IGP-based Source Address Validation in Intra-domain Network (Intra-domain SAVNET)

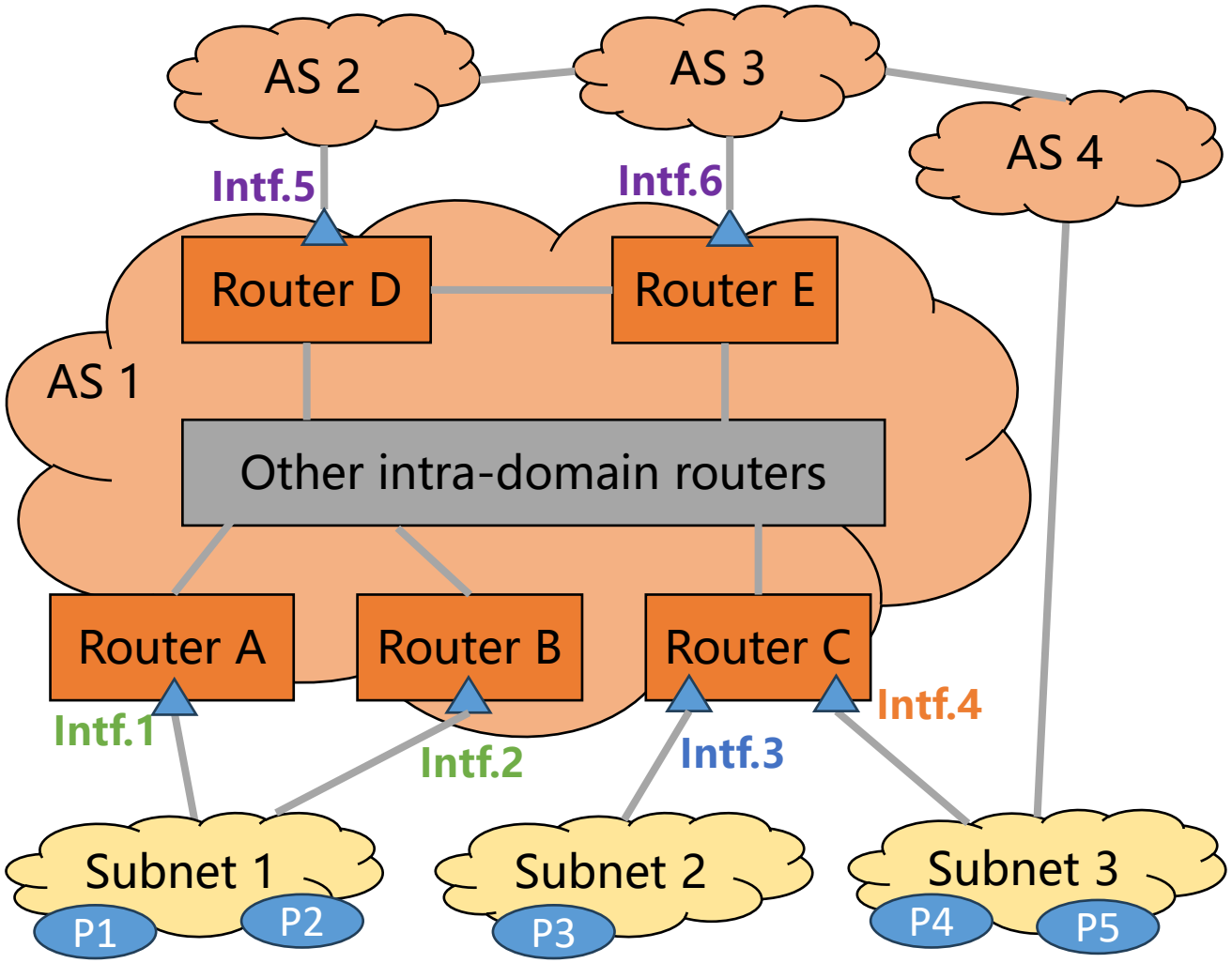
Dan Li, Lancheng Qin, Xueyan Song, Changwang Lin, Shengnan Yue

July 23, 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 customer-facing routers, host-facing routers, and AS border routers
  - Generate SAV rules by using SAV-specific information exchanged among routers
- draft-li-savnet-source-prefix-advertisement proposes a protocol-independent SAV solution under intra-domain SAVNET architecture
- Following the above three documents, this document proposes IGP-based solution for Intra-domain SAVNET
  - Allow routers communicate SAV-specific information through IGP

