draft-li-savnet-intra-domain-problem-statement-03, IETF 115 SAVNET WG

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

Nov 11, 2022

Background

□ Goals

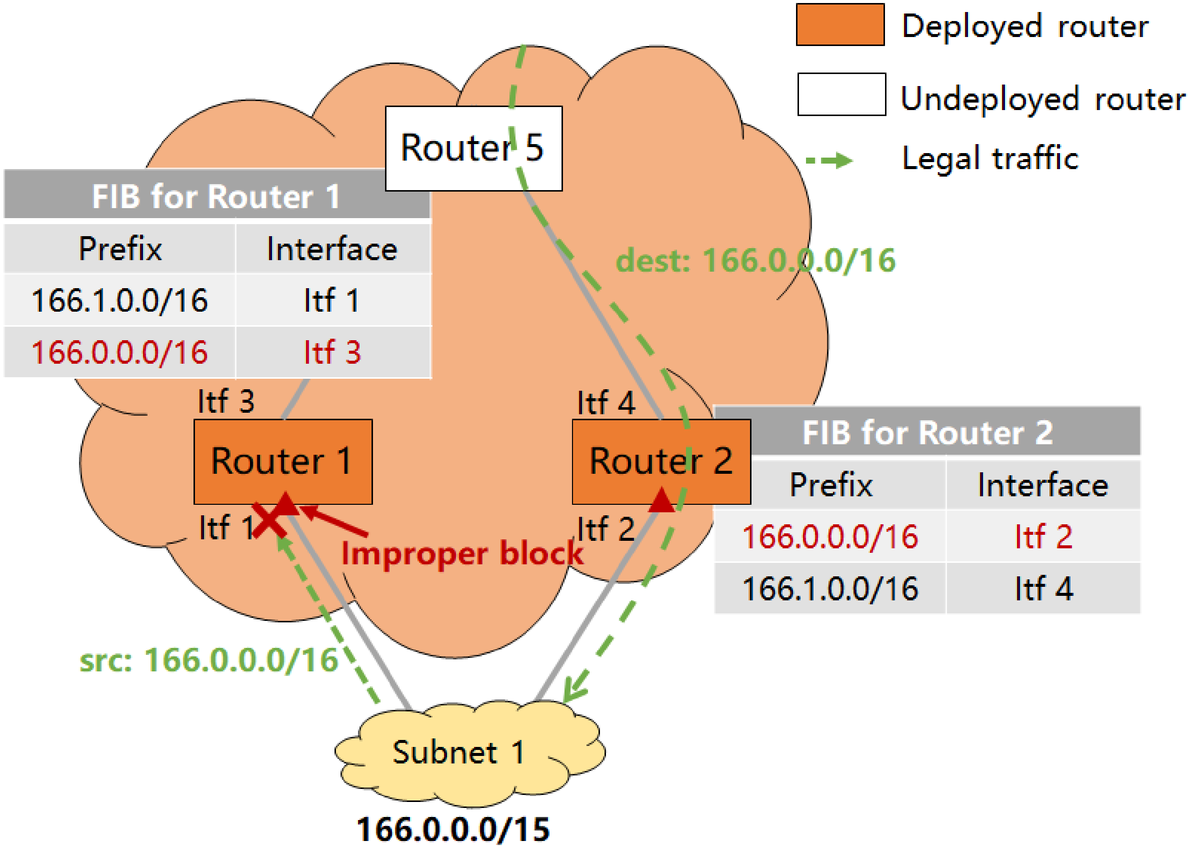
- ◆Provide the gap analysis of existing intra-domain SAV mechanisms
- ◆Summarize the fundamental problems of existing intra-domain SAV mechanisms
- ◆Define the requirements for the new intra-domain SAV mechanism

□ Versions

- ◆draft-li-savnet-intra-domain-problem-statement-00, IETF 114 SAVNET WG
- ◆draft-li-savnet-intra-domain-problem-statement-01, Sep 25, 2022
- ◆draft-li-savnet-intra-domain-problem-statement-02, Oct 22, 2022
- ◆draft-li-savnet-intra-domain-problem-statement-03, IETF 115 SAVNET WG

