# Source Prefix Advertisement for Intra-domain SAVNET

Dan Li, Nan Geng, Lancheng Qin

July 23, 2024

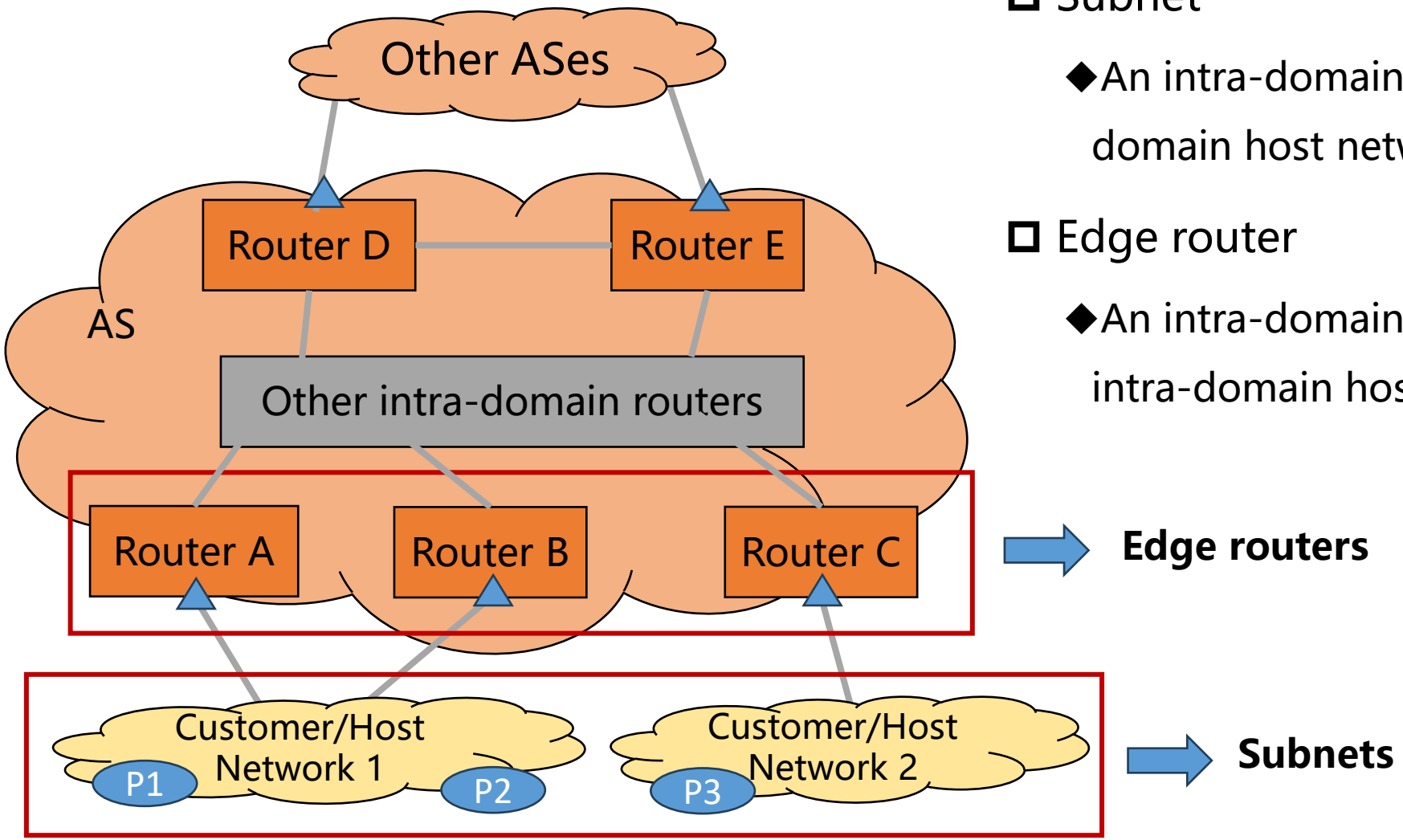
# Introduction

- 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
- Following the above two documents, this document proposes the Source Prefix Advertisement (SPA) solution for Intra-domain SAVNET, named SPA-based SAVNET
  - Allow routers communicate SAV-specific information through SPA messages

# Scope of This Document

- The goal of SPA-based SAVNET
- The protocol-independent design of SPA-based SAVNET
  - ◆The content of SPA message
  - ◆The process of SAV rule generation by using SPA messages
- How to transmit SPA messages is not in the scope
  - ◆SPA messages can be transmitted by a new protocol or an extension to an existing protocol (e.g., IS-IS, OSPF, BGP)
  - ◆Protocol designs or extensions are not in the scope