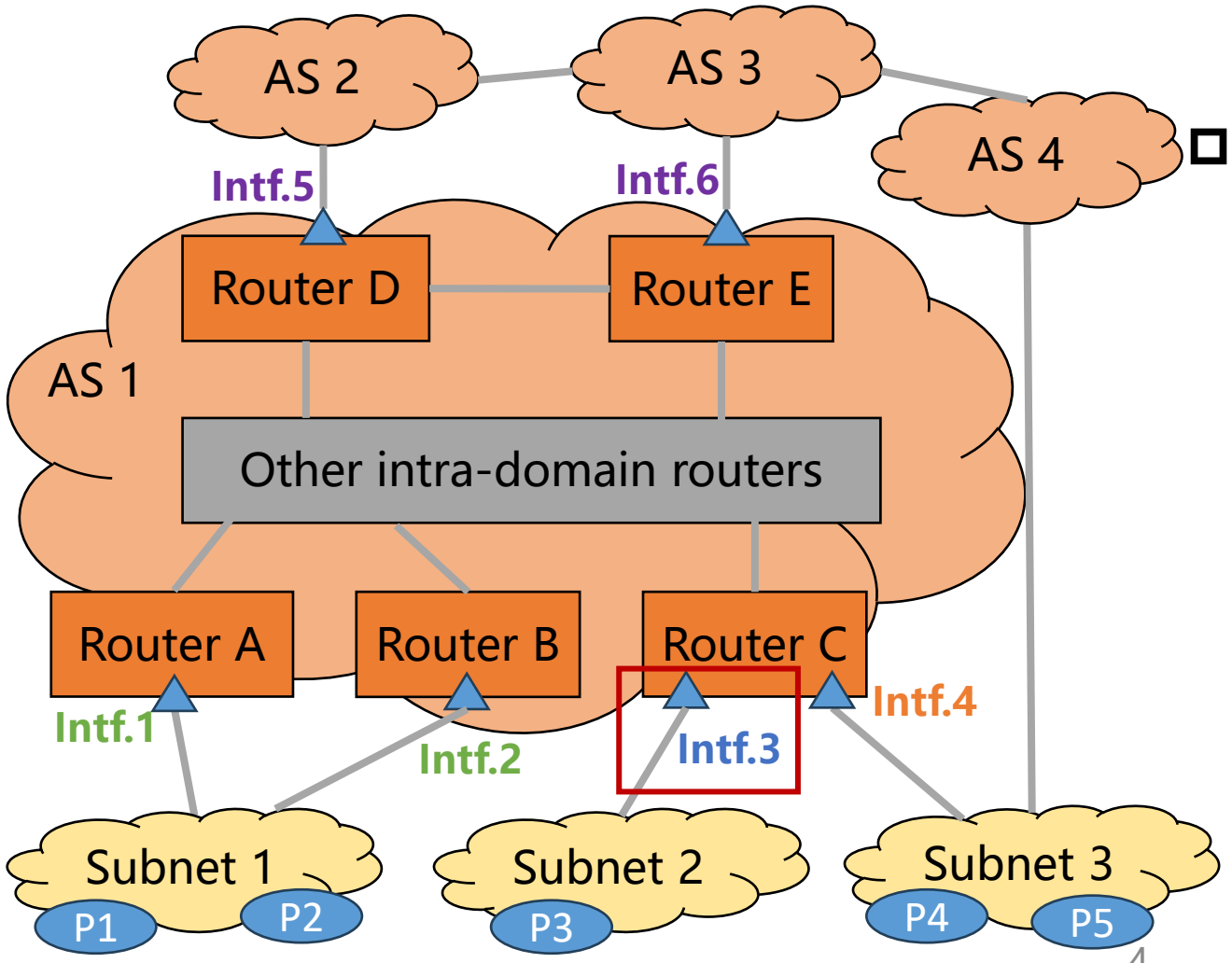
Four Types of Interface



- Single-homing interface
  - The interface of an edge router that faces to a single-homed subnet (e.g., Intf.3)
- Complete multi-homing interface
  - If all routers facing a multi-homed subnet are in the local AS, the interfaces facing this subnet are complete multi-homing interfaces (e.g., Intf.1 and Intf.2)
- Incomplete multi-homing interface
  - If some routers facing a multi-homed subnet are in other ASes, the interfaces facing this subnet are incomplete multi-homing interfaces (e.g., Intf.4)
- Internet interface
  - The interface of an AS border router that faces to another AS (e.g., Intf.5 and Intf.6)

Goal of Intra-domain SAVNET

Automatically generate prefix allowlist or blocklist on the four types of interface

