Towards More Accurate and More Incentive Source Address Validation in the Internet

Dan Li (Tsinghua University)

Jul, 2022

Outline

□Background

□Gap Analysis & Requirement

□SAVNET Solution

□IETF SAVNET WG

SAV is Important and Challenging

□SAV (source address validation) is important

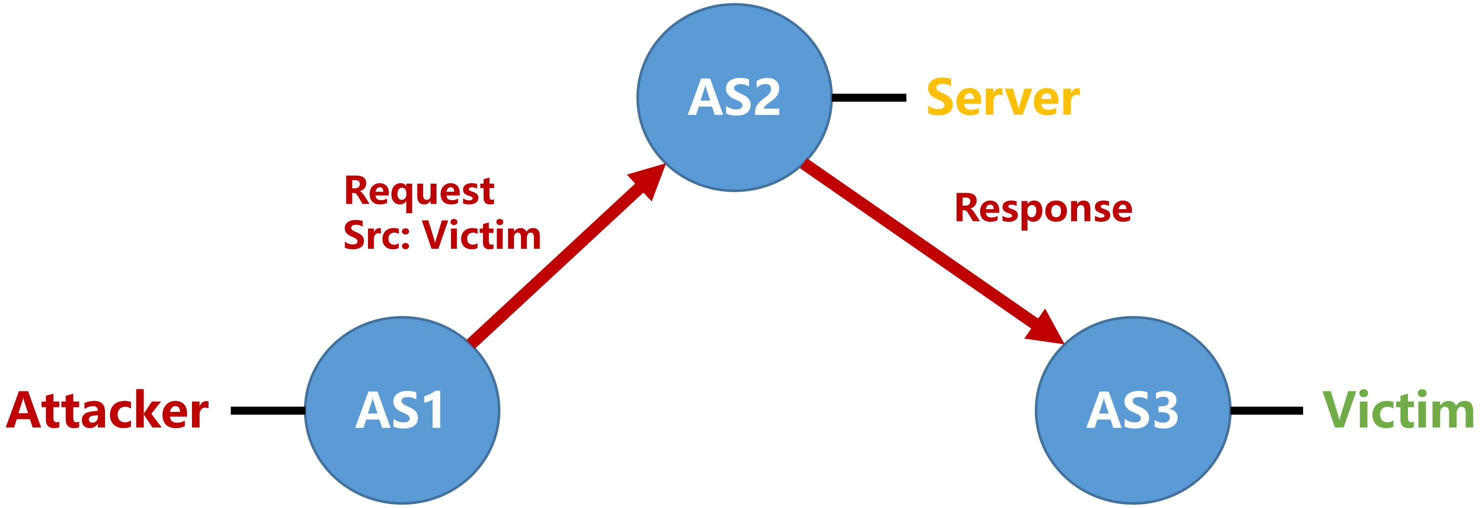
- ◆Source address spoofing leads to various malicious attacks, represented by reflective DDoS attack
- ◆Network devices deploy SAV to permit traffic with valid source address and block traffic with invalid source address
- ◆Since 2014, the MANRS initiative is calling on network operators to implement SAV as close to the source as possible

□SAV is challenging

- ◆Accuracy: avoid improper block and reduce improper permit as much as possible
- ◆incentive: when partially deployed, deployers can get benefit
- ◆Cost: the deployment cost should be affordable

Potential Attacks by Source Address Spoofing

- Most typical attack by source address spoofing: reflective DDoS



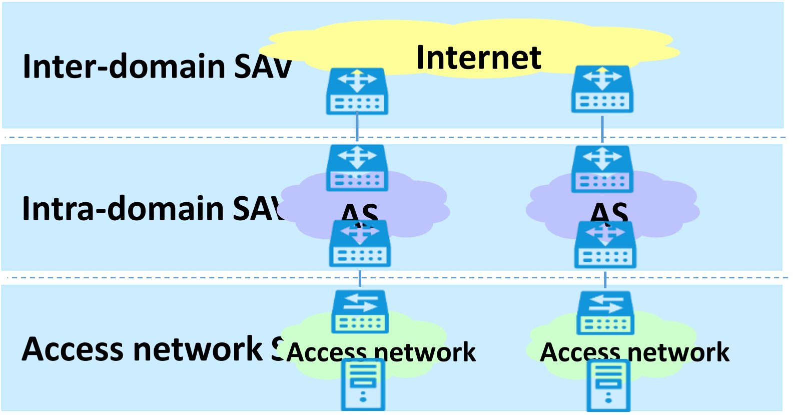
- Other potential attacks [RFC 6959]
  - Blind attacks: single-packet attacks, flood-based DoS, poisoning attacks, spoof-based worm/malware propagation, accounting subversion
  - Non-blind attacks: man-in-the-middle, third-party recon

IETF Efforts for SAV Mechanisms

SAV is a problem with long history of attention in IETF

- □Ingress filtering/ACL based SAV [RFC 2267&2827, BCP 38], Jal 1998 - May 2000
  - ◆Problem: manual configuration
- □Strict-uRPF / Feasible-uRPF [RFC 3704, BCP 84], Mar 2004
  - ◆Problem: improper block under asymmetric routing
- □Feasible-uRPF / Loose-uRPF [RFC 3704, BCP 84], Mar 2004
  - ◆Problem: improper permit
- □SAVI [RFC 6620, 6959, 7039, 7219, 7513, 8074], May 2012 - Feb 2017
  - ◆Host-level SAV in access networks (enterprise networks)
- □EFP(enhanced feasible path)-uRPF [RFC 8704, BCP 84], Feb 2020
  - ◆Mitigating the problem of strict-uRPF / feasible-uRPF in some cases

Necessity of New Intra-/Inter-domain SAV Mechanisms



- SAVA architecture [RFC 5210] divides SAV into three checking levels
  - Access-network SAV, intra-domain SAV, inter-domain SAV
- SAVI for access-network SAV is not enough
  - The number of operators for access networks is huge, so it is difficult to require all access networks to deploy SAVI
  - When some access networks do not deploy SAVI, intra-domain and inter-domain SAV can help filter spoofing traffic as close to the source as possible
- uRPF-based technology for intra-/inter-domain SAV is not enough
  - Strict-uRPF, feasible-uRPF and loose-uRPF have well-known improper block or improper permit problems
  - EFP-uRPF does not completely solve the problem

Outline

□Background

□Gap Analysis & Requirement

□SAVNET Solution

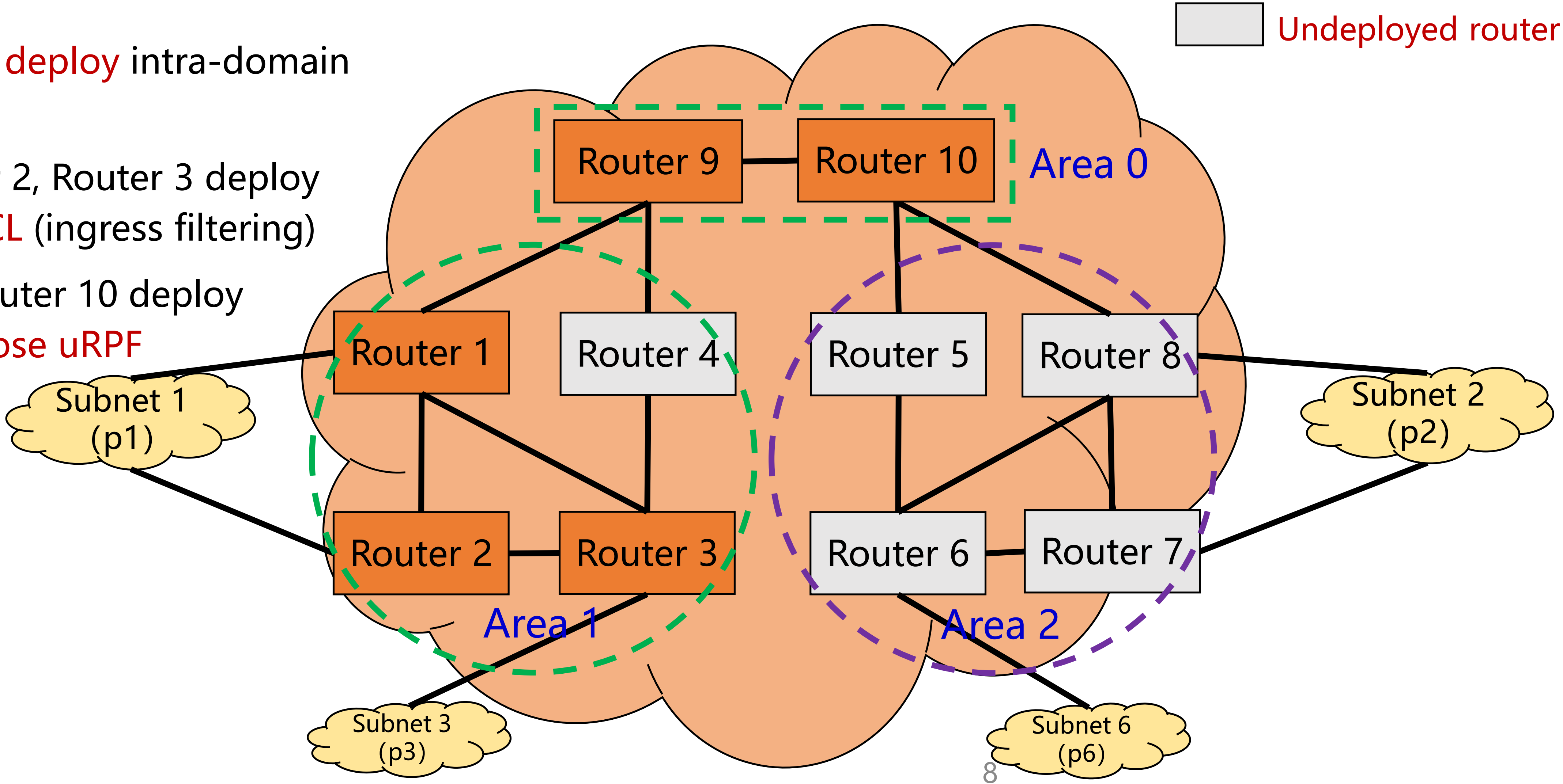
□IETF SAVNET WG

A Typical Intra-domain Scenario

- Area 0 and Area 1 deploy intra-domain SAV mechanism
- Area 2 does not deploy intra-domain SAV mechanism
- Router 1, Router 2, Router 3 deploy strict uRPF or ACL (ingress filtering)
- Router 9 and Router 10 deploy strict uRPF or loose uRPF