Gap Analysis in Version-00

Scenario #1: Multi-homed Subnet



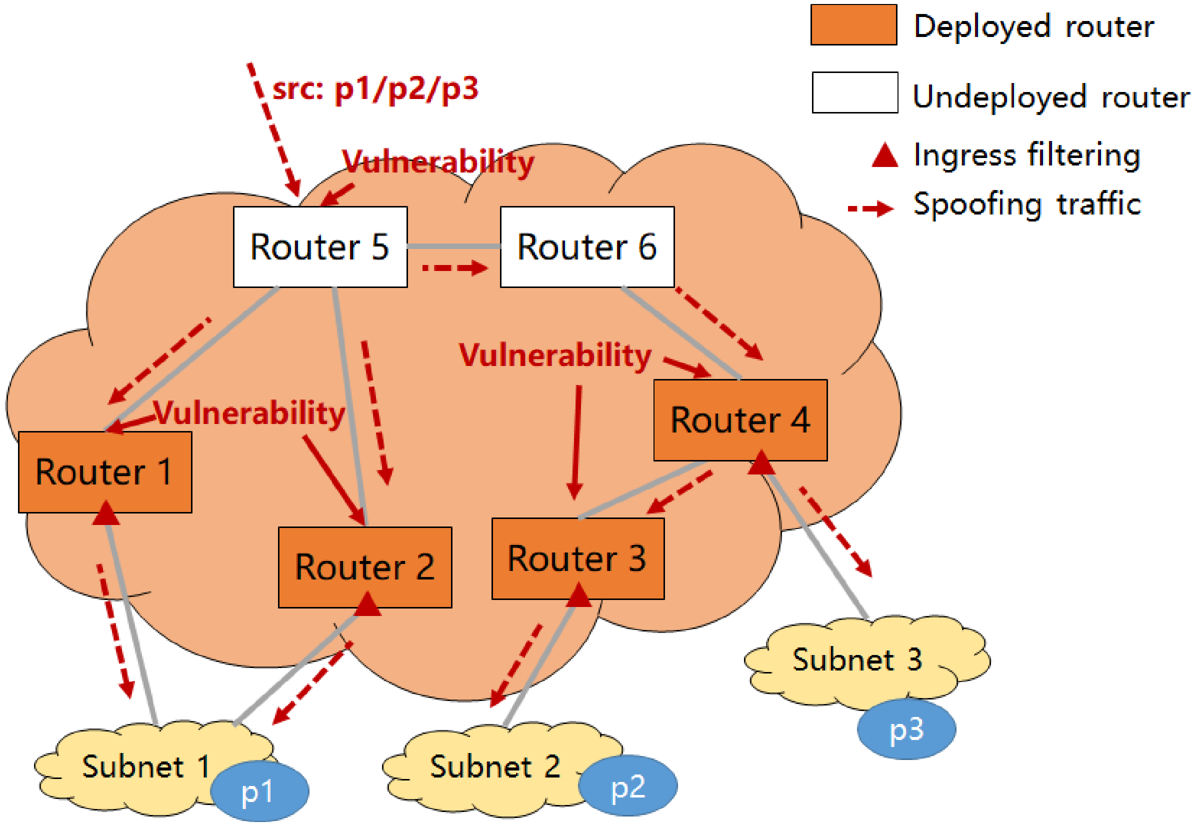
FIB for Router 1

Prefix	Interface
166.1.0.0/16	Itf 1
166.0.0.0/16	Itf 3

FIB for Router 2

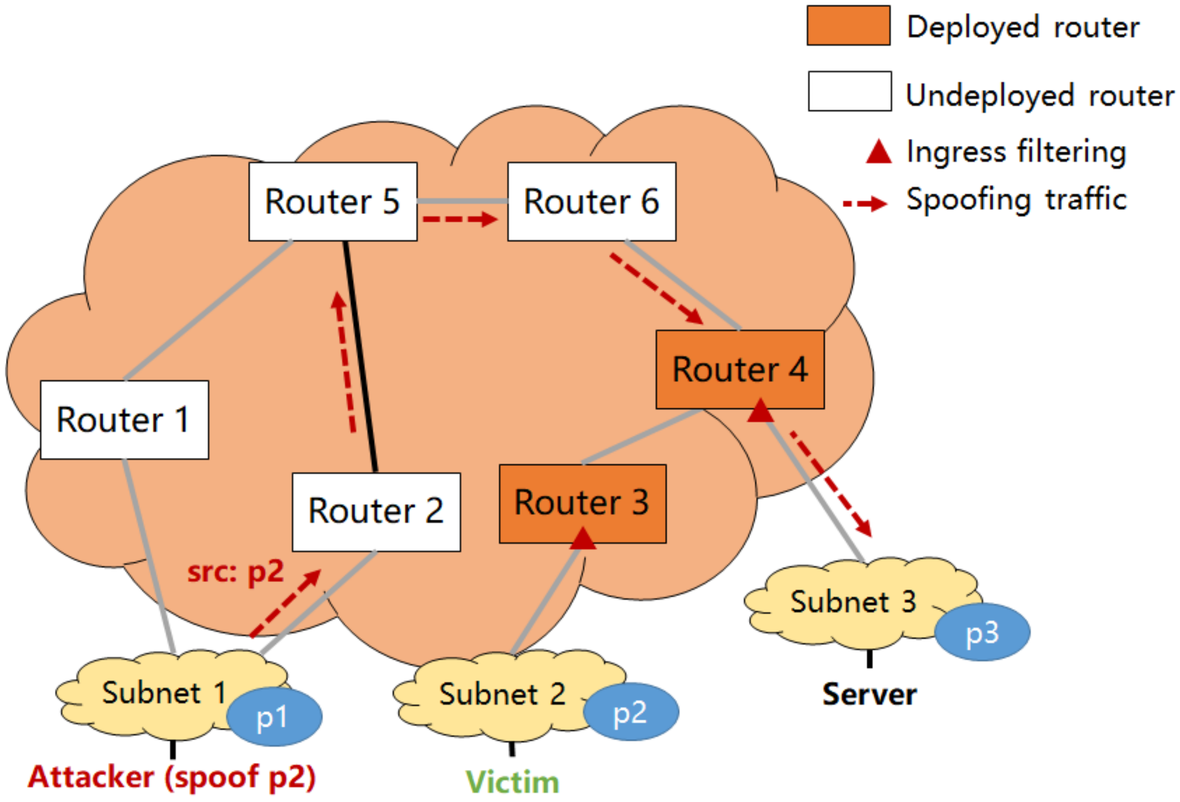
Prefix	Interface
166.0.0.0/16	Itf 2
166.1.0.0/16	Itf 4