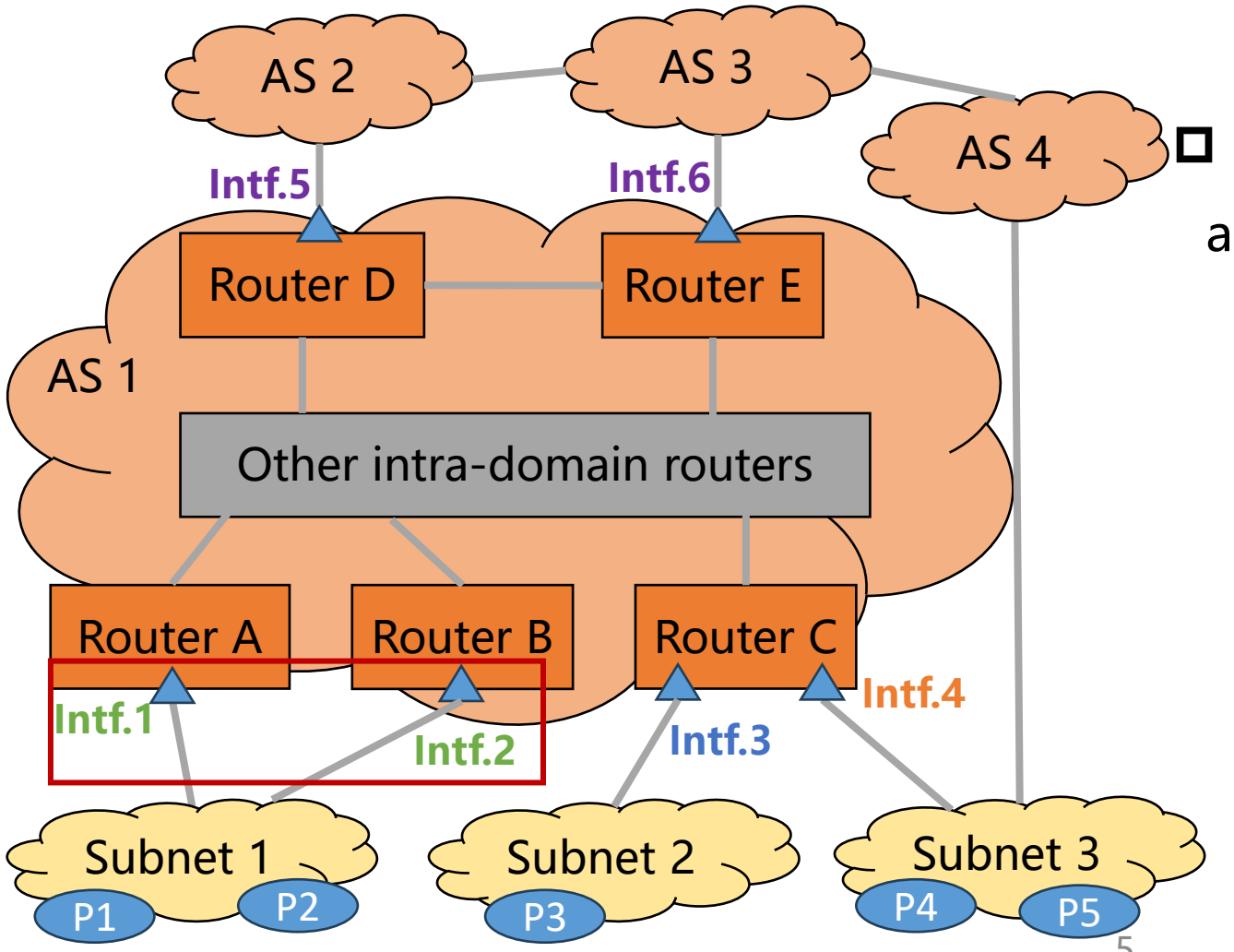


- For single-homing interface Intf.3
  - ◆Generate a prefix allowlist * containing all source prefixes (i.e., P3) of the facing single-homed subnet (i.e., Subnet 2)
  - ◆Only allow data packets from that subnet using source addresses in the prefix allowlist

* Mode 1 in draft-huang-savnet-sav-table

Goal of Intra-domain SAVNET

Automatically generate prefix allowlist or blocklist on the four types of interface

