Source Prefix Advertisement for Intra-domain SAVNET

Presenter: Lancheng Qin

November 2024

Introduction

- draft-ietf-savnet-intra-domain-problem-statement summarizes the problems of existing intra-domain SAV solutions [BCP38, BCP84]
  - Ingress filtering [BCP38, RFC2827] has the problem of high operational overhead
  - uRPF-based SAV [BCP84, RFC3704] has the problem of inaccurate validation
    - Strict uRPF improperly blocks legitimate traffic in multi-homing and asymmetric routing scenario
    - Loose uRPF improperly permits spoofing traffic
- draft-ietf-savnet-intra-domain-architecture proposes the architecture of intra-domain SAVNET
  - SAV on host-facing routers, customer-facing routers, and AS border routers should be more effective and efficient
  - Automatically generate SAV rules by communicating SAV-specific information among routers
- Following the above two documents, this document proposes the Source Prefix Advertisement (SPA) solution for Intra-domain SAVNET, named SPA-based SAVNET

Terminology

- SAVNET Router: An intra-domain router that deploys SPA-based SAVNET
- Single-homed Stub Network: A stub network (e.g., a host network, a customer network, a stub OSPF area, or a stub AS) that is belonging to or connected to only one AS
- Multi-homed Stub Network: A stub network that is belonging to or connected to multiple ASes

Overview of SPA-based SAVNET

- SPA-based SAVNET requires SAVNET routers to signal SAV-specific information through SPA message communication
  - SAV-specific information contains the necessary information that improves the accuracy of SAV rules and cannot be learned from existing routing information
- SAVNET router can be an intra-domain router facing a stub network or facing an external AS
  - To achieve **the first Goal** in intra-domain PS document, SPA-based SAVNET generates an **allowlist** on interfaces facing a host network or a customer network
    - Allowlist contains source prefixes belonging to the corresponding network and blocks spoofing data packets from a host network or a customer network that use source addresses of other networks
  - To achieve **the second Goal** in intra-domain PS document, SPA-based SAVNET generates a **blocklist** on interfaces facing an external AS
    - The blocklist contains source prefixes only belonging to the local AS and blocks spoofing data packets from other ASes that use source addresses of the local AS

Source Prefix Advertisement Procedure

Source prefix advertisement procedure includes three main steps

- SPA Message Generation
  - ◆SAVNET routers facing a single-homed stub network (but there can be multiple links between the intra-domain network and the stub network) generate SPA messages
- SPA Message Communication
  - ◆SAVNET routers provide their SPA messages to other SAVNET routers
- SAV Rule Generation
  - ◆SAVNET routers generate allowlists or blocklists by using SPA messages

SPA Message Generation

- A SPA message contains two main types of information
  - Source Prefix: This information contains source addresses that can only be used by data packets received from the stub network
    - Source prefix can be learned from the router's local routes to its stub network, , i.e., the locally-known source prefixes of the stub network
    - Since the locally-known source prefixes of the stub network may only be a part of source prefixes of the stub network, **SAVNET routers facing the same stub network should exchange their locally-known source prefixes of the stub network**
  - Stub Network Identifier (SNI): For each source prefix contained in the SPA message, it is binded with a Stub Network Identifier. The SNI is used to identify which stub network owns the source prefix.
    - Prefixes belonging to the same stub network MUST have an identical and unique SNI value

