Source Address Validation in Intra-domain Networks (Intra-domain SAVNET) Gap Analysis, Problem Statement, and Requirements

Dan Li, Jianping Wu, Lancheng Qin, Mingqing Huang, Nan Geng

Jul 25, 2022

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Necessity of Intra-domain SAV

- Source address validation (SAV) is important for defending against source address spoofing attacks, such as reflection attack
- Since 2014, the MANRS initiative is calling on network operators to implement SAV as close to the source as possible
- When an access network does not deploy SAV at the source (e.g., SAVI), intra-domain SAV helps block spoofed packets

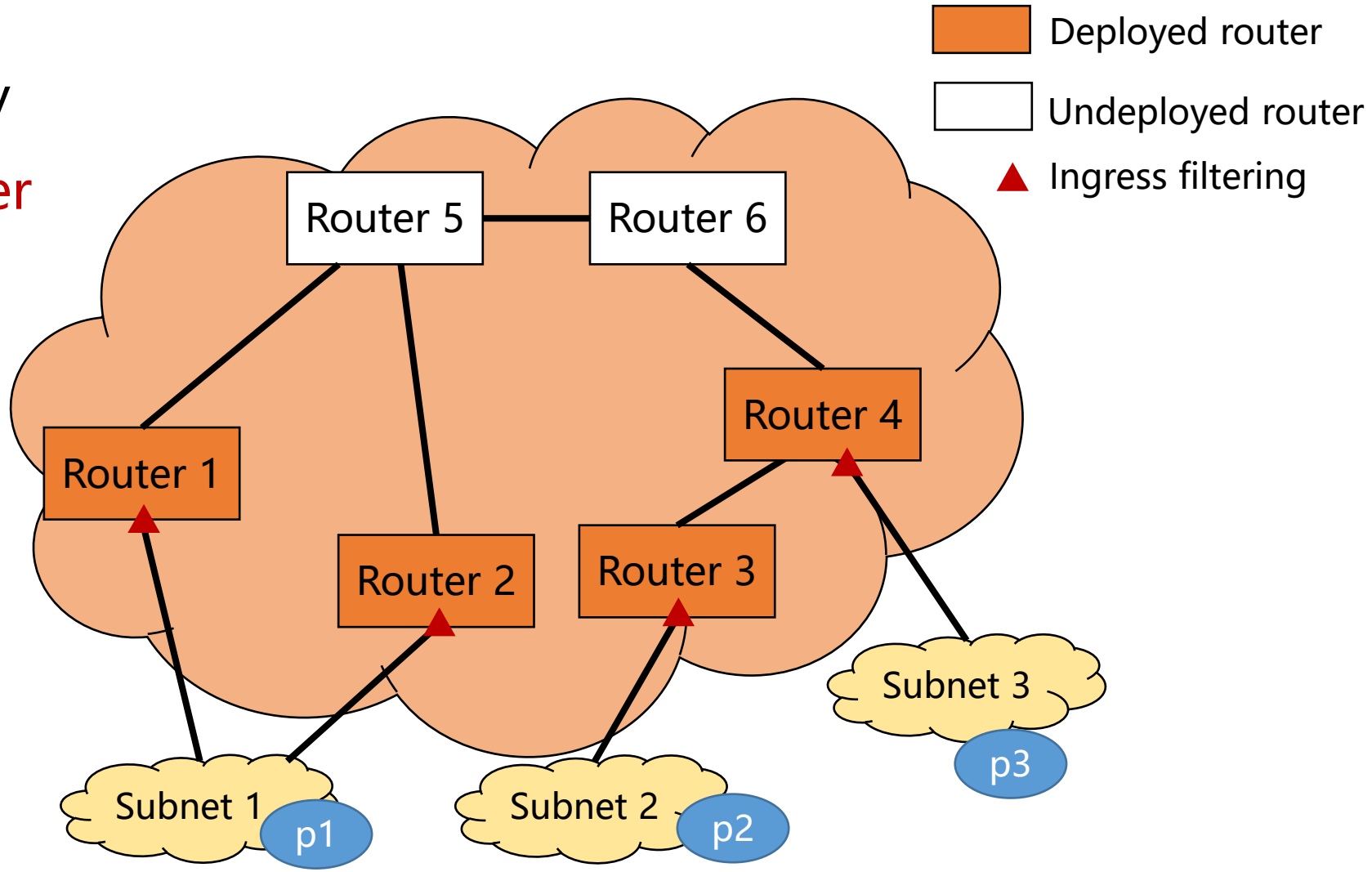
Existing Intra-domain SAV Mechanism

Ingress filtering [RFC 2827, RFC 3704] is the current practice of intra-domain SAV

- ACL-based SAV
  - Manually configures filtering rules to specify which source addresses are acceptable
- Strict uRPF
  - Looks up the source address in local FIB, and requires that the incoming interface be the same as the corresponding forwarding interface
- Feasible uRPF/Loose uRPF
  - Two other alternative implementations of ingress filtering, which are not suitable for intra-domain SAV due to their overly loose validation

Typical Adoption of Ingress filtering

- Ingress filtering is typically deployed at the edge router connecting a subnet
  - Blocks spoofing traffic from directly connected subnet



Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

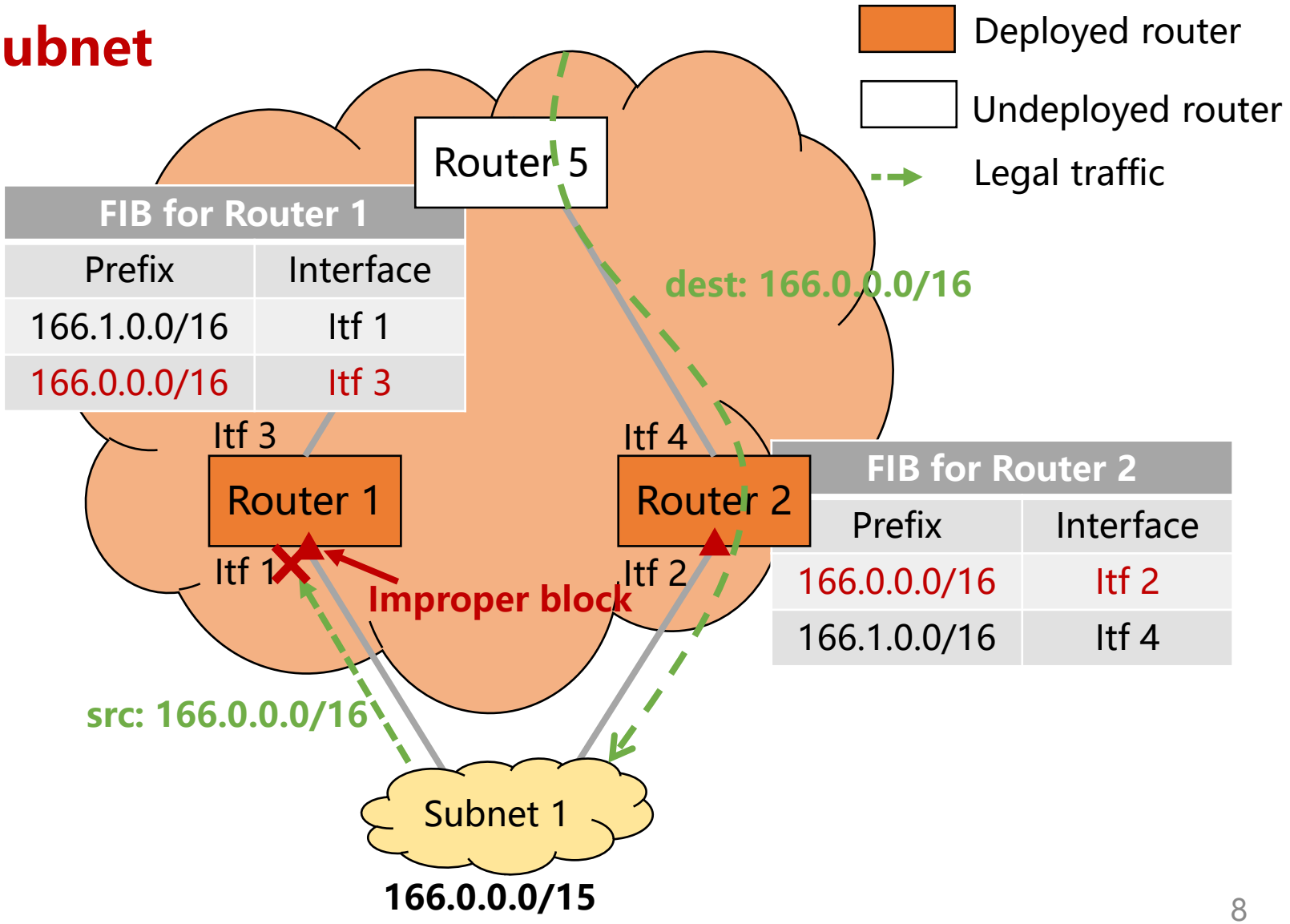
Gap #1: Improper Block

Scenario 1: Multi-homed Subnet

- Router 1 only advertises 166.1.0.0/16 in IGP
- Router 2 only advertises 166.0.0.0/16 in IGP

Behavior

- If applying strict uRPF
  - Improper block
- If applying ACL-based SAV
  - Manual update given prefix or topology update in Subnet 1



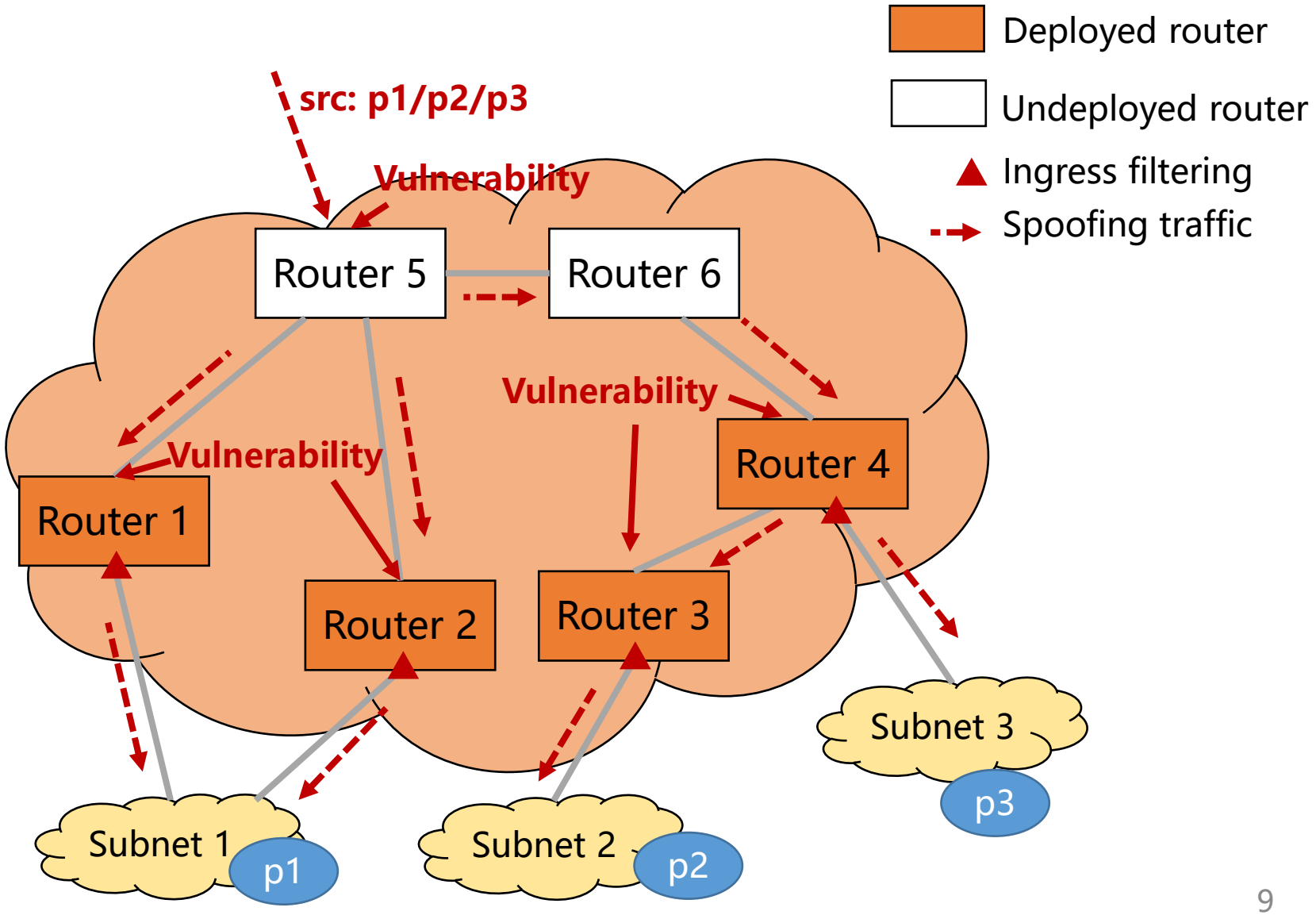
Gap #2: Vulnerability in Inbound Direction