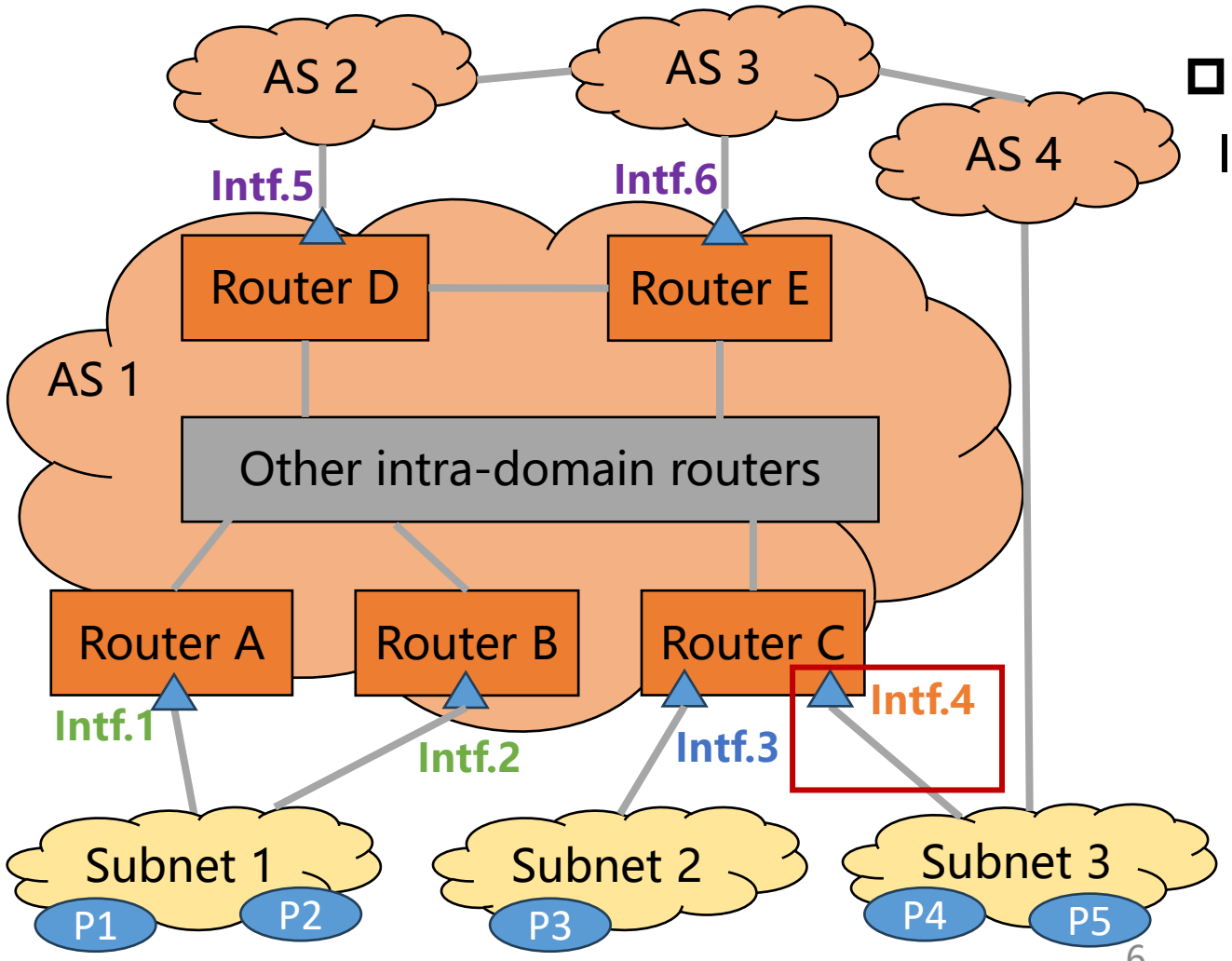


- For complete multi-homing interfaces Intf.1 and Intf.2
  - ◆Generate a prefix allowlist * containing all source prefixes (i.e., P1 and P2) of the facing multi-homed subnet (i.e., Subnet 1)
  - ◆Only allow data packets from that subnet using source addresses in the prefix allowlist

* Mode 1 in draft-huang-savnet-sav-table

Goal of Intra-domain SAVNET

Automatically generate prefix allowlist or blocklist on the four types of interface

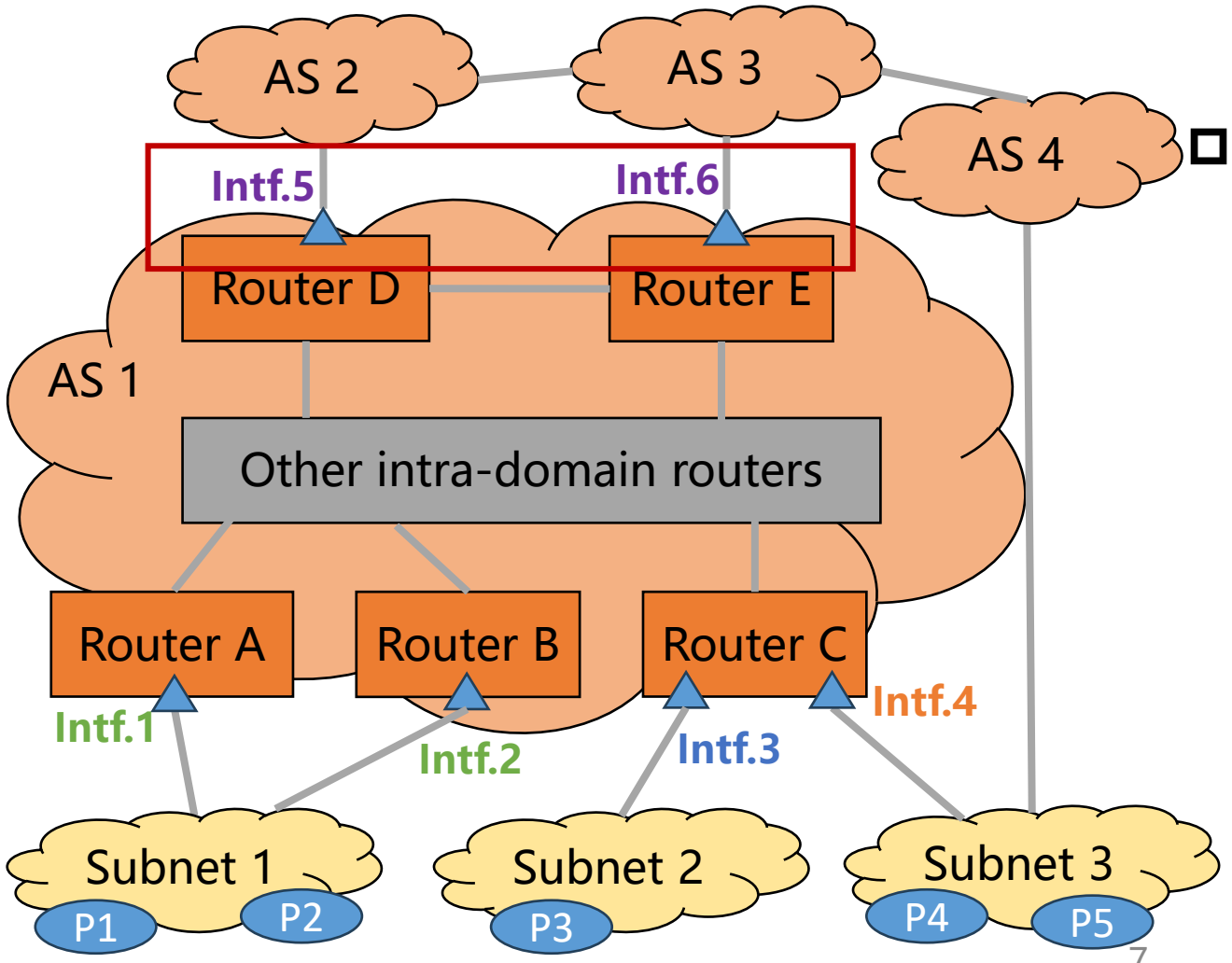


- For incomplete multi-homing interface Intf.4
  - ◆Generate a prefix blocklist * containing source prefixes (i.e., P1, P2, and P3) of single-homed subnet (i.e., Subnet 1) and complete multi-homed subnet (i.e., Subnet 2)
    - ➢Router C may not identify all source prefixes of Subnet 3 without communication between AS4 in routing asymmetry scenario
  - ◆Block data packets from the facing subnet using source addresses in the prefix blocklist

