# Intra-domain SAVNET Architecture

draft-li-savnet-intra-domain-architecture-00

@IETF 115 SAVNET WG

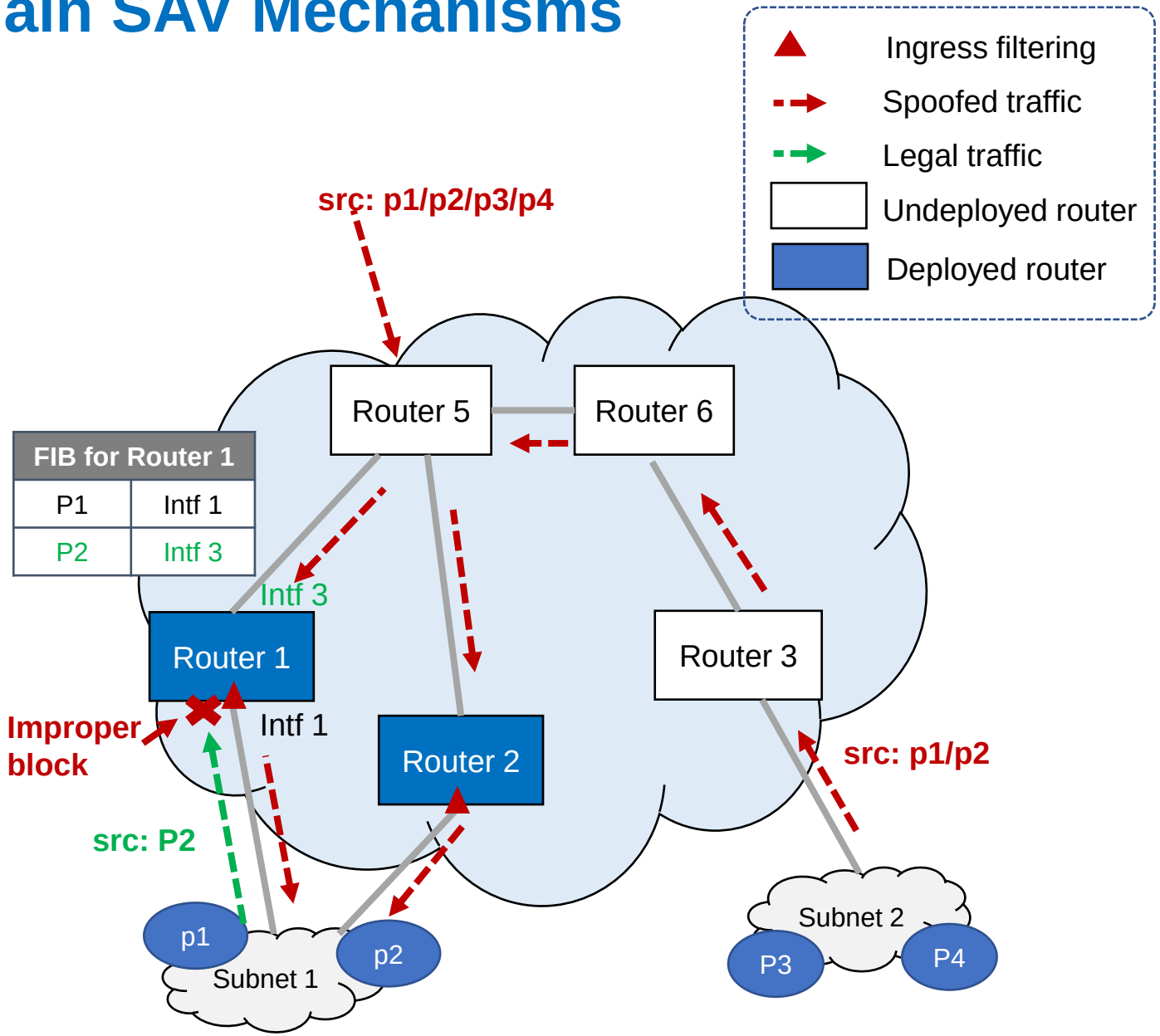
D. Li, J. Wu, L. Qin, **F. Gao**, N.Geng, T. Zhou

# Agenda

- Goals and Requirements
- SAVNET Core Workflow
- Effect of SAVNET Implementation

# Problems of Existing Intra-domain SAV Mechanisms

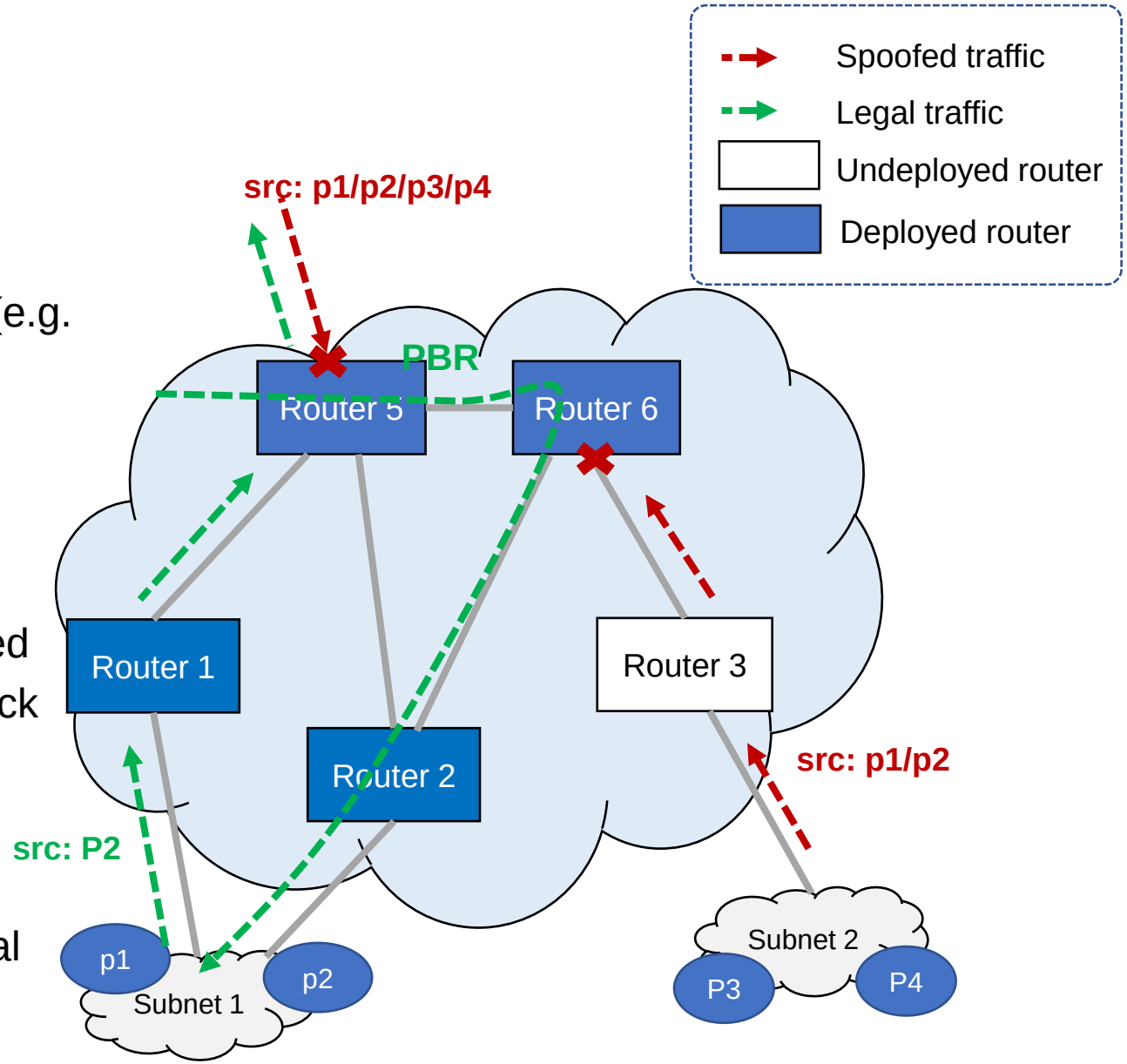
- **Inaccurate validation:**
  - **Improper block** under asymmetric routing scenario
- **Limited protection:**
  - Failing to block spoofed traffic from **outside AS and undeployed edge routers**
- **High operational overhead:**
  - ACL–based ingress filtering need **continuous manual operation** to keep accuracy.