# Two New Terminologies

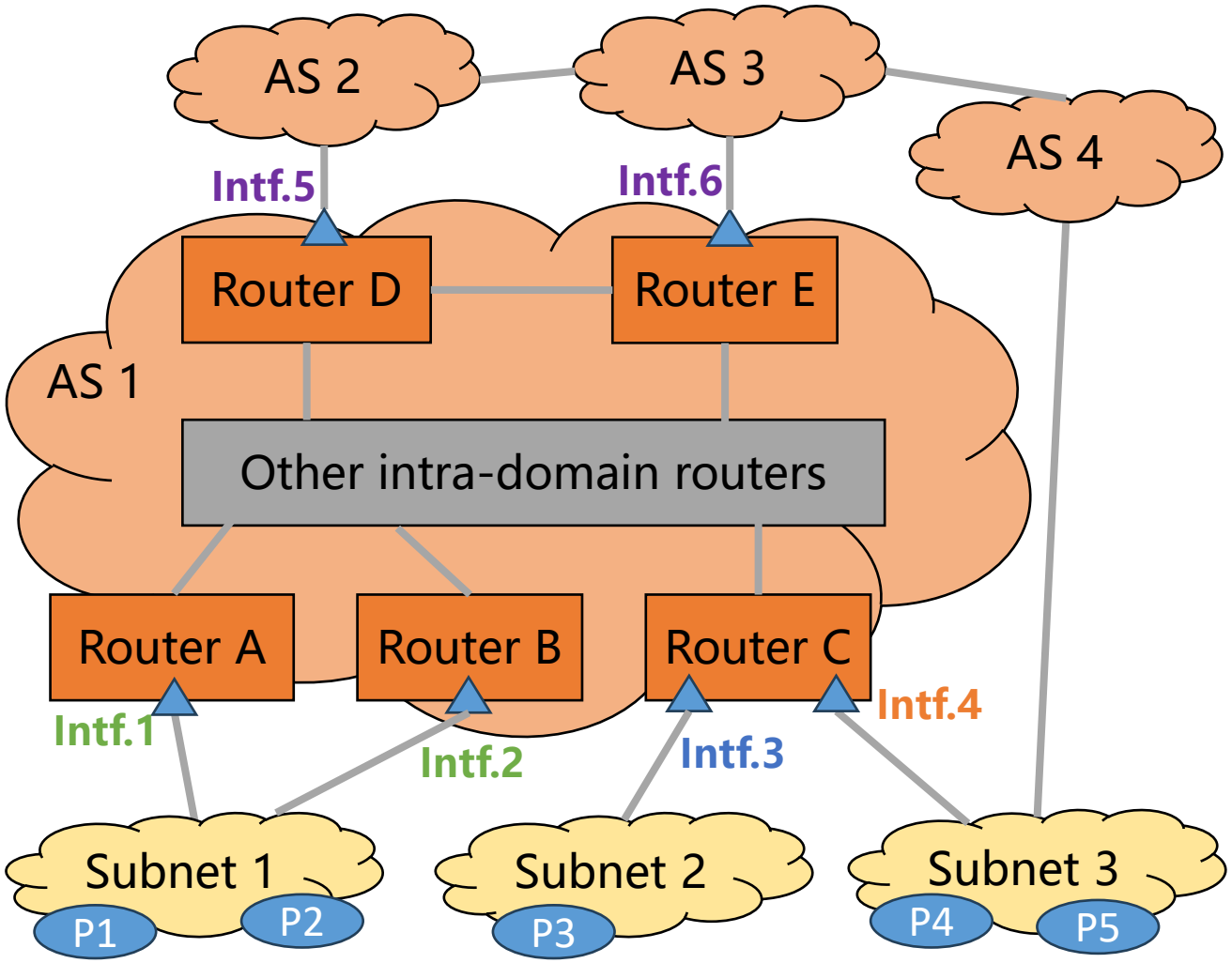



- Subnet
  - ◆An intra-domain customer network or an intra-domain host network
- Edge router
  - ◆An intra-domain customer-facing router or an intra-domain host-facing router