* Mode 2 in draft-huang-savnet-sav-table

Goal of Intra-domain SAVNET

Automatically generate prefix allowlist or blocklist on the four types of interface



- For Internet interfaces Intf.5 and Intf.6
  - Generate a prefix blocklist * containing source prefixes (i.e., P1, P2, and P3) of single-homed subnet (i.e., Subnet 1) and complete multi-homed subnet (i.e., Subnet 2)
  - Block data packets from the facing subnet using source addresses in the prefix blocklist

* Mode 2 in draft-huang-savnet-sav-table

SAV Procedure

- SAV-specific information generation
  - Edge routers generate SAV-specific information containing four types of information
- SAV-specific information communication
  - Edge routers provides SAV-specific information to other routers
- SAV rule generation
  - Edge routers and AS border routers generate prefix allowlists or blocklists by using SAV-specific information

SAV-specific Information Generation

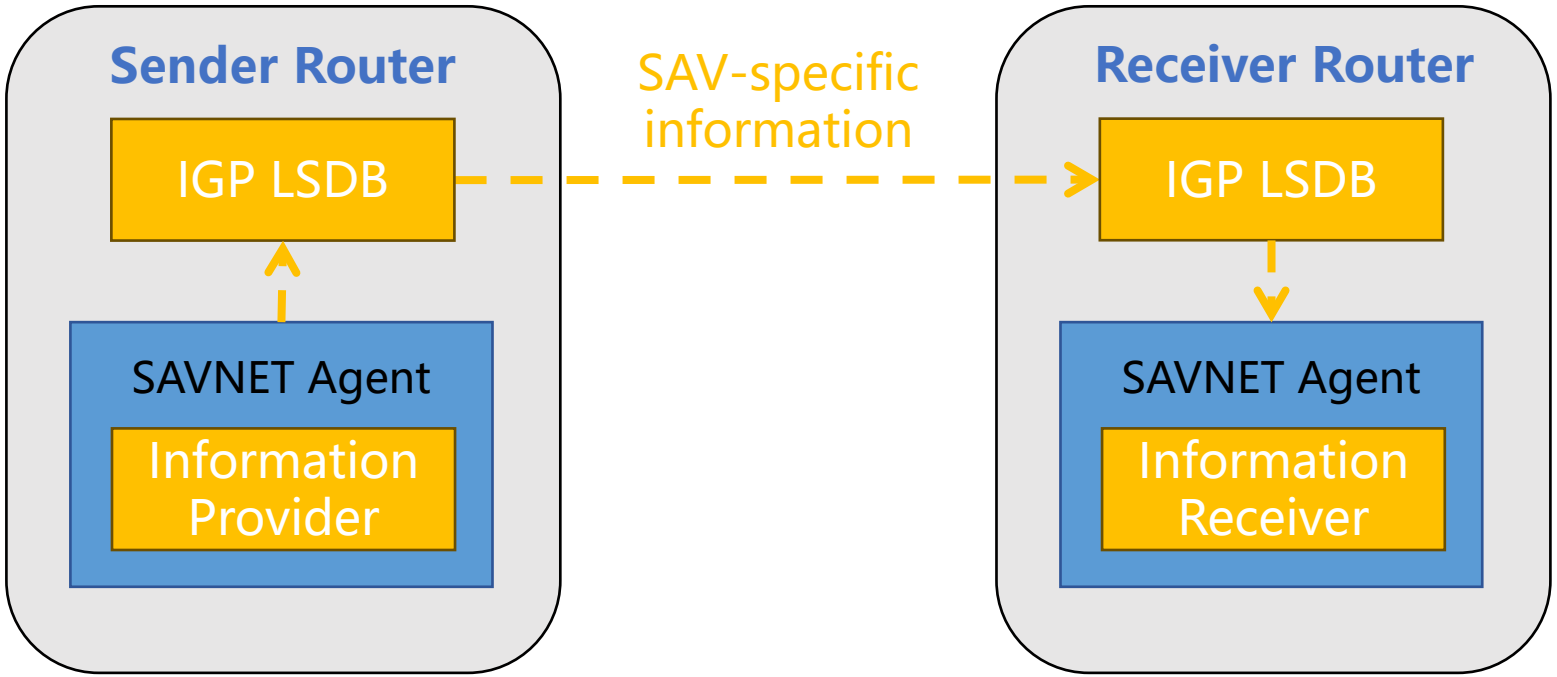
- Edge routers generate SAV-specific information containing four types of information
  - **Source Prefix:** The source prefix learned through its **local routes to the facing subnet**
  - **Interface Type:** The type of the interface facing the subnet
    - Single-homing Interface (SI), Complete Multi-homing Interface (CMI), or Incomplete Multi-homing Interface (IMI)
  - **Subnet Tag:** A unique tag value that identifies the subnet that owns the source prefix
    - Prefixes belonging to the same subnet MUST have the same subnet tag value
    - Different subnets MUST have different tag values
  - **Only Source Flag:** This flag indicates whether the source prefix is only used by the subnet
    - By default, the flag is set
    - But for multi-source prefixes (e.g., anycast prefixes or direct server return (DSR) prefixes), the flag should be unset (possibly manually)