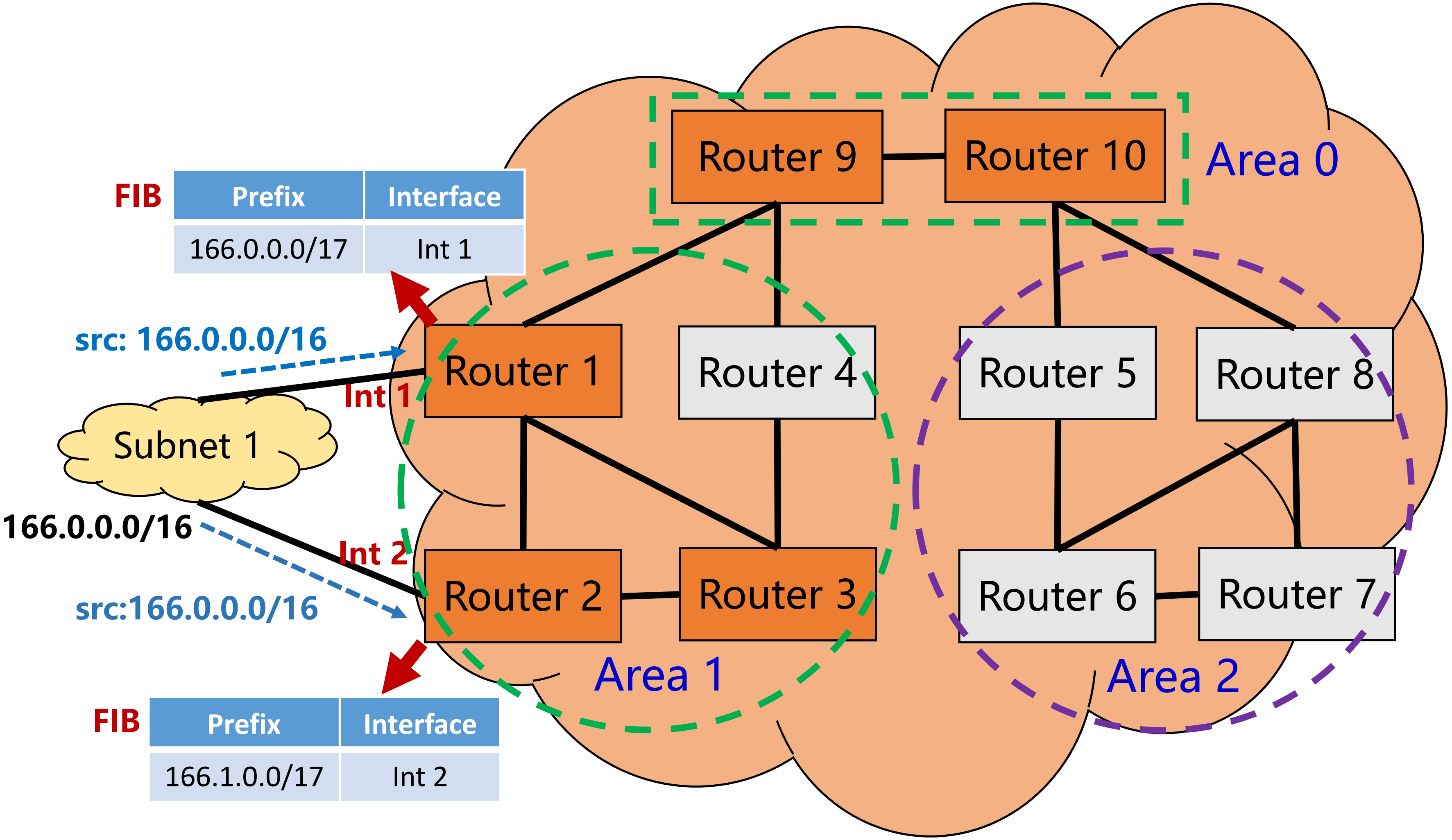
🟧 Deployed router

⬜ Undeployed router



Problem #1: Improper Block (1)

- □If applying strict uRPF in Router 1 and Router 2
  - ◆Improper block
- □If applying ACL (ingress filtering) in Int 1 and Int 2
  - ◆Manual update given prefix update in Subnet 1
  - ◆Manual update given topology update for Subnet 1



FIB

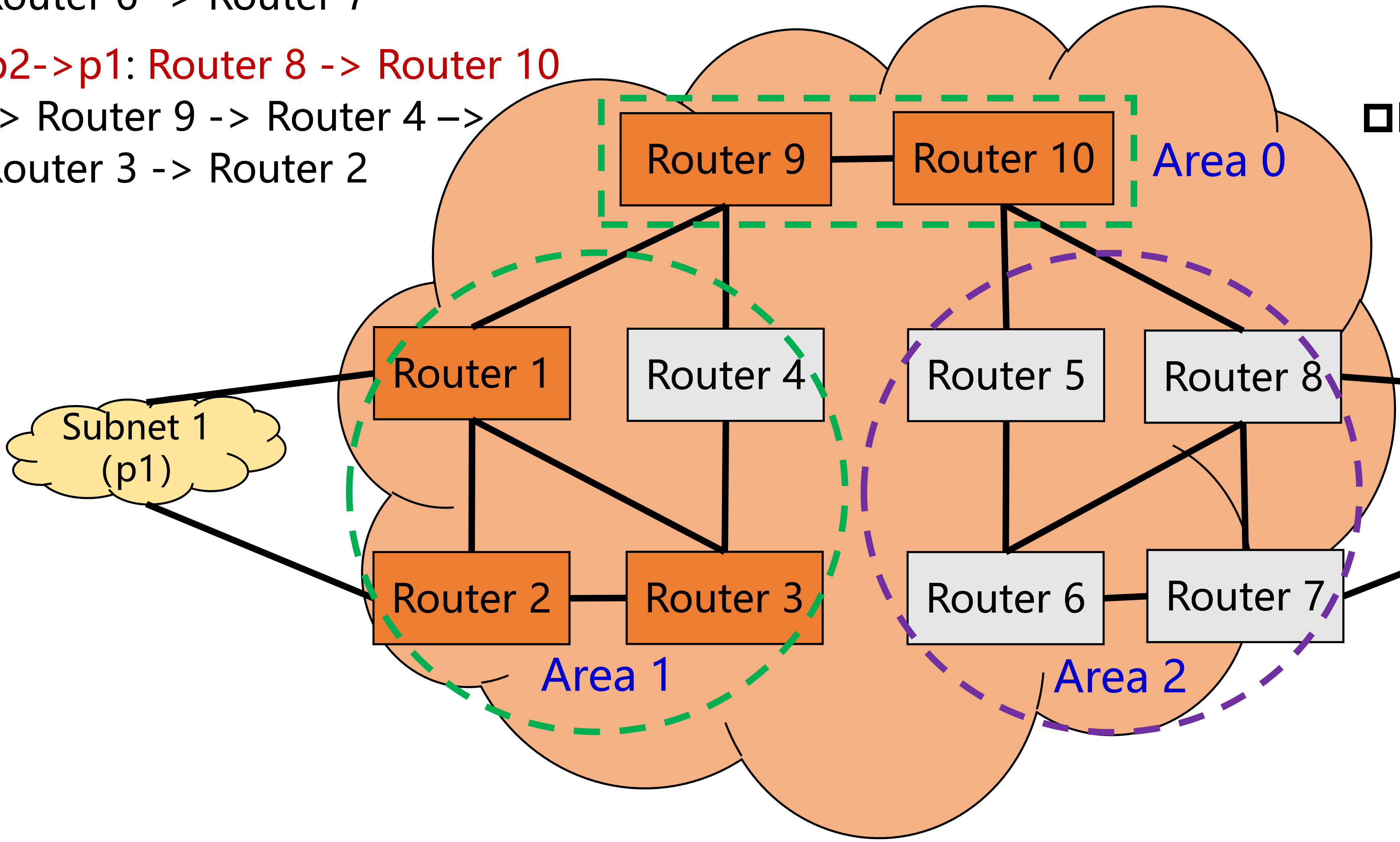
Prefix	Interface
166.0.0.0/17	Int 1

FIB

Prefix	Interface
166.1.0.0/17	Int 2

Problem #1: Improper Block (2)