☐ Scenario 2: Spoofing from Inbound Direction

Behavior

☐ Ingress filtering does not work for inbound traffic

- ◆Spoofing traffic (with intra-domain source addresses) can easily enter from inbound direction

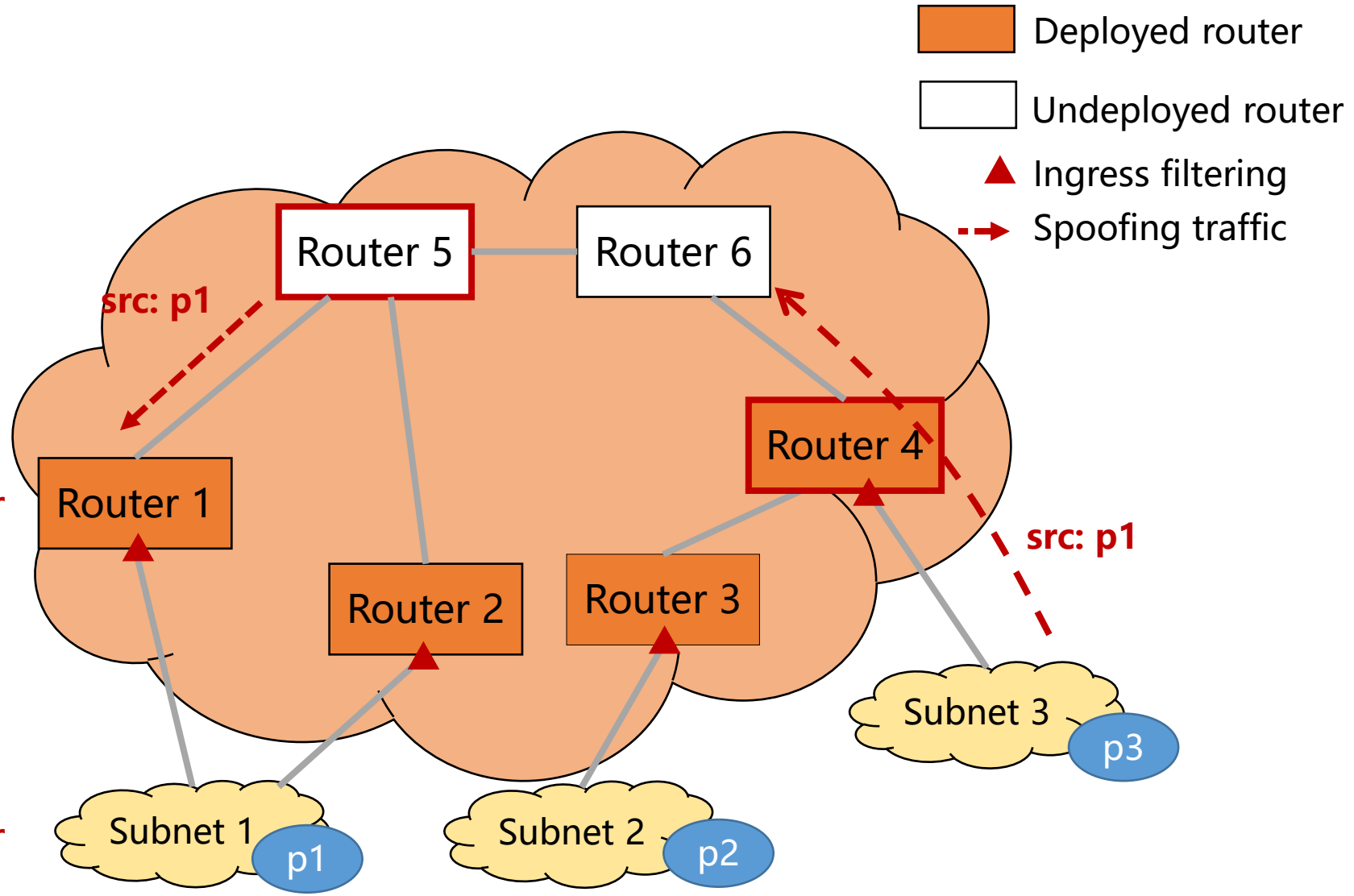


Gap #3: Misbehaved Router

Scenario 3: Misbehaved or compromised router

Behavior

- If Router 4 does not strictly conduct SAV
  - Spoofing traffic from subnet 3 cannot be blocked by other routers, such as Router 6
- If Router 5 originates spoofing traffic
  - Spoofing traffic from Router 5 cannot be blocked by other routers, such as Router 1



