Source Prefix Advertisement for Intra-domain SAVNET

Presenter: Lancheng Qin

November 2024

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

- Deployment Scope: **SAV at the edge**
  - SPA-based SAVNET is deployed on routers facing a stub network or an external AS
    - **Advantage #1**: These edge routers are **closer to the source/host** and thus will be **more effective in blocking source-spoofed data packets**
    - **Advantage #2**: Compared to SAV on inner routers, SAV on the edge should be **more feasible and easier to implement** because it would not be affected by FRR and other complex forwarding policies
    - **Advantage #3**: **Provide incremental benefits** when these edge routers incrementally deploy SPA-based SAVNET
  - If we already have SAV at the edge, SAV on inner routers will not be needed
- Generate prefix allowlists or prefix blocklists on specific router interfaces by using SAV-specific information
  - Allowlist defaults to blocking ANY but allows source prefixes in the allowlist
  - Blocklist defaults to allowing ANY but blocks source prefixes in the blocklist

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
    - In multi-homing and asymmetric routing scenario, **the locally-known source prefixes** 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): The SNI is used to identify which stub network owns the source prefix. For each source prefix contained in the SPA message, it is binded with an SNI value
    - Prefixes belonging to the same stub network MUST have an identical and unique SNI value

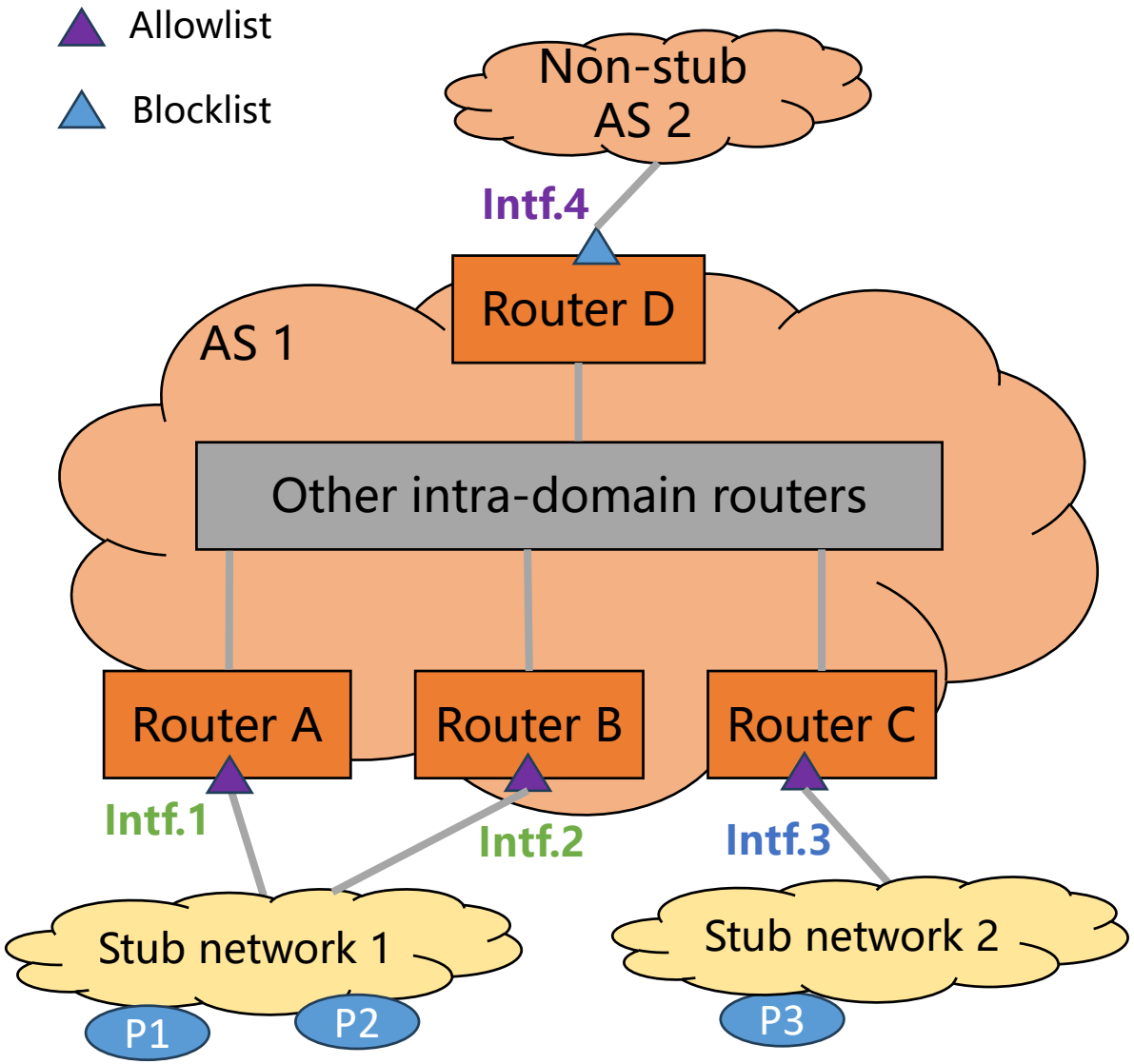
SPA Message Communication

- After generating SPA messages, the SAVNET router will provide its SPA messages to other SAVNET routers in the same intra-domain network
- It is recommended to communicate SPA messages using existing routing protocols
  - Carry the SNI value with IP information when distributing IP information
    - [draft-li-lsr-igp-based-intra-domain-savnet] implements SPA-based SAVNET by using OSPF and IS-IS
    - [draft-geng-idr-bgp-savnet] implements SPA-based SAVNET by using iBGP

