Revised Validation Procedure for BGP flow specifications

(draft-djsmith-bgp-flowspec-oid-00.txt)

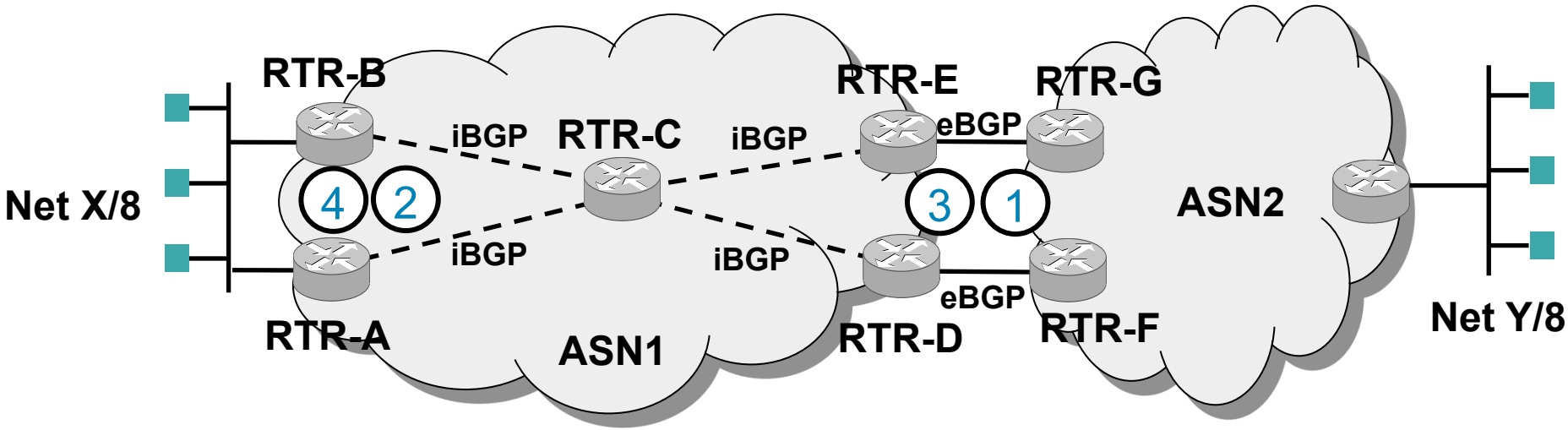
IETF 83 IDR WG – Paris – March 26, 2012

Clarence Filsfils
Pradosh Mohapatra
David Smith
Cisco

James Uttaro
AT&T

BGP Flowspec (RFC5575)

1. Downstream border routers advertise path reachability to Net Y/8
2. Upstream border routers install paths via RTR-G and RTR-F to Net Y/8



3. Downstream border routers advertise flowspec for specific traffic flows toward Net Y/8
4. Upstream border routers install flowspec if considered feasible

BGP Flowspec Validation Procedure

- Per RFC 5575……

  A flow specification NLRI must be validated such that it is considered feasible if and only if:

  a) The originator of the flow specification matches the originator of the best-match unicast route for the destination prefix embedded in the flow specification.

  b) There are no more specific unicast routes, 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).

- Step (a) only allows BGP speakers within the data forwarding path (such as autonomous system border routers) to originate BGP flow specifications.

Proposed Changes to BGP Flowspec Validation Procedure

- Make step (a) of the validation procedure specified in RFC 5575, section 6 OPTIONAL for IBGP learned flow specification NLRIs.
- This OPTIONAL behavior MAY be configurable on BGP speakers, however, it SHOULD be disabled by default for IBGP learned flow specification NRLIs.
- This is necessary given the BGP route controller is originating the flow specification not reflecting it, and to avoid the complexity of having to determine the egress border router whose path was chosen as the best in each of the ingress border routers.

Benefits

- Enables flow specifications to be originated from a centralized BGP route controller.
- Allows flow specifications to be distributed in a standard & scalable manner throughout an autonomous system.
- Greatly simplifies distribution of intra-domain traffic filtering policies in an autonomous system with a large number of border routers having complex BGP policies.
- Facilitates rapid response to security attacks in a scalable intra-domain manner.

Conclusion

- No new security issues or risks
- No actions for IANA
- Comments are welcome
- We would like this draft to be a WG document