Refer to: draft-li-savnet-intra-domain-problem-statement

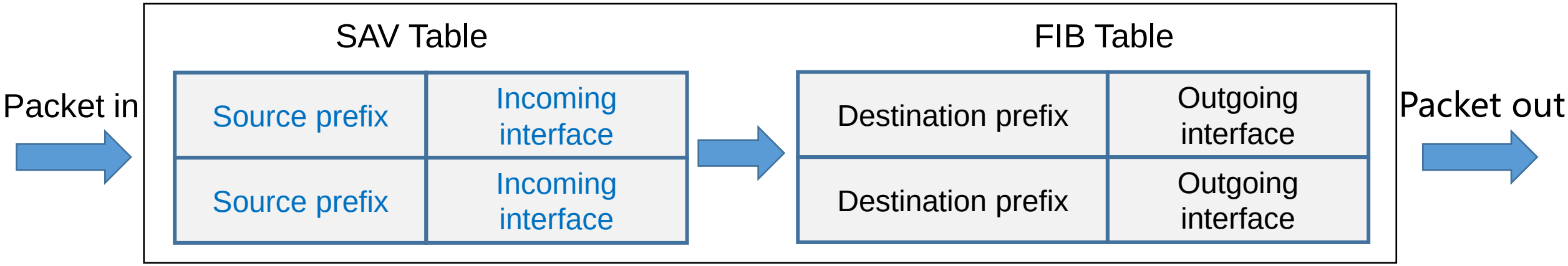
# Goals of Intra-domain SAVNET

- **Accurate SAV:**
  - **Avoid improper block** under asymmetric routing(e.g. Multi-homing, PBR, bidirectional IGP Cost)
- **All-direction protection:**
  - Validate traffic from **all directions**
  - Work at more routers to block intra-domain spoofed traffic as **close to the source** as possible and block spoofed traffic from **outside AS**.
- **Acceptable overhead:**
  - **Reduce the configuration** complexity and manual operation cost



# Key Ideas of Intra-domain SAVNET

- Generate an independent and accurate SAV table in each router, which follows the real data-plane forwarding path
  - Discover the real data-plane forwarding path via hop-by-hop notification, and generating SAV rules along the path
    - Each router learns the real incoming interfaces for source prefixes of other routers
- Data-plane SAV
  - Validate packets received from all directions based on local SAV table
  - Protect source addresses of deployed area from being forged



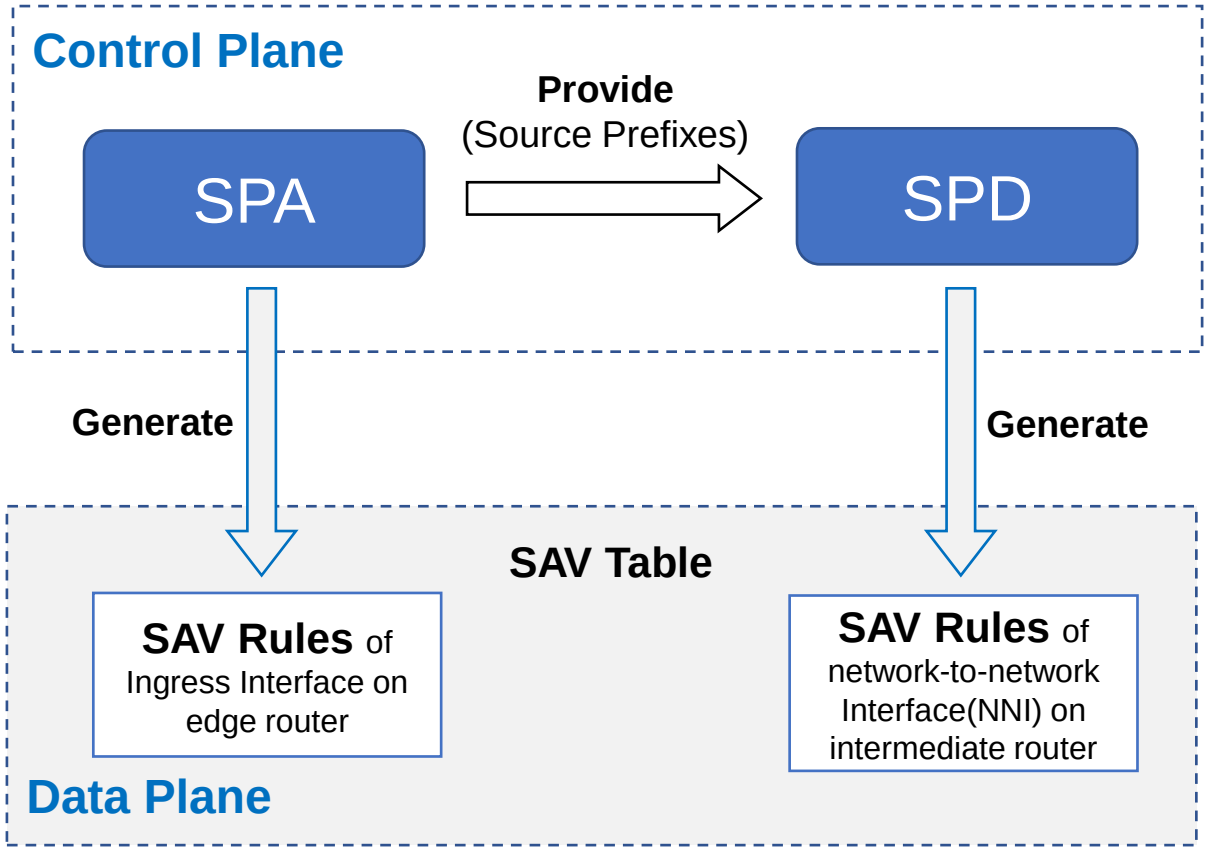
# Overall Architecture of Intra-domain SAVNET

## ➢ Control Plane

- **Source Prefix Advertisement (SPA)**
  - › Obtain complete local source prefixes
  - › Support to generate SAV rules on edge routers
  - › Support SPD to generate SAV rules
- **Source Path Discovery (SPD)**
  - › Identify accurate incoming interfaces for source prefixes by discovering real data-plane forwarding paths
  - › Generate SAV rules on intermediate routers

## ➢ Data Plane

- Validate the authenticity of source IP addresses of received packets by querying local SAV table




**More scenarios, All directions, Automation.**

# Step1: Source Prefix Advertisement (SPA) Procedure

## ➢ Target

- Obtaining the complete source prefixes set of origin routers;

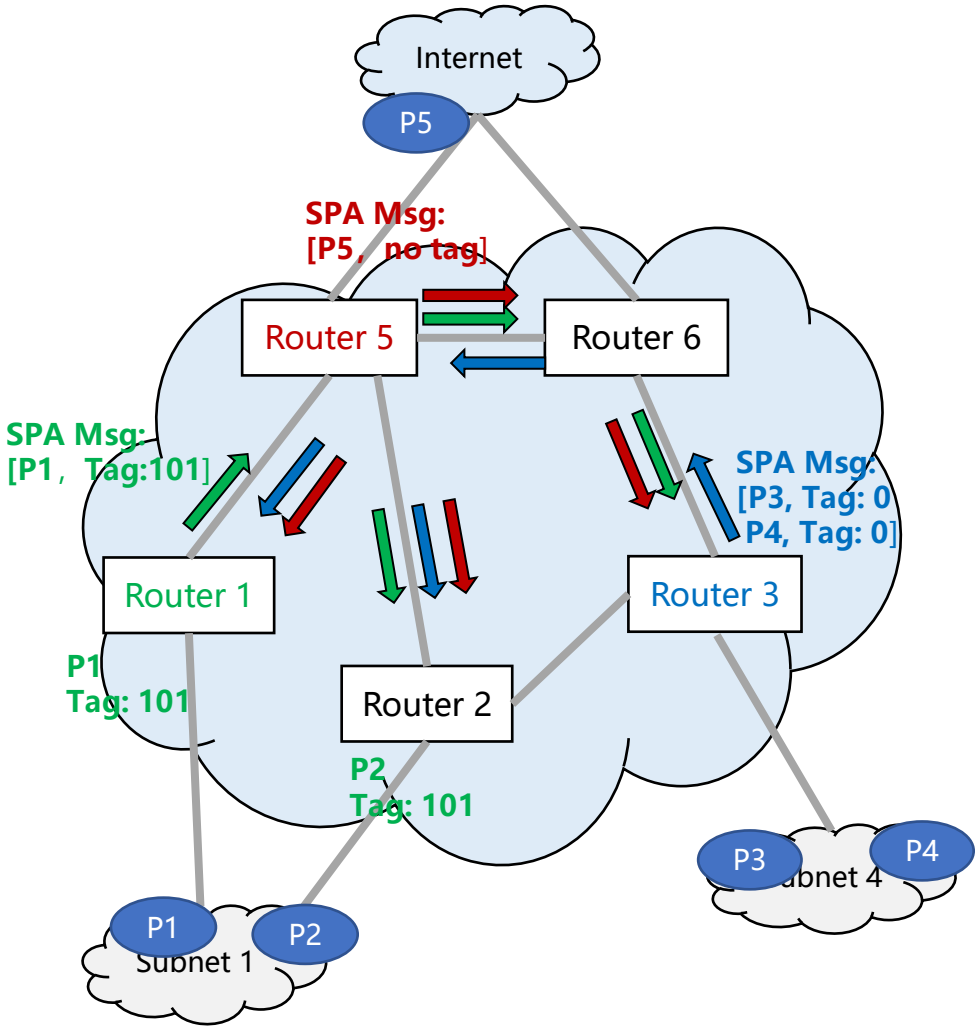
## ➢ SPA process:

- Set tags for ingress interfaces; e.g. **Multi-homing** interfaces will take the **same tag** value;
- A router **advertises** its **source prefixes** to all other routers;
- All **other routers** know source prefixes of the origin router through SPA, and build an **association mapping** table.