Scenario #2: Spoofing from inbound direction

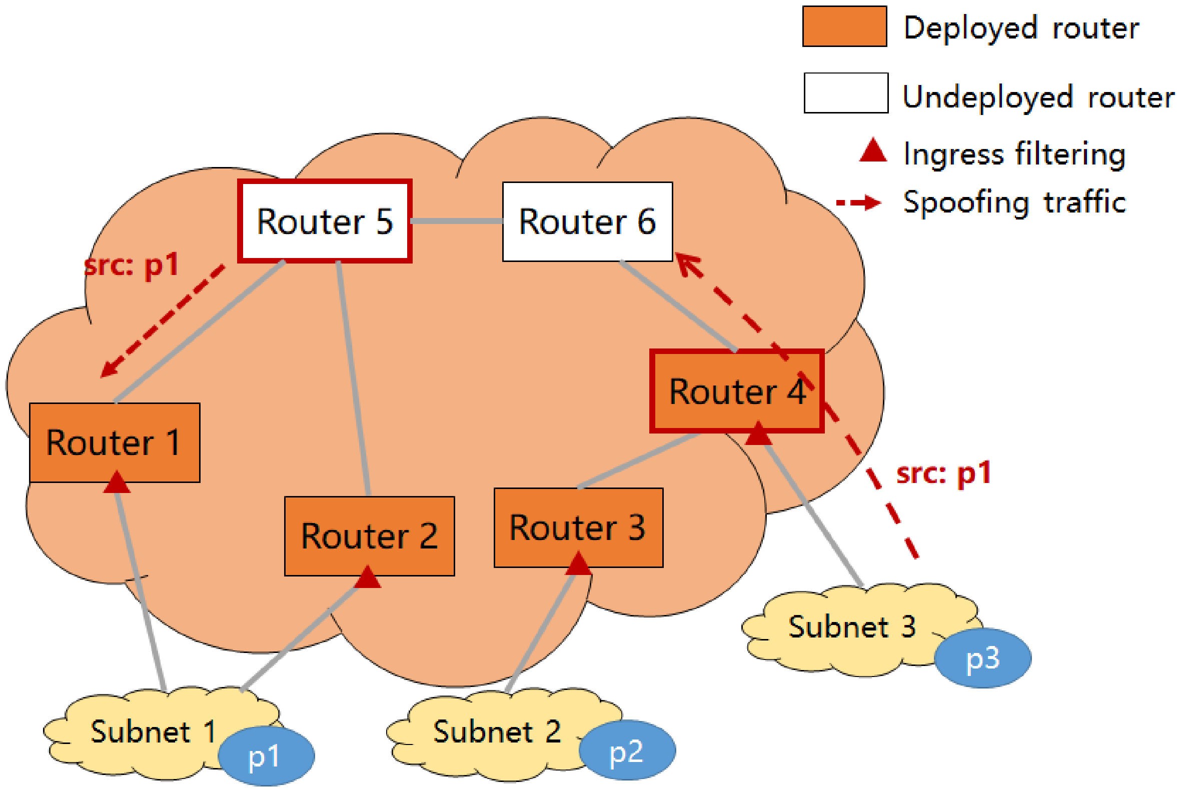


Gap Analysis in Version-00

Scenario #3: Partial deployment

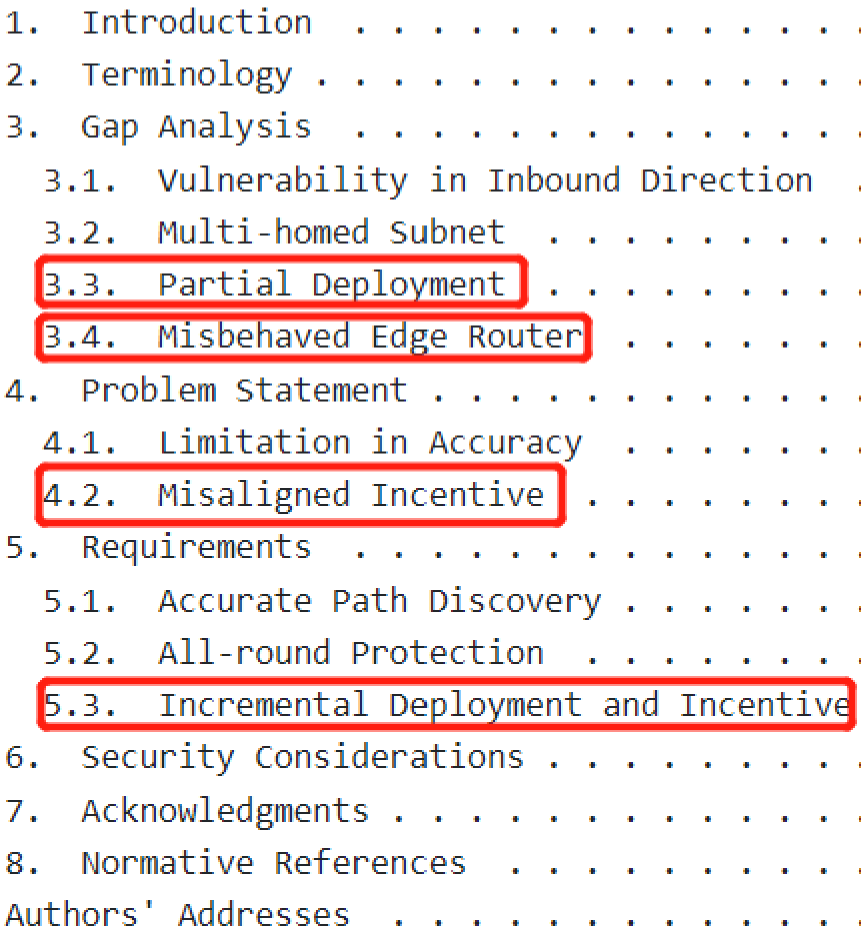


Scenario #4: Misbehaved router



Comments on Version-00

Version-00



- □ Why could not you deploy SAV at all routers in the intra-domain network?
- □ Defining network elements are trusted vs untrusted is hard
- □ Misaligned incentive means “the costs of deploying SAV are paid by an operator itself while its benefits are only experienced by other operators”, but an intra-domain network is rarely managed by multiple operators
- □ Are we talking about non-IP packets as well?
- □ ......

Main Updates Compared to Version-00

- □ Updates in gap analysis
  - ◆Explain the reasons for partial deployment
  - ◆Remove the scenario of “misbehaved router”
- □ Updates in problem statement
- □ Updates in requirements
- □ Two new sections

Reasons for Partial Deployment

- □ There are two main reasons for partial deployment
  - ◆Technical limitations make it hard to deploy SAV on all routers
    - ➢ACL-based SAV requires manual configuration in dynamic networks
    - ➢Strict uRPF ingress filtering blocks legal traffic in the scenario of asymmetric routing
  - ◆Some routers cannot support SAV due to router capabilities, versions, and vendors
- □ Behavior gap in the scenario of partial deployment
  - ◆When ingress filtering is partially deployed, spoofing traffic from undeployed edge routers cannot be blocked by other routers

Main Updates Compared to Version-00

□ Updates in gap analysis

□ Updates in problem statement

- ◆Remove the problem of “ misaligned incentive ”
- ◆Add the problem of “ high operational overhead”
- ◆Revise the description of other problems

