# openPenny

***An Open-Source Tool to Identify Non-Spoofed Traffic***

**Presented by Petros Gigis**

(In collaboration with UCL)

RIPE NCC Open House

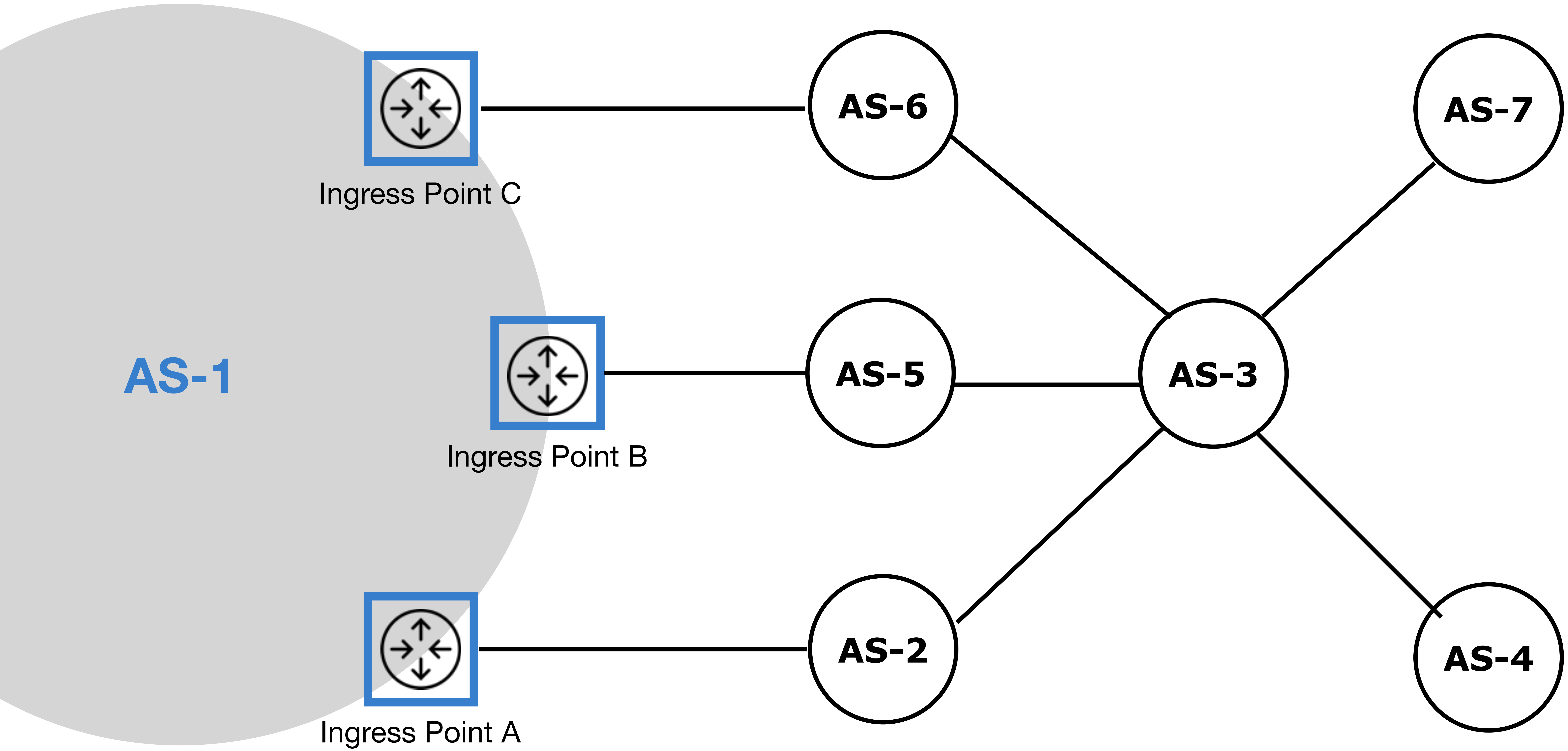
6 February 2025

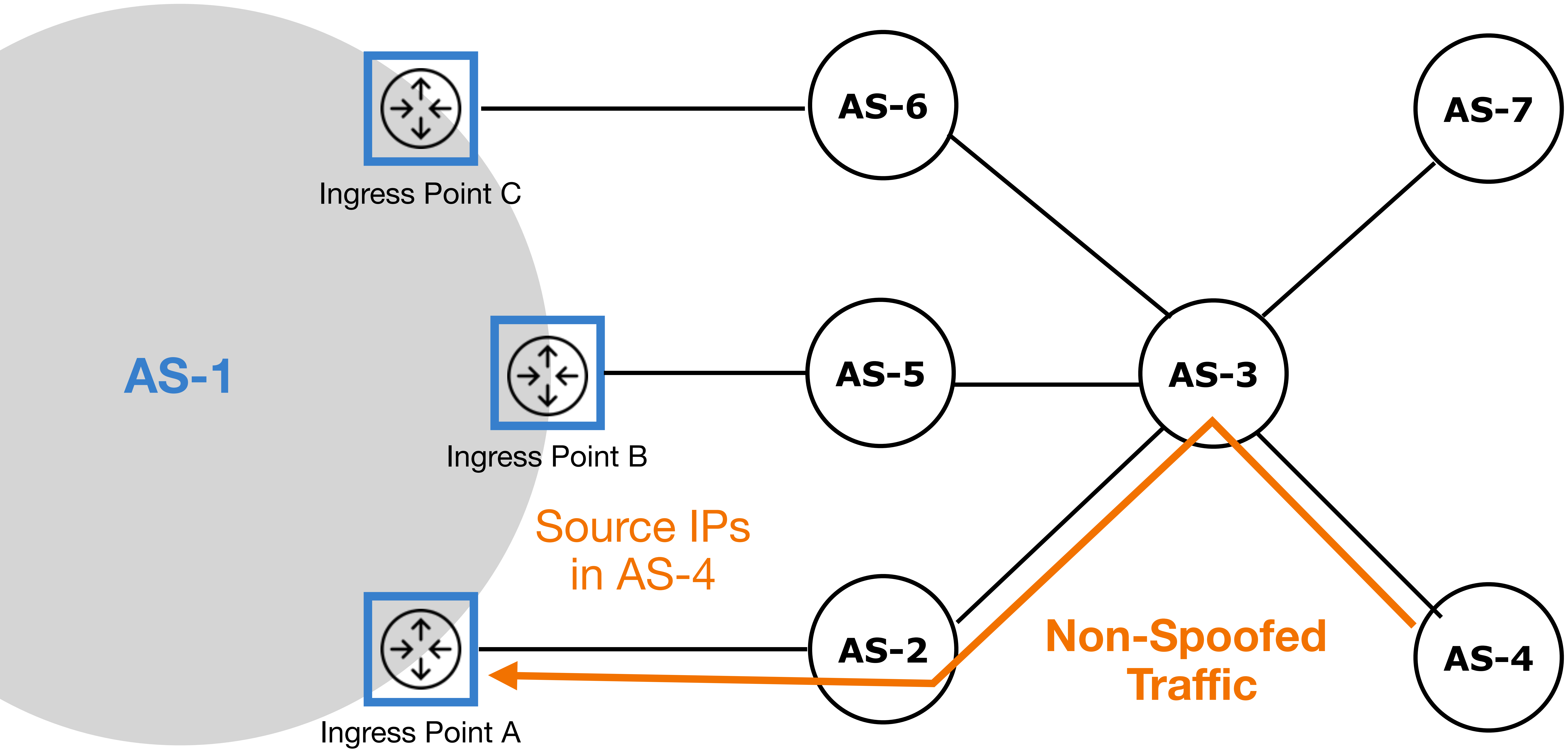
# Detecting Non-Spoofed Traffic is Important