SAV Rule Generation

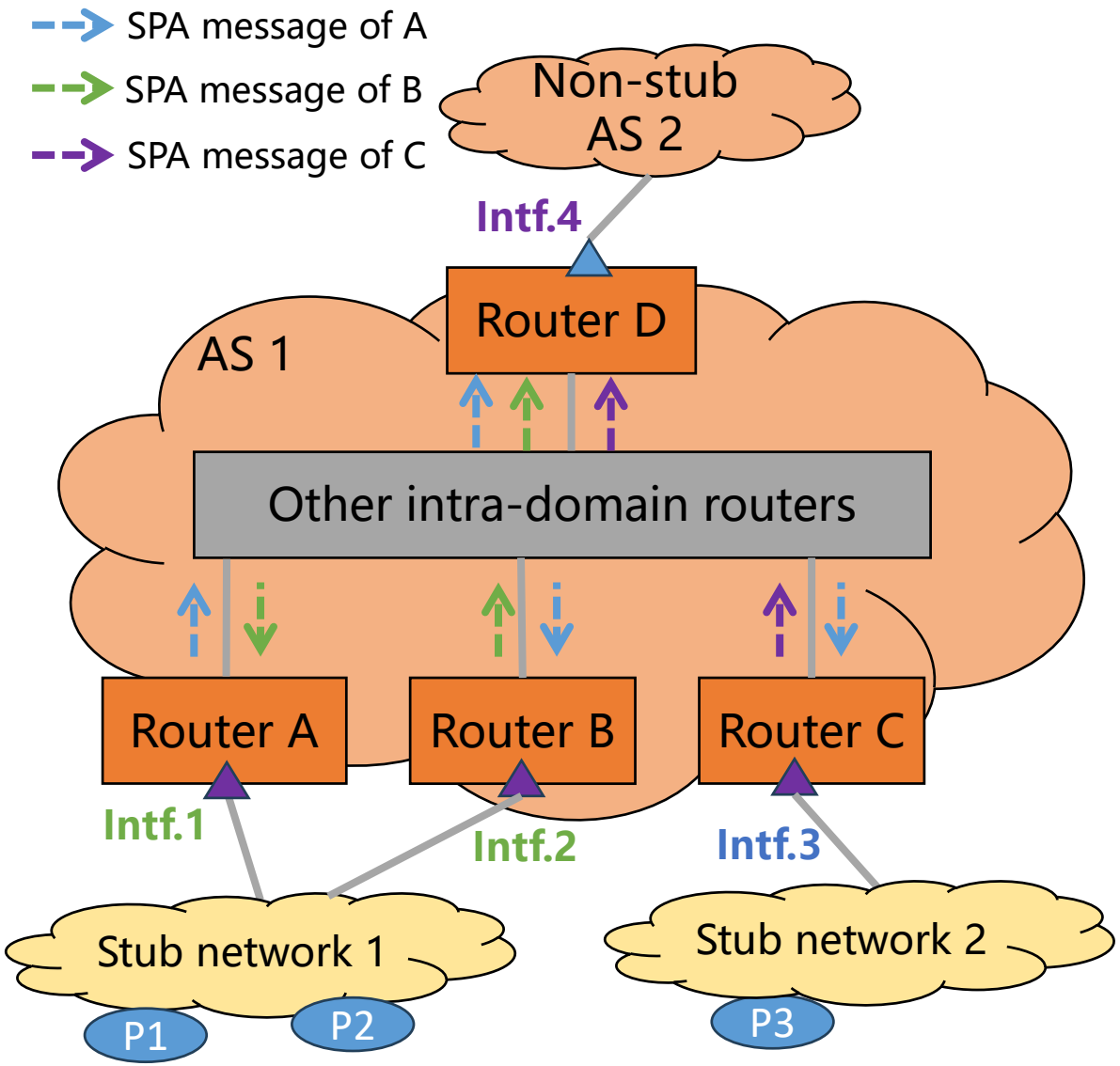
- After receiving SPA messages from other SAVNET routers, each SAVNET router will generate allowlists or blocklists on specific interfaces
  - Allowlist Generation: A SAVNET router **facing a single-homed stub network** can generate an allowlist on the interface by including all source prefixes in SPA messages with the SNI of its stub network
  - Blocklist Generation: A SAVNET router **facing an external AS or facing a multi-homed stub network** can generate a blocklist on the interface by including all source prefixes in SPA messages