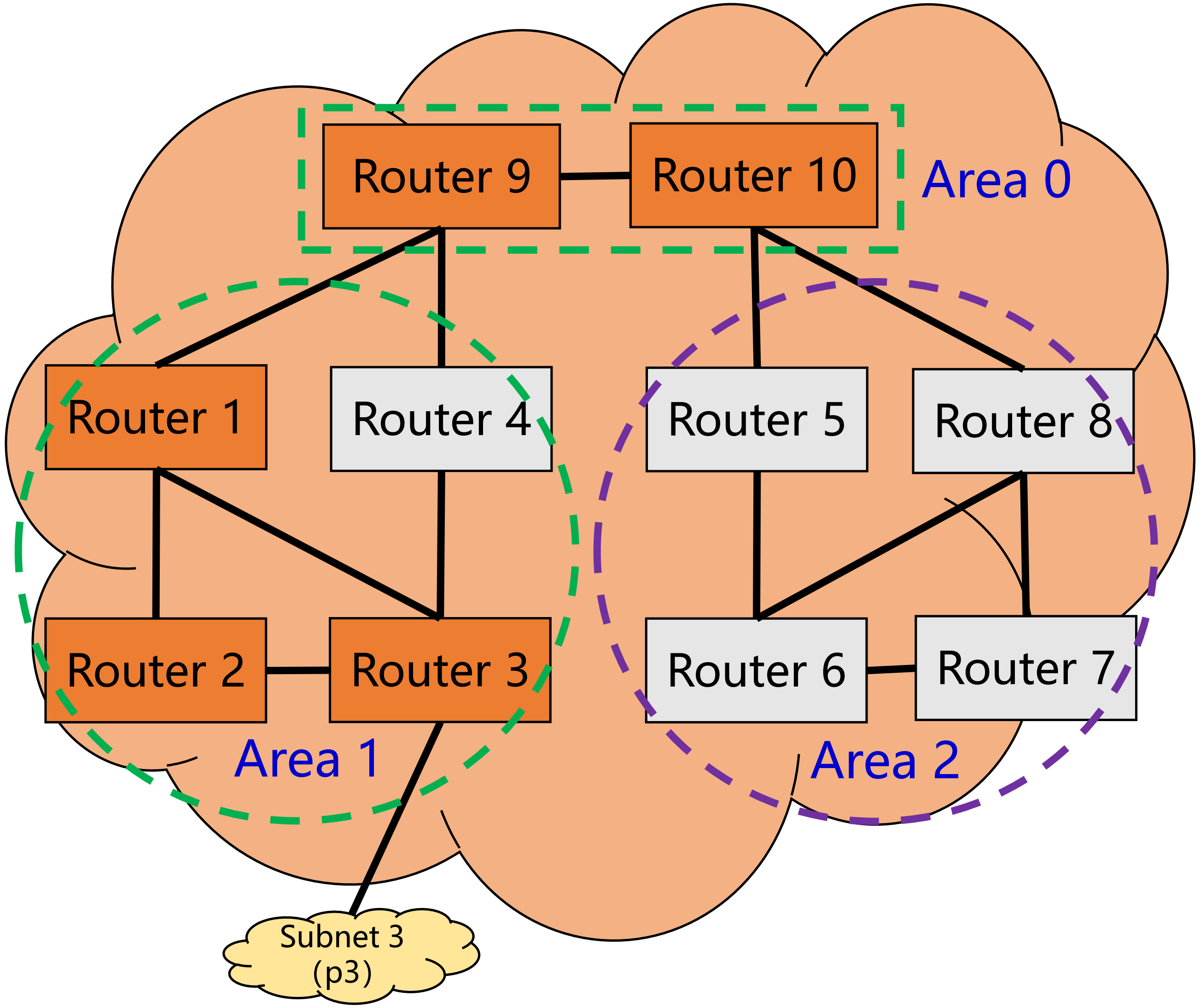
- p1->p2: Router 1 -> Router 9 -> Router 10 -> Router 5 -> Router 6 -> Router 7
- p2->p1: Router 8 -> Router 10 -> Router 9 -> Router 4 –> Router 3 -> Router 2



- If Router 10 applies strict uRPF
  - Legal traffic from subnet 2 will be improperly blocked
- If Router 10 applies loose uRPF
  - Traffic from subnet 2 can use spoofing source addresses

Problem #2: Misbehaved Router

- ☐ If Router 3 misbehaves or is compromised
  - ◆ Router 3 does not conduct SAV functionality
  - ◆ Spoofing traffic from subnet 3 cannot be blocked by downstream routers, such as Router 4



Problem #3: Misaligned Incentive

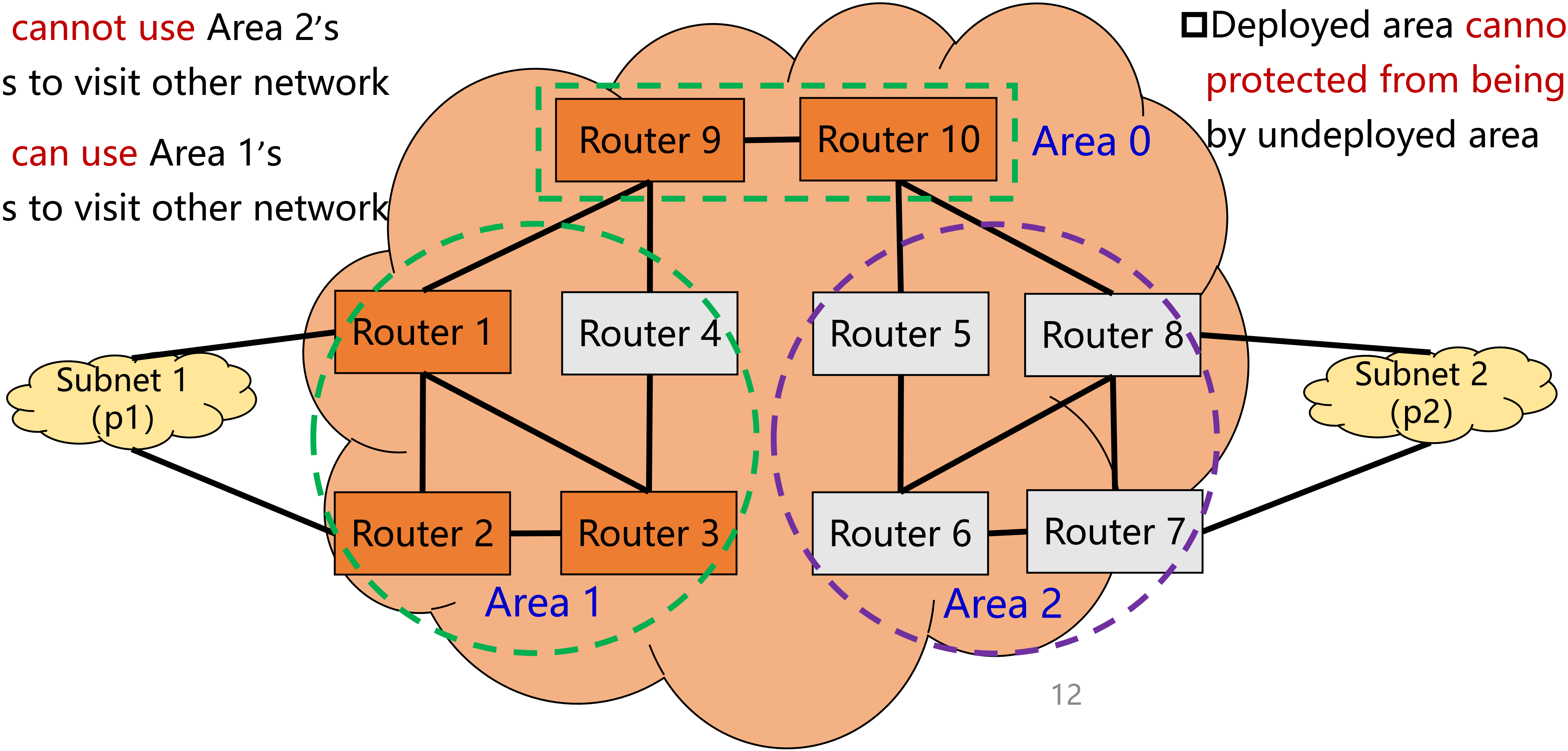
□Area 1 deploys SAV while Area 2 does not deploy SAV