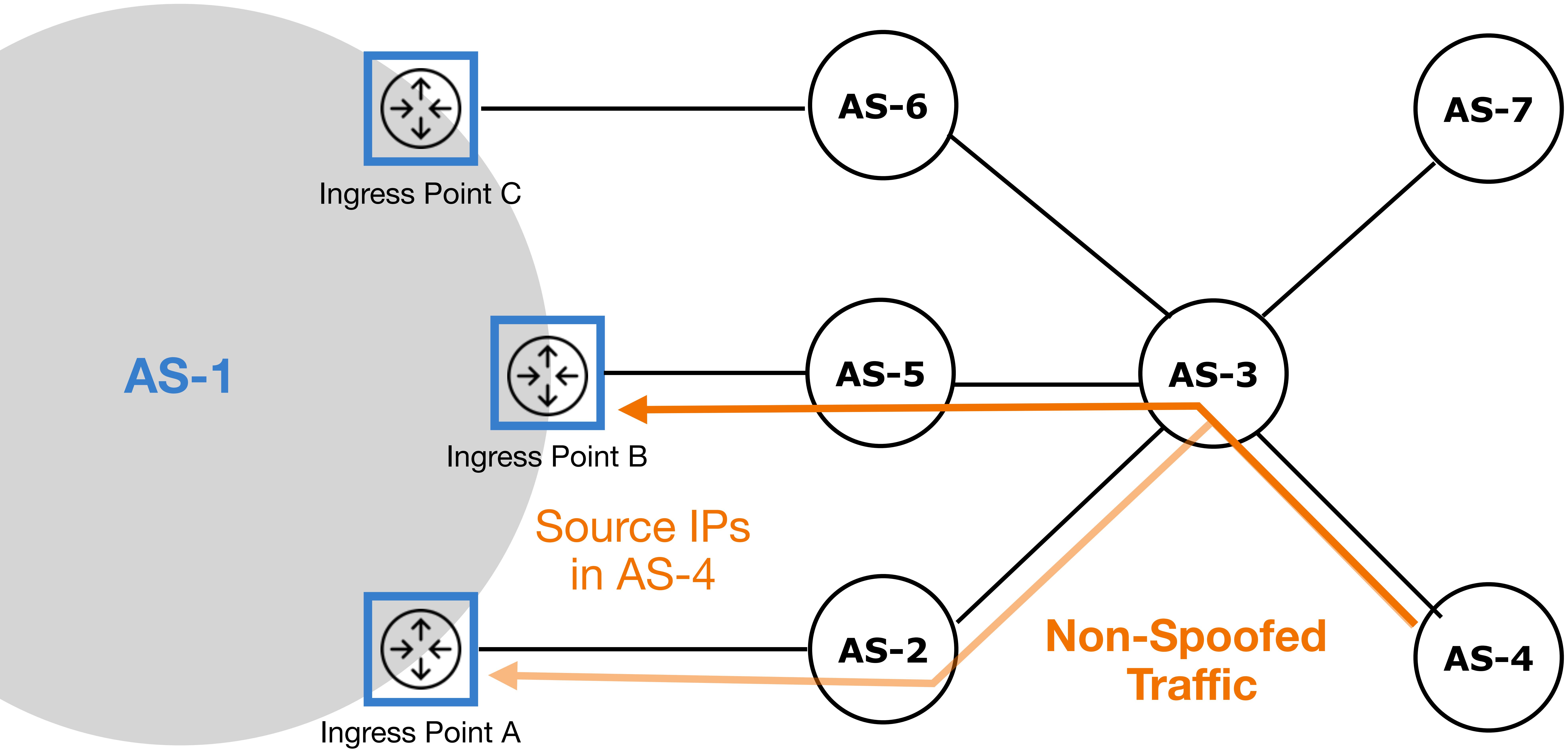
- **Scenario: An ISP receives unexpected traffic in an ingress point.**
  - Easily detect using ACLs and packet counters.