Source Prefix Advertisement for Intra-domain SAVNET

Presenter: Lancheng Qin

November 2024

Overview of SPA-based SAVNET

- Deployment Scope: **SAV on routers facing an internal host network or external network/AS**
  - **Advantage #1**: These 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 these routers should be **more feasible and easier to implement** because it would not be affected by FRR and other complex forwarding policies in the intra-domain network
  - **Advantage #3**: **Provide incremental benefits** when these routers incrementally deploy SPA-based SAVNET
  - **Advantage #4**: If we already have SAV on these routers, SAV on inner routers would not be needed
- Generate prefix allowlists or prefix blocklists on specific router interfaces in an automatic way
  - Allowlist defaults to blocking ANY but allows source prefixes in the allowlist
  - Blocklist defaults to allowing ANY but blocks source prefixes in the blocklist

Two Goals of SPA-based SAVNET

- SAV on interfaces facing an internal host network
  - Block source-spoofed data packets from that network that use source IP addresses of other internal host networks or other external networks/ASes
  - Use an allowlist containing source prefixes of that internal host network
- SAV on interfaces facing an external network/AS
  - Block source-spoofed data packets from that network/AS that use source IP addresses of internal prefixes
  - Use a blocklist containing internal source prefixes

How to Generate Allowlist and Blocklist

Source prefix advertisement procedure includes three main steps

- SPA Message Generation
  - ◆SAVNET routers facing an internal host networks 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 from the host network
    - Source prefix can be learned from the router's local route to its host network, , i.e., the locally-known source prefixes of the host network
    - In some multi-homing and asymmetric routing scenario, the **locally-known source prefixes** may be **incomplete**, SAVNET routers facing the same host network should **exchange their locally-known source prefixes** to obtain complete source prefixes
  - Host Network Identifier (HNI): The HNI is used to identify which host network owns the source prefix. For each source prefix contained in the SPA message, it is binded with an HNI value
    - Prefixes belonging to the same host network MUST have an identical and unique HNI value