□ Updates in requirements

□ Two new sections

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 outside AS and undeployed edge router

◆Reason: only working for traffic from directly connected subnets

□ Problem #3: High operational overhead

◆Behavior gap: manual update when routing state changes

◆Reason: failing to adapt to dynamic or asymmetric routing scenarios

Main Updates Compared to Version-00

- □ Updates in gap analysis
- □ Updates in problem statement
- □ Updates in requirements
    - ◆Remove the requirement of “ direct incentive ”
    - ◆Add the requirement of “ acceptable overhead ”
    - ◆Revise the description of other requirements
- □ Two new sections

Requirements for New Intra-domain SAV Mechanism

- □ Requirement #1: The mechanism MUST ensure accurate SAV
  - ◆Match real data-plane forwarding path
  - ◆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 (from outside AS and undeployed edge router) as close to the source as possible
- □ Requirement #3: The mechanism MUST not induce much overhead
  - ◆Minimize manual update
  - ◆Avoid data-plane packet modification
  - ◆Limit the number of control-plane protocol messages

Main Updates Compared to Version-00

□ Updates in gap analysis

□ Updates in problem statement

□ Updates in requirements

□ Two new sections

- ◆Intra-domain SAVNET work scope
- ◆Security considerations

Two new sections

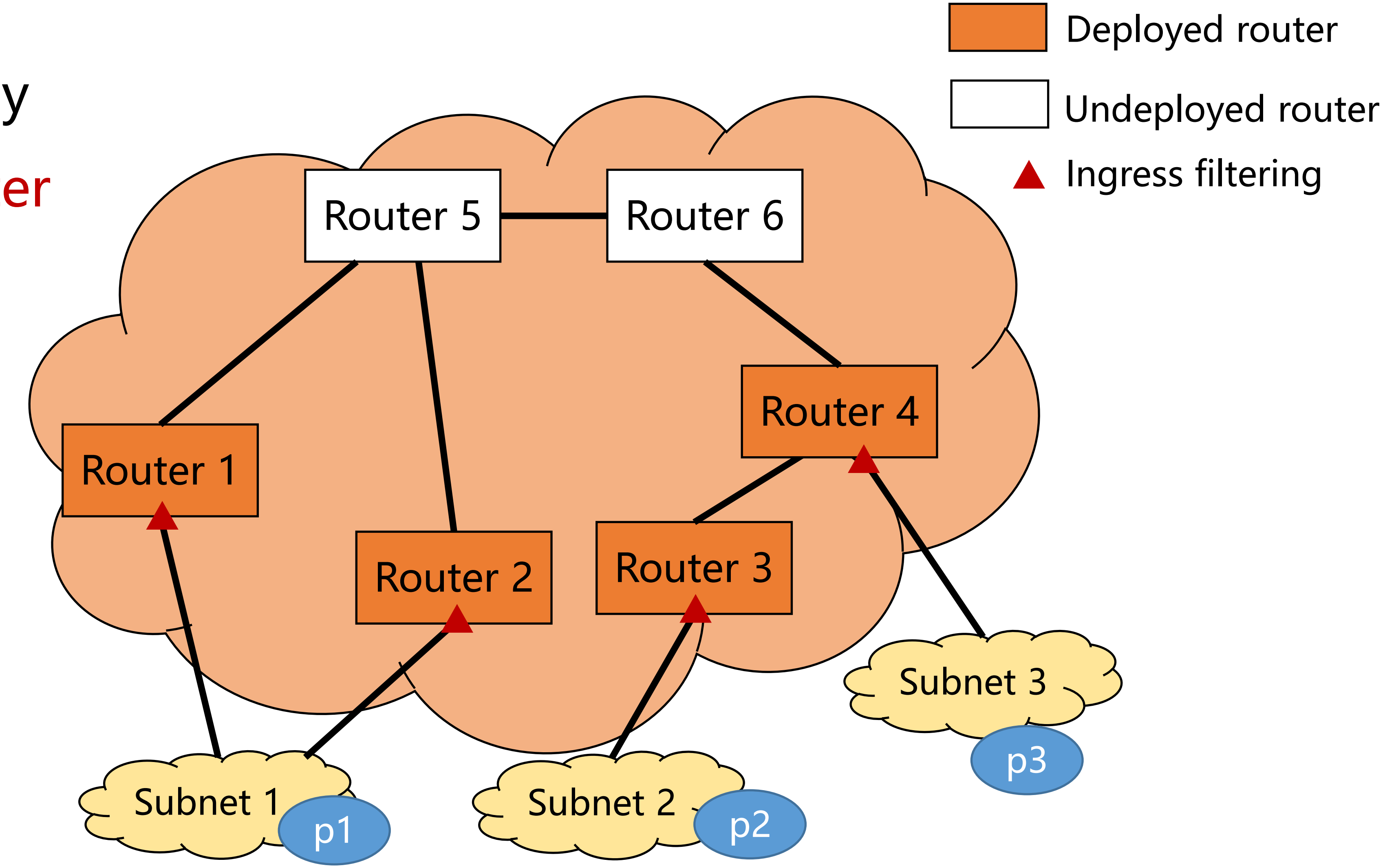
- Intra-domain SAVNET work scope
  - All IP-encapsulated scenarios are in scope
    - including both IPv4 and IPv6 addresses
  - Non-IP packets are out of scope
- Security considerations
  - SAVNET focuses on routing protocol-based mechanisms, so the security scope of intra-domain SAVNET should be similar to that of intra-domain routing protocols
    - Ensure integrity and authentication of control-plane protocol messages
    - Does not provide protection against compromised routers that poison existing control-plane protocols