SPA Message Communication

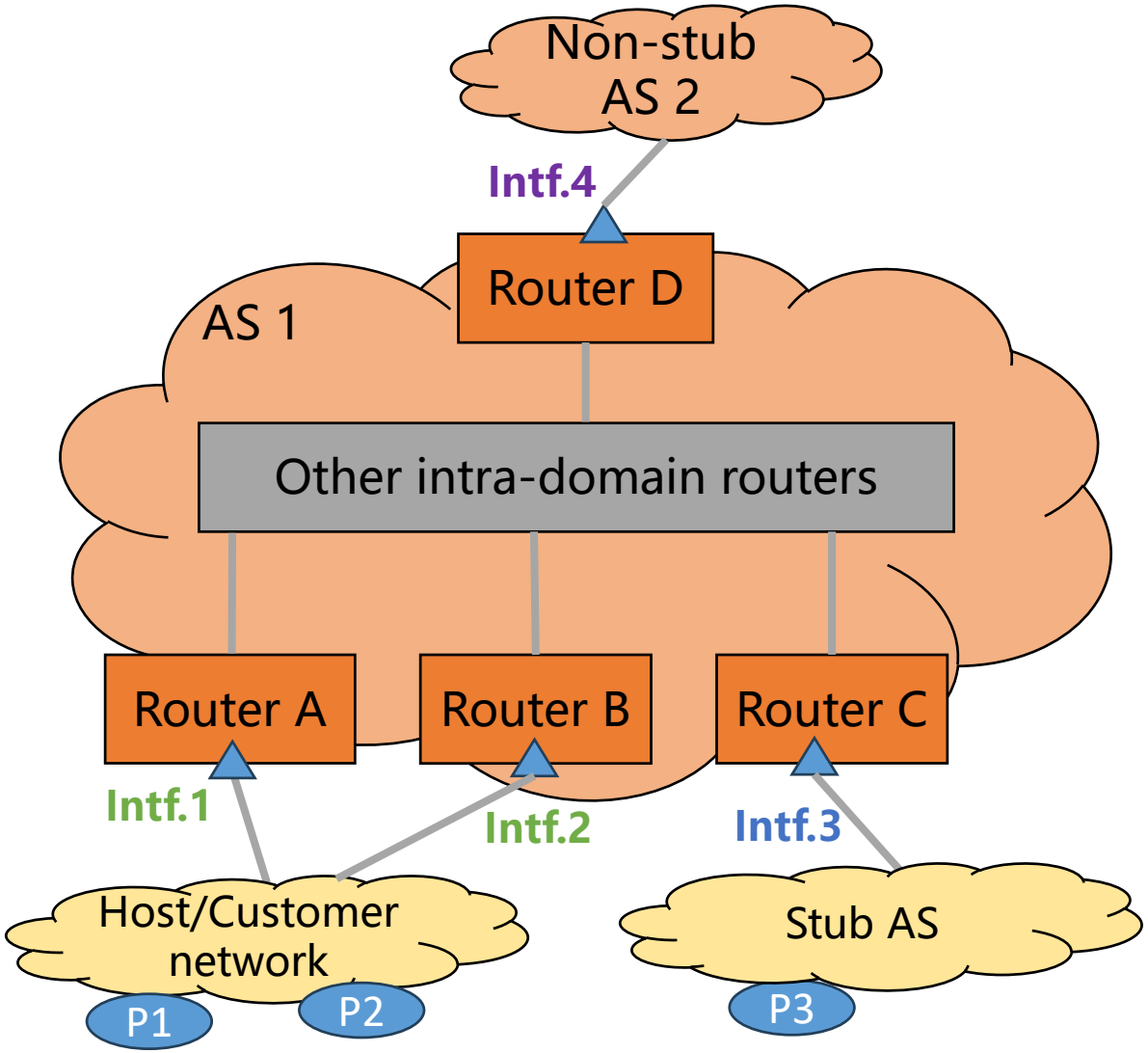
- After generating SPA messages, the SAVNET router will provide its SPA messages to other SAVNET routers in the same intra-domain network

- Implementation considerations
  - Since the SPA message contains source prefixes of a stub network, SPA message communication can be implemented by using existing intra-domain routing protocols (e.g., OSPF, IS-IS, iBGP)
  - When distributing the IP information of the stub network through the intra-domain routing protocol, the SAVNET router can bind the SNI with the IP information