**Edge routers**

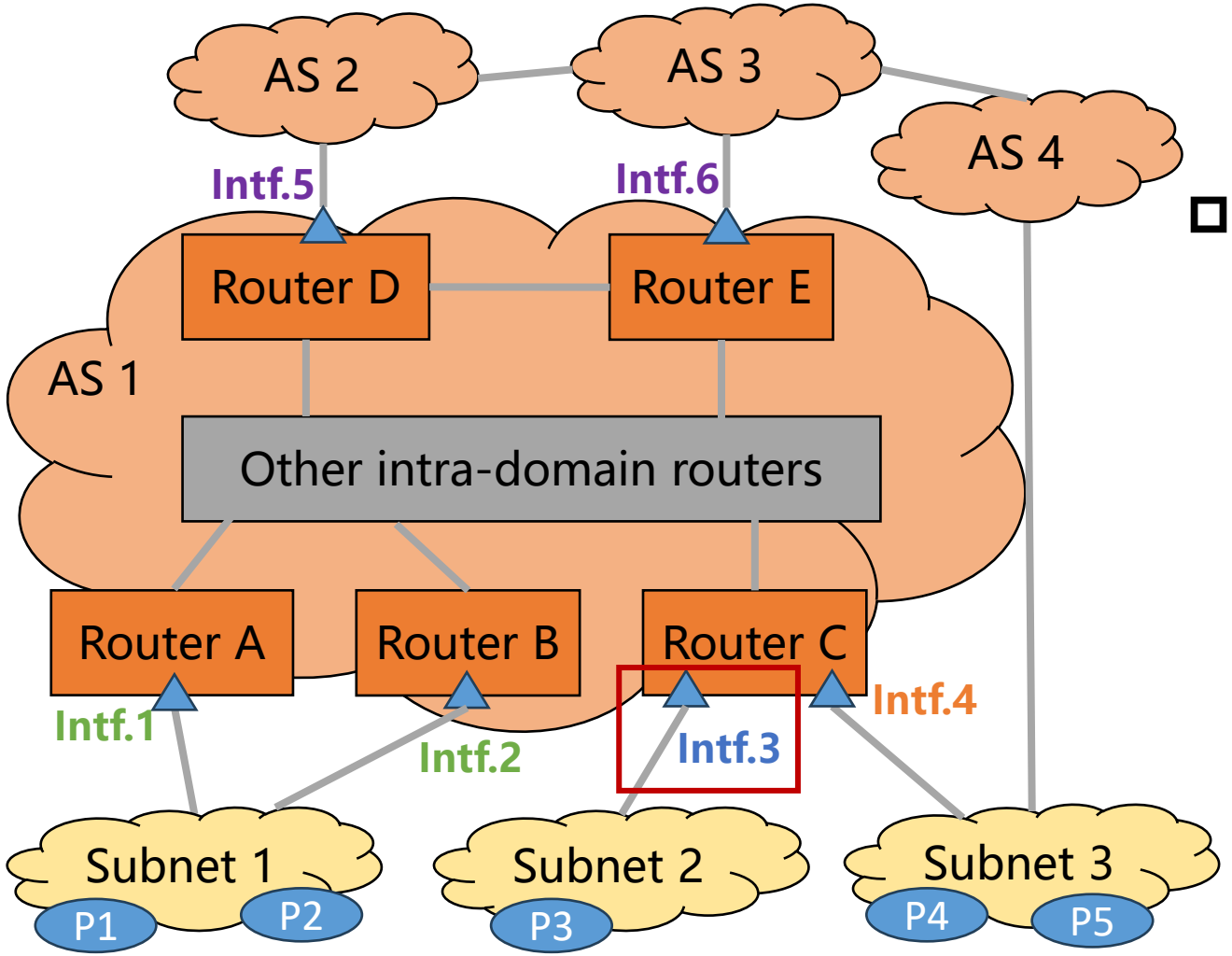
**Subnets**

# 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)

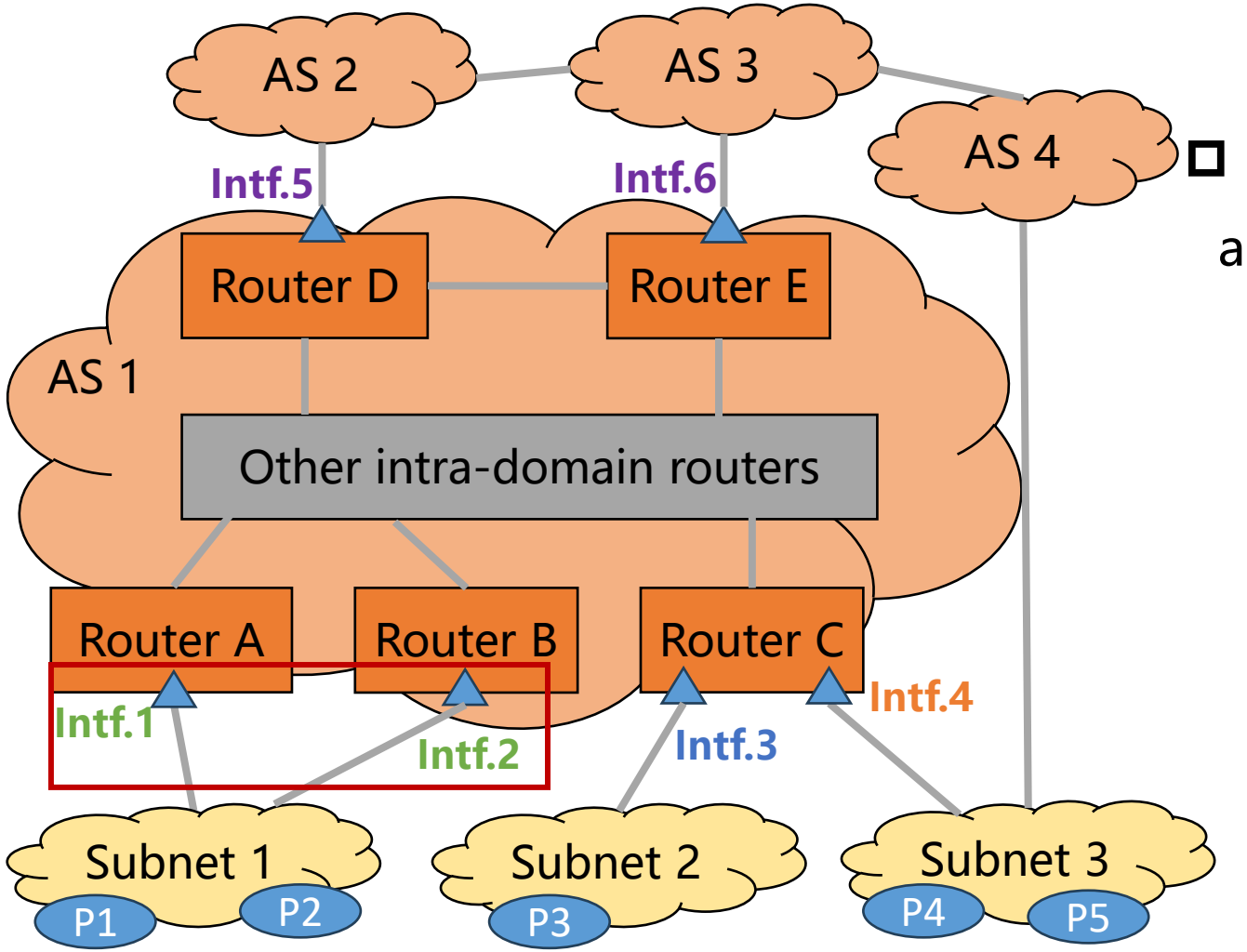
# Validation Mode for Single-homing Interface




