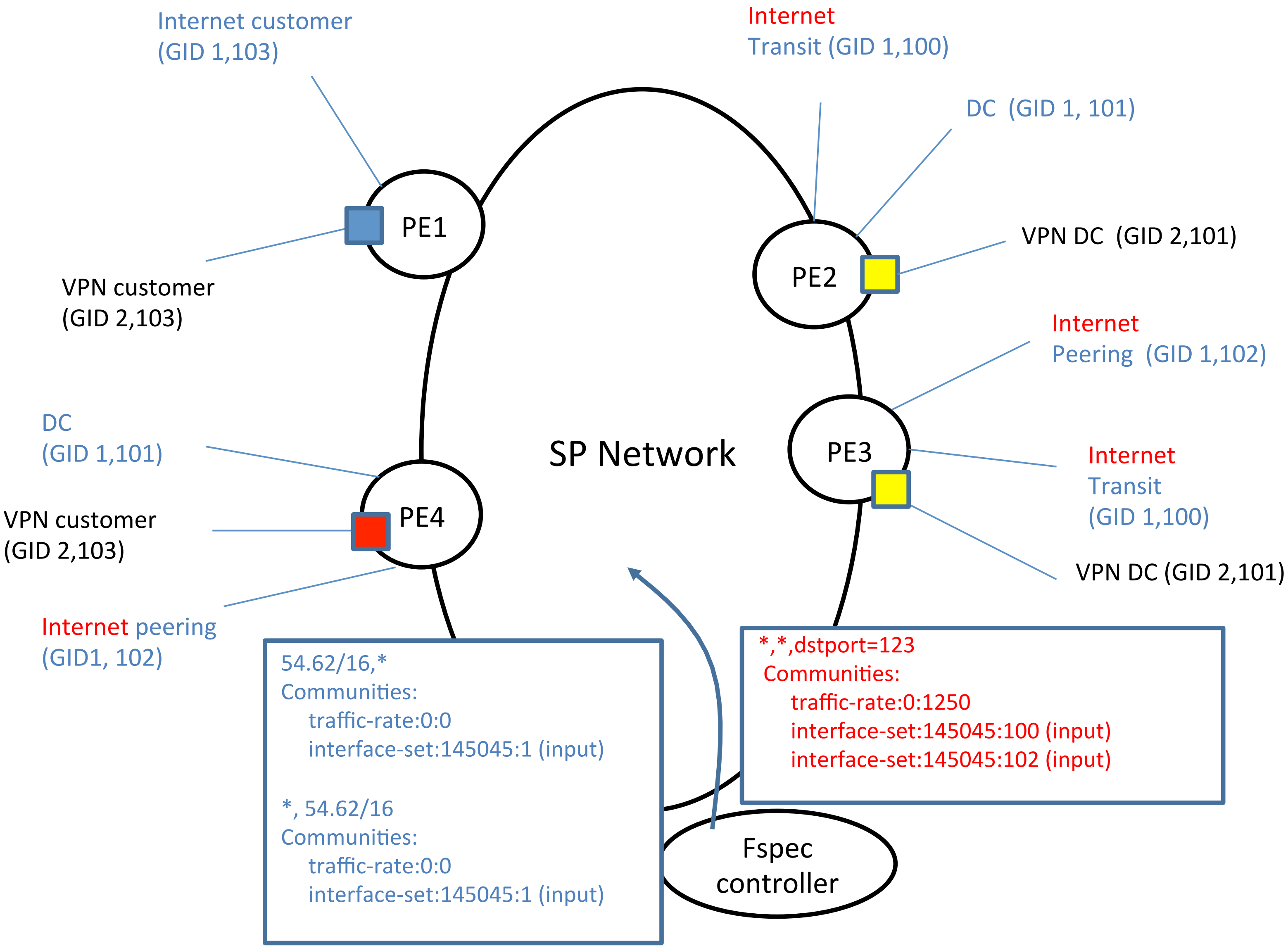
- Multiple interface-set on the same Fspec NLRI means « match-any »

Example



Group ID	Description
1	Internet connection
2	VPN connection
100	Transit connection
101	DC connection
102	Peering connection
103	Customer

Example



Internet customer
(GID 1,103)

VPN customer
(GID 2,103)

PE1

Internet
Transit (GID 1,100)

DC (GID 1, 101)