SAV Rule Generation

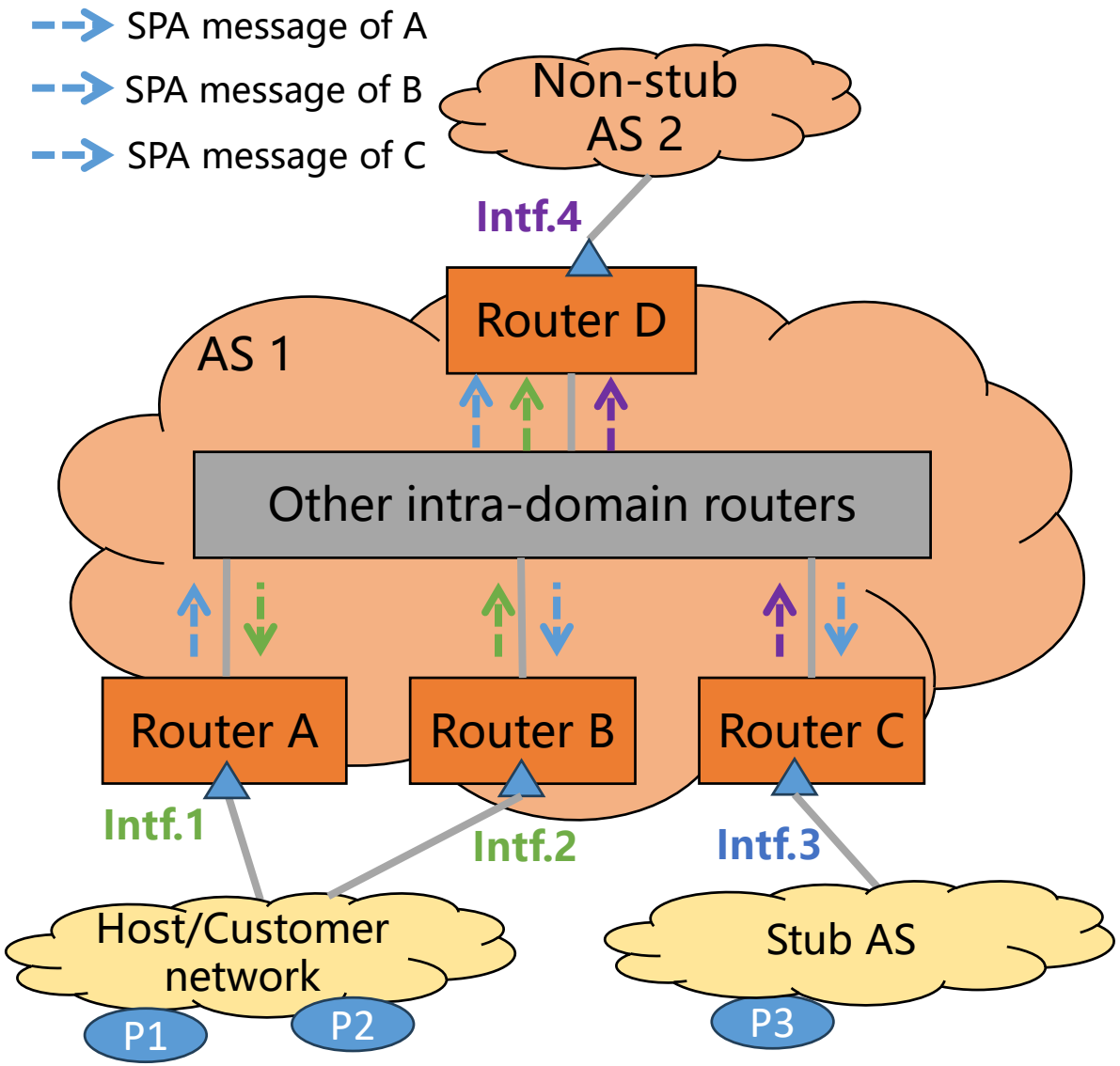
- After receiving SPA messages from other SAVNET routers, each SAVNET router will generate allowlists or blocklists on specific interfaces
  - Allowlist Generation: A SAVNET router **facing a single-homed stub network (e.g., a host network, a customer network, a stub OSPF area, or a stub AS)** can generate an allowlist on the corresponding interface. All source prefixes in SPA messages with the SNI of the stub network will be added into the allowlist
  - Blocklist Generation: The blocklist is recommended to be used on interfaces **facing an external AS or facing a multi-homed stub network.** All source prefixes in SPA messages will be added into the blocklist