Gap #4: Misaligned Incentive

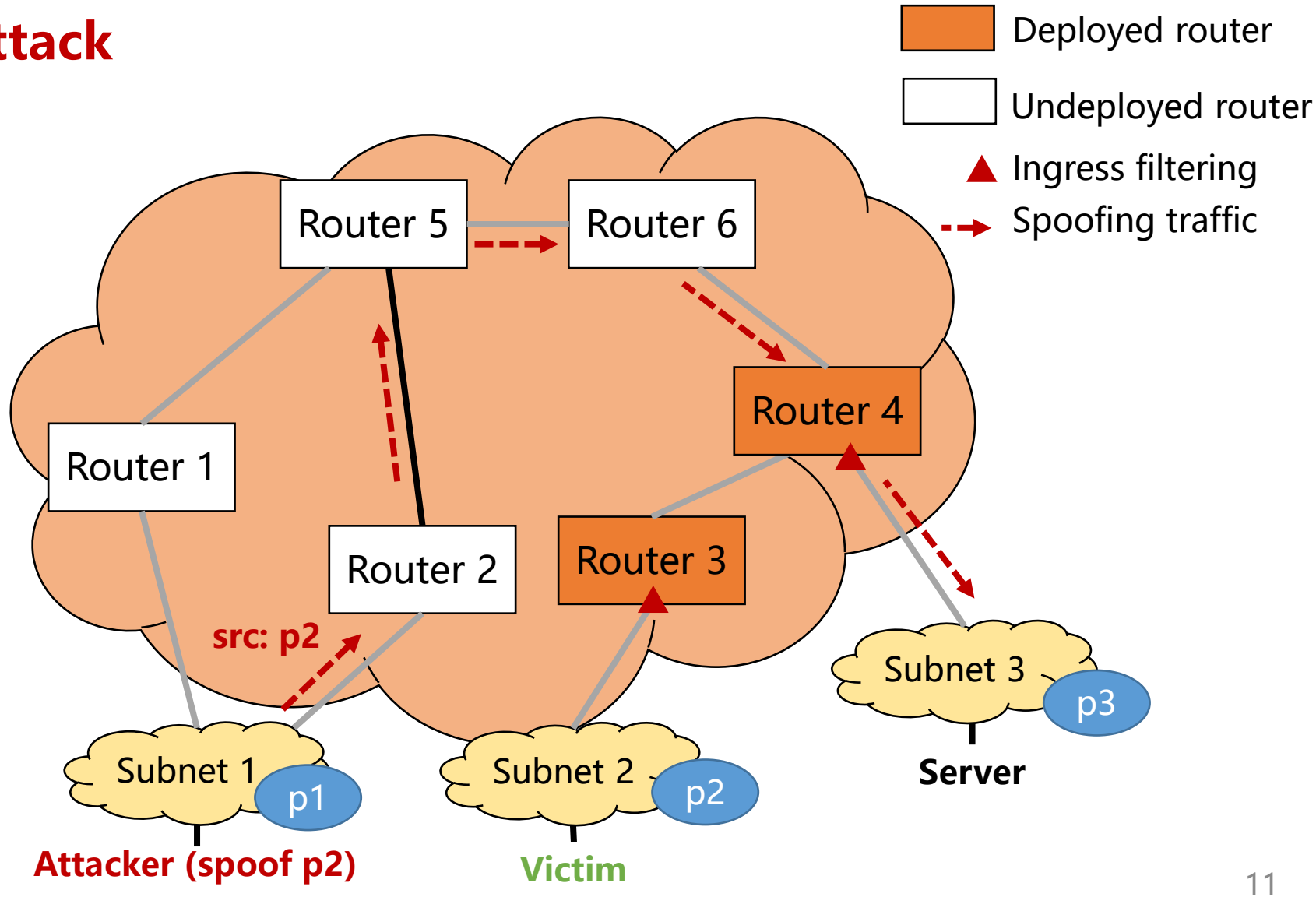
Scenario 4: Reflection attack

- Attacker: Subnet 1
- Victim: Subnet 2
- Reflective server: Subnet 3

Behavior

When partially deployed:

- Deployed subnet cannot forge source addresses
- Undeployed subnet can forge source addresses of deployed subnet to conduct reflection attack



Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Problem Statement

- Problem #1: Inaccurate validation
  - Behavior gap: improper block under asymmetric routing
  - Reason: conducting SAV based on local FIB which may not match the real data-plane forwarding path from the source
- Problem #2: Limited protection
  - Behavior gap: failing to block spoofing traffic from inbound direction or misbehaved routers
  - Reason: only working for traffic from directly connected subnets
- Problem #3: Misaligned incentive
  - Behavior gap: suffering reflection attacks even when SAV mechanisms have been deployed by victim
  - Reason: constraining the behavior of the deployed subnet rather than protecting the deployed subnet from attack

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Requirements for New Intra-domain SAV Mechanism