VPN DC (GID 2,101)

PE2

Internet
Peering (GID 1,102)

PE3

Internet
Transit
(GID 1,100)

VPN DC (GID 2,101)

SP Network

DC
(GID 1,101)

VPN customer
(GID 2,103)

PE4

Internet peering
(GID1, 102)

54.62/16,*
Communities:
traffic-rate:0:0
interface-set:145045:1 (input)

*, 54.62/16
Communities:
traffic-rate:0:0
interface-set:145045:1 (input)

,,dstport=123
Communities:
traffic-rate:0:1250
interface-set:145045:100 (input)
interface-set:145045:102 (input)

Fspec
controller

Security considerations

- Managing infra ACLs using Fspec may be dangerous as Filters are ephemeral (linked to life of the BGP path)

- An attacker may break Fspec BGP session and open all the network doors (probability low …)

- LLGR for FSpec AFI/SAFIs would help to make filters more persistent

Discussions outcomes

- Some text to fix :
  - Community format error handling (both flags set to 0)
  - Logical operation to clarify when having multiple interface-set for a single NLRI
- Encoding :
  - Using wide-communities would help (more flexibility in encoding and group logic)
  - Using wide-community is a good idea but would slow down availability of the use case (wide-comm specification is not yet finalized)
  - Authors would prefer to use existing communities for now. Wide communities could be used in addition when available to bring more flexibility.

Discussions outcomes

- Define assigned interface-sets ??
  - – Idea is that system automatically binds some group ID to an interface

Registry Name: Assigned Flow spec interface-set

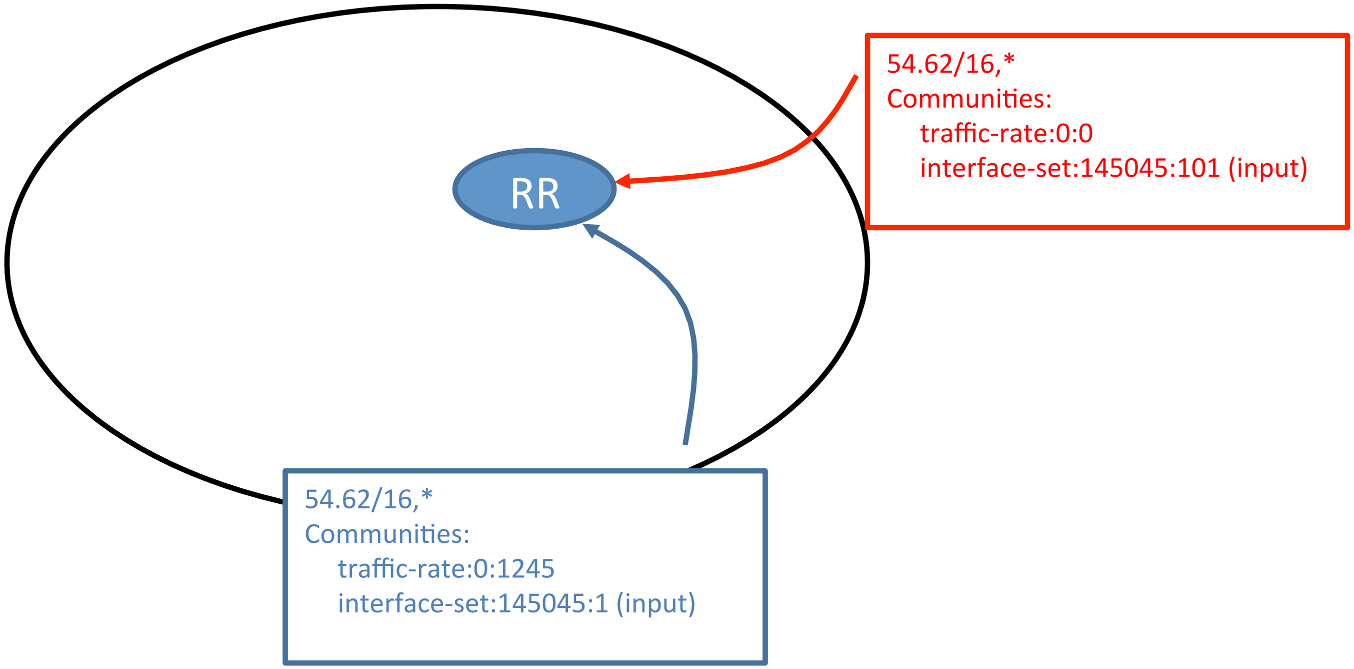
Range	Registration Procedures
0x0000-3EFF	Reserved for private use.
0x3F00-3FFF	Standards Action/Early IANA Allocation.