How to learn the Interface Type and Subnet Tag

- The **Interface Type** is configured based on the topology
- Each subnet is assigned a unique **Subnet Tag** value when it first connects to the edge routers
- The edge router can **automatically** match the Interface Type and Subnet Tag to source prefixes of the corresponding subnet
- Different from ACL-based SAV, manual configurations are not needed when the source prefix of a subnet changes
  - ◆Only Interface Type may need to be updated when the topology changes
    - ➢For example, from Single-homing Interface to Complete Multi-homing Interface
  - ◆Require **less operational overhead** than ACL-based SAV

SAV-specific Information Communication

- The SAVNET Agent of a Sender Router can provide its SAV-specific information to other SAVNET routers by using IGP
  - ◆When an edge router distributes IP prefix information of its subnet via IGP, it can carry the Interface Type, Subnet Tag, and Only Source Flag with the IP prefix information



Two Approaches to SAV-specific Information Communication

- Approach #1: Use the existing Administrative Tag Sub-TLV to carry Interface Type, Subnet Tag, and Only Source Flag

- Approach #2: Define a new SAVNET Tag Sub-TLV to carry Interface Type, Subnet Tag, and Only Source Flag

Approach #1

- Use the existing Administrative Tag Sub-TLV of IGP
  - Administrative Tag Sub-TLV of IS-IS [RFC 5130]
  - Administrative Tag Sub-TLV of OSPF [draf-ietf-lsr-ospf-admin-tags]
  - Administrative Tag Sub-TLV of OSPFv3 [draf-ietf-lsr-ospf-admin-tags]
- Limitation
  - Since the Administrative Tag Sub-TLV is not designed for SAV, using the Administrative Tag Sub-TLV may conflict with other routing policies that also use Administrative Tags
    - Additional operations are needed to avoid possible conflicts

Approach #2

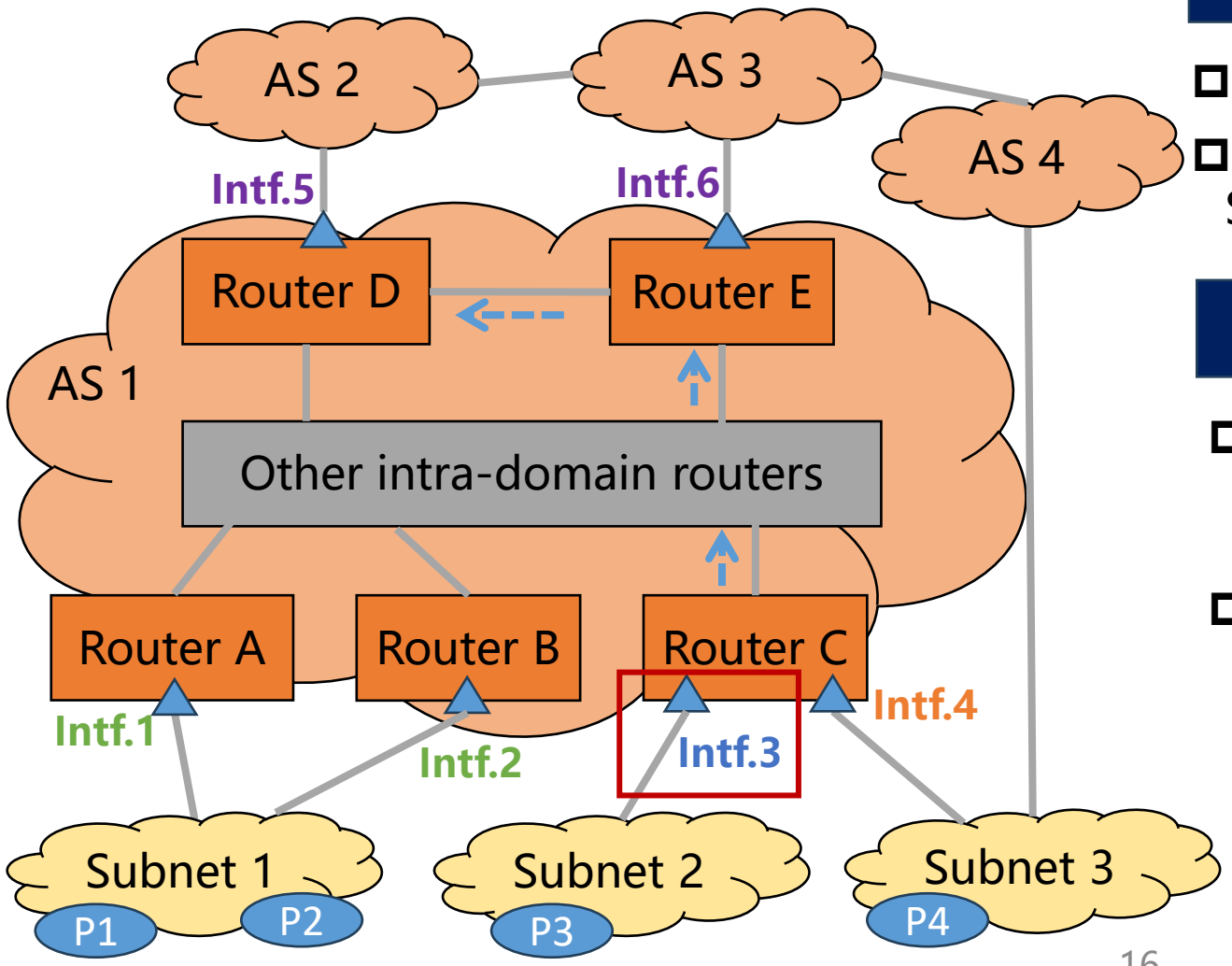
- Define a new SAVNET Tag Sub-TLV for IGP
  - A new SAVNET Tag Sub-TLV for IS-IS
  - A new SAVNET Tag Sub-TLV for OSPF
  - A new SAVNET Tag Sub-TLV for OSPFv3
- Advantage
  - Avoid conflicts with routing policies using existing Sub-TLVs and facilitate the operation of SAV