## ➢ Result: Association Map

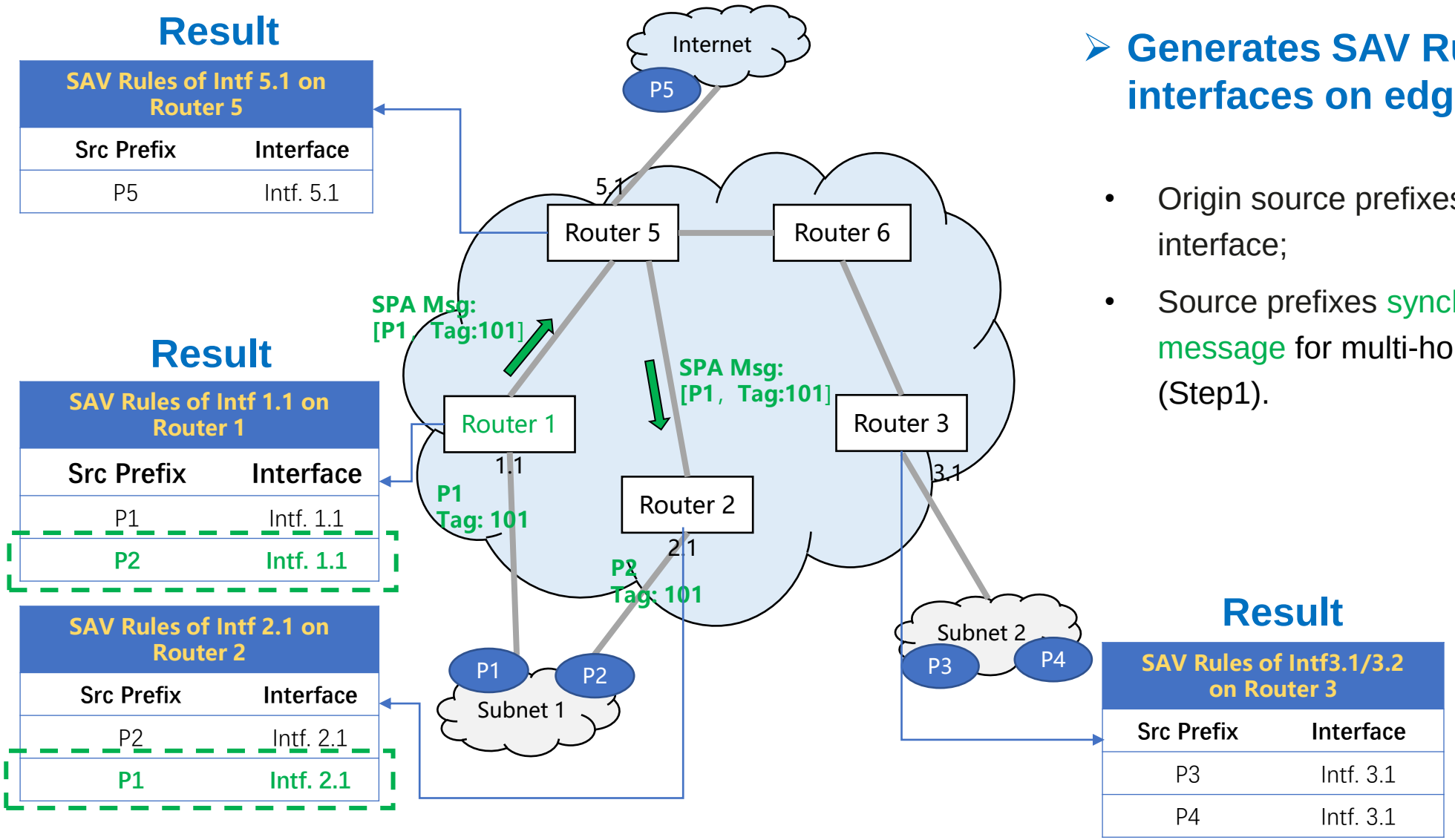
| Router-ID | Src Prefix |
|---|---|
| Router1 | P1 (tag 101) |
| Router2 | P2 (tag 101) |
| Router3 | P3,P4 |
| Router5 | P5 |

Multi-homing




**Multi-homing** interfaces will use the tag as an identifier for **source prefixes synchronization.**

# Step2: SAV Rule Generation of Ingress Interfaces




## ➢ Generates SAV Rules of ingress interfaces on edge router:

- Origin source prefixes belong to the interface;
- Source prefixes synchronized by SPA message for multi-homing scenario (Step1).

# Step3: Source Path Discovery (SPD) Procedure

## ➢ Main Idea

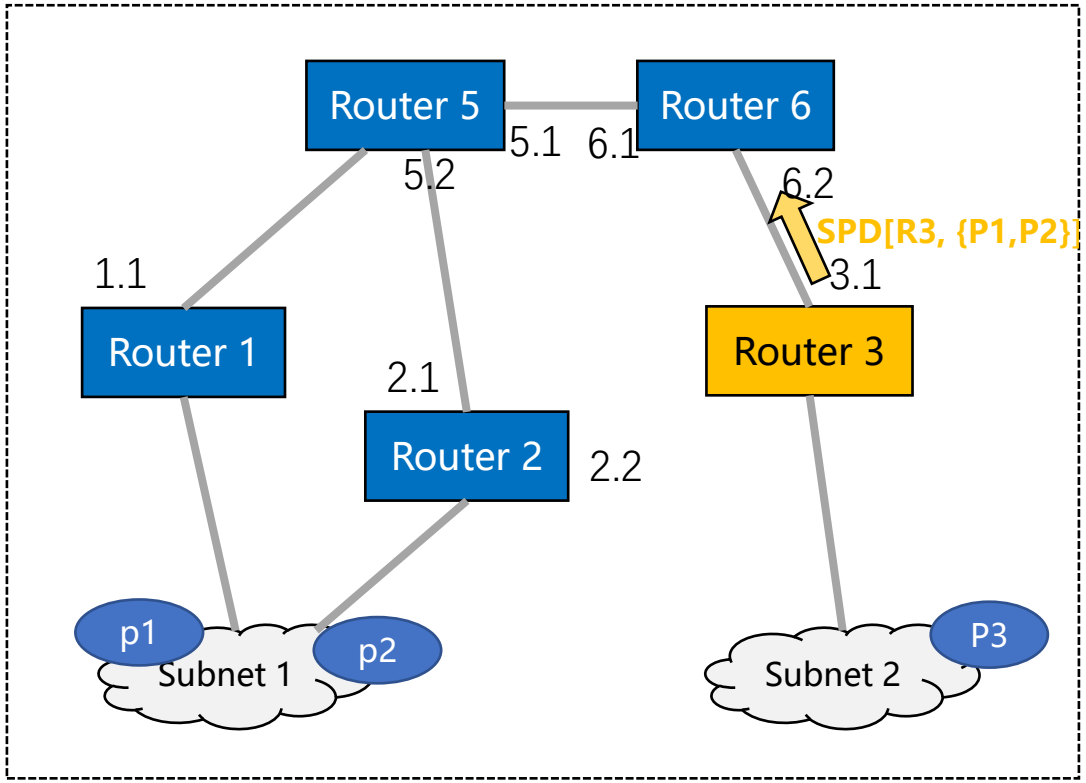
- Routers send SPD messages on preferred path according to **real data-plane** information;
- Routers know **the incoming directions** of origin source prefixes through received SPD messages and mapping table in Step 1.

➢ Each router conducts these **3 operations**:

1. **SPD origination**
2. **SPD relaying or termination**
3. **SAV rule generation**

During SPD procedure, all factors affect forwarding path(e.g. FIB forwarding, PBR ) will determine the direction of SPD Message .