- 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

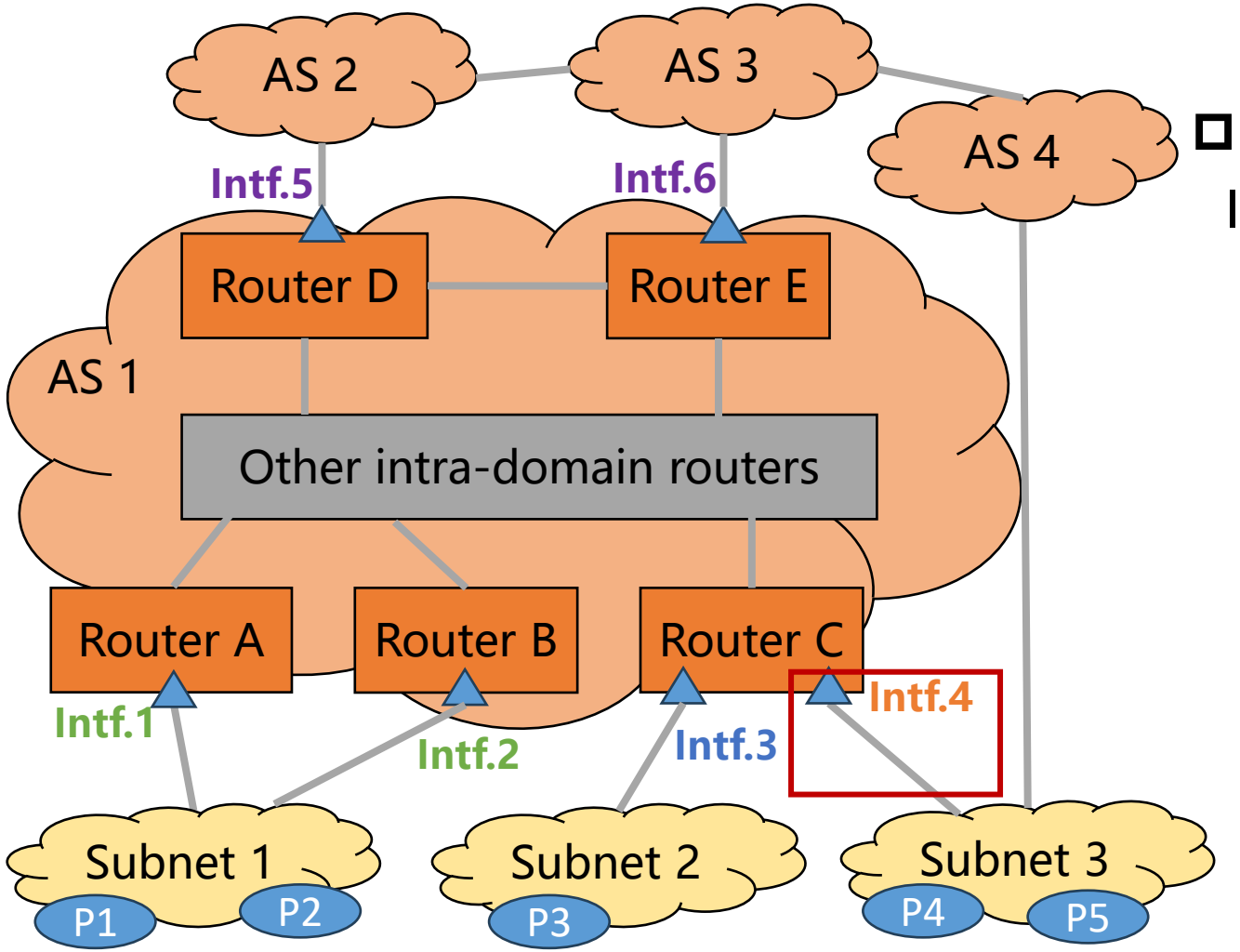
# Validation Mode for Complete Multi-homing Interface




- 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

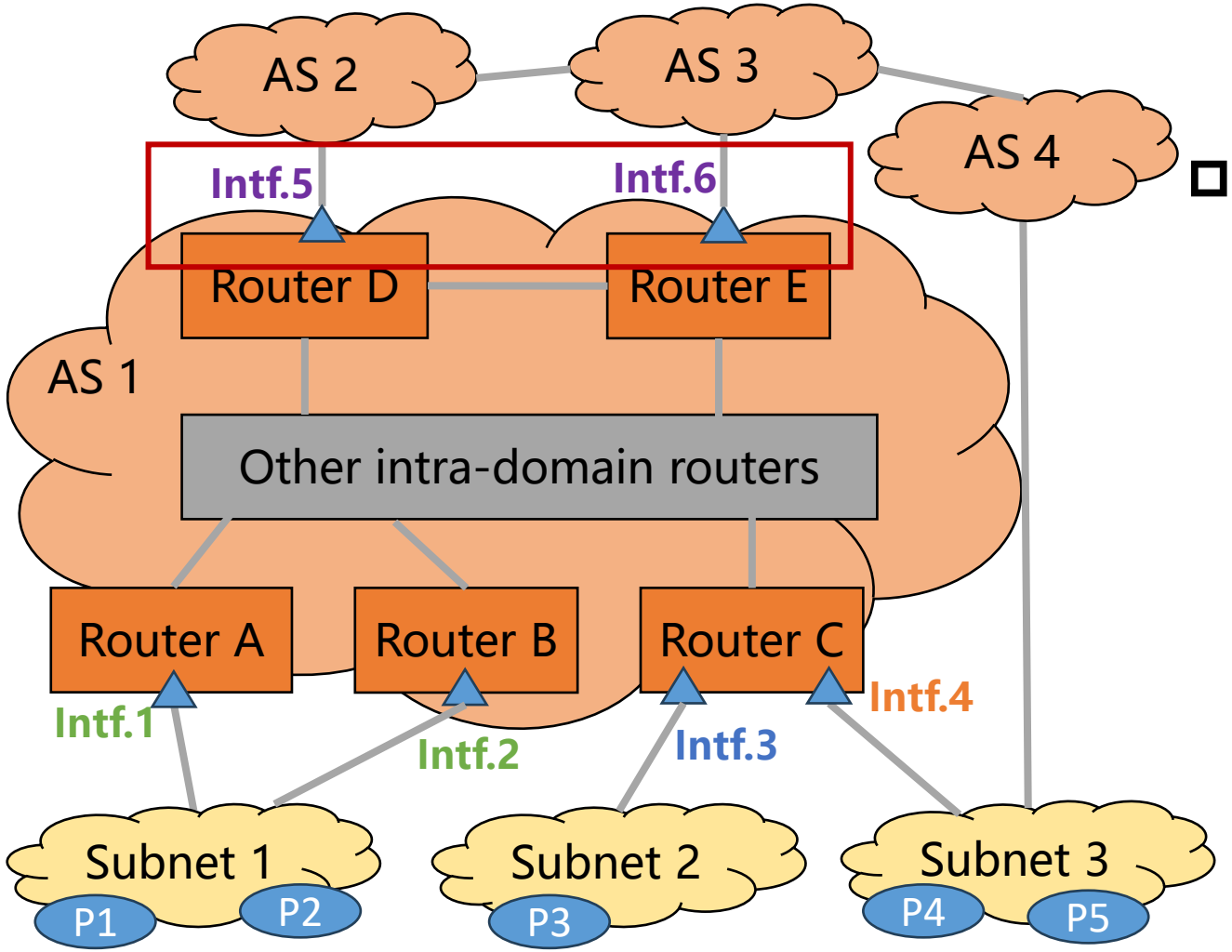
# Validation Mode for Incomplete Multi-homing Interface




