Anti-spoofing beyond the local link - possible enhancement to RPF?

Jun Bi
Tsinghua Univ./CERNET
IETF 82 SAVI Meeting at Taipei
2011.11.15

Content

- **Introduction**
- Intra-AS scenario
- Inter-AS scenario
- Discussion on possible enhancements

Introduction(1)

- It is just to trigger the discussion at IETF82, not make decision. Deeper discussion will be continued at IETF83
- This PPT tries to analyze in inter-AS and intra-AS scenarios
  - From the viewpoint of deplorers (enterprise net owner vs. ISP)
  - Intra-AS has one administrator to control
    - Intra-AS here means “inside a campus network or enterprise network”
    - When local link SAVI can not be 100% deployed at all local links, shall we deploy sth at IGP router or layer 3 switches
    - feasible to be fixed with a global view of paths in an AS
  - Inter-AS (the whole Internet level) is tougher
    - No single administration, asymmetric flows are more common, harder to have global view of paths in the whole Internet
- Fred Baker prefers to analyzing by different routing algorithm types (Link-state and Distance vector)
  - It is also reasonable. He will comment it later

Introduction (2)

- Currently SAVI prevents IP spoofing within the local link.
- Ingress filtering with RPF is the only practical solution for anti-spoofing beyond local link
- RPF [bcp84] has five modes
  - Ingress Access Lists: to manually filter
  - Strict RPF: using FIB entry+ reverse direction to filter
  - Feasible RPF: using RIB entry+ reverse direction to filter
  - Loose RPF: using FIB entry to filter (lost direction info)
  - Loose RPF ignoring default route: using FIB entry (without default entry) to filter (lost direction info and default info.)

Introduction (3)

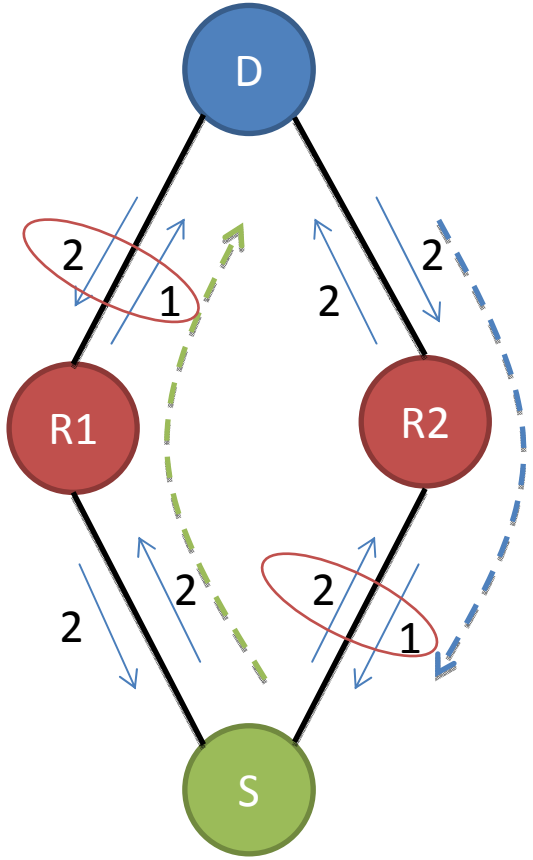
- RPF works well in most cases
- RPF still has problems in some situations
  - False positive (FP) in some asymmetric routing cases
    - Inter-AS: asymmetric flows are common
    - Intra-AS: better, but sometimes still has asymmetric flows
  - False negative (FN)
    - If deployment ratio is low, then FN for spoofing flows at the same direction
    - Loose mode only check prefixes existence, high FN
- How to make RPF work better?
  - Practice guidelines
  - Enhancing routing algorithms
  - Routing protocol revision or other methods

Content

- Introduction
- **Intra-AS scenario**
- Inter-AS scenario
- Discussion on possible enhancements

Intra-AS Scenario (1)

- Asymmetric link cost
  - For a link-state routing protocol, a link may have different costs in different directions (e.g. for TE)
  - Dijkstra algorithm is a greedy algorithm that only fast compute the shortest path into RIB
  - Thus two routers S and D use different paths towards each other, which makes RPF with FP
- Possible enhancement
  - Enhancing SPF algorithm to calculate "reverse path tree" with all reverse paths into RIB



The cost of (S, R2) is evaluated differently by S and R2, so is (D, R1). S and D will choose different path towards each other, thus asymmetry.