□Area 1 cannot use Area 2's address to visit other network

□Area 2 can use Area 1's address to visit other network

□Subnet 1 can be attacked by subnet 2 by reflective DDoS

□Deployed area cannot be protected from being attacked by undeployed area

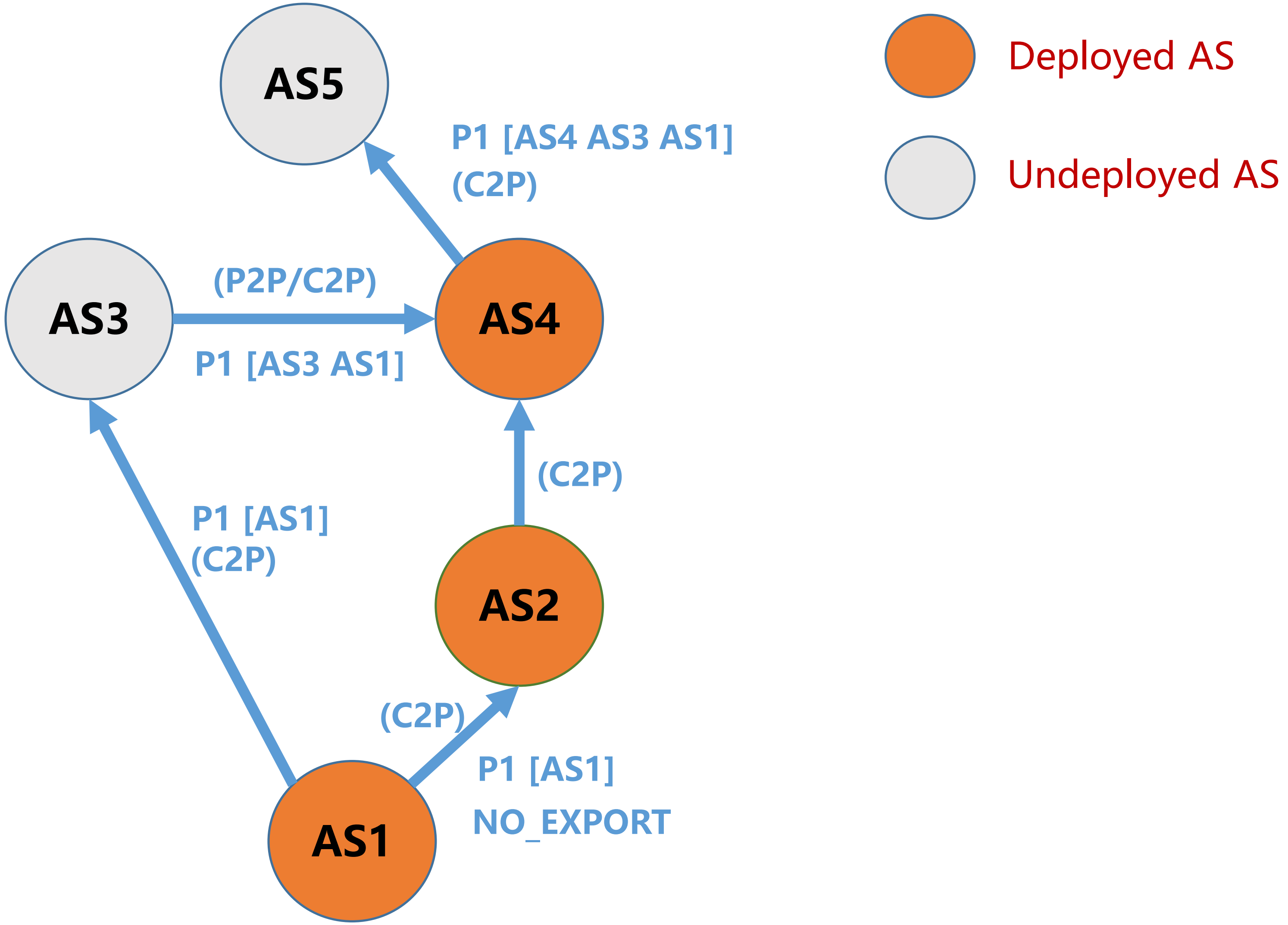


Requirements for New Intra-domain SAV

- Requirement #1: SAV mechanism should discover the real data-plane forwarding path among routers
  - Avoids improper block under asymmetric routing
- Requirement #2: SAV mechanism should be deployed in more routers than only the first-hop router (ingress filtering)
  - Increases the resilience against router’s misbehavior
- Requirement #3: SAV mechanism should disseminate the prefixes of deployed areas as far as possible
  - Helps block traffic which spoof these prefixes as close to the source as possible
  - Provides incentives to the deployed areas

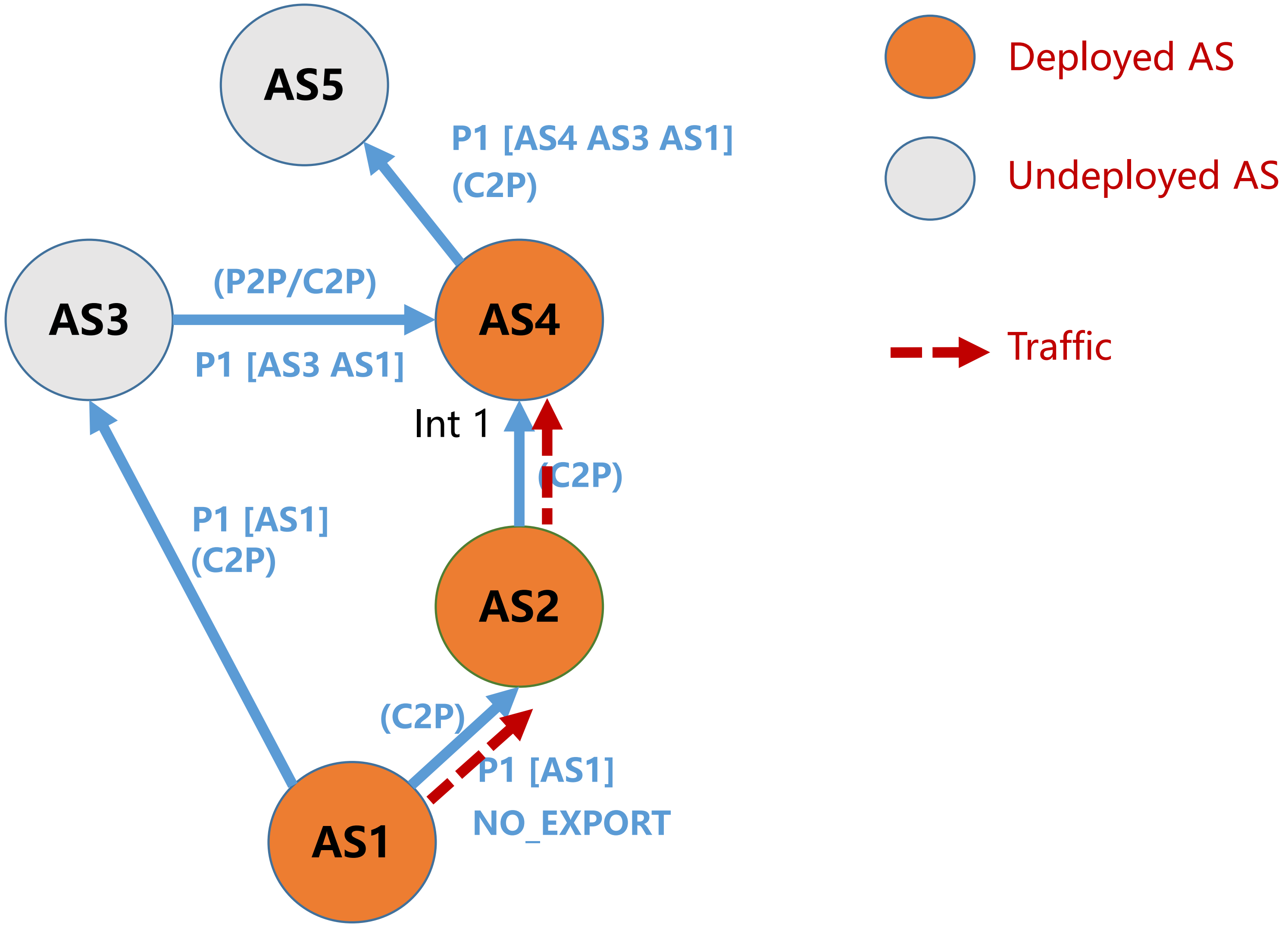
A Typical Inter-domain Scenario

- □AS1, AS2, AS4 deploy inter-domain SAV mechanism (EFP-uRPF [RFC 8704])
- □AS3 and AS5 do not deploy inter-domain SAV mechanism
- □EFP-uRPF works at ASBR for inbound traffic
    - ◆Algorithm A: each customer interface independently learns the prefixes by BGP update message
    - ◆Algorithm B: each customer interface shares the learned prefix information



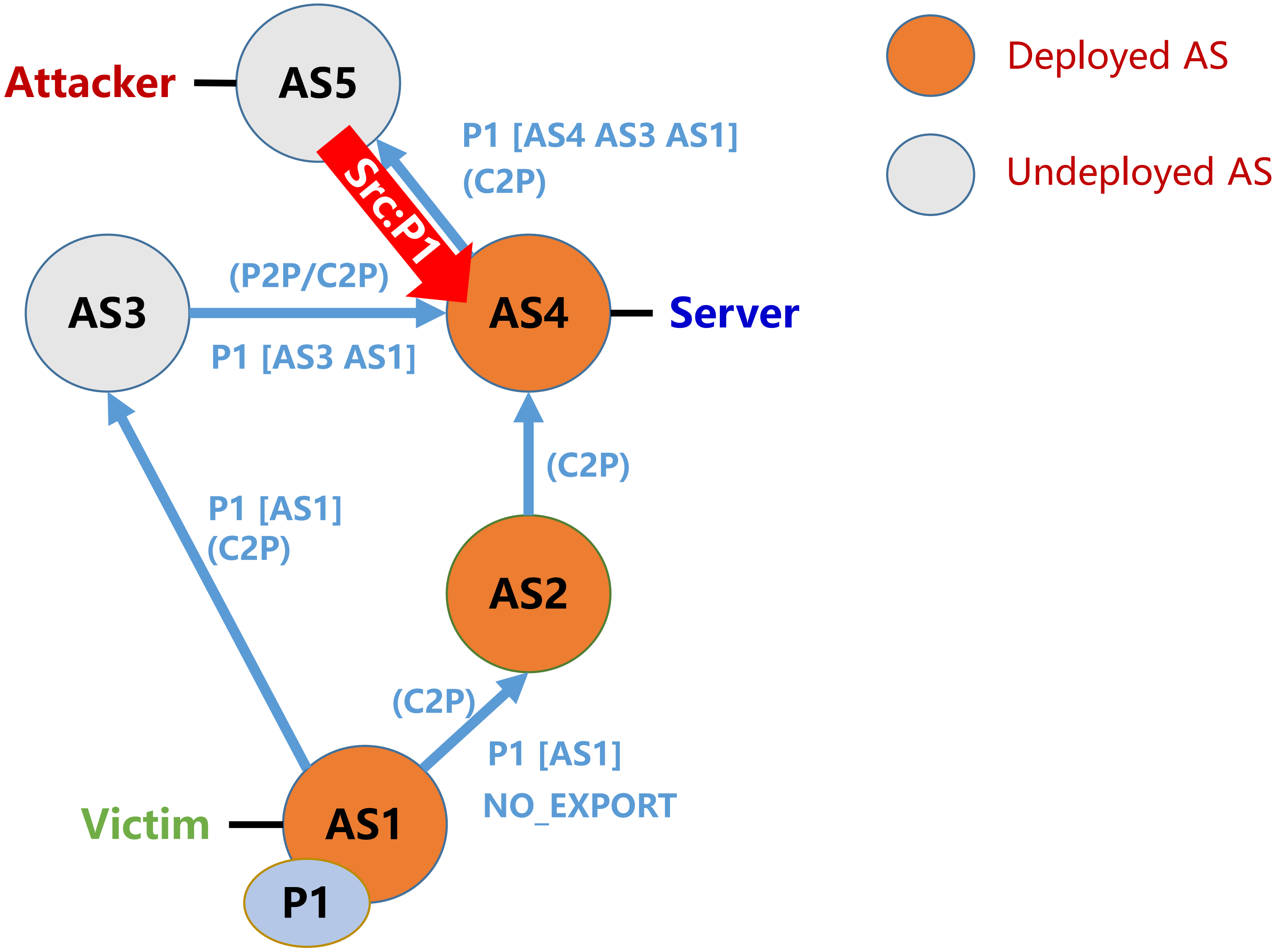
Problem #1: Improper Block

- Assuming AS1 sends traffic to AS4 along the path AS1->AS2->AS4
- If AS4 runs EFP-uRPF Algorithm A
  - Improper block at Int 1
- If AS4 runs EFP-uRPF Algorithm B
  - If AS3 is customer of AS4: no problem
  - If AS3 is peer of AS4: improper block at Int 1