The Most Recommended Use Case



- SPA-based SAVNET is highly recommended to be deployed at host-facing routers, customer-facing routers, and AS border routers
  - ◆Because these routers are closer to the source and thus will be more effective in identifying and discarding source-spoofed data packets
- Generate allowlists on interfaces facing a single-homed host network, customer network, or stub AS
- Generate blocklists on interfaces facing a non-stub AS

The Most Recommended Use Case



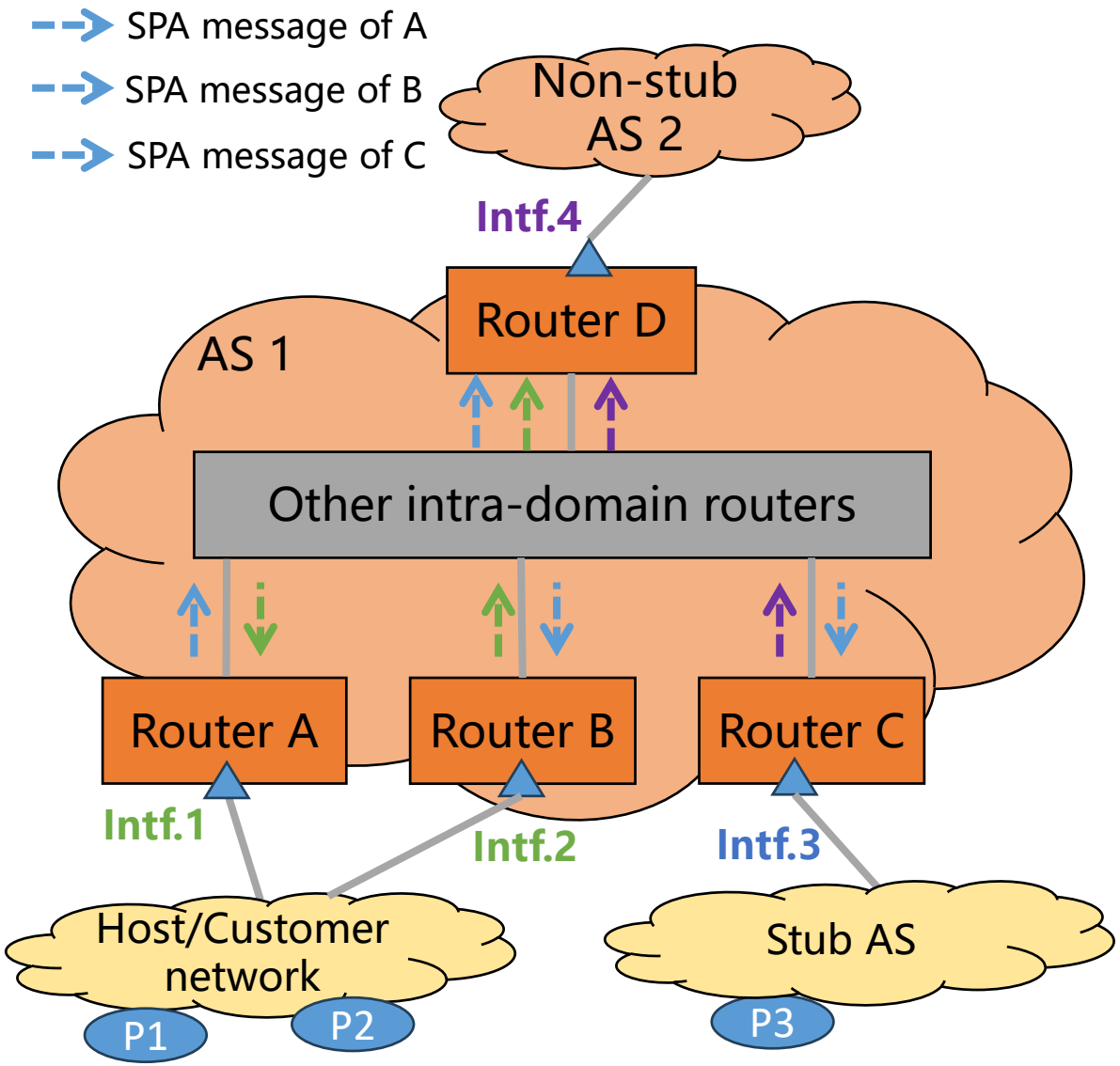
Scenario

- Router A only learns source prefix P1 from its local route to the host/customer network
- Router B only learns source prefix P2 from its local route to the host/customer network

SPA Procedure

- SPA message of Router A: [source prefix: P1, SNI: x]
- SPA message of Router B: [source prefix: P2, SNI: x]
- SPA message of Router C: [source prefix: P3, SNI: y]
- **Allowlist on Intf.1 and Intf.2: {P1, P2}**
- **Allowlist on Intf.3: {P3}**
- **Blocklist on Intf.4: {P1, P2, P3}**

Compare SPA-based SAVNET with uRPF



Scenario

- Router A only learns source prefix P1 from its local route to the host/customer network
- Router B only learns source prefix P2 from its local route to the host/customer network

SAV Results

- If apply strict uRPF on Routers A and B
  - **Improper block** data packets from the host/customer network
- If apply loose uRPF on Router D
  - **Improper permit** spoofing data packets from the non-stub AS 2
- If apply SPA-based SAVNET on Routers A, B, and D
  - **Accurately block** spoofing data packets (meeting the two goals in page 4) with **no improper block**

An Alternative Use Case & Two Corner Use Cases

- Alternative Use Case
  - SPA-based SAVNET can also be used on Area Border Routers (ABR) in inter-area cases