- 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

# Validation Mode for Internet 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

# Source Prefix Advertisement Procedure

**Source prefix advertisement procedure includes three main steps**

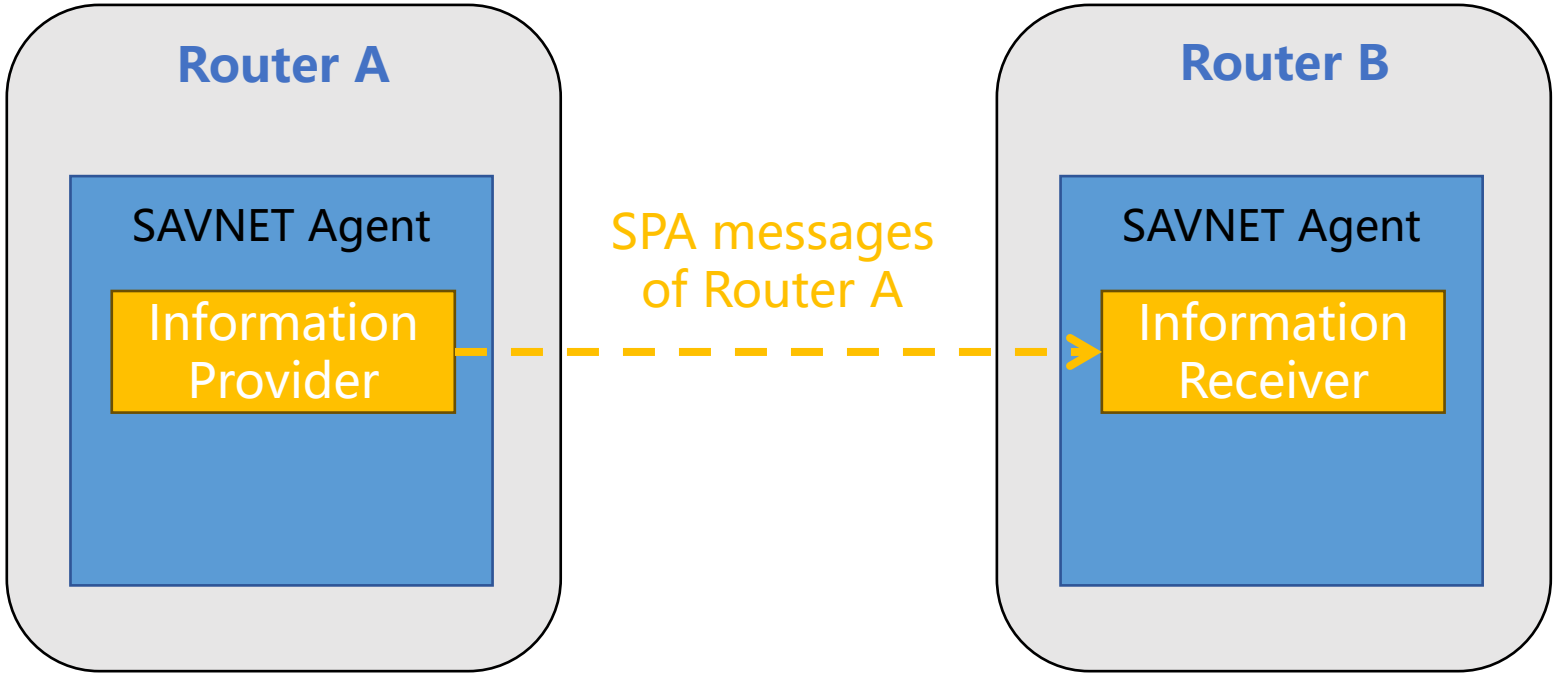
- SPA message generation
  - Edge routers generate SPA messages containing SAV-specific information
- SPA message communication
  - Edge routers send their SPA messages to other routers
- SAV rule generation
  - Edge routers and AS border routers generate SAV rules by using SPA messages

# SPA Message Generation

- Edge routers generate a SPA message 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)

# SPA Message Communication

- After generating SPA messages, the edge router will send its SPA messages to other routers
- SPA messages can be transmitted through either a new protocol or an extension to an existing protocol
  - Not in the scope of this document