The IANA is requested to update the registry "Assigned Flow spec interface-set" as follows:

0x3F00:	IGP interface
0x3F01:	non IGP interface
0x3F02:	eBGP interface
0x3F03:	non eBGP interface
0x3F04:	VRF interface
0x3F05:	non VRF interface

Issue to solve

- What about multi-originator scenario ?
  - The issue is not linked to interface-set
  - Already present with basic RFC5575

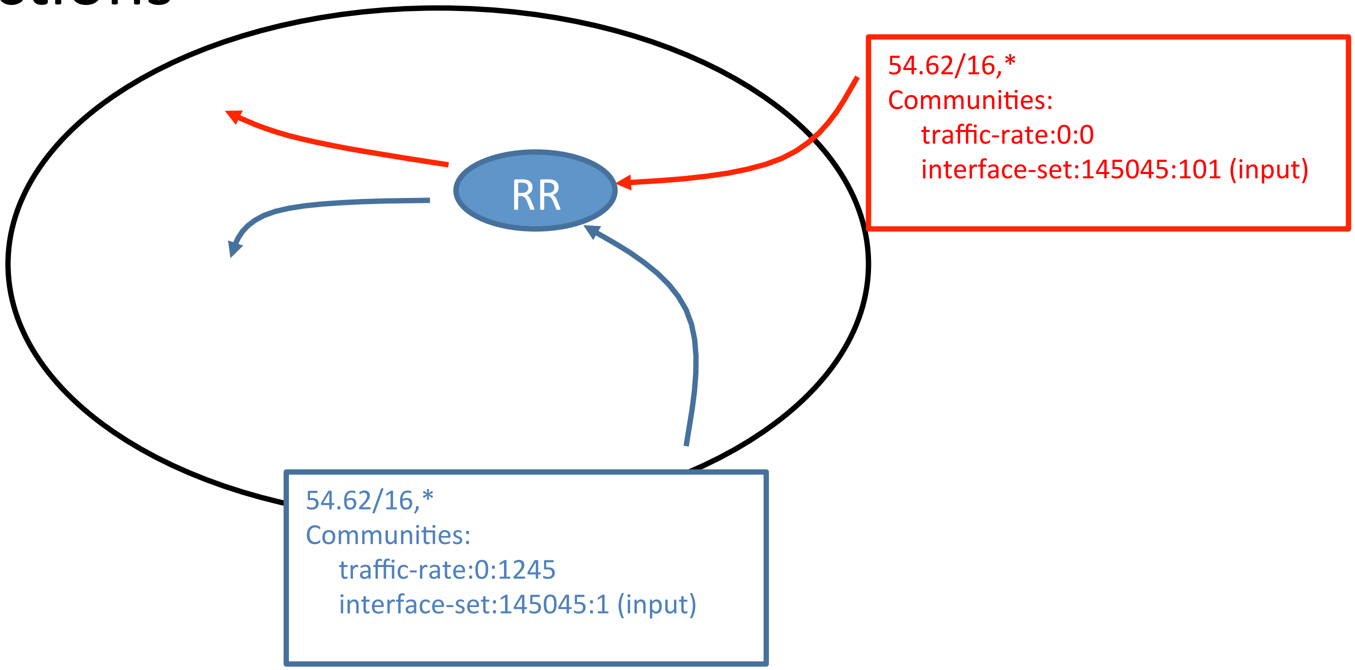


54.62/16,*
Communities:
traffic-rate:0:0
interface-set:145045:101 (input)

54.62/16,*
Communities:
traffic-rate:0:1245
interface-set:145045:1 (input)

Issue to solve

- Multi-originator issue could be partially solved using ADD-PATH
  - But there is still a need to handle conflicting actions



54.62/16,*
Communities:
traffic-rate:0:0
interface-set:145045:101 (input)

54.62/16,*
Communities:
traffic-rate:0:1245
interface-set:145045:1 (input)

Next steps …

- Requires feedback from WG
- Address comments from the list in next version