Thanks!

Backup slides

Typical Adoption of Ingress filtering

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



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

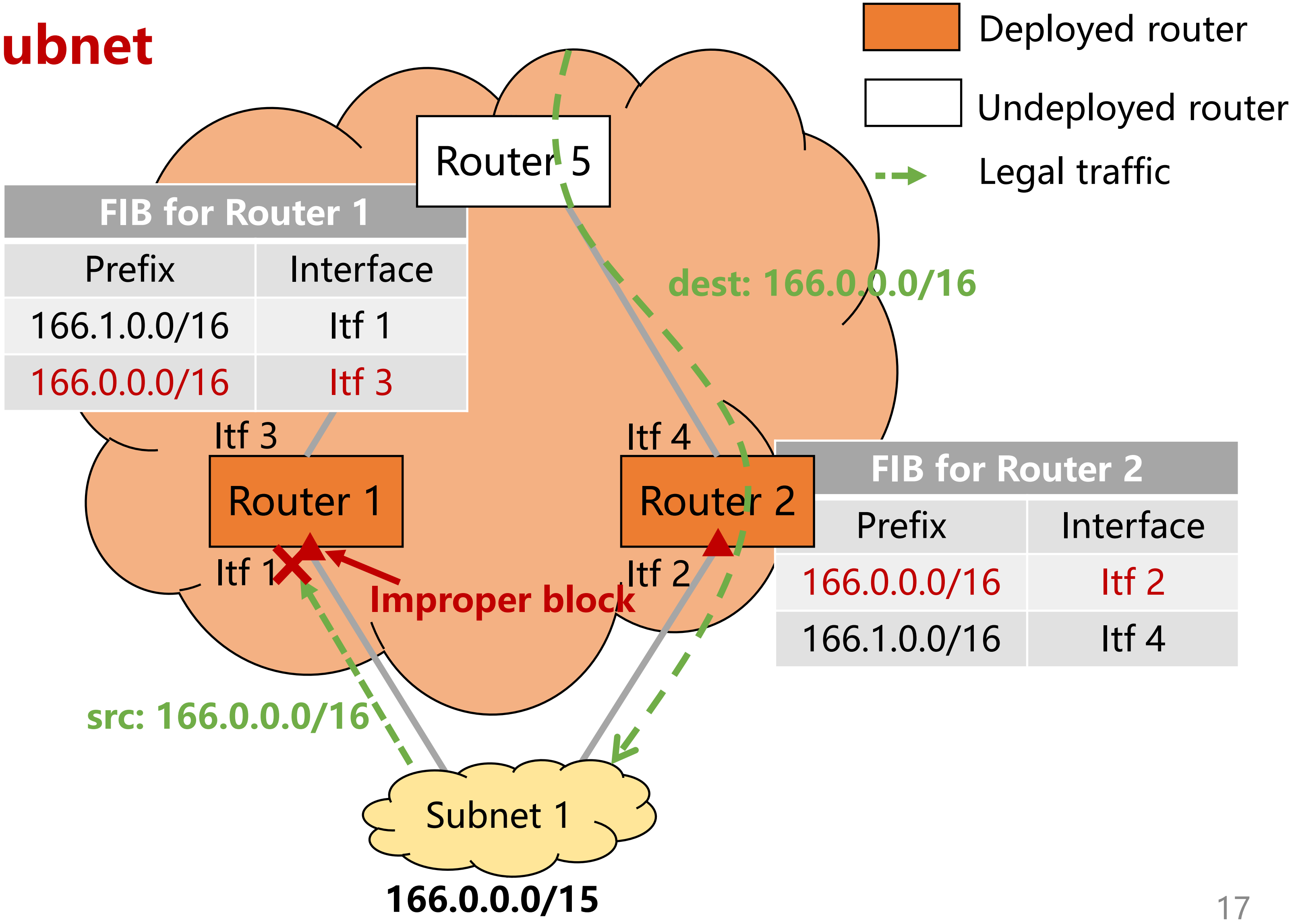
Behavior

□ If applying strict uRPF

- ◆Improper block

□ If applying ACL-based SAV