## 1. SPD Origination



# Step3: Source Path Discovery (SPD) Procedure

## ➢ Main Idea

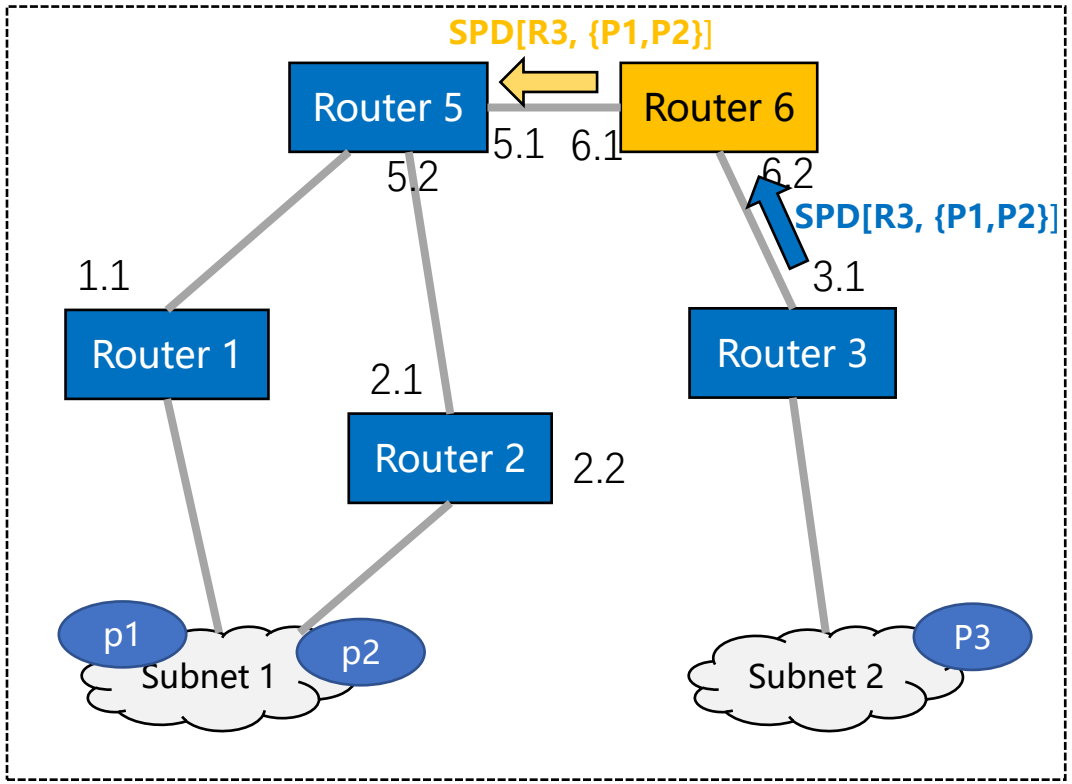
- Routers send SPD messages on preferred path according to **real data-plane** information;
- Routers know **the incoming directions** of origin source prefixes through received SPD messages and mapping table in Step 1.

➢ Each router conducts these **3 operations**:

1. **SPD origination**
2. **SPD relaying or termination**
3. **SAV rule generation**

During SPD procedure, all factors affect forwarding path(e.g. FIB forwarding, PBR ) will determine the direction of SPD Message.

## 2.1 SPD Relaying




## 3.Result

Rroutr6-SAV Rule Generation:
<source prefix: P3, incoming Intf. :6.2>

# Step3: Source Path Discovery (SPD) Procedure

## ➢ Main Idea

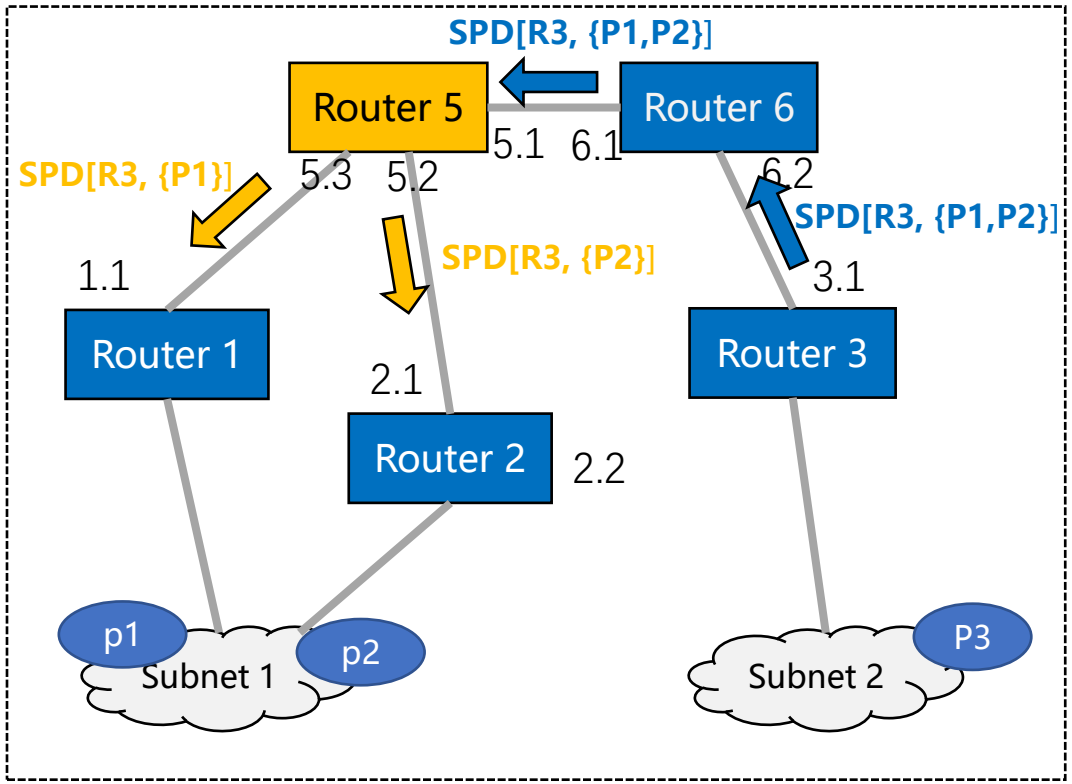
- Routers send SPD messages on preferred path according to **real data-plane** information;
- Routers know **the incoming directions** of origin source prefixes through received SPD messages and mapping table in Step 1.

➢ Each router conducts these **3 operations**:

1. **SPD origination**
2. **SPD relaying or termination**
3. **SAV rule generation**

During SPD procedure, all factors affect forwarding path(e.g. FIB forwarding, PBR ) will determine the direction of SPD Message.

## 2.2 SPD Relaying




## 3.Result

Rroutr5-SAV Rule Generation:
<source prefix: P3, incoming Intf. :5.1>

# Step3: Source Path Discovery (SPD) Procedure

## ➢ Main Idea

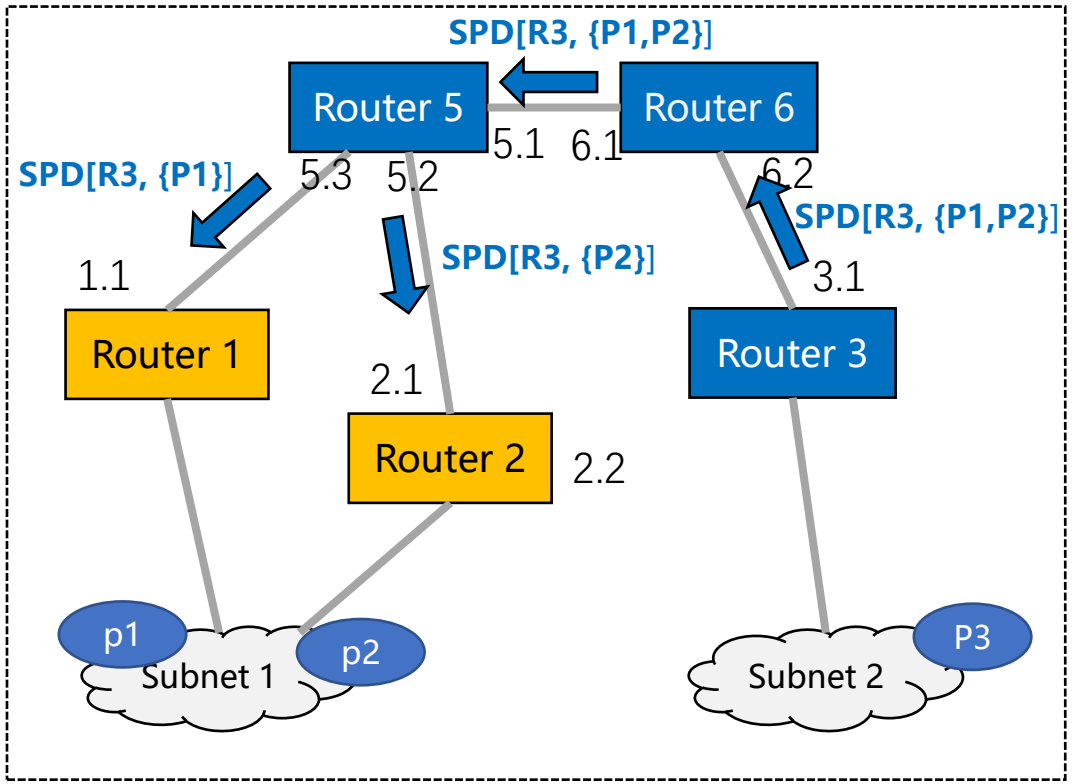
- Routers send SPD messages on preferred path according to **real data-plane** information;
- Routers know **the incoming directions** of origin source prefixes through received SPD messages and mapping table in Step 1.

➢ Each router conducts these **3 operations**:

1. **SPD origination**
2. **SPD relaying or termination**
3. **SAV rule generation**

During SPD procedure, all factors affect forwarding path(e.g. FIB forwarding, PBR ) will determine the direction of SPD Message.