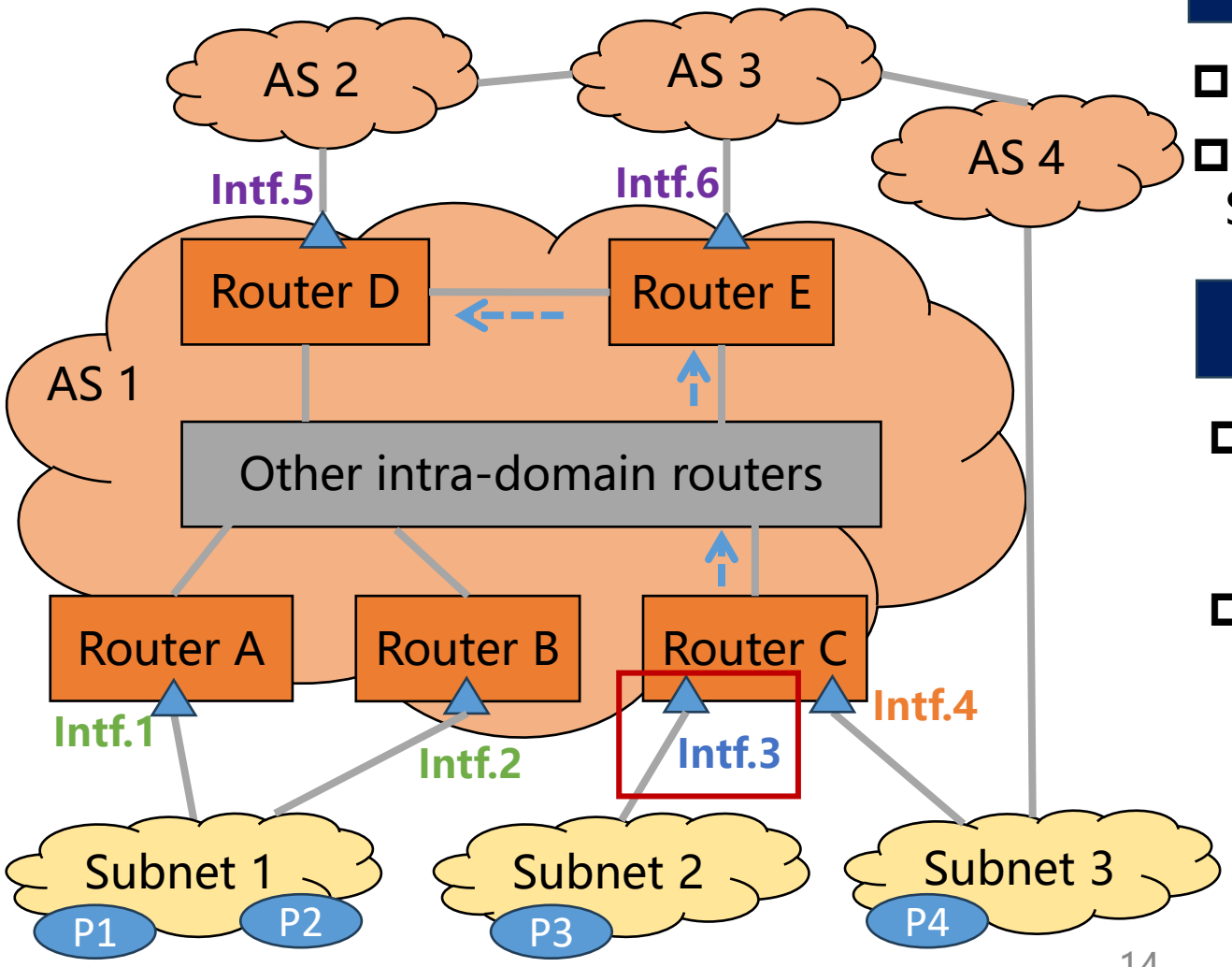


# SAV Rule Generation

- For Single-homing Interface
  - The router generates a prefix allowlist by using its own SPA messages without SPA messages from other routers
    - The prefix allowlist contains source prefixes learned through its local routes to the facing subnet