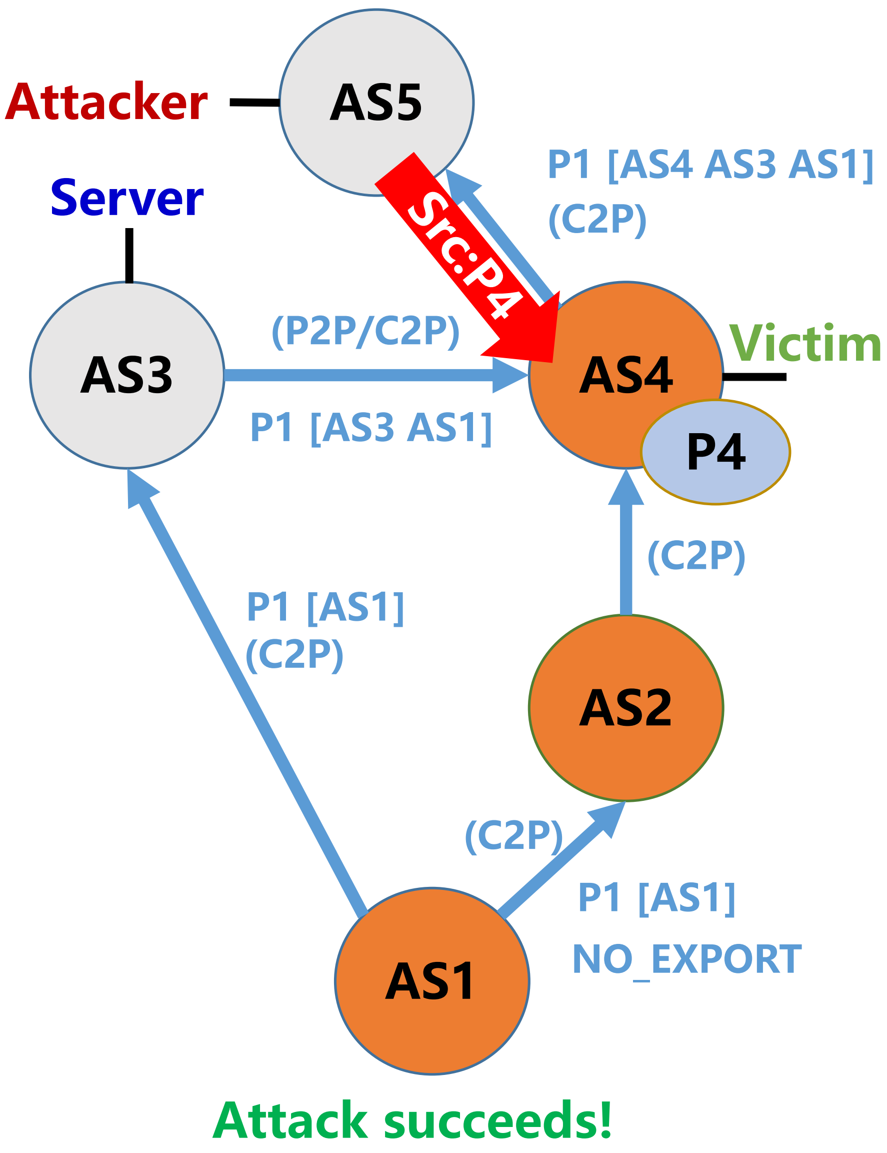
Problem #2: Ineffective Defense

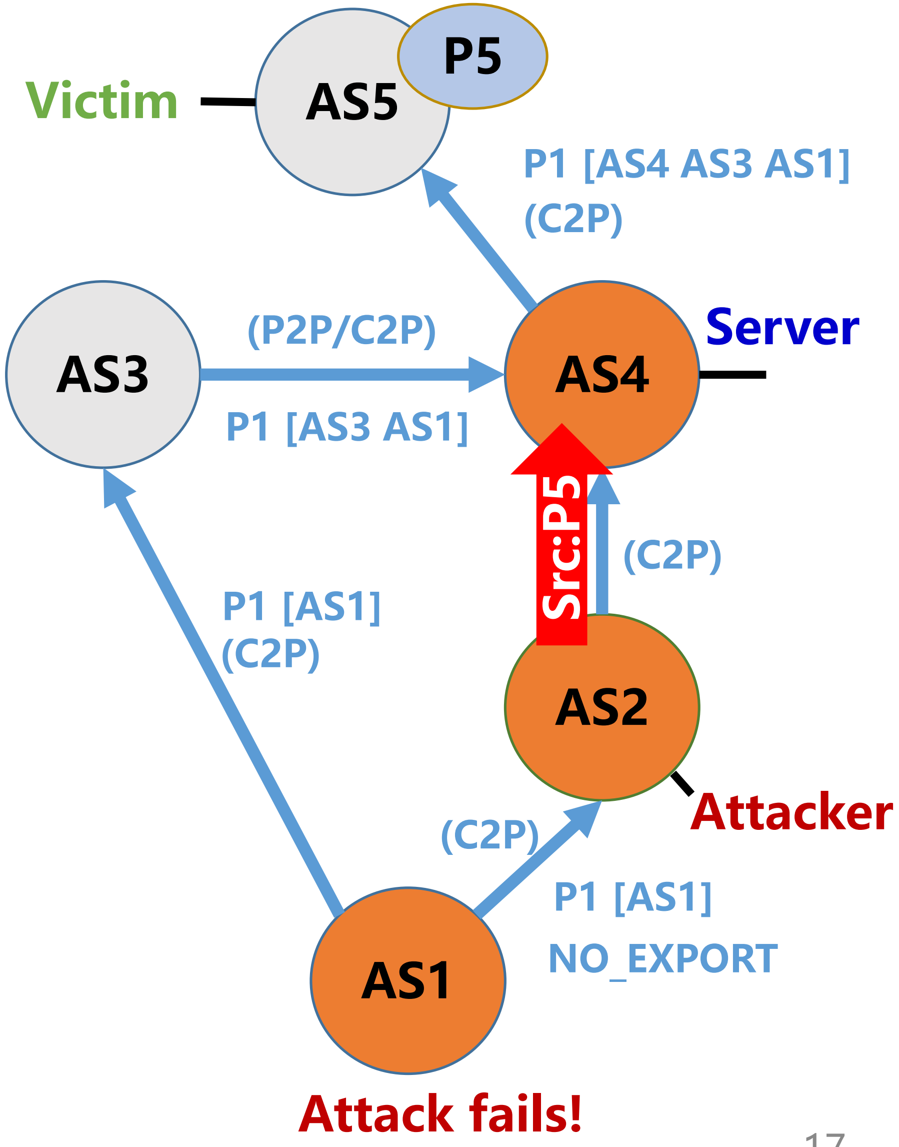
- An example of reflective DDoS attack
  - Attacker: AS5
  - Reflective server: AS4
  - Victim: AS1
- AS4 cannot block the spoofing traffic from AS5
  - EFP-uRPF do not work at provider interface



Problem #3: Misaligned Incentive

- □AS5 can launch reflective DDoS attack for AS4
- □AS2 cannot launch reflective DDoS attack for AS5
- □Deployed ASes are not protected from being attacked by undeployed ASes
- □ASes do not benefit from deploying SAV mechanism





Requirements for New Inter-domain SAV

- Requirement #1: SAV mechanism should discover the real data-plane forwarding path among ASes
  - Avoids improper block under asymmetric routing
- Requirement #2: SAV mechanism should enable all-direction validation
  - EFP-uRPF (BAR-SAV) only works in customer/peering interfaces
  - Most attacking traffic come from remote ASes via provider interfaces
- Requirement #3: SAV mechanism should disseminate the prefixes of deployed ASes as far as possible
  - Helps block traffic which spoof these prefixes as close to the source as possible
  - Provides incentives to the deployed ASes

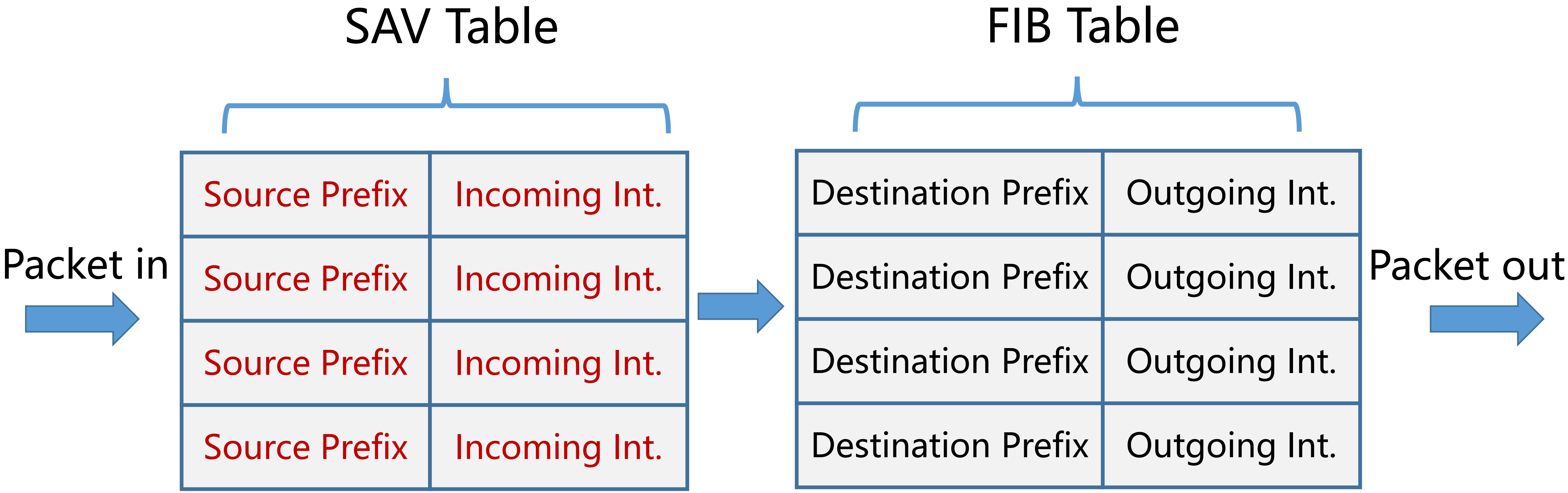
Outline

- □Background
- □Gap Analysis & Requirement
- □SAVNET Solution
- □IETF SAVNET WG

Basic Idea of SAVNET

- [Resilience:] Each router builds a SAV table to validate source addresses
  - If prefixes are not learned in the SAV table, the incoming packet is permitted
  - If prefixes are learned in the SAV table but incoming interface of a packet does not match, the packet is blocked
  - More resilient than single-hop checking at ingress routers
- [Correctness:] Routers’ SAV tables follow the real forwarding path in the data plane
  - Ensure correct validation even with asymmetric routing
- [Incentive:] Prefixes of deployed areas (subnets, ASes) are disseminated as far as possible
  - Traffic forging these prefixes can be blocked as close to the source as possible
  - Mitigate reflective DDoS attack targeting at these prefixes
- [Cost:] Control-plane protocol extension, without data-plane packet modification
  - Existing IGP/BGP routing protocols are extended to carry the necessary information to build the SAV tables in routers

SAV Table in SAVNET Routers



Packet in

SAV Table

Source Prefix	Incoming Int.
Source Prefix	Incoming Int.
Source Prefix	Incoming Int.
Source Prefix	Incoming Int.