SAV Rule Generation

- For Single-homing Interface
  - The router generates a prefix allowlist by using its own SAV-specific information
    - The prefix allowlist contains source prefixes learned through its local routes to the facing subnet

Example #1

SAV-specific information of Router C: [P3, SI, 2, Only Source]



Scenario

- Intf.3 is a Single-homing Interface (SI)
- Router C learns prefix P3 through its local routes to Subnet 2

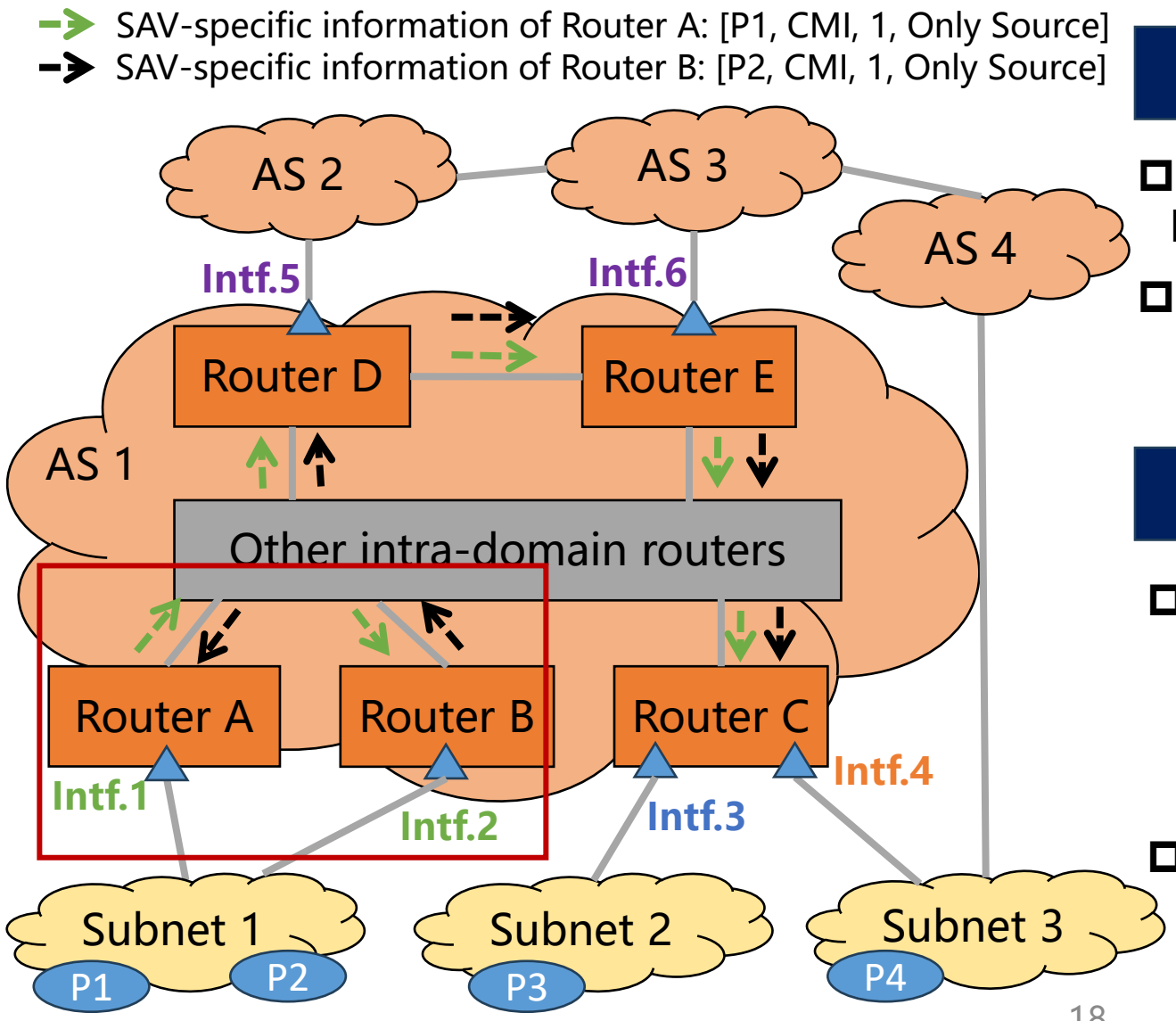
SAV Procedure

- SAV-specific information generation
  - SAV-specific information of Router C
    - [**source prefix: P3**, **Interface Type: SI**, Subnet Tag: 2, Only Source]
- SAV rule generation
  - **Prefix allowlist at Intf.3**
    - **[P3]**

SAV Rule Generation

- For Complete Multi-homing Interface
  - The router generates a prefix allowlist by using its own SAV-specific information and SAV-specific information from other routers facing the same subnet
    - Prefixes with the same Subnet Tag of the facing subnet will be added into the prefix allowlist

Example #2



Scenario

- Intf.1 and Intf.2 are Complete Multi-homing Interfaces (CMI)
- Due to traffic engineering and asymmetric routing
  - Router A only learns prefix P1 through its local route to Subnet 1
  - Router B only learns prefix P2 through its local route to Subnet 1