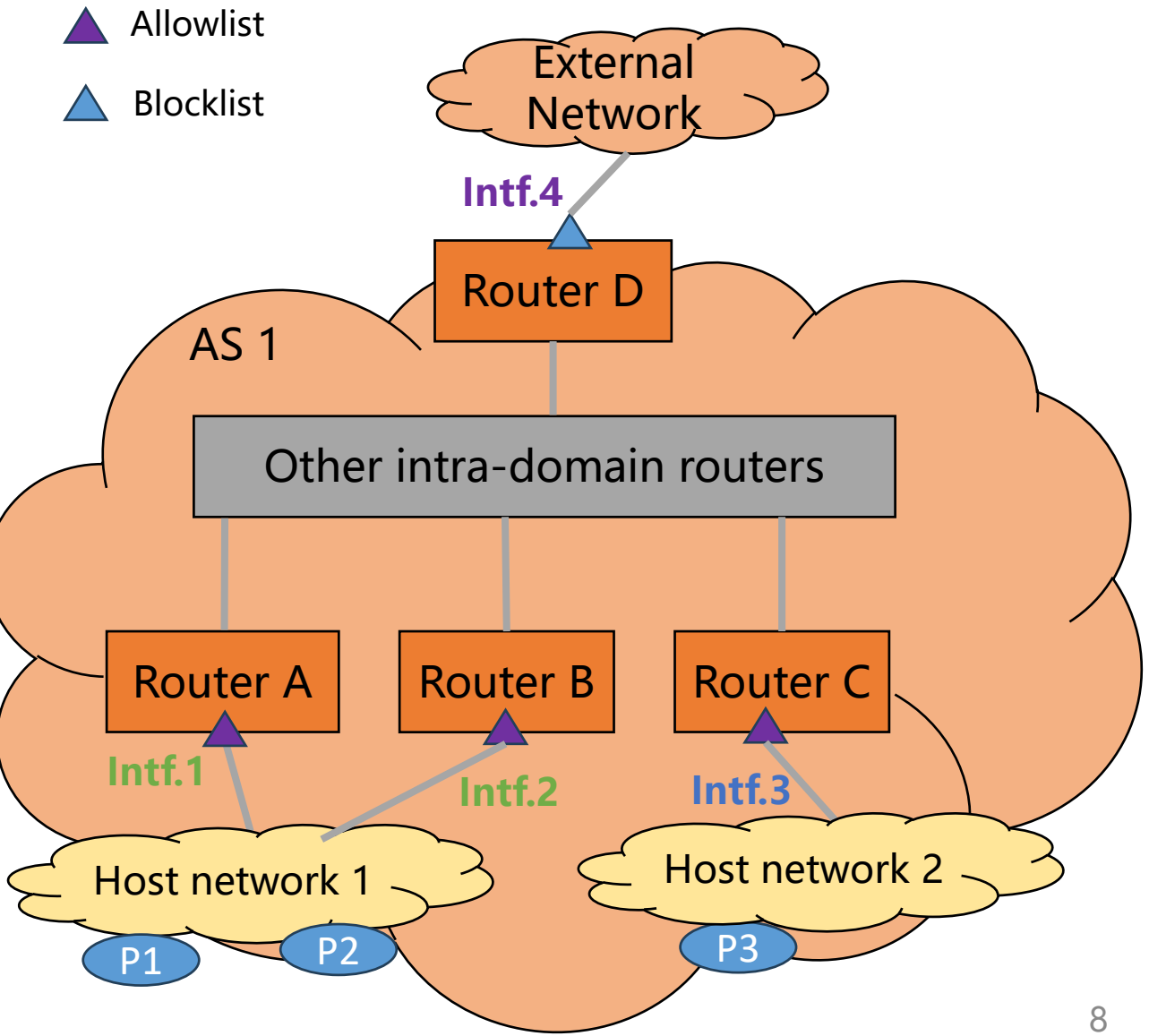
SPA Message Communication

- After generating SPA messages, SAVNET router will provide its SPA messages to other SAVNET routers in the same intra-domain network
  - This document introduces protocol-independent designs. How to signal SAV-specific information and how to transmit SPA messages are not in the scope.

SAV Rule Generation

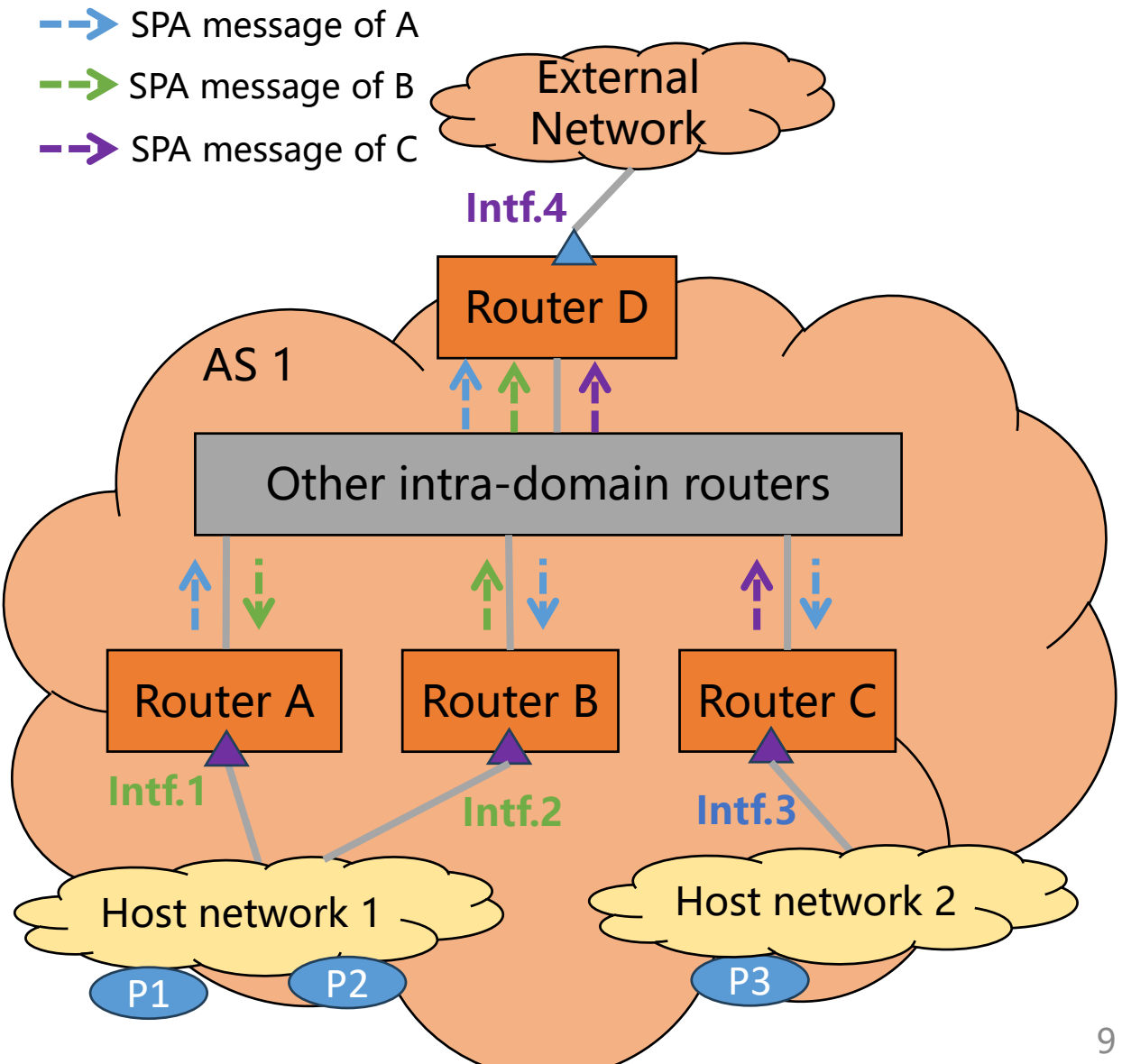
- After receiving SPA messages from other SAVNET routers, each SAVNET router will generate allowlist or blocklist on specific interfaces
  - Allowlist Generation: A SAVNET router **facing an internal host network** can generate an allowlist on the interface by including all source prefixes in SPA messages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