FIB Table

Destination Prefix	Outgoing Int.
Destination Prefix	Outgoing Int.
Destination Prefix	Outgoing Int.
Destination Prefix	Outgoing Int.

Packet out

SAVNET Protocol Architecture to Generate SAV Tables

□SAVNET Protocol Architecture

- ◆Discovering the real data-plane forwarding path via hop-by-hop prefix notification, and generating SAV tables in routers along the path
- ◆Separating the protocol into an intra-domain part and an inter-domain part, both sharing the same high-level idea

□Terminologies

- ◆Node: A router in intra-domain SAVNET or an AS in inter-domain SAVNET
- ◆Prefix notification: The process by which a node notifies the incoming direction of its source prefixes to all the other nodes in the network
- ◆During prefix notification, each node conducts one of the three operations
  - ➢Message origination: A node generates original notification messages
  - ➢Message relaying: A node generates relaying notification messages after receiving a notification message
  - ➢Message termination: A node terminates the received notification message

SAVNET Notification Message Format

The SAVNET notification message contains two main fields

◻Source prefix field

◆This field contains the source prefixes of the initial node

◆When receiving a message, the node generates SAV rules for the source prefixes

◆This field remains unchanged during the prefix notification process

◻Propagation scope field

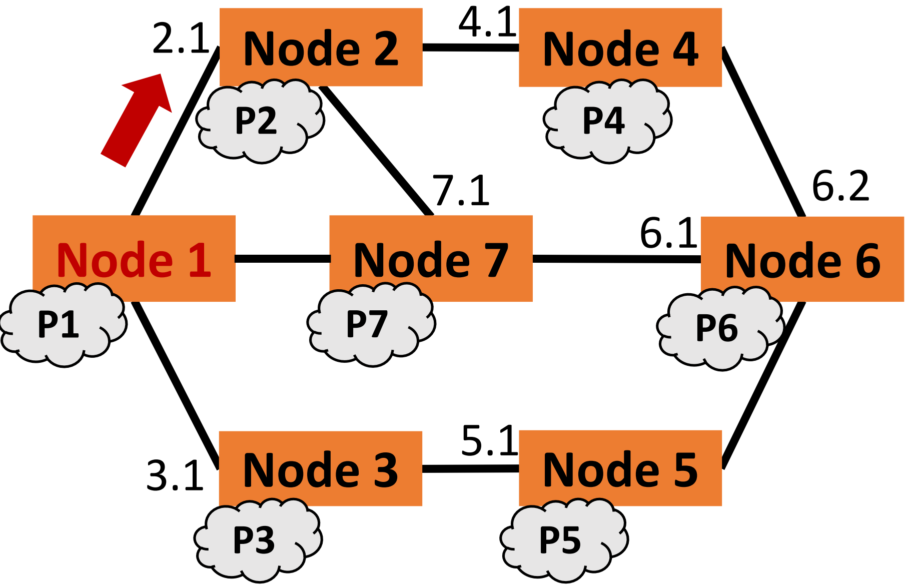
◆This field contains a list of destination prefixes which take the neighboring node as the next hop (from FIB)

◆This field is used to discover the real data-plane forwarding path

◆This field changes hop by hop during the prefix notification process

An Example of SAVNET Protocol Workflow (1)

FIB for Node 1	
Dest Prefix	Next hop
P2	Node 2
P3	Node 3
P4	Node 2
P5	Node 3
P6	Node 2
P7	Node 2



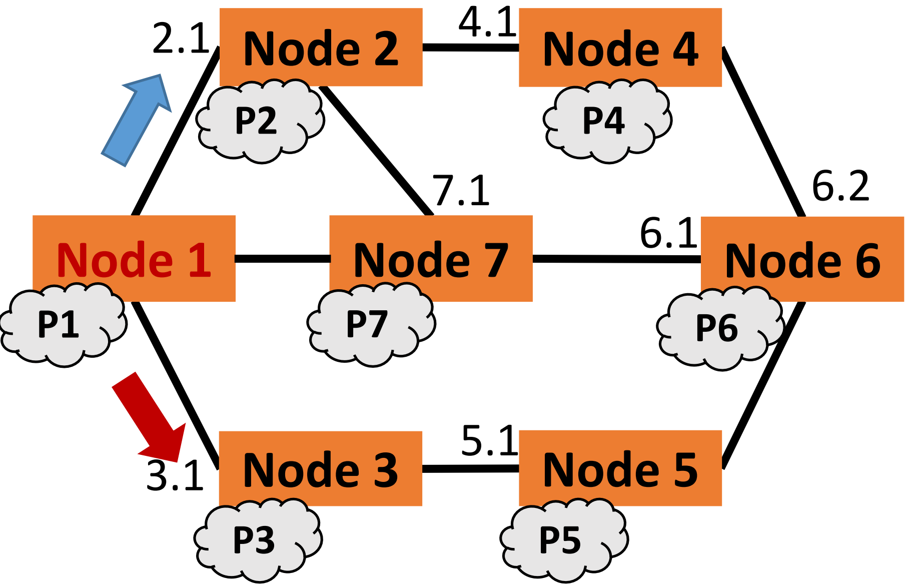
The process of prefix notification for P1

Node 1 conducts message origination since P1 is the source prefix of Node 1

- From Node 1's FIB, P2, P4, P6, P7 take Node 2 as the next hop, so Node 1 generates an original notification message to Node 2
  - Message from Node 1 to Node 2
    - Source prefix → P1
    - Propagation scope → P2, P4, P6, P7

An Example of SAVNET Protocol Workflow (1)

FIB for Node 1	
Dest Prefix	Next hop
P2	Node 2
P3	Node 3
P4	Node 2
P5	Node 3
P6	Node 2
P7	Node 2



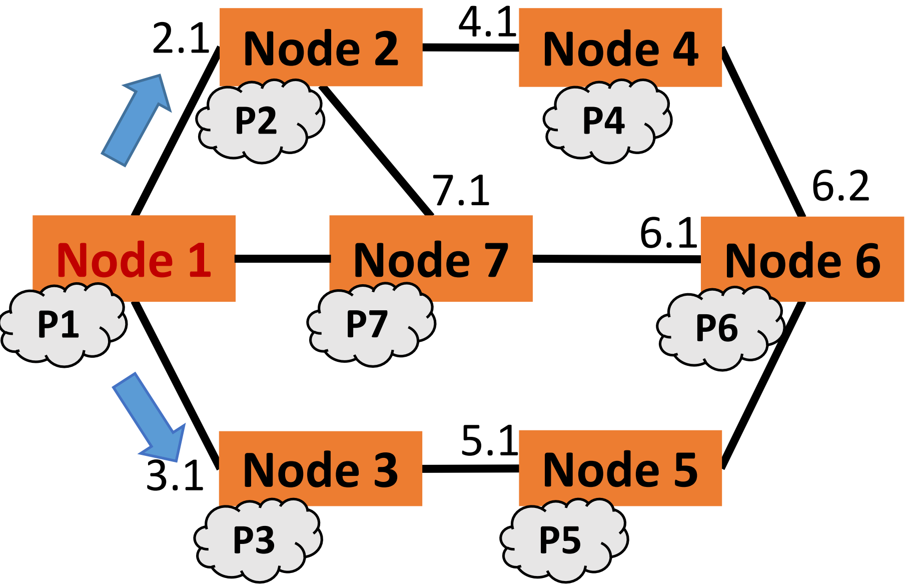
The process of prefix notification for P1

Node 1 conducts message origination since P1 is the source prefix of Node 1

- ◻From Node 1's FIB, P3, P5 take Node 3 as the next hop, so Node 1 generates an original notification message to Node 3
  - ◆Message from Node 1 to Node 3
    - ➢Source prefix → P1
    - ➢Propagation scope → P3, P5

An Example of SAVNET Protocol Workflow (1)

FIB for Node 1	
Dest Prefix	Next hop
P2	Node 2
P3	Node 3
P4	Node 2
P5	Node 3
P6	Node 2
P7	Node 2