Intra-AS Scenario (2)

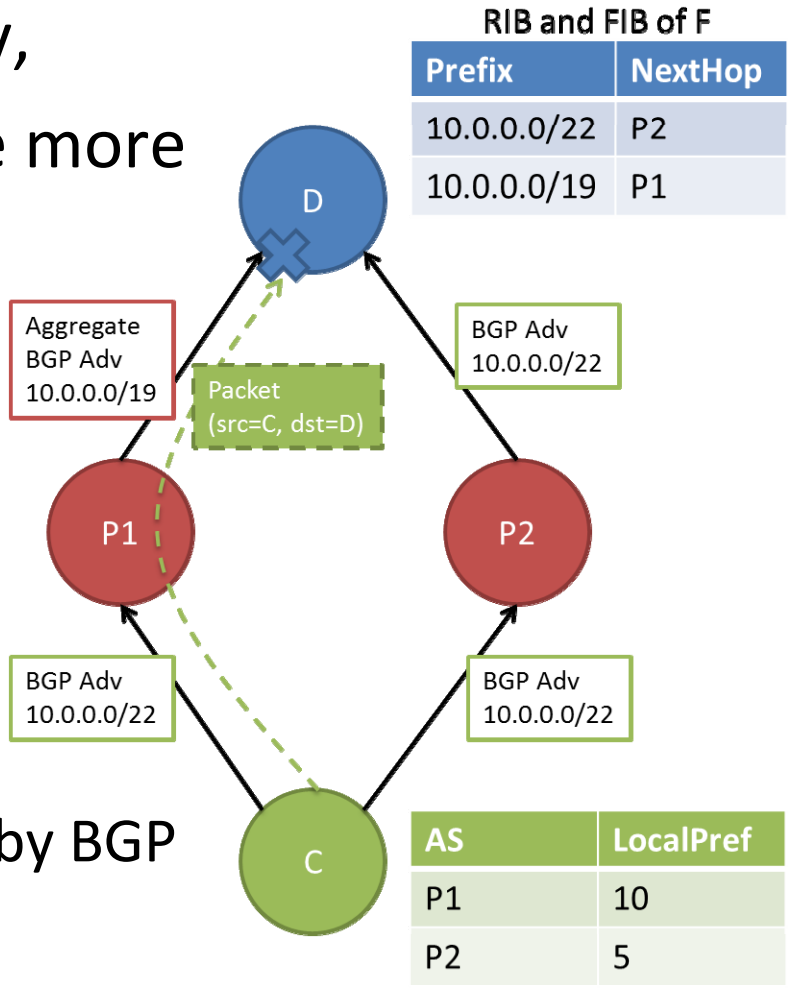
- ECMP
  - In some topology, it may have many ECMPs (e.g. 20). between S and D. All ECMPs may be used.
  - FIB entries of IGP router is limited (today most of IGP routers in campus/enterprise are layer 3 switches with limited hardware), usually only limited number (e.g. 8) of ECMPs entries are loaded into FIB.
  - S and D may respectively load different 8 ECMPs into FIB among all 20 ECMPs, generate asymmetric FIB, then FP
- IGP fast route
  - Commented by Joel Halpern, RPF may cause difficulties with IGP fast route

Content

- Introduction
- Intra-AS scenario
- **Inter-AS scenario**
- Discussion on possible enhancements

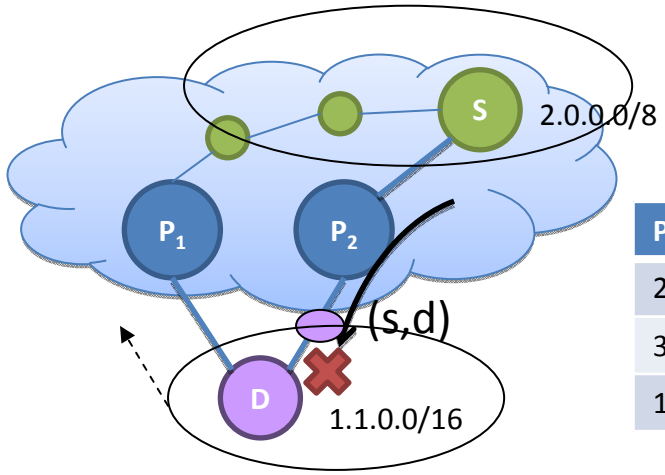
Inter-AS Scenario (1)

- Asymmetric Routing
  - – Due to complexity of BGP policy, hot potato…asymmetric flows are more common than intra-AS.
  - – E.g. Prefix Aggregation
    - C's prefix is aggregated by P1
    - Due to LPM, D chooses P2
    - C prefers P1 to P2
  - – Reason of FP
    - local preference is not announce by BGP
    - LPM at RPF implantation
    - More complicated cases to cause asymmetric flows



Inter-AS Scenario (2)

- Commented by Joel Halpern, hot-potato routing wherein each ISP chooses to hand off traffic to peers/transit/customers as quickly as possible makes more asymmetric traffic

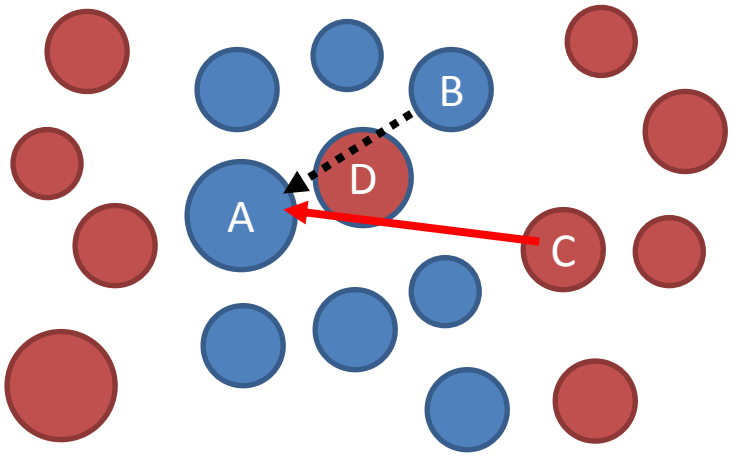


FIB of D

Prefix	Next Hop
2.0.0.0/8	P_1
3.0.0.0/8	P_2
1.1.0.0/16	Local

Inter-AS Scenario (3)

- Deployment Incentive
  - ASes are operated by different ISPs, who always want to maximize benefits with lowest deployment cost. So a method is incentive only when it can protect deployers.
  - It is also desirable for a method to protect deployer from being spoofed by others
  - A and B deloyed RPF, but B can still be spoofed by C to attack A (inter-AS is big, there are always lots of not deployed AS like D between deployed AS)



Content

- Introduction
- Intra-AS scenario
- Inter-AS scenario
- **Discussion on possible enhancements**

Discussion on Possible Solutions

- Intra-AS
  - Easier because the same administration, global view of path in an AS is possible
  - Possible enhancement
    - Guidelines on practical operations
    - Revise routing algorithms
    - Extend routing protocols
    - New approaches, like generate filtering entries in a central server

Discussion on Possible Solutions

- Inter-AS
  - Hope FP=0 with acceptable FN
  - Deployment Incentive in incomplete deployment environment is important for inter-AS case, because no central administration
    - Source Address Validation Alliance?
      - protect alliance members from beijing spoofed inside the alliance of ASes.

Thanks!