The Most Recommended Use Case: SAV at the Edge



- Generate allowlists on interfaces facing an internal host network
- Generate blocklists on interfaces facing an external network/AS

The Most Recommended Use Case: SAV at the Edge



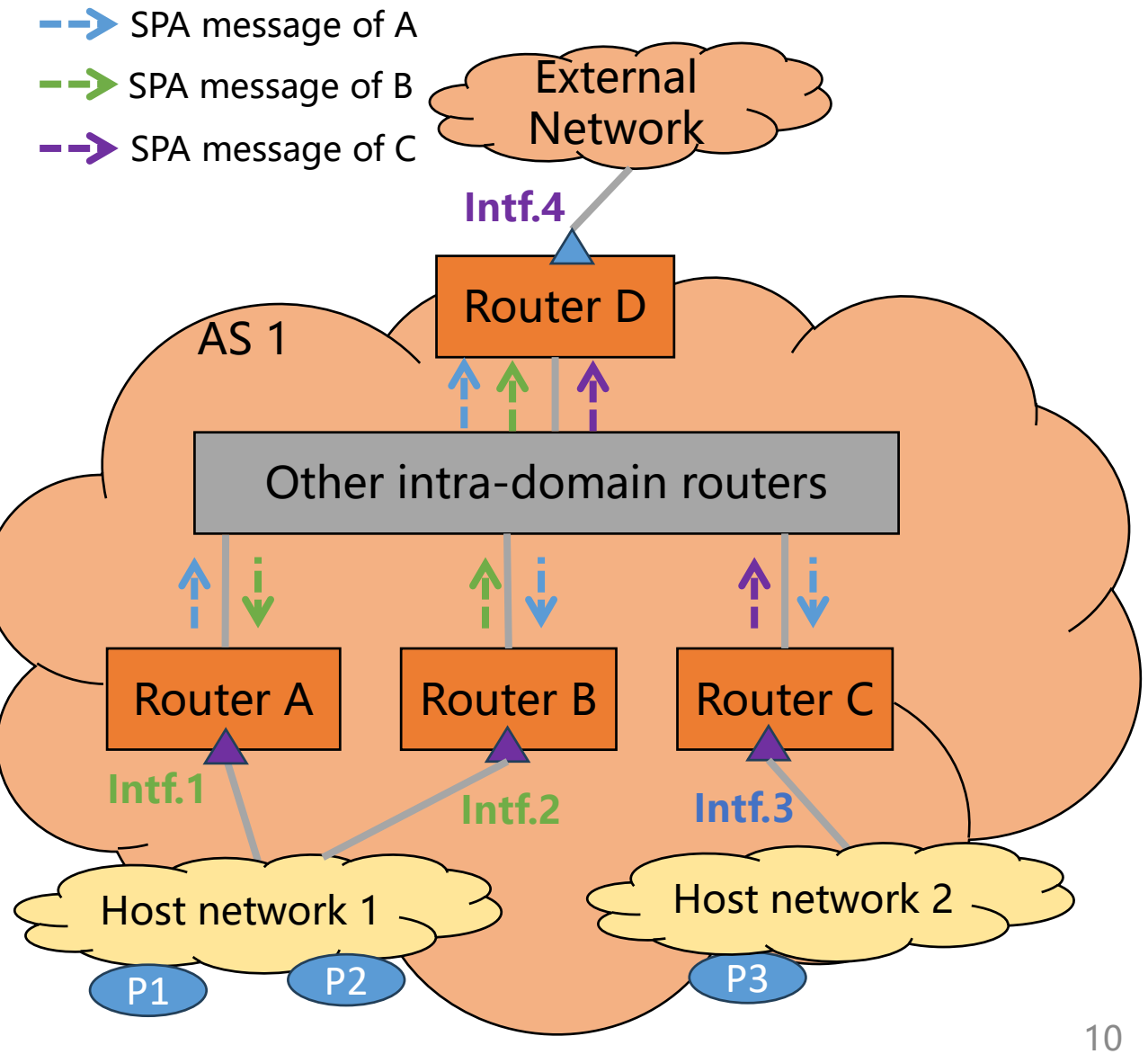
Asymmetric Routing Scenario

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

SPA Procedure

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

Compare SPA-based SAVNET with Existing Intra-domain SAV Solutions



Results

- If use ACL-based ingress filtering
  - **Manual update → High operational overhead**
- If use strict uRPF
  - **Improper blocks in asymmetric routing scenarios**
- If use loose uRPF
  - **Too many improper admits**
- If use SPA-based SAVNET
  - **Automatically** generate allowlist or bloclist
  - **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

Alternative Use Case

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

Next Step

- How to implement SPA-based SAVNET by using OSPF or IS-IS?
  - Towards effective and efficient
    - MUST avoid affecting the normal OSPF and IS-IS and avoid signaling too much information
    - It is possible to use the existing Sub-TLV to signal the HNI value
- Comments and suggestions are welcome

Thanks!