- ◆Manual update given prefix or topology update in Subnet 1



FIB for Router 1

Prefix	Interface
166.1.0.0/16	Itf 1
166.0.0.0/16	Itf 3

FIB for Router 2

Prefix	Interface
166.0.0.0/16	Itf 2
166.1.0.0/16	Itf 4

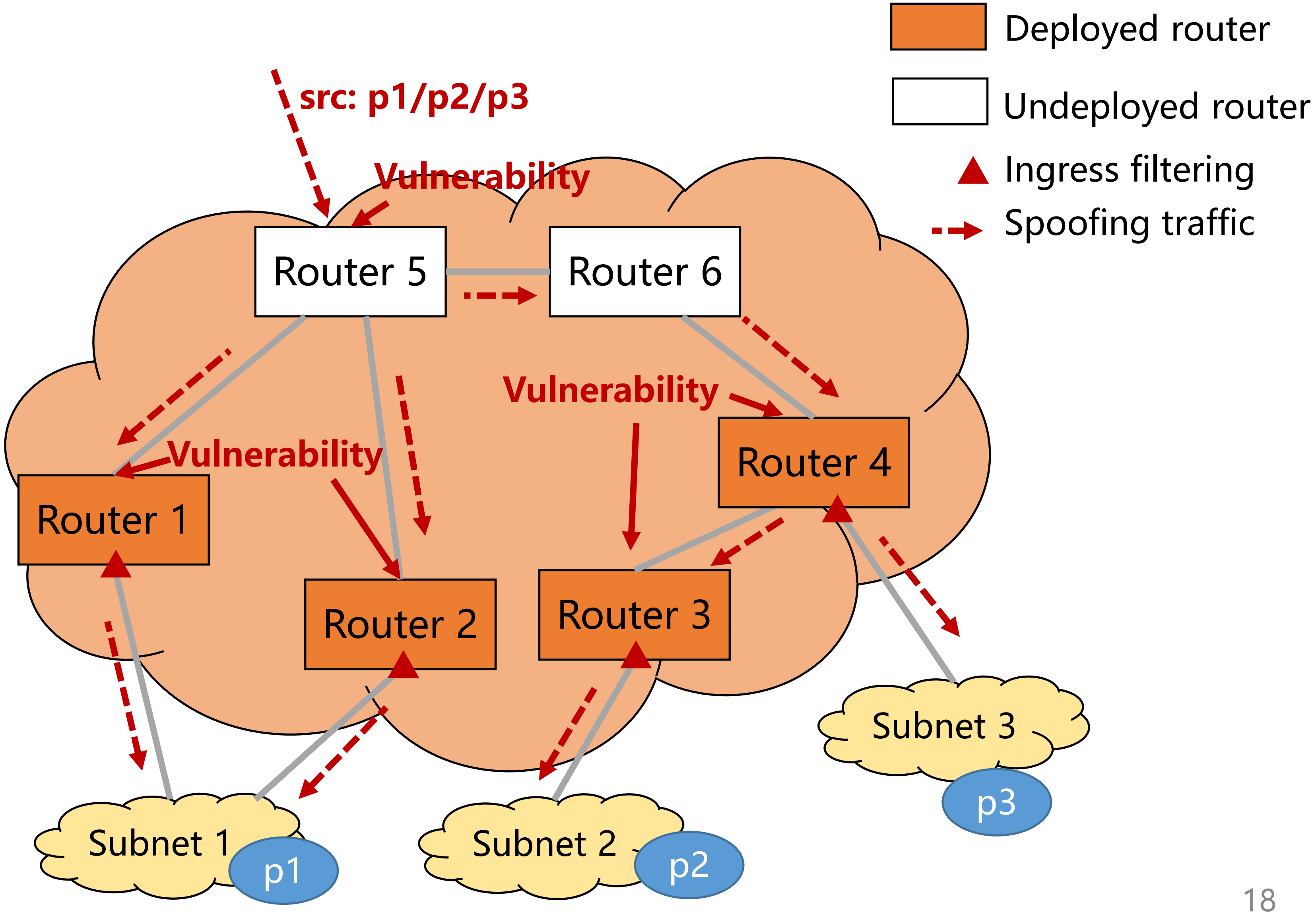
Gap #2: Vulnerability in Inbound Direction