## 2.3 SPD Termination




## 3.Result

Rroutr1-SAV Rule Generation:
Router1:<source prefix: P3, incoming Intf. :1.1>
Rroutr2-SAV Rule Generation:
Router2:<source prefix: P3, incoming Intf. :2.1>

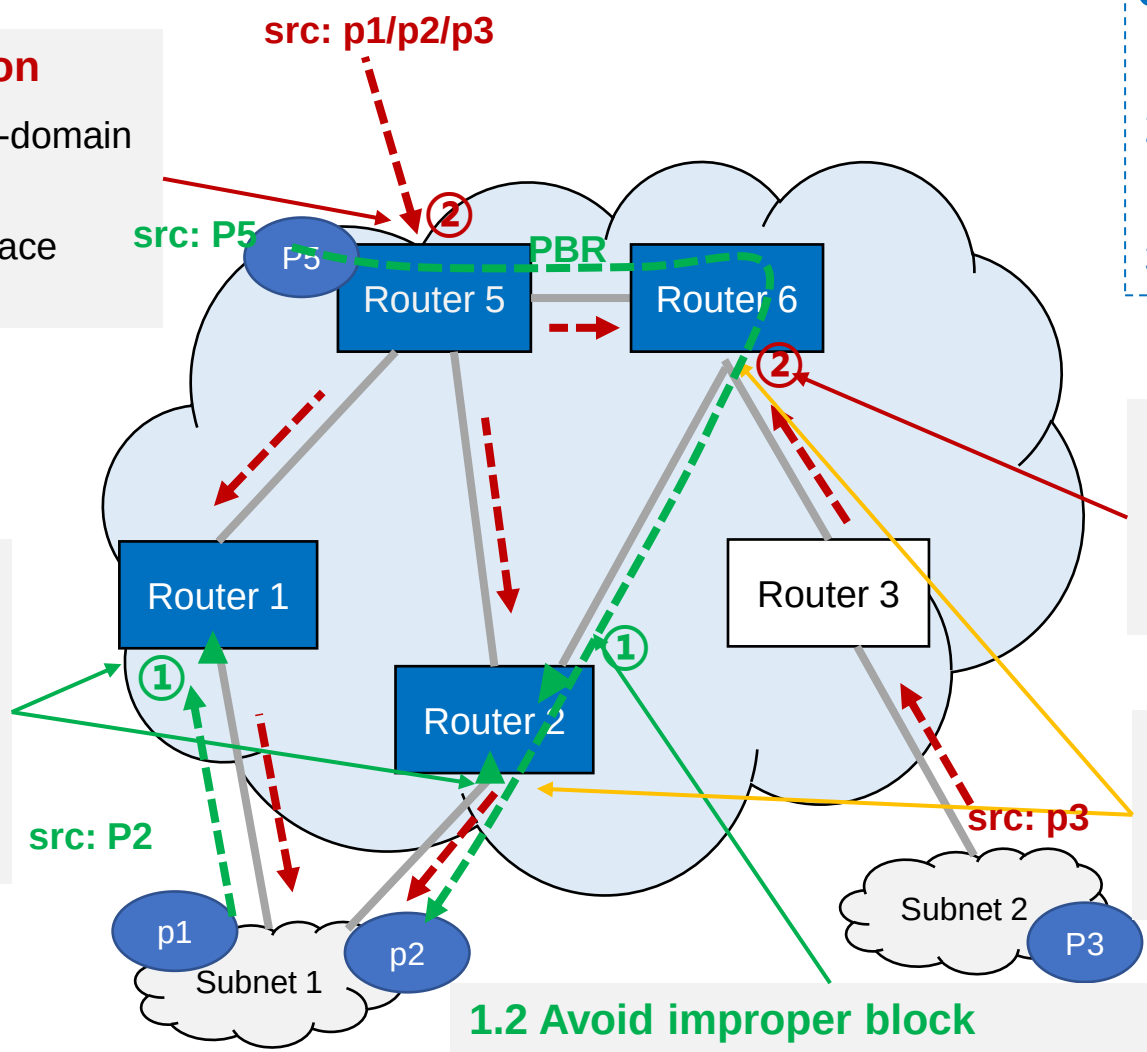
# Comparison between SAVNET and Existing SAV Mechanisms

## 2.1 Work on inbound direction

- Generate **SAV rules** for intra-domain source prefixes by SPD
- Mode 3[1]: Prefix-based interface allowlist

## 1.1 Avoid improper block

- **Multi-homing**: Generates complete **SAV rules** interfaces by SPA
- Mode 1[1]: Interface-based Prefix allowlist




## SAVNET Benefit:

1. Apply to more scenarios;
2. Protect deployed area from spoofing attacks on all direction;
3. Generate SAV rule dynamically.

## 2.2 Work on NNI[2] interfaces

- Generate **SAV rules** on **NNI interfaces** to prevent spoofing from **non-deployed** routers by SPD

## 3 Reduce implement complexity

- Generate and update **SAV rules dynamically by SPA&SPD**

## 1.2 Avoid improper block

- Get legitimate **Incoming interface** basing on **PBR** by SPA

[1]:Source Address Validation Table Abstraction and Application
[2] NNI: Network-to-Network interface

# Convergency Consideration

## ➢ Convergency Principle:

- Fast new SAV rule installing and slow SAV rule removing.

## ➢ Basic Mechanism

- Periodic Update: SPD are generated periodically.
- Aging Mechanism: SAV rules expires with aging mechanism.

## ➢ Fast Convergency Mechanism

- Triggered Update: When awarding route state changes, new SPA or SPD messages are generated.
- FRR Deployment: When IP-FRR is deployed, SAVNET sends SPD messages to the backup forwarding paths in advance , backup SAV rules are generated before failures .

# Incremental Deployment principle

## ➢ Device Capability:

- Recommend to preferentially deploy on **higher capability** device to achieve more effective SAV, then expand to **relatively low capability** device gradually;
- Recommend to preferentially deploy in **aggregation and core layer**, then expand to **accessing layer** gradually;

## ➢ IGP Scenario:

- Recommend to deploy intra-domain SAVNET in **backbone area**(Area-0 of OSPF or Level-2 of ISIS) as the first step.
- Expanding the deployment area hop by hop in the **non-backbone area**.

# Conclusion

- **Goal**: Generates accurate SAV rules dynamically at interfaces of all directions
  - Avoid improper block, minimize improper permit, validating on all direction and reducing implement cost.
- **SPA**: Origin router advertise source prefixes to other routers
  - Original router obtains accurate and complete source prefixes on access interface
- **SPD**: Each router forwards the message according to real data-plane
  - Each router gets accurate and complete incoming directions of source prefixes.
- **SAV Mode:** Executes different actions for “unknown[1]” packet .
  - Avoid improper block by adopt applicable mode for interface based on the completeness of prefixes achievements.
- The architecture is **protocol-independent**. Extensions of routing protocols are not the focus of this document.

[1]:Source Address Validation Table Abstraction and Application

# Thank you!

- Backup

# One More Thinking: Comparison with SAVE

- Main idea of SAVE: Each router  generate an individual protocol message for each destination prefix in the local FIB table;

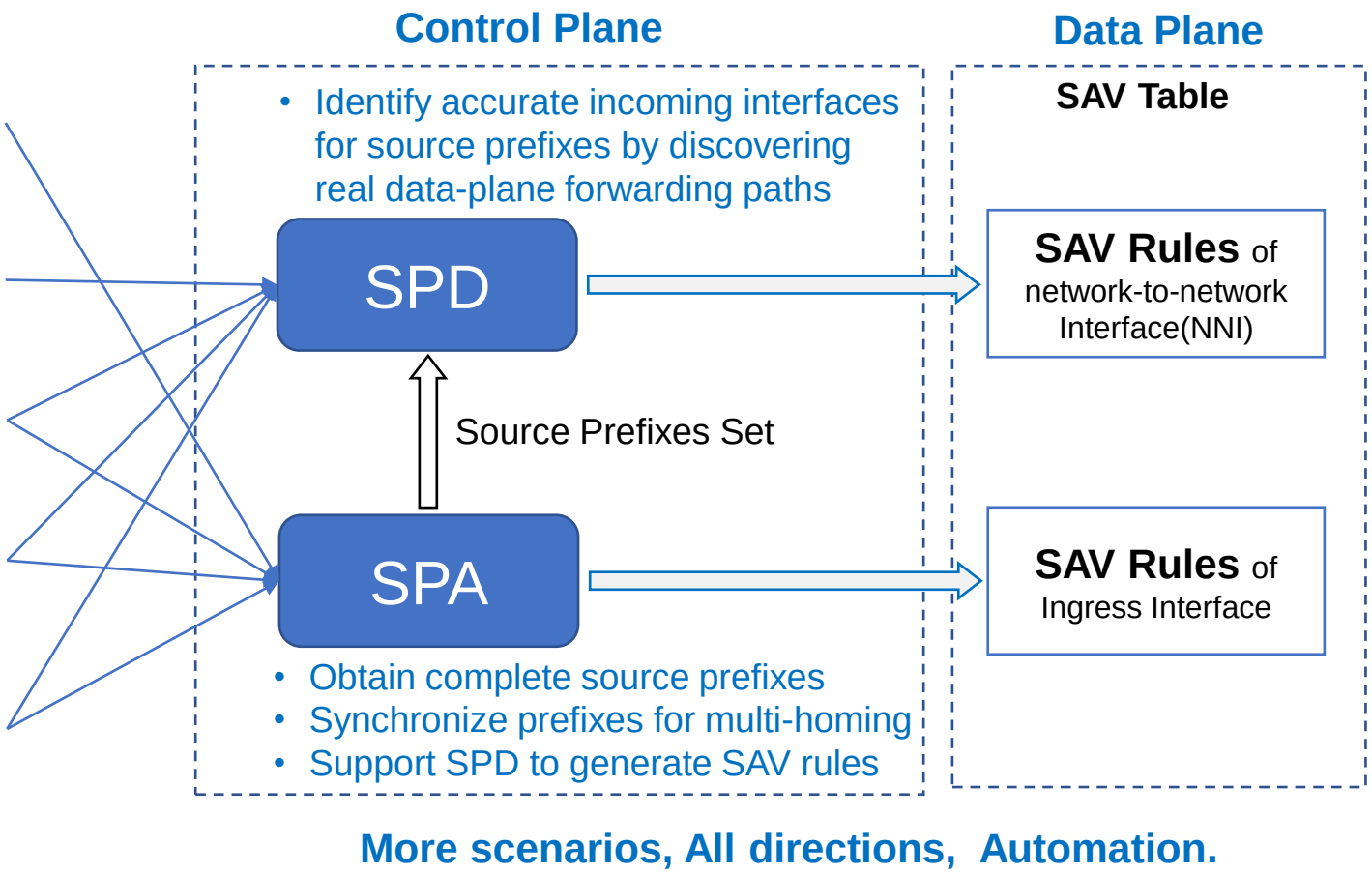
| | SAVE | SAVNET |
|---|---|---|
| **Mechanism** | A pure data plane mechanism. SAVE generates detection messages on forwarding plane.(similar as a Ping plus mechanism) | A control plane mechanism basing on SPA and SPD, which is takes all forwarding facts into consideration. |
| **Scalability** | SAVE generates an individual protocol message for each destination prefix in the local FIB table ,which will induce a large number of protocol messages. | SAVNET contains multiple destination prefixes in each protocol message and thus a router only needs to generate one protocol message to each neighboring router |
| **Accuracy** | Limitation on scenarios: ECMP, PBR.<br>SAVE cannot cover the 5-Tuple of real packet:<br>• ECMP scenario: The intermediate router forwards message to only one next hop;<br>• PBR scenario: SAVE messages only cover the Dst-IP, and it fails to take effect when ACL matches other tuples . | In SPD procedure, control plane collects all possible forwarding paths according to forwarding plane information.<br>SAVNET could generate SAV rules in ECMP and PBR scenario; |