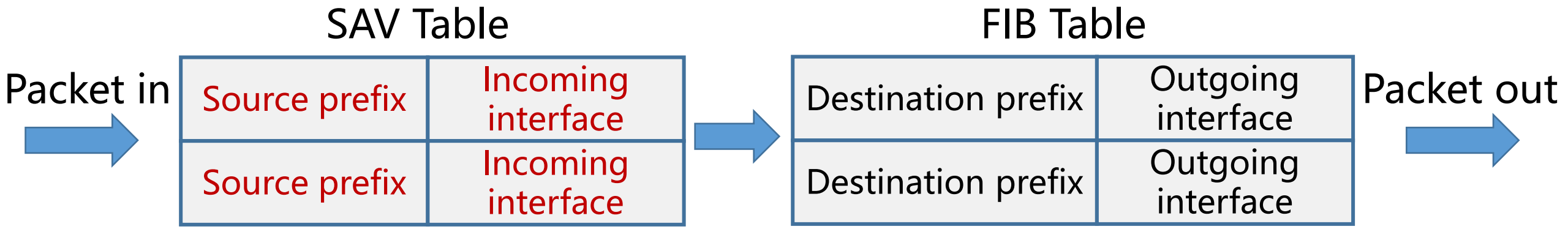
- Requirement #1: The mechanism must discover the real data-plane forwarding path among routers
  - Avoid improper block under asymmetric routing
- Requirement #2: The mechanism must work for all kinds of intra-domain spoofing traffic
  - Validate traffic from all directions
  - Block spoofing traffic as close to the source as possible
- Requirement #3: The mechanism must provide direct incentives
  - Help deployed subnet mitigate reflection attacks from undeployed subnet
- Requirement #4: The mechanism must not induce much overhead
  - Avoid data-plane packet modification
  - Limit the number of control-plane protocol messages

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Preliminary Idea

- SAV table generation
  - Discovering the real data-plane forwarding path among routers via hop-by-hop prefix notification, and generating SAV tables in routers along the path
    - Each router learns the real incoming interfaces for source addresses of the deployed area
- Data-plane SAV
  - Validating packets received from all directions based on local SAV table
  - Protecting source addresses of deployed area from being forged



Thanks!