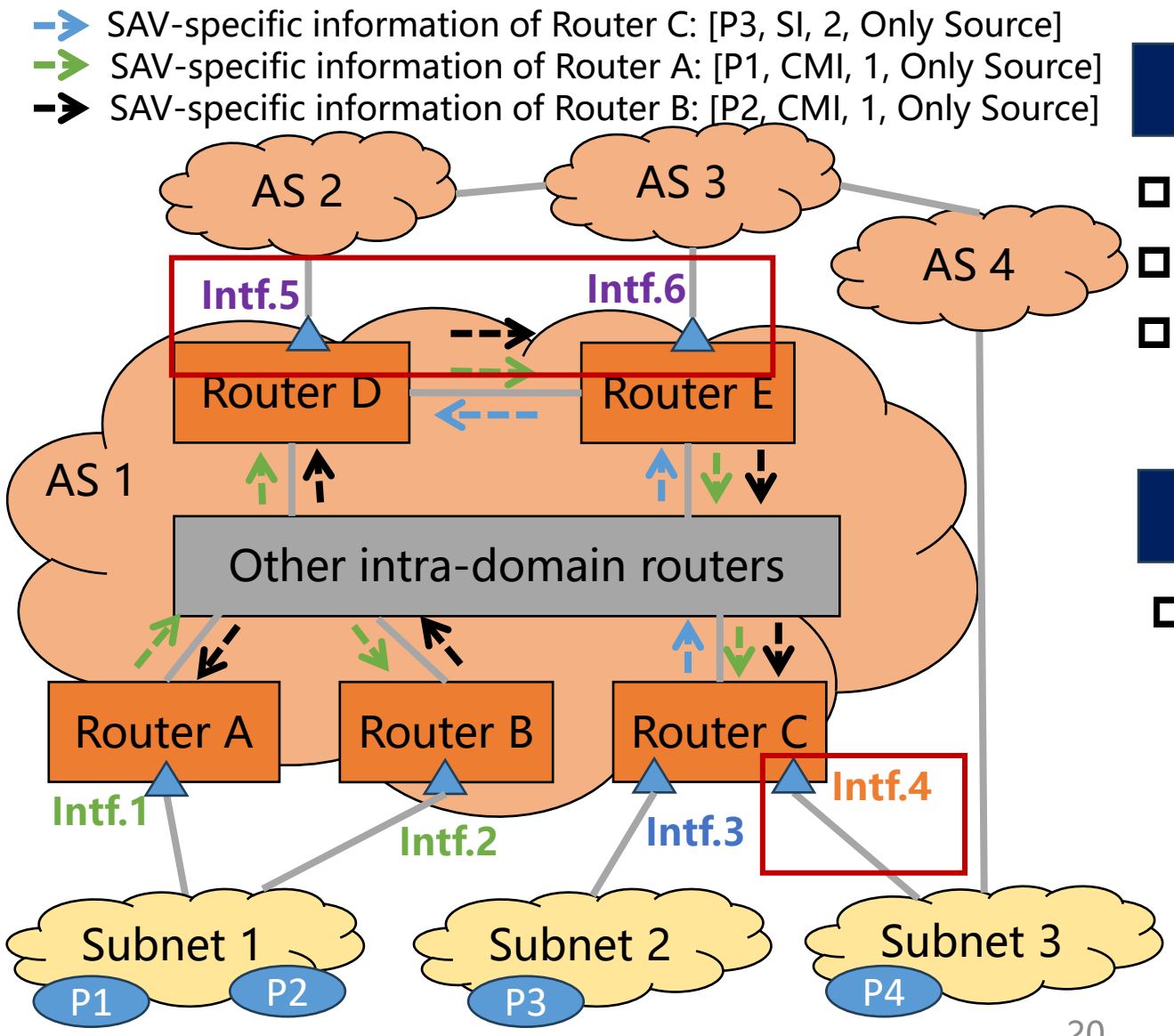
SAV Procedure

- SAV-specific information generation
  - SAV-specific information of Router A
    - [**source prefix: P1**, Interface Type: CMI, **Subnet Tag: 1**, Only Source]
  - SAV-specific information of Router B
    - [**source prefix: P2**, Interface Type: CMI, **Subnet Tag: 1**, Only Source]
- SAV rule generation
  - **Prefix allowlist at Intf.1 and Intf.2**
    - **[P1, P2]**

SAV Rule Generation

- For Incomplete Multi-homed Interface and Internet Interface
  - The router generates a prefix blocklist by using its own SAV-specific information (if any) and SAV-specific information from other routers
    - Prefixes with "Single-homing Interface" or "Complete Multi-homing Interface" Type and Only Source Flag will be added into the prefix blocklist
    - Prefixes with "Incomplete Multi-homed Interface" Type or without Only Source Flag should not be added into the prefix blocklist

Example #3



Scenario

- Intf.4 is an Incomplete Multi-homing Interface
- Intf.5 and Intf.6 are Internet Interfaces
- P1, P2, P3 have SI/CMI Tag and Only Source Flag

SAV Procedure

- SAV rule generation
  - **Prefix blocklist at Intf.4, Intf.5, and Intf.6**
    - **[P1, P2, P3]**

Next Step

- Improve the preliminary design of IGP-based method
- Your comments and suggestions are welcome!
  - Which approach is more appropriate?
  - Can Interface Type, Subnet Tag, and Only Source Flag be configured and updated in an automatic way?
  - ……

Thanks!