# Example #1

SPA message 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

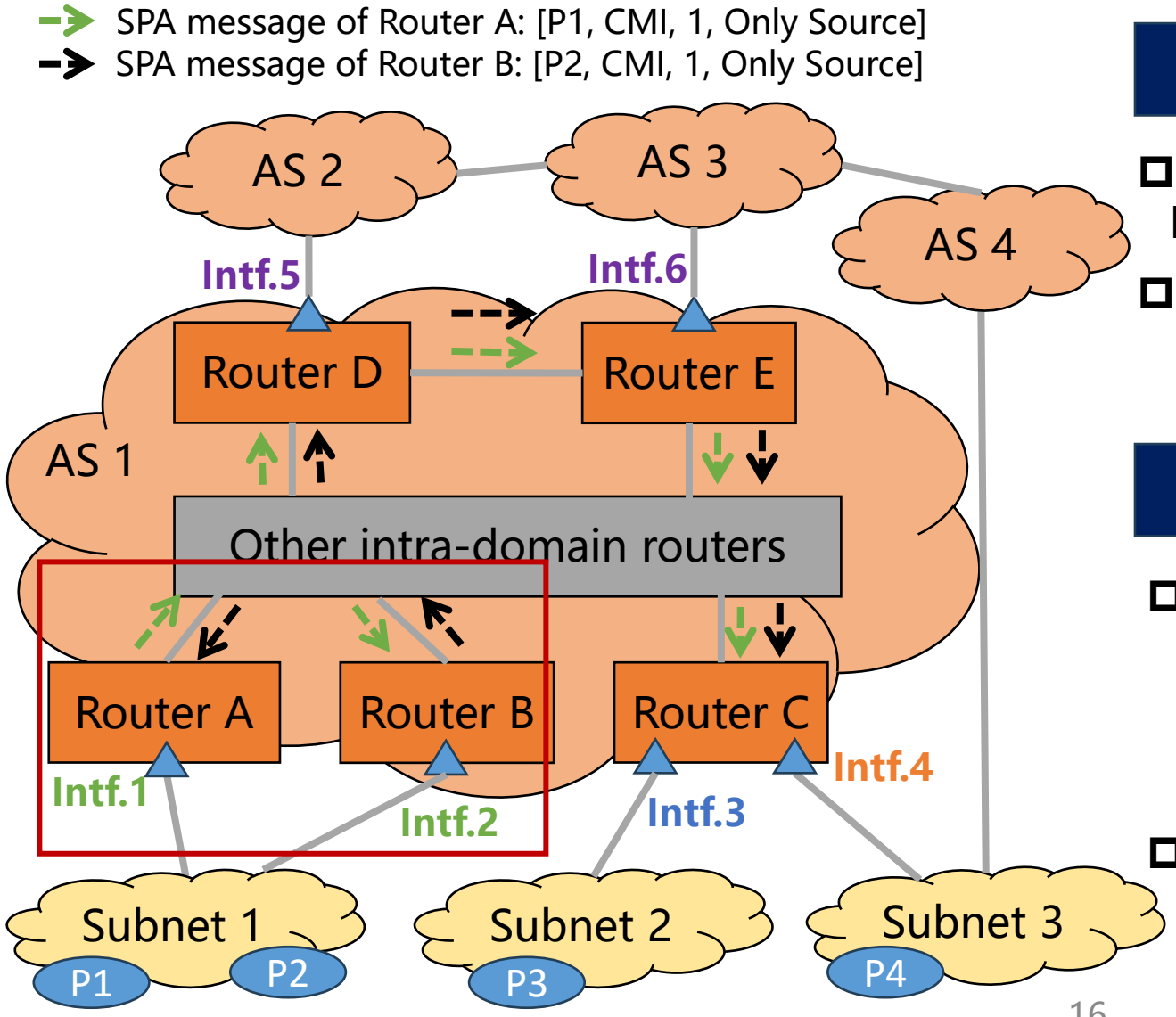
## SPA Procedure

- SPA message generation
  - SPA message 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 SPA messages and SPA messages from other routers facing the same subnet
    - Prefixes in SPA messages 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