# Challenges and Key Ideas to Narrow the Gaps

## Challenges

- Get **Complete** source prefixes of **multi-homing** scenarios
- Discover incoming interfaces under **asymmetric routing** scenarios
- Validation on **all directions**
- Block spoofing traffic from **non-deploying edge** router
- Generates SAV rules **dynamically** based on changes

## Key Idea

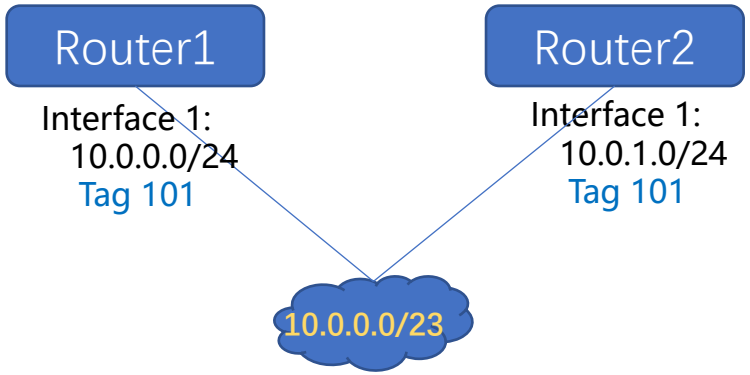


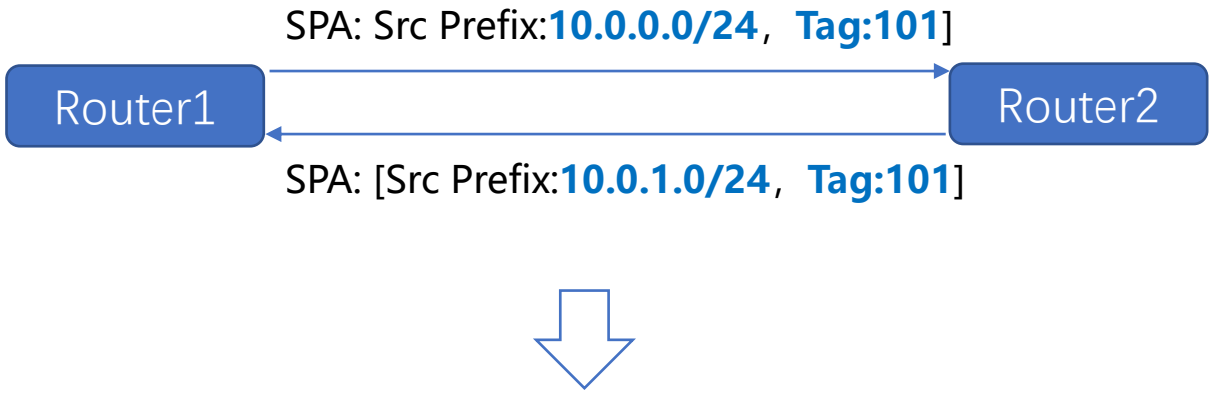

**More scenarios, All directions, Automation.**

**SPA:** Source Prefix Advertisement; **SPD:** Source Path Discovery.

# Local Source Prefixes Identification(2)

**Multi-homing scenario**




| SAV Table on Router 1 | |
|---|---|
| **Src Prefix** | **Interface** |
| 10.0.0.0/24 | Intf. 1 |
| 10.0.1.0/24 | Intf. 1 |

| SAV Table on Router 2 | |
|---|---|
| **Src Prefix** | **Interface** |
| 10.0.0.0/24 | Intf. 1 |
| 10.0.1.0/24 | Intf. 1 |

**SAVNET steps for Source prefixes Synchronization:**

① Configure the **same Tag value 101** on multi-homing interface of both Router1 and Route 2;

② Router1 sends **SPA message** for [Source prefix:10.0.0.0/24] **with [Tag:101];**

③ Route2 receives SPA messages and **identifies** the [Source prefix:10.0.0.0/24] from Route1 **take the same Tag** value with local interface 1, Router 2 considers [10.0.0.0/24] as one of its local source prefixes;

④ Route 2 **generates SAV rule locally** for [Source prefix:10.0.0.0/24], and take interface 1 as the legal incoming interface.

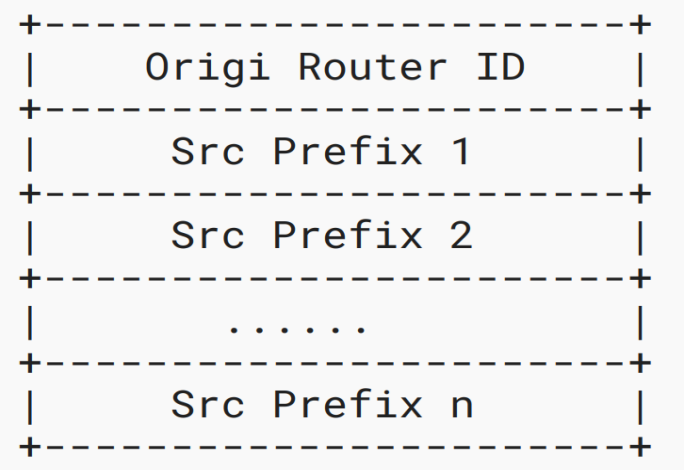
# SPA Message(1)

**SPA message is used to advertise the relationship between source prefixes and router IDs.**

- Normally, **SPA message for single-homing** access scenario has two main fields:

I. **Origin Router ID:** This field contains the router ID of the origin router.

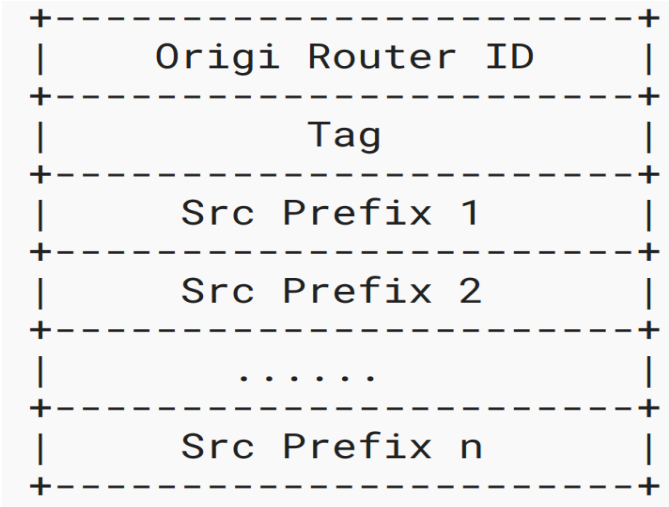
II. **Src Prefix:** This field contains a list of local source prefixes of the origin router.