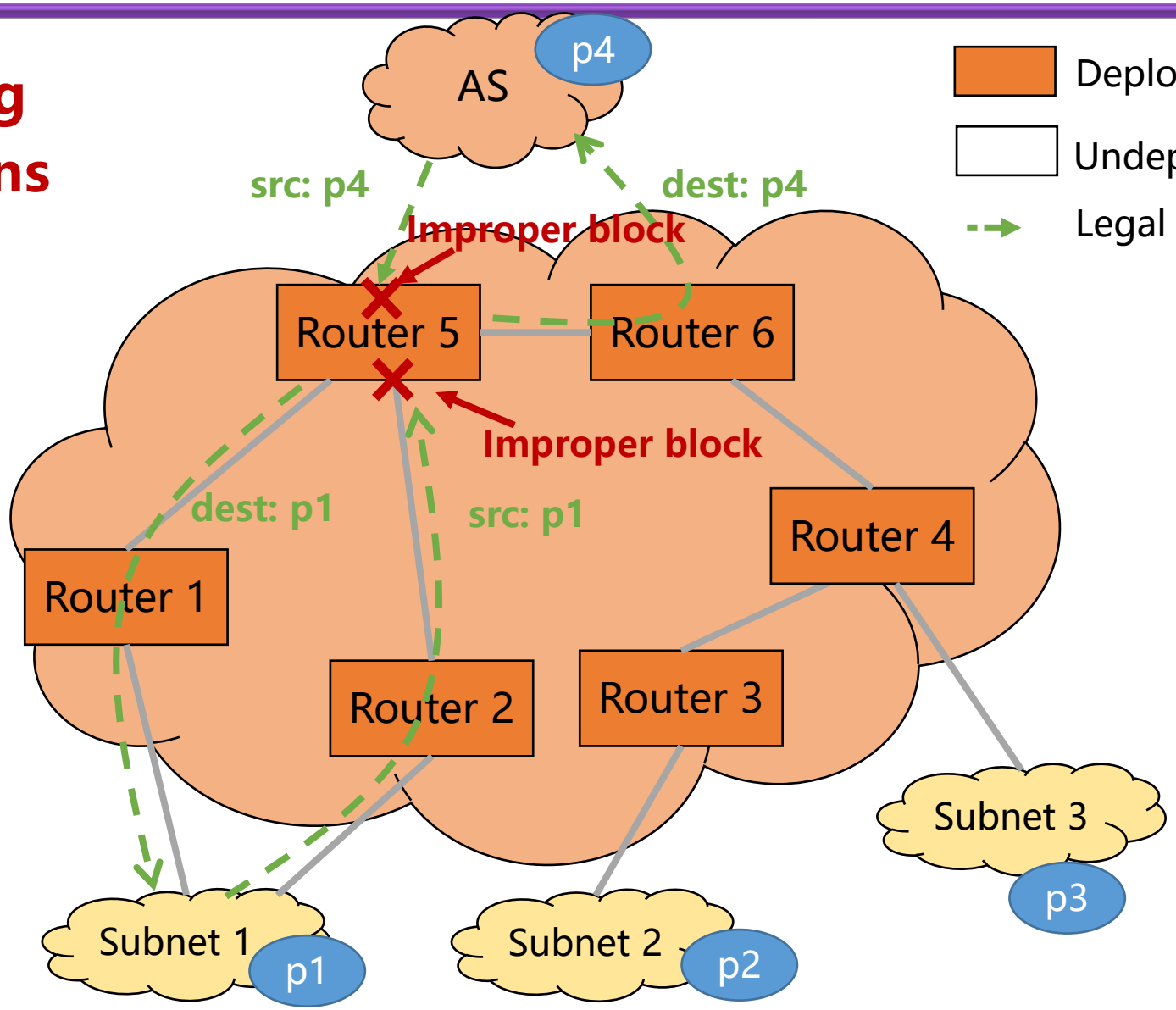
Backup slides

Gap #5: Improper Block

- **Scenario 5: Implementing strict uRPF for all directions**

Behavior

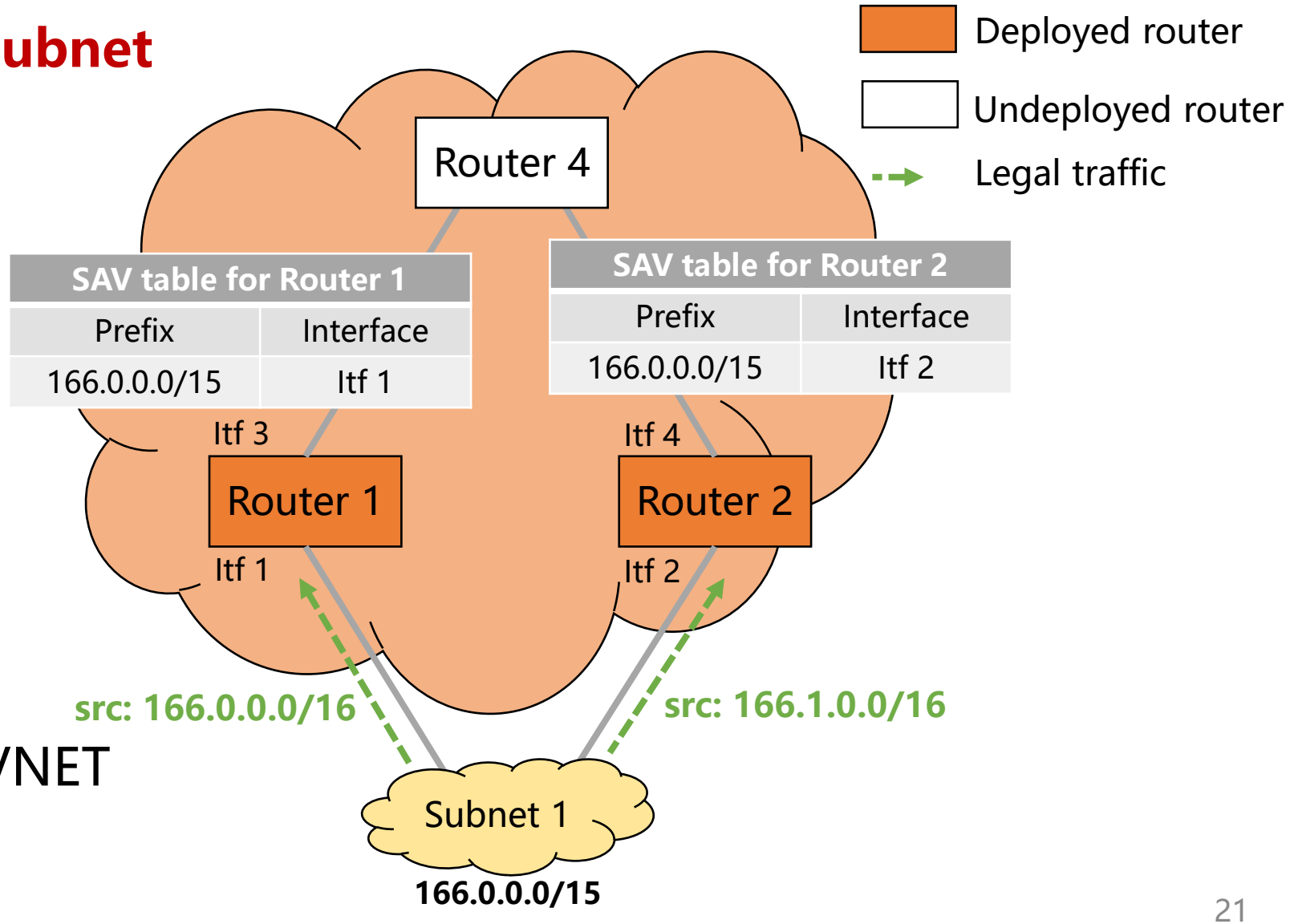
- If Router 5 applies strict uRPF for all direction
  - Improper block under asymmetric routing



Intra-domain SAVNET: Accurate Validation

Scenario 1: Multi-homed Subnet

- Router 1 only advertises 166.1.0.0/16 in IGP
- Router 2 only advertises 166.0.0.0/16 in IGP