The Most Recommended Use Case: SAV at the Edge



- SPA-based SAVNET on host-facing routers, customer-facing routers, and AS border routers
- 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: SAV at the Edge



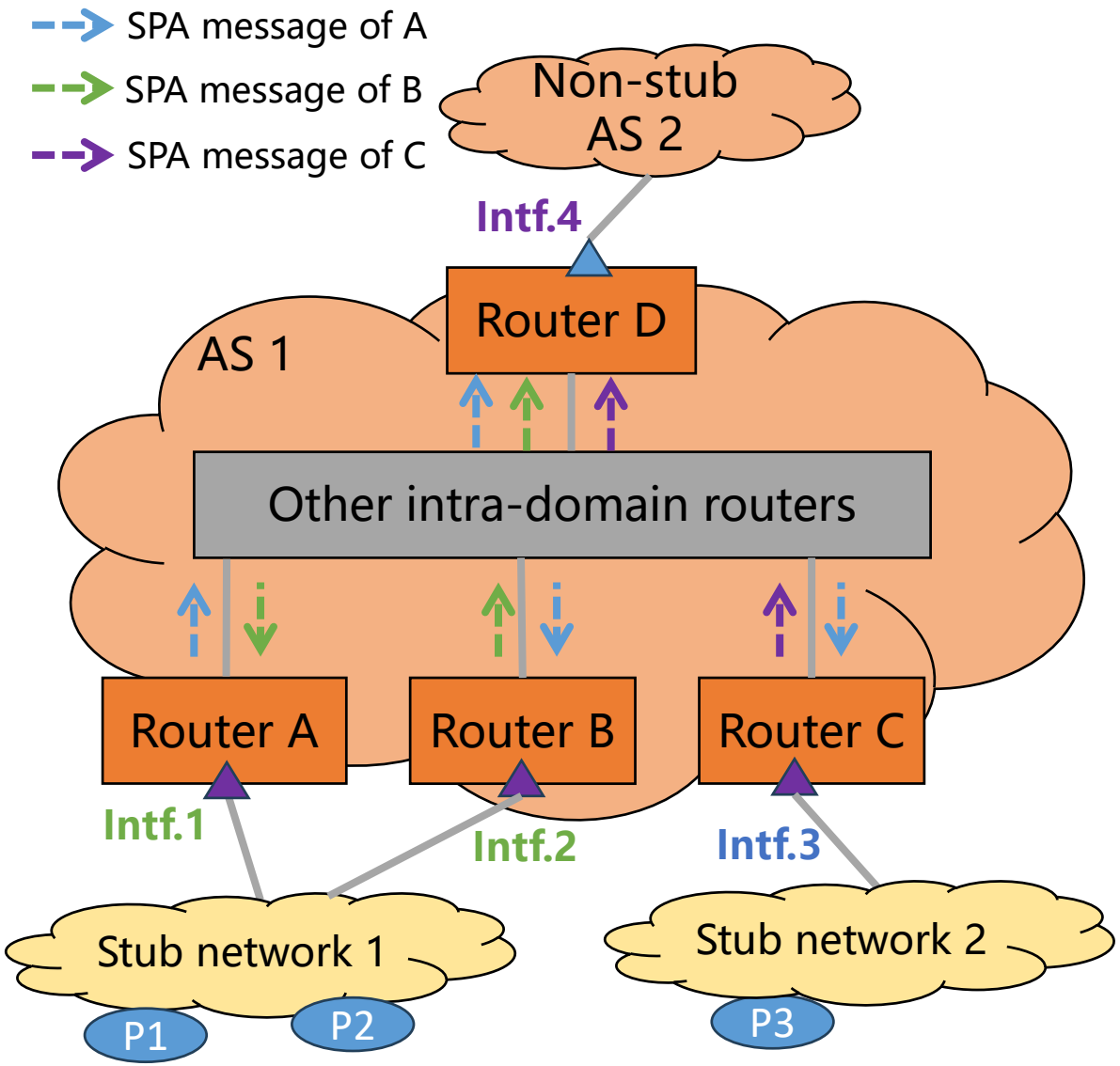
Asymmetric Routing Scenario

- Router A only learns source prefix P1 from its local route to stub network 1
- Router B only learns source prefix P2 from its local route to stub network 1

SPA Procedure

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

Compare SPA-based SAVNET with uRPF



Asymmetric Routing Scenario

- Router A only learns source prefix P1 from its local route to stub network 1
- Router B only learns source prefix P2 from its local route to stub network 1

SAV Results

- If use strict uRPF on Routers A and B
  - **Improper block**
- If use loose uRPF on Routers A, B, and D
  - **Improper permit**
- If use SPA-based SAVNET on Routers A, B, and D
  - **Accurately block** spoofing data packets (meeting the two goals of intra-domain SAV [1]) with **no improper block**

[1] draft-ietf-savnet-intra-domain-problem-statement

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**
  - Use the blocklist on interfaces facing a multi-homed stub network

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 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