□ **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 #2: Vulnerability in Inbound Direction

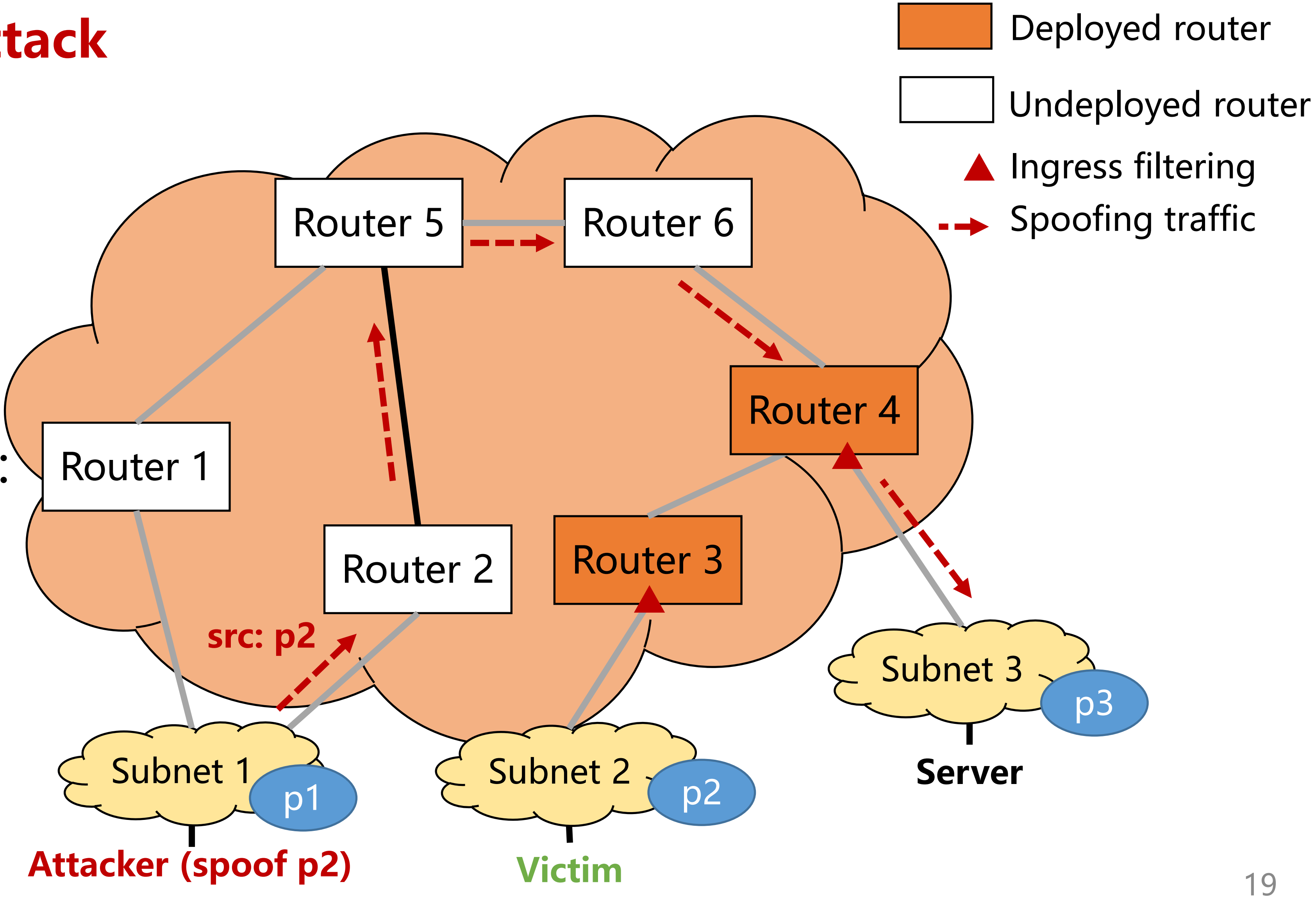
□ Scenario 3: Reflection attack

- ◆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



Deployed router
Undeployed router
Ingress filtering
Spoofing traffic
Router 5
Router 6
Router 4
Router 1
Router 2
Router 3
src: p2
Subnet 1
p1
Subnet 2
p2
Subnet 3
p3
Server
Attacker (spoof p2)
Victim