Behavior

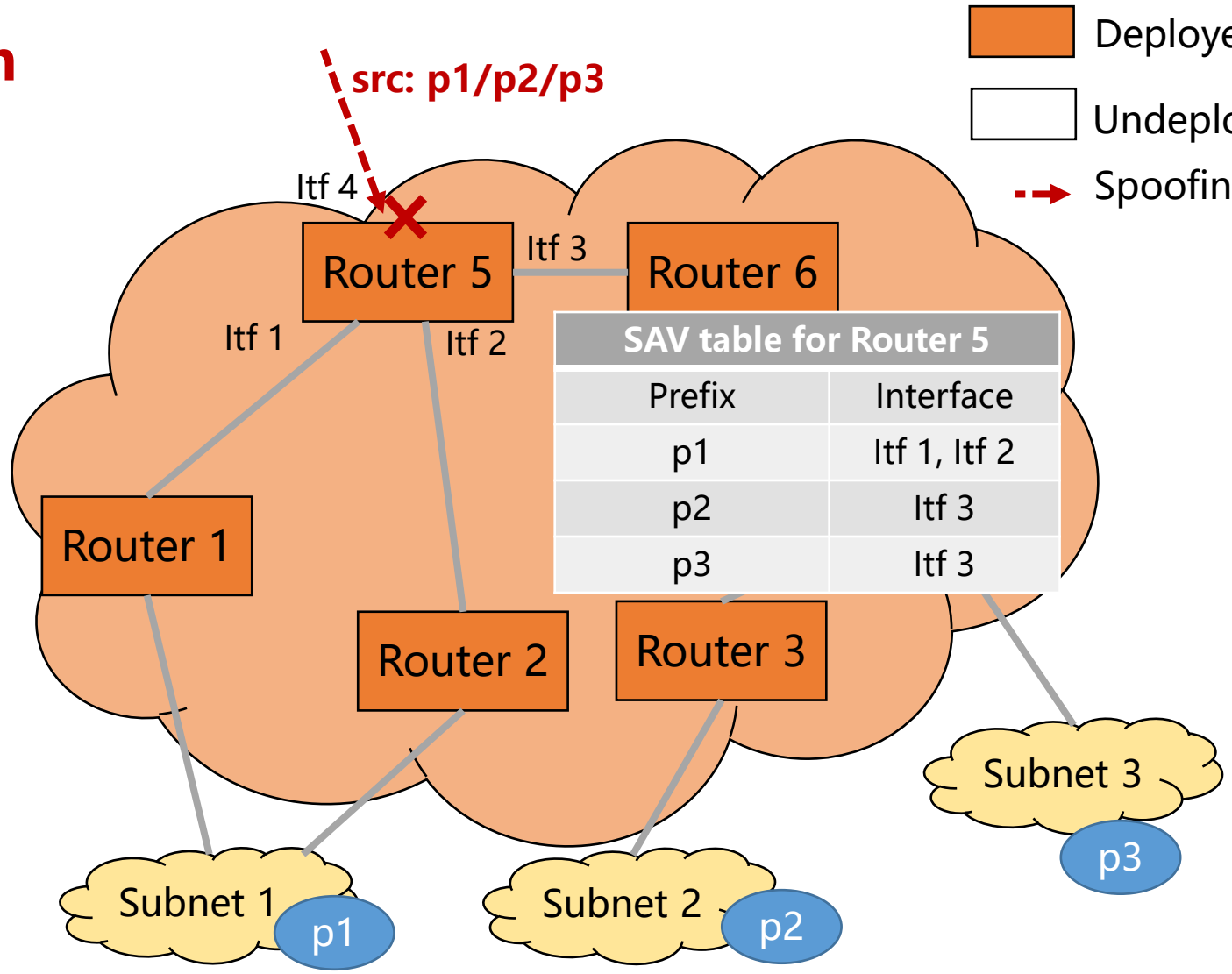
- If applying strict uRPF
  - Improper block
- If applying ACL-based SAV
  - Manual update
- If applying intra-domain SAVNET
  - Works well

Intra-domain SAVNET: All-round Protection (1)

Scenario 2: Spoofing from Inbound Direction

Behavior

- If applying ingress filtering
  - ◆Cannot block spoofing traffic from inbound direction
- If applying intra-domain SAVNET
  - ◆Effectively blocks spoofing traffic from inbound direction

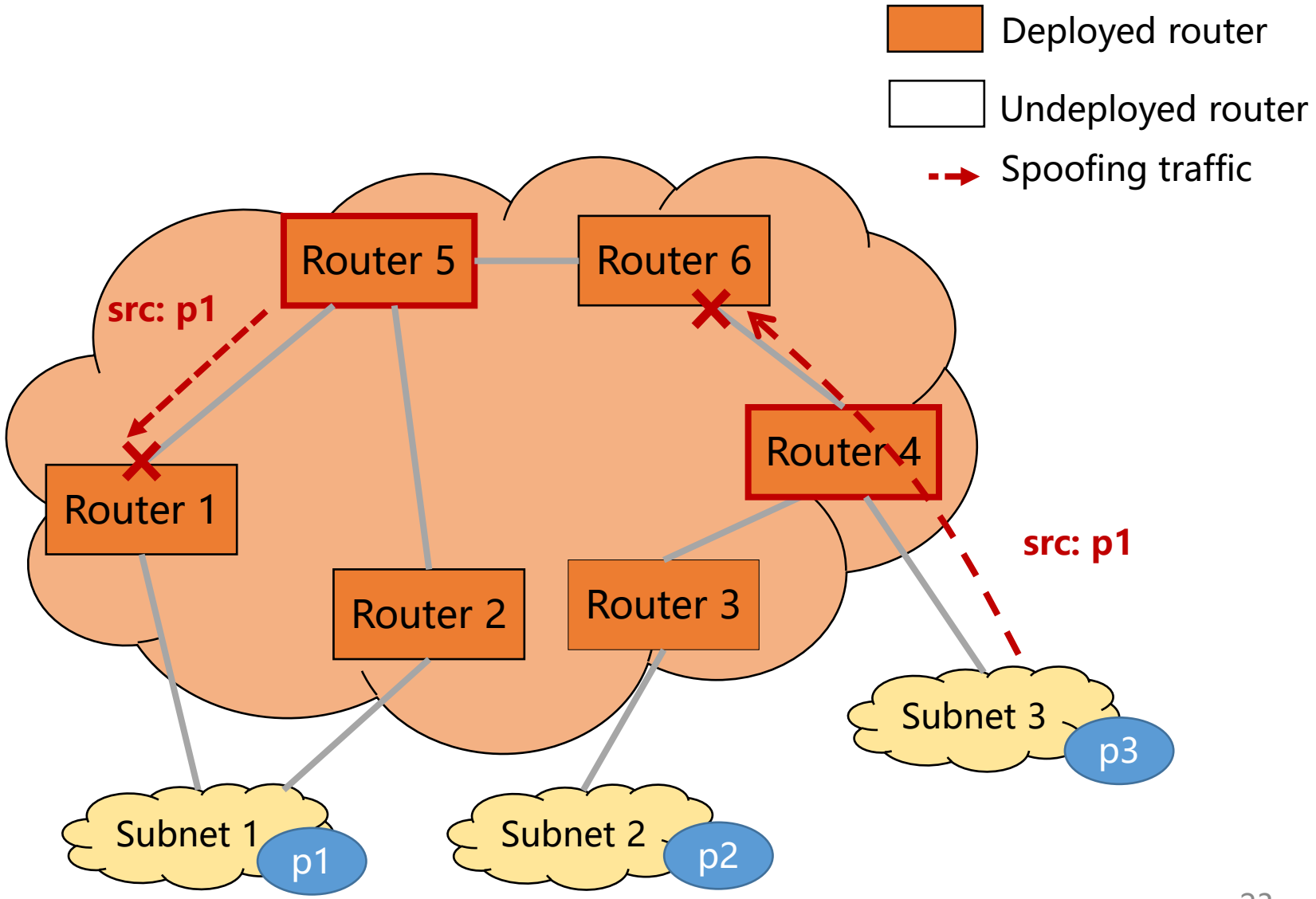


Intra-domain SAVNET: All-round Protection (2)