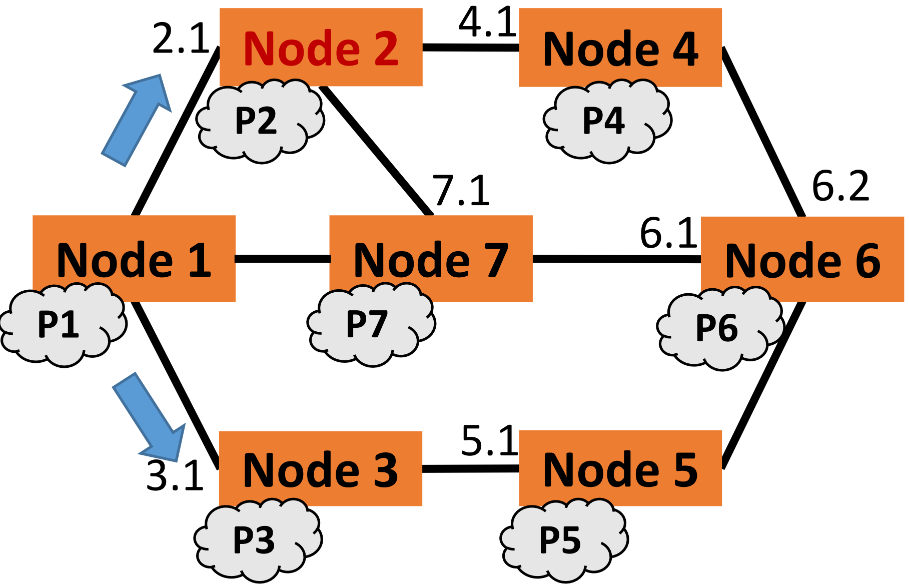
The process of prefix notification for P1

Node 1 conducts message origination since P1 is the source prefix of Node 1

- From Node 1's FIB, no prefix takes Node 7 as the next hop, so Node 1 does not send any notification message to Node 7

An Example of SAVNET Protocol Workflow (2)

FIB for Node 2	
Dest Prefix	Next hop
P1	Node 1
P3	Node 1
P4	Node 4
P5	Node 4
P6	Node 4
P7	Node 7



The process of prefix notification for P1

When Node 2 receives the message from Node 1 at port 2.1

- ◆Message from Node 1 to Node 2
  - ➢Source prefix → P1
  - ➢Propagation scope → P2, P4, P6, P7

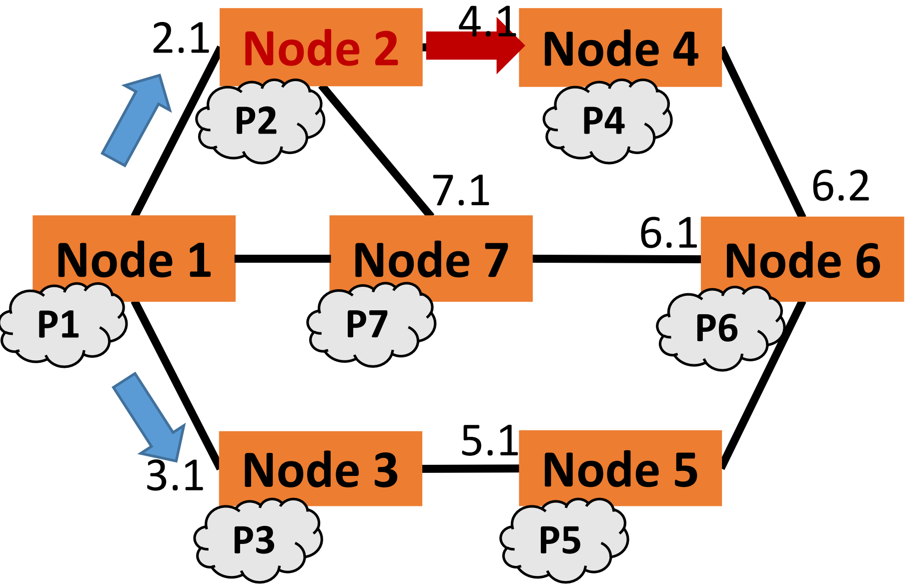
□Node 2 generates the SAV rule for source prefix P1

- ◆<source prefix P1, incoming port 2.1>

An Example of SAVNET Protocol Workflow (2)

FIB for Node 2

Dest Prefix	Next hop
P1	Node 1
P3	Node 1
P4	Node 4
P5	Node 4
P6	Node 4/7
P7	Node 7



The process of prefix notification for P1

When Node 2 receives the message from Node 1 at port 2.1

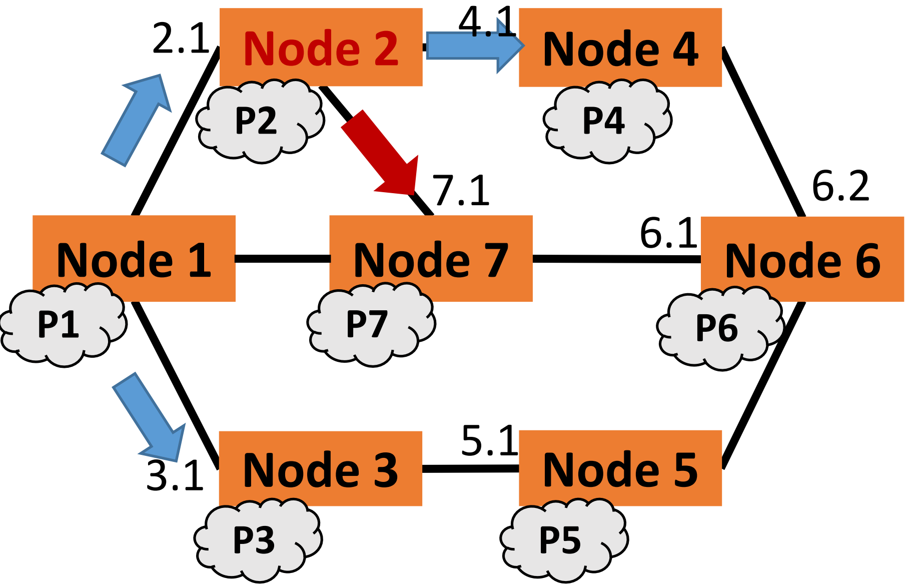
- ◆Message from Node 1 to Node 2
  - ➢Source prefix → P1
  - ➢Propagation scope → P2, P4, P6, P7

□From Node 2's FIB, P4, P6 take Node 4 as the next hop, so Node 2 conducts message relaying and generates a relaying notification message to Node 4

- ◆Message from Node 2 to Node 4
  - ➢Source prefix → P1
  - ➢Propagation scope → P4, P6

An Example of SAVNET Protocol Workflow (2)

FIB for Node 2	
Dest Prefix	Next hop
P1	Node 1
P3	Node 1
P4	Node 4
P5	Node 4
P6	Node 4/7
P7	Node 7



The process of prefix notification for P1

When Node 2 receives the message from Node 1 at port 2.1

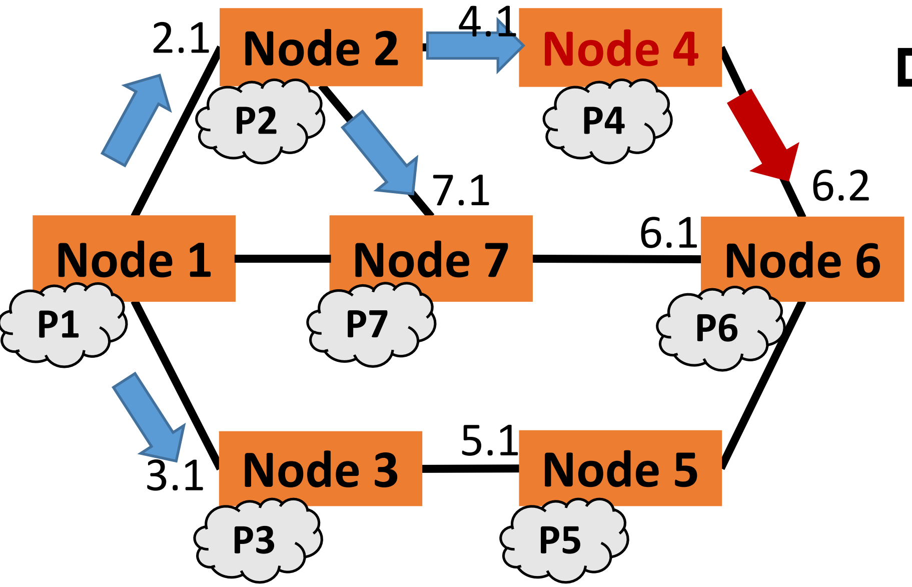
- ◆Message from Node 1 to Node 2
  - ➢Source prefix → P1
  - ➢Propagation scope → P2, P4, P6, P7

□From Node 2's FIB, P6, P7 take Node 7 as the next hop, so Node 2 conducts message relaying and generates a relaying notification message to Node 7

- ◆Message from Node 2 to Node 7
  - ➢Source prefix → P1
  - ➢Propagation scope → P6, P7

An Example of SAVNET Protocol Workflow (3)

FIB for Node 4	
Dest Prefix	Next hop
P1	Node 2
P2	Node 2
P3	Node 2
P5	Node 6
P6	Node 6
P7	Node 2



The process of prefix notification for P1

When Node 4 receives the message from Node 2 at port 4.1

- ◆Message from Node 2 to Node 4
  - ➢Source prefix → P1
  - ➢Propagation scope → P4, P6

□Node 4 generates the SAV rule for source prefix P1

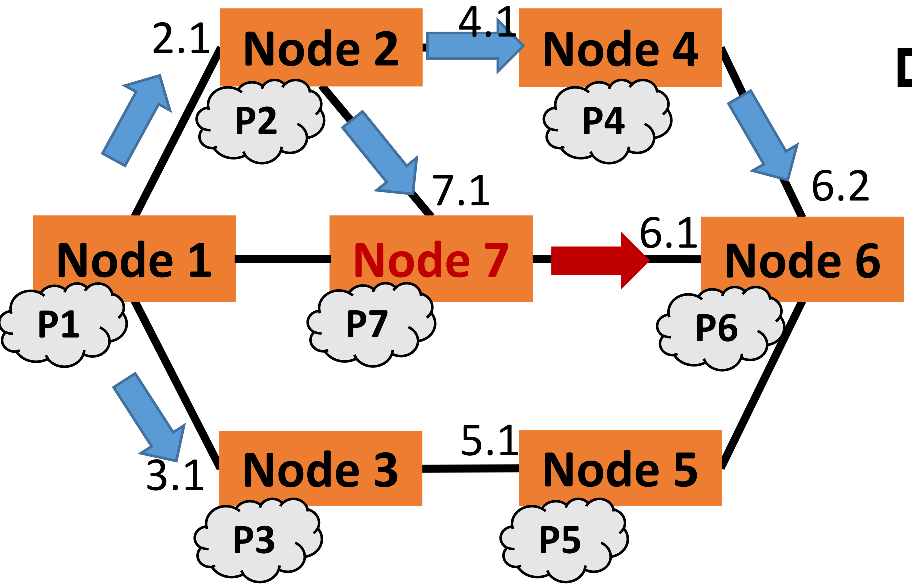
- ◆<source prefix P1, incoming port 4.1>