**SPA Message**

# SPA Message(2)

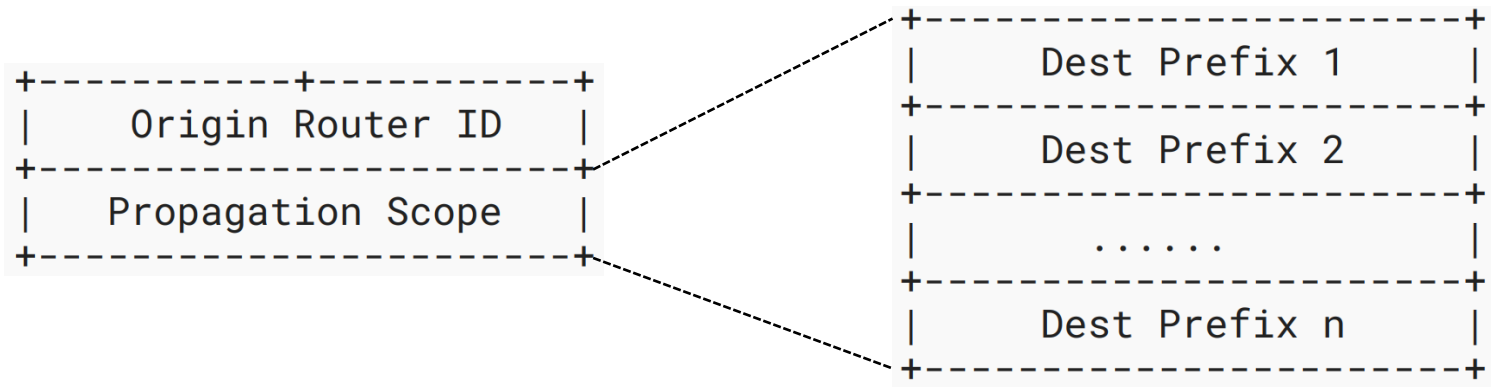
- The **extended SPA message for multi-homing** source prefixes synchronization has three main fields:
  - **I. Origin Router ID:** This field contains the router ID of the origin router.
  - **II. Tag:** This field contains a tag value configured for a directly connected subnet.
  - **III. Src Prefix list:** This field contains a list of local source prefixes learned from the interface configured with the tag value.




**Extended SPA Message**

# SPD Message

- **SPD message** is used to discover the real forwarding data-plane path from the source and generate SAV rules in routers along the path. It consists of two main fields:
  I. **Origin Router ID:** This field contains the router ID of the origin router and remains unchanged. This field is used to generate SAV rules of SAV tables.
  II. **Propagation Scope:** This field contains a list of destination prefixes which take the neighboring router as the next hop (from FIB) and changes hop by hop. This field is used to discover the real data-plane forwarding path.

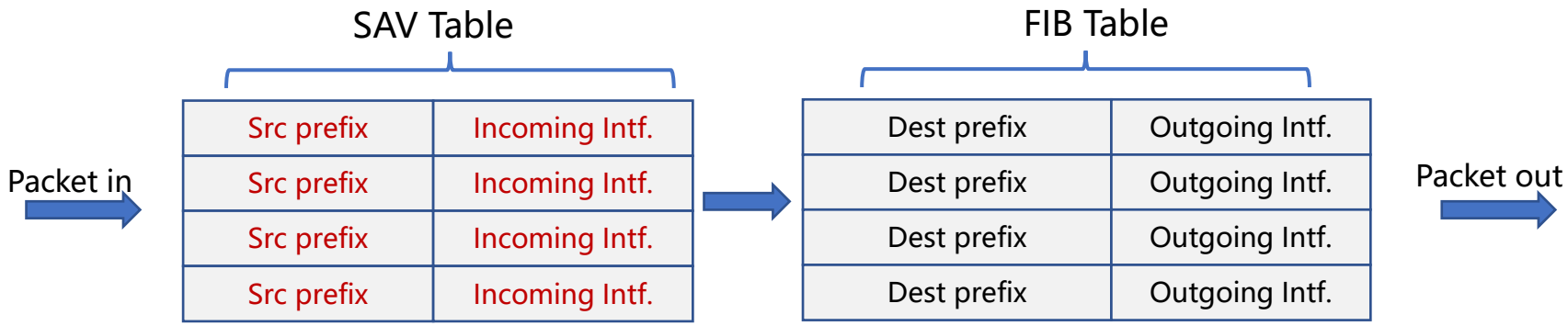



**SPD Message**

# SAV Table

## Traffic Forwarding Procedure

**Perform SAV before FIB lookup**




## SAV Table Structure

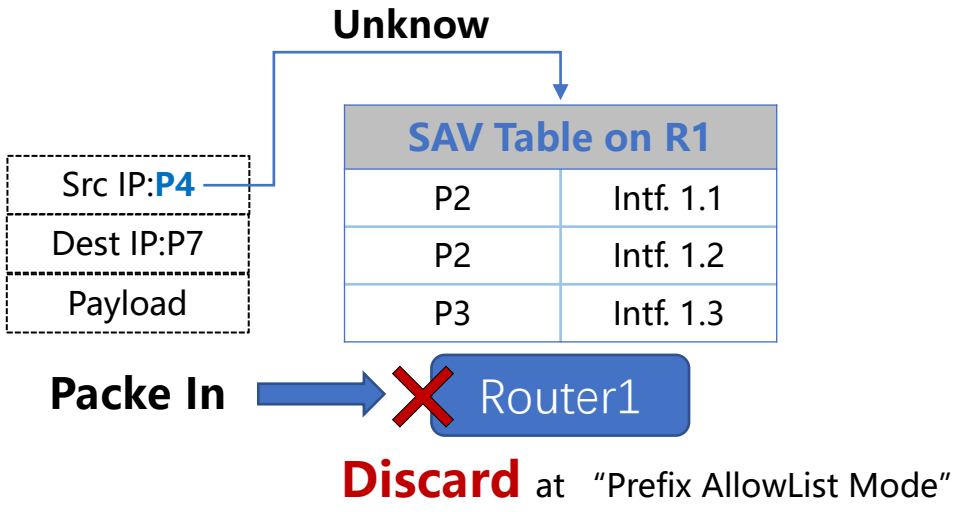
| Source prefix | Incoming interface |
|---|---|
| P1 | Intf.1 |
| P2 | Intf.2, Intf.3 |
| P3 | Intf.4 |

### Validity States:

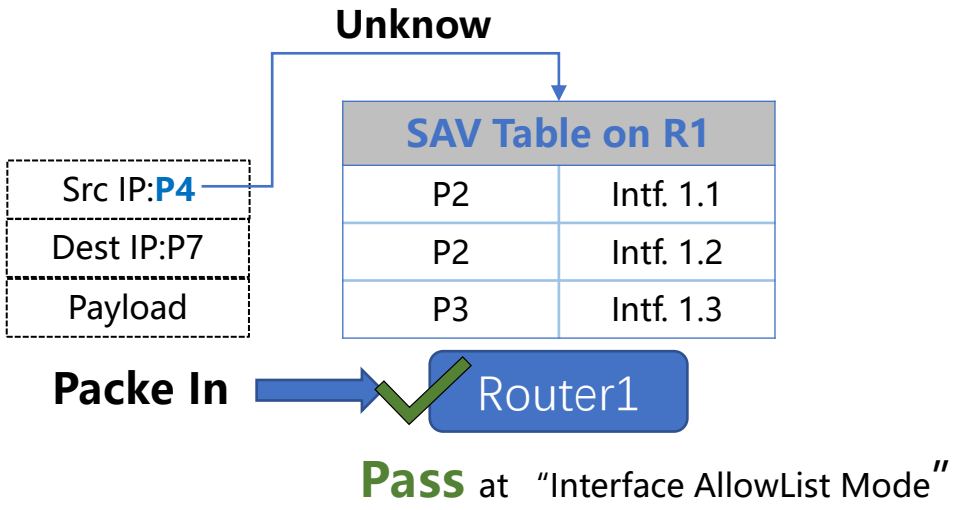
- **Valid** :a source prefix and a valid incoming interfaces both matched, **execute action "Pass";**
- **Invalid** : source prefix existed, but incoming interface of the packet does not match, **execute action "Drop";**
- **Unknown** : no source prefix existed in SAV table, **action executing depends on the "Validation Mode".**

# SAV Mode

- **Prefix Allowlist Mode**: Block any packets whose source addresses are not included in the allowlist of the interface
  - **"Unknown" packets are discarded**
  - Only adopted when the SAV table has determined all acceptable source prefixes for the specific interface.
  - Suitable to the interfaces connecting to a subnet
  - Corresponds to "Mode 1" in draft-XX-savnet-sav-table-mode




- **Interface Allowlist Mode**: Check whether the packets with specific source addresses arrive at expected interfaces
  - **"Unknown" packets are passed**
  - Adopted when the SAV table does not determine all acceptable source prefixes for the specific interface
  - Suitable to the interface with a default route or the interface connecting to the another AS can hardly promise to know all the legal source prefixes
  - Corresponds to "Mode 3" in draft-XX-savnet-sav-table-mode