- **Scenario 3: Misbehaved or compromised router**

Behavior

- If applying ingress filtering
  - Cannot block spoofing traffic
- If applying intra-domain SAVNET
  - Effectively blocks spoofing traffic



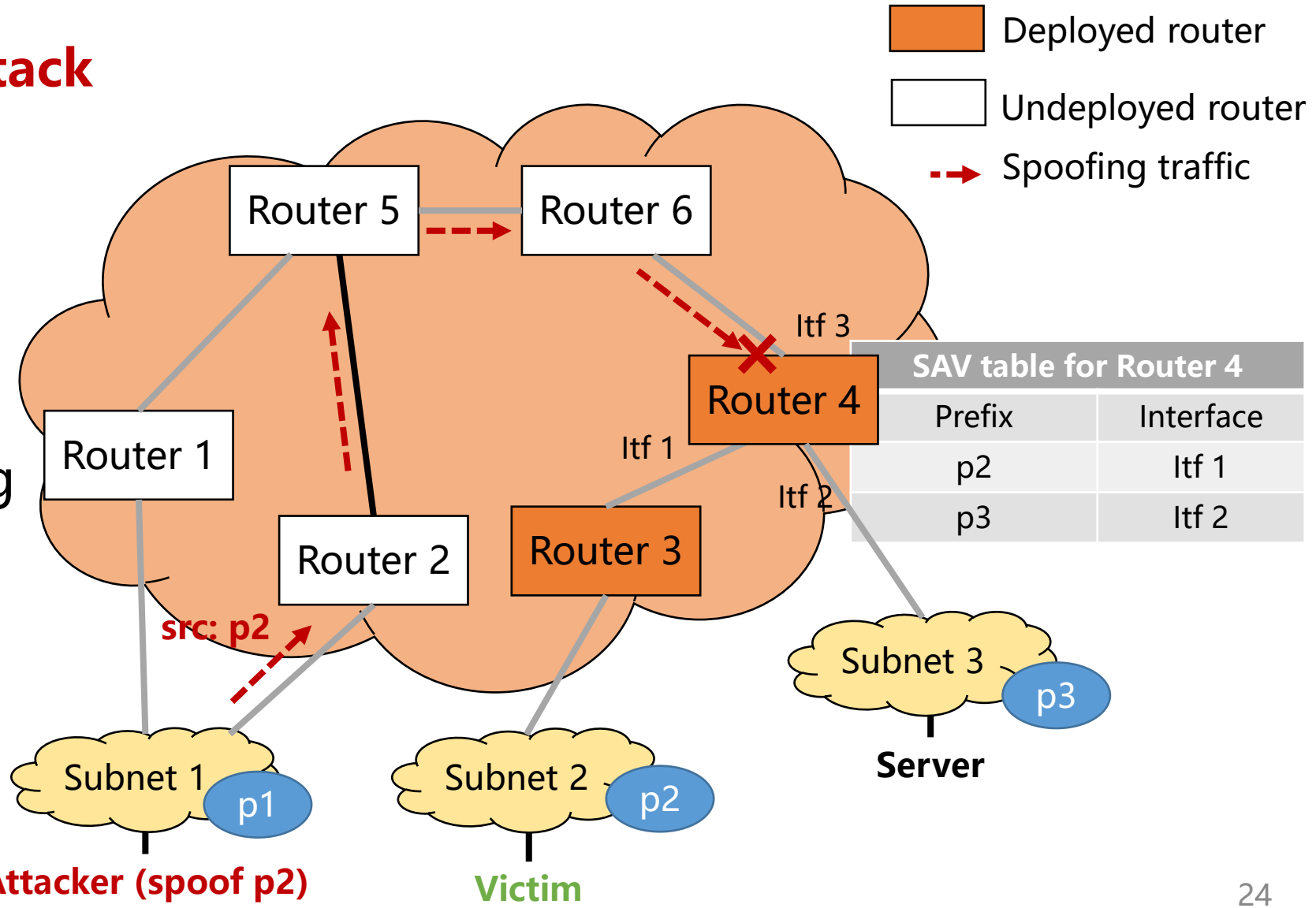
Intra-domain SAVNET: Aligned Incentive

Scenario 4: Reflection attack

- Attacker: Subnet 1
- Victim: Subnet 2
- Reflective server: Subnet 3

Behavior

- If applying ingress filtering
  - Cannot block spoofing traffic
- If applying intra-domain SAVNET
  - Effectively blocks spoofing traffic



Intra-domain SAVNET: Features

- [Resilience:] Each router builds a SAV table to validate traffic from all directions
  - 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:] Source prefixes of deployed subnets are protected by all deployed routers
  - Traffic forging these source prefixes can be blocked as close to the traffic source as possible
  - Mitigate reflective DDoS attack targeting at these source prefixes
- [Cost:] Control-plane protocol extension, without data-plane packet modification
  - Existing IGP routing protocols are extended to carry the necessary information to build the SAV tables in routers