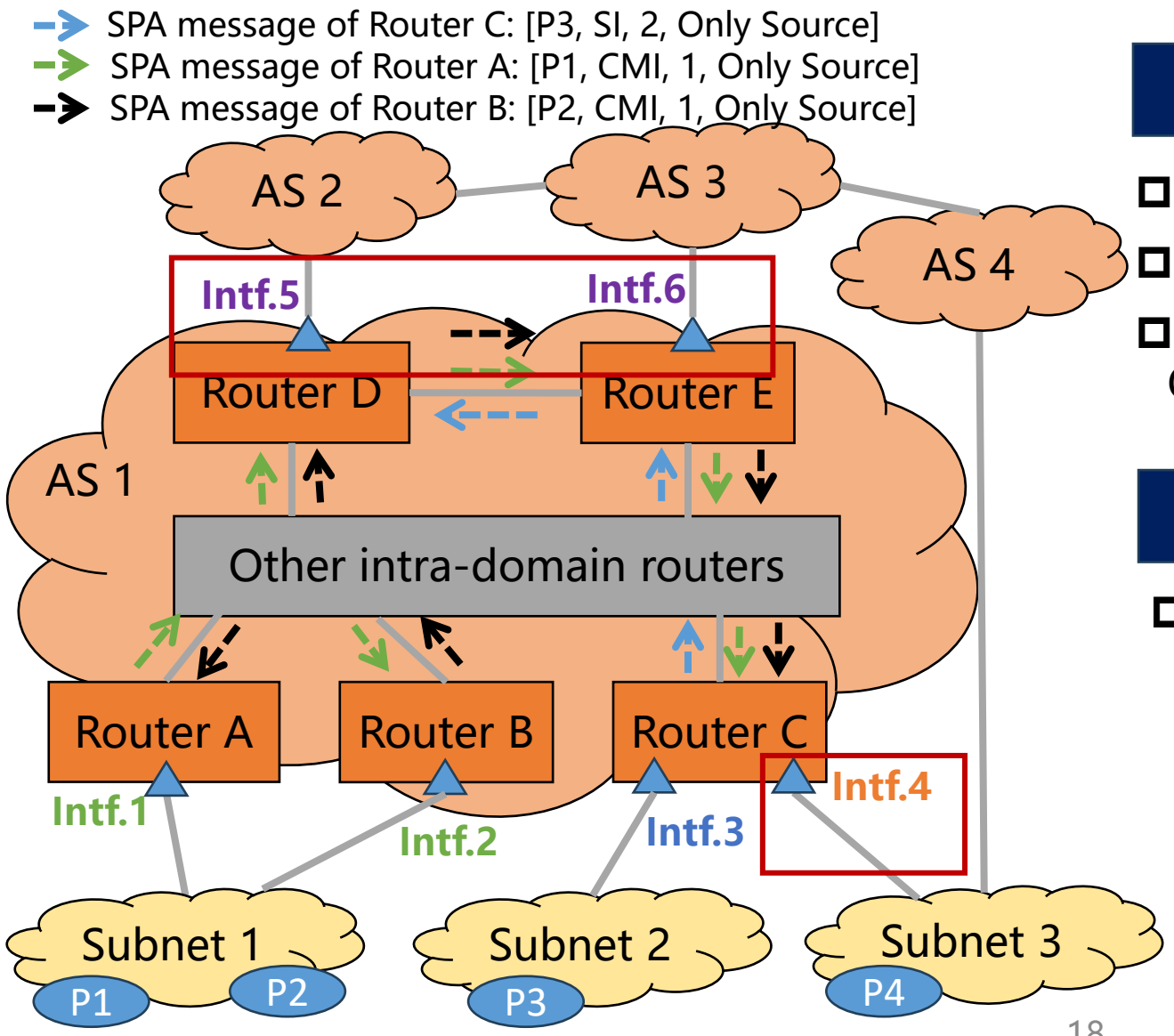
## SPA Procedure

- SPA message generation
  - SPA message of Router A
    - [**source prefix: P1**, Interface Type: CMI, **Subnet Tag: 1**, Only Source]
  - SPA message 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 SPA messages (if any) and SPA messages from other routers
    - Prefixes in SPA messages with "Single-homing Interface" or "Complete Multi-homing Interface" Type and Only Source Flag will be added into the prefix blocklist
    - Prefixes in SPA messages 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 in SPA messages have SI/CMI Tag and Only Source Flag

## SPA Procedure

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

# 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 at edge routers and AS border routers by using SPA messages
- SPA-based SAVNET is a protocol-independent intra-domain SAV
  - It is recommended to communicate SPA messages by IGP or BGP

# 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
    - Edge routers facing the same multi-homed subnet 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

# Next Step

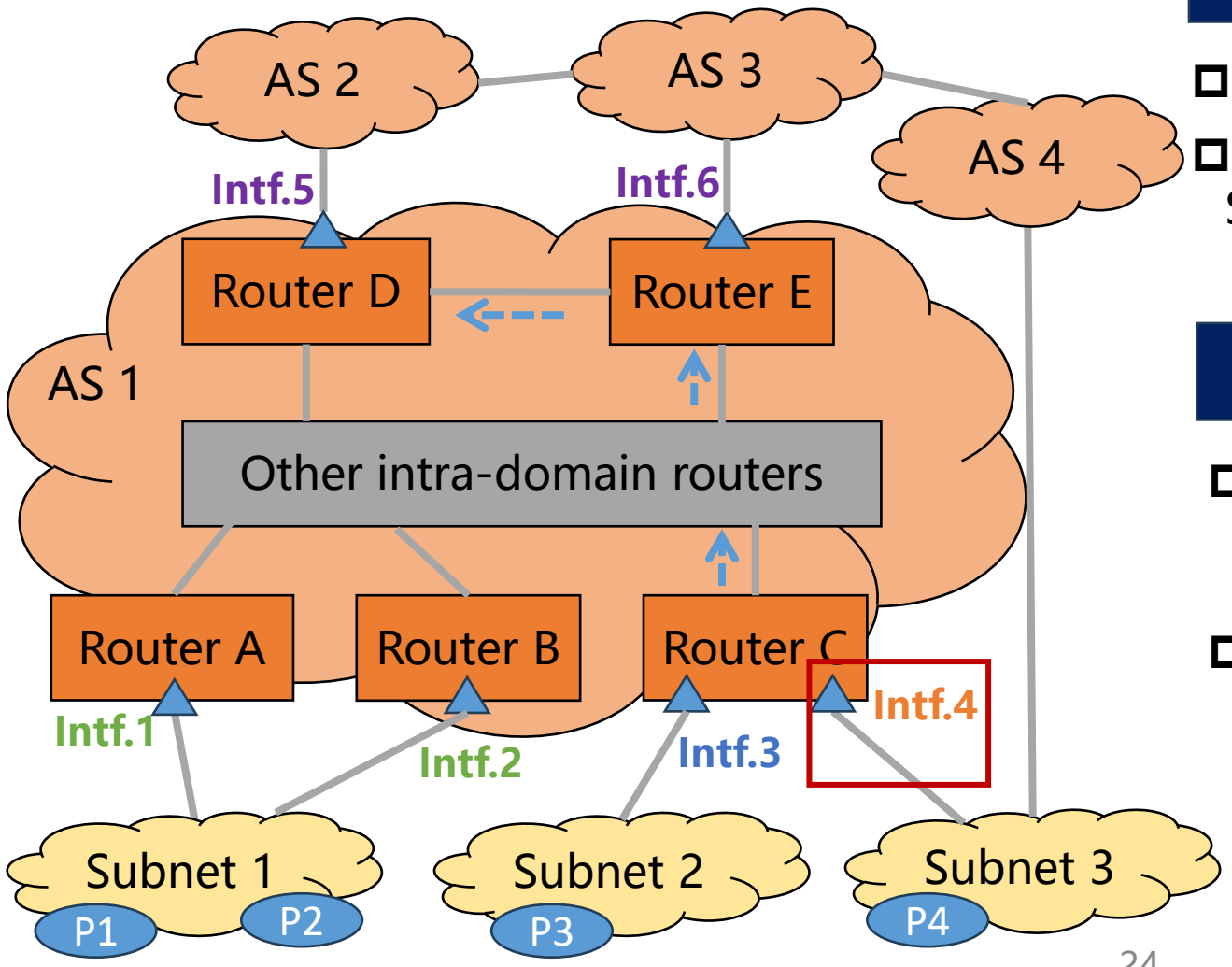
- Improve the preliminary design
  - Your comments and suggestions are welcome
- Collaboration is welcome!

Thanks!

# Backup

# Example #4

SPA message of Router C: [P4, IMI, 3]




## Scenario

- Intf.4 is an Incomplete Multi-homing Interface (IMI)
- Router C learns prefix P4 through its local routes to Subnet 3
  - P4 is a multi-source prefix

## SPA Procedure

- SPA message generation
  - SPA message of Router C
    - [source prefix: P4, Interface Type: IMI, Subnet Tag: 3]
- SAV rule generation
  - P4 should not be added in the prefix blocklist at Intf.4, Intf.5, and Intf.6