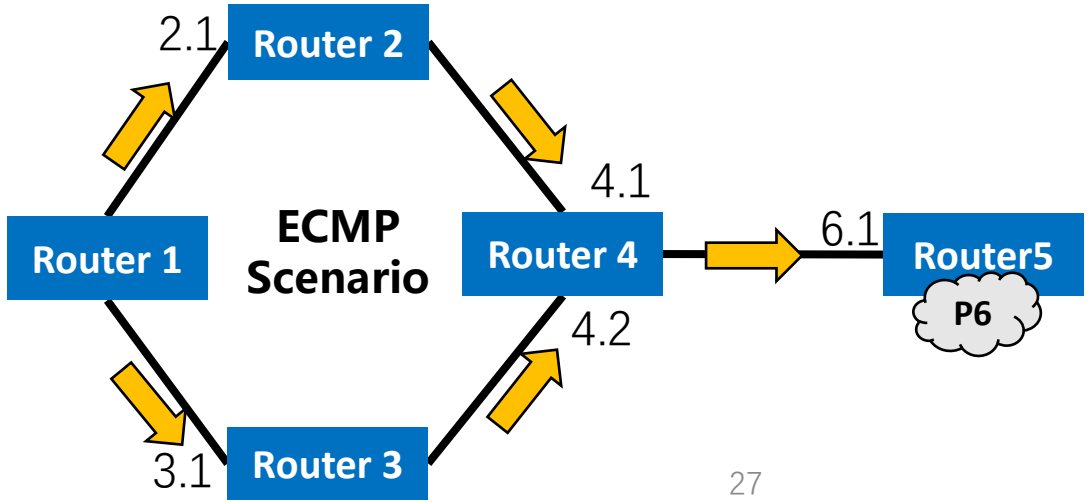
# Accuracy(1)—FIB Forwarding

## FIB Forwarding with a single next hop

- SPD message determine the single next hop based on destination IP-prefix, as demonstrated in [section: Core workflow]

## ECMP/UCMP

- SPD message must be sent to all these next hops
- SAV rules generates on each ECMP、UCPM path



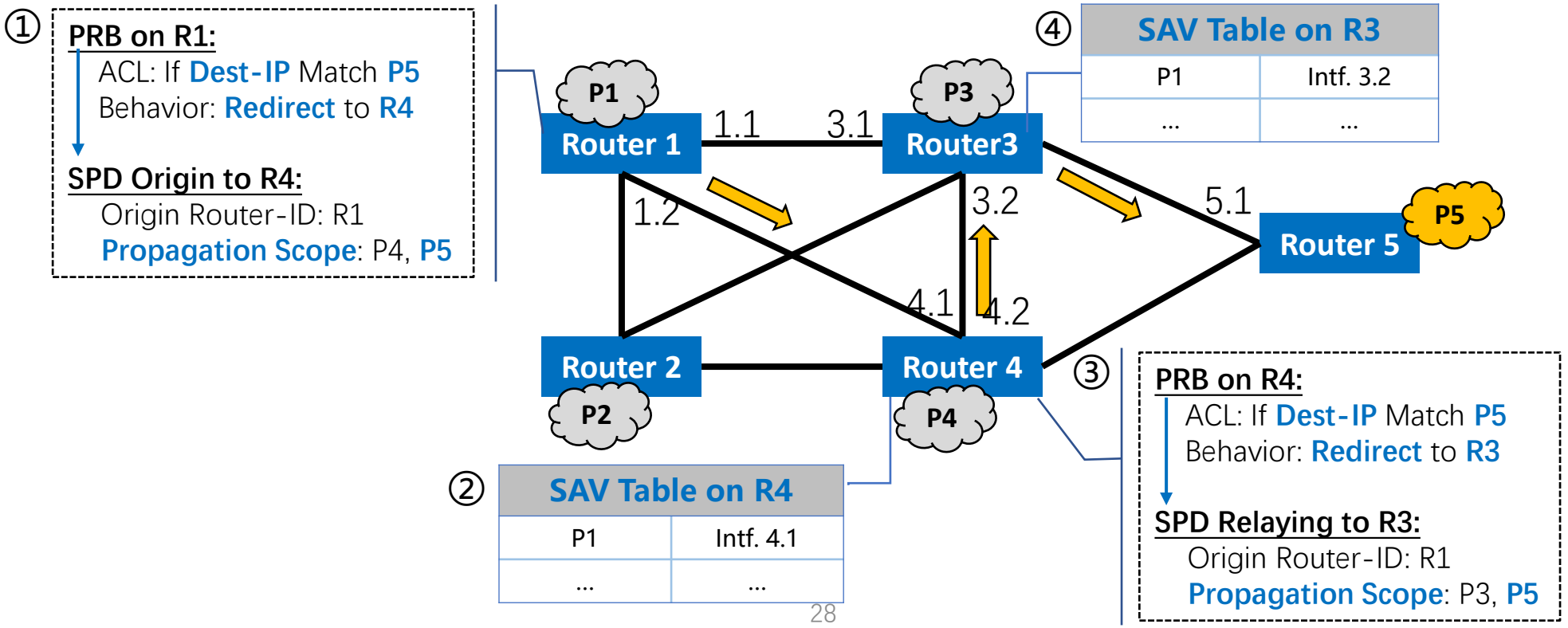


27

# Accuracy(2)—PBR Scenario

## PBR with ACL rule matching Dest-IP:

- **SPD Origination** : SAVNET adds the matched destination prefix into the propagation scope of the original SPD message sent to the redirected next hop;
- **SPD Relaying** : SAVNET adds the matched destination prefix into the propagation scope of the relaying SPD message sent to the redirected next hop.





28

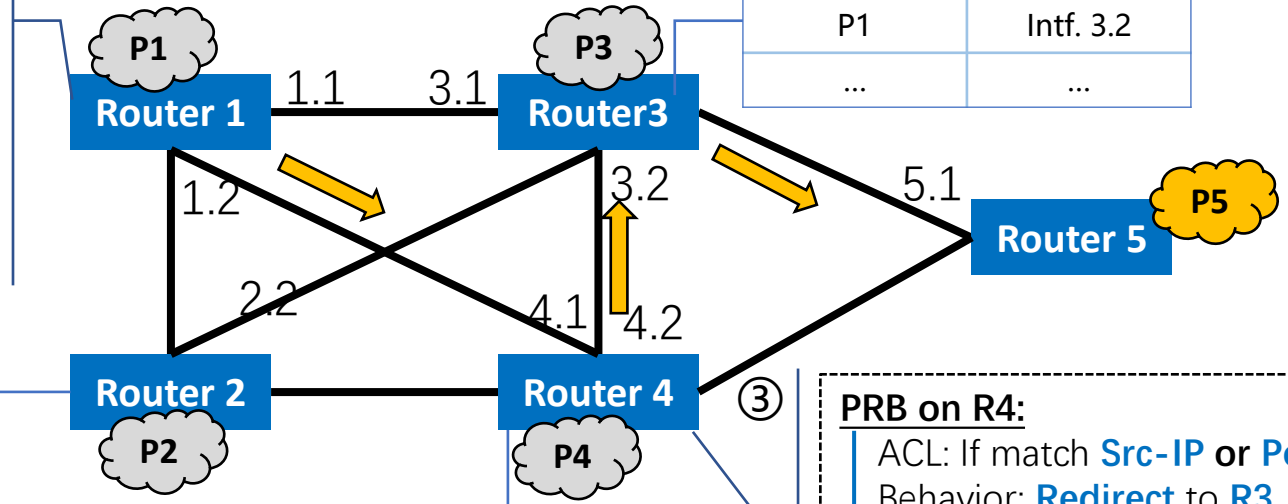
# Accuracy(2)—PBR Scenario

## ☐PBR with ACL rule **not** matching Dest-IP:

- **SPD Origination** : SAVNET adds all destination prefixes in local FIB into the propagation scope of the original SPD message sent to the redirected next hop ;
- **SPD Relaying** : SAVNET adds all destination prefixes carried in the received SPD message into the propagation scope of the relaying SPD message sent to the redirected next hop .

① **PRB on R1:**
ACL: If match **Src-IP** or **Port** or **Any**
Behavior: **Redirect** to **R4**

**SPD Origin to R4:**
Origin Router-ID: R1
**Propagation Scope**: P4, **P2, P3, P5**




④ **SAV Table on R3**

| P1 | Intf. 3.2 |
|---|---|
| … | … |

**SAV Table on R2**

| P1 | Intf. 2.2 |
|---|---|
| P1 | Intf. 2.2 |
| … | … |

② **SAV Table on R4**

| P1 | Intf. 4.1 |
|---|---|
| … | … |

③ **PRB on R4:**
ACL: If match **Src-IP** or **Port** or **Any**
Behavior: **Redirect** to **R3**

**SPD Relaying to R3:**
Origin Router-ID: R1
**Propagation Scope**: P3, **P2, P5**


29

# Accuracy(3)—Tunning Scenarios

- Tunnel technologies, such as MPLS, SR-MPLS, SRv6,and GRE, are usually used for forwarding in scenario when need control the forwarding path or data transparent transmission:
  - Intra-domain SAVNET performs data-plane SAV only on routers before and after the tunnel.

    The ingress router will send an SPD message directly to the corresponding egress router based on local control-plane information of tunnel technology

  - If there is a need to perform data plane SAV for IP prefixes in IP-encapsulation tunnel (such as SRv6 and GRE), Just outer-layer IP header is validated.

    The SPD message needs to be propagated from the ingress router to the egress router hop by hop, thus generating SAV rules on routers inside the tunnel