□From Node 4's FIB, P6 takes Node 6 as the next hop, so Node 4 conducts message relaying and generates a relaying notification message to Node 6

- ◆Message from Node 4 to Node 6
  - ➢Source prefix → P1
  - ➢Propagation scope → P6

An Example of SAVNET Protocol Workflow (4)

FIB for Node 7	
Dest Prefix	Next hop
P1	Node 1
P2	Node 2
P3	Node 1
P4	Node 2
P5	Node 6
P6	Node 6



The process of prefix notification for P1

When Node 7 receives the message from Node 2 at port 7.1

◆Message from Node 2 to Node 7

➢Source prefix → P1

➢Propagation scope → P6, P7

□Node 7 generates the SAV rule for source prefix P1

◆<source prefix P1, incoming port 7.1>

□From Node 7's FIB, P6 takes Node 6 as the next hop, so Node 7 conducts message relaying and generates a relaying notification message to Node 6

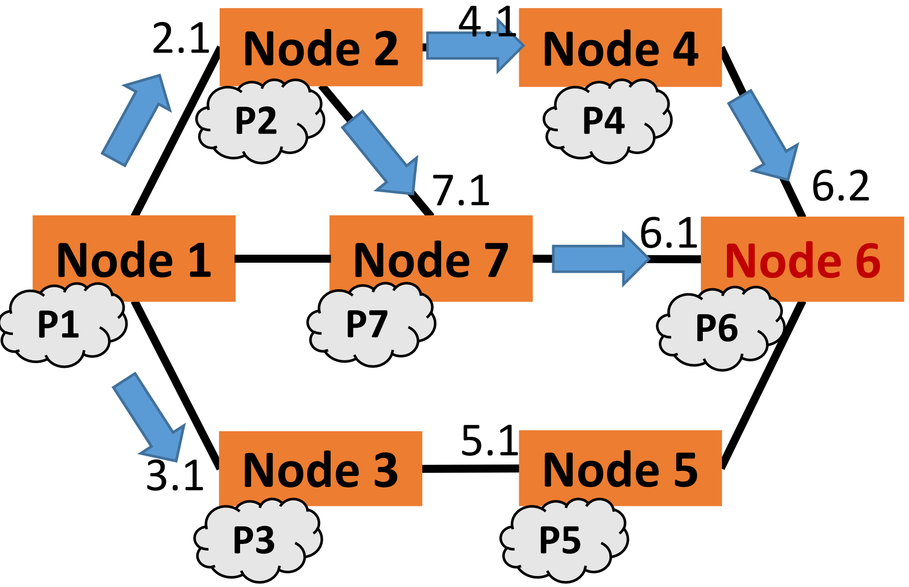
◆Message from Node 7 to Node 6

➢Source prefix → P1

➢Propagation scope → P6

An Example of SAVNET Protocol Workflow (5)

FIB for Node 4	
Dest Prefix	Next hop
P1	Node 2
P2	Node 2
P3	Node 2
P5	Node 6
P6	Node 6
P7	Node 2



The process of prefix notification for P1

When Node 6 receives the message from Node 4 at port 6.2 and the message from Node 7 at port 6.1

- ◆Message from Node 4 to Node 6
  - ➢Source prefix → P1
  - ➢Propagation scope → P6
- ◆Message from Node 7 to Node 6
  - ➢Source prefix → P1
  - ➢Propagation scope → P6

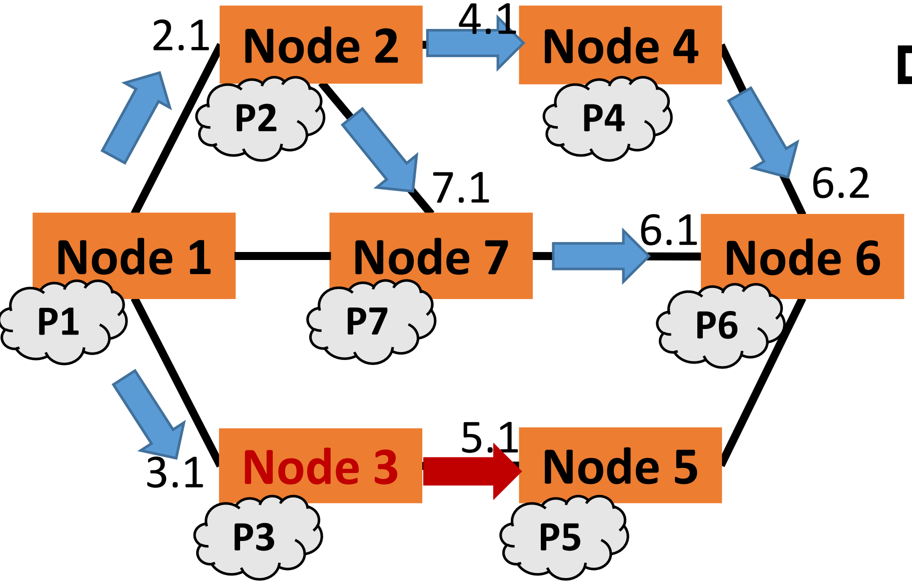
□Node 6 generates the SAV rule for source prefix P1

- ◆<source prefix P1, incoming port 6.1 and 6.2>

□Node 6 conducts message termination because P6 is the source prefix of Node 6

An Example of SAVNET Protocol Workflow (6)

FIB for Node 3	
Dest Prefix	Next hop
P1	Node 1
P2	Node 1
P4	Node 5
P5	Node 5
P6	Node 5
P7	Node 1



The process of prefix notification for P1

When Node 3 receives the message from Node 1 at port 3.1

- ◆Message from Node 2 to Node 3
  - ➢Source prefix → P1
  - ➢Propagation scope → P3, P5

□Node 3 generates the SAV rule for source prefix P1

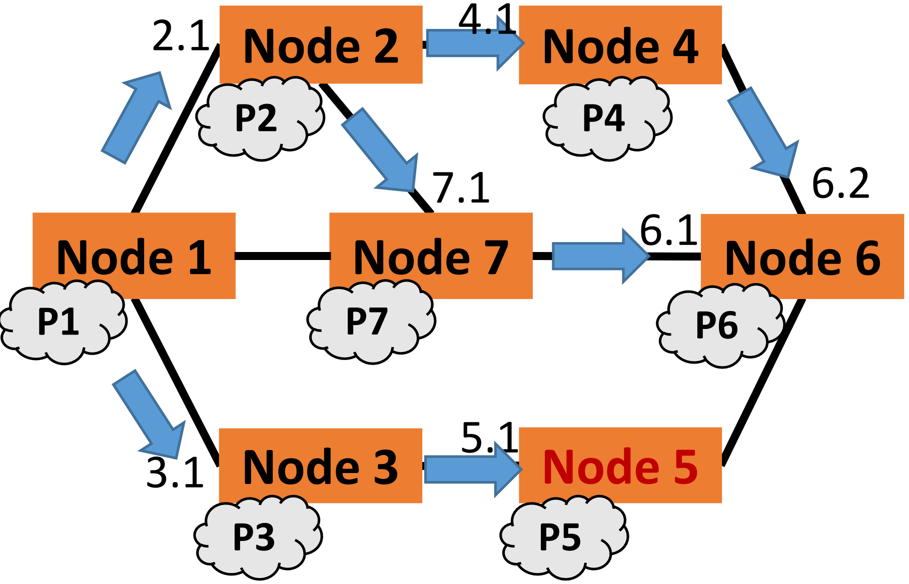
- ◆<source prefix P1, incoming port 3.1>

□From Node 3's FIB, P5 takes Node 5 as the next hop, so Node 3 conducts message relaying and generates a relaying notification message to Node 5

- ◆Message from Node 3 to Node 5
  - ➢Source prefix → P1
  - ➢Propagation scope → P5

An Example of SAVNET Protocol Workflow (7)

FIB for Node 3	
Dest Prefix	Next hop
P1	Node 1
P2	Node 1
P4	Node 5
P5	Node 5
P6	Node 5
P7	Node 1



The process of prefix notification for P1

When Node 5 receives the message from Node 3 at port 5.1

- ◆Message from Node 3 to Node 5
  - ➢Source prefix → P1
  - ➢Propagation scope → P5

□Node 5 generates the SAV rule for source prefix P1

- ◆<source prefix P1, incoming port 5.1>

□Node 5 conducts message termination because P5 is the source prefix of Node 5

During the prefix notification, each node generates accurate SAV rules for P1 and receives only one message except for multi-path routing.

SAVNET Update

□ Periodic update

- ◆ Each initial node generates protocol messages periodically

□ Triggered update

- ◆ When routing state changes, the initial node generates protocol messages to add updated SAV rules or delete outdated SAV rules for the affected nodes

We suggest intra-domain SAVNET supports both periodic update and triggered update, while inter-domain SAVNET only supports triggered update

Outline

- □Background
- □Gap Analysis & Requirement
- □SAVNET Solution
- □IETF SAVNET WG

IETF SAVNET WG

□SAVNET BOF, IETF 113, Mar 24, 2022

- ◆Proponent: Dan Li (Tsinghua University), Jianping Wu (Tsinghua University), Lancheng Qin (Tsinghua University), Mingqing Huang (Huawei), etc.

□SAVNET WG, formed in Jun 17, 2022

- ◆Name: Source Address Validation in Intra-domain and Inter-domain Networks
- ◆Acronym: savnet
- ◆Area: Routing Area (RTG)
- ◆Chairs: Aijun Wang, Joel M. Halpern
- ◆Mailing list: savnet@ietf.org

□First SAVNET WG meeting, IETF 114, July 25, 2022

Thanks!