  - Generate an allowlist on interfaces facing the stub OSPF area and thus only allow data packets using source addresses belonging to the stub OSPF area
- Corner Use Cases
  - Direct Server Return (DSR)
    - To avoid blocking DSR data packets, these specially used source addresses should be added into allowlists on interfaces facing a stub network where the content server locates
  - Multi-homed Stub Network
    - Generate a blocklist on interfaces facing a multi-homed stub network

Summary

- SPA-based SAVNET addresses the problems raised in the intra-domain problem statement draft and meets the design requirements under the intra-domain SAVNET architecture
  - SPA-based SAVNET automatically generates accurate prefix allowlist or blocklist on SAVNET routers by using SPA messages
- It is recommended to communicate SPA messages by using existing routing protocols
  - [draft-li-lsr-igp-based-intra-domain-savnet] implements SPA-based SAVNET by using OSPF and IS-IS
    - **(1) Use the existing Administrative Tag Sub-TLV or (2) extend a new Sub-TLV?**
  - [draft-geng-idr-bgp-savnet] implements SPA-based SAVNET by using iBGP

Next Step

- Collaboration is welcome!
- Your comments and suggestions are welcome

Thanks!

Considerations

- Convergence considerations
  - SAV-specific information SHOULD at least have a similar propagation speed as routing information
  - When designing SPA message communication methods, routing protocol-based methods should be preferred
- Deployment considerations
  - SPA-based SAVNET can support incremental deployment by providing incremental benefits
    - SAVNET routers facing the same multi-homed stub network are suggested to deploy SPA-based SAVNET simultaneously
- Security considerations
  - The security considerations described in [draft-ietf-savnet-intra-domain-problem-statement] and [draft-ietf-savnet-intra-domain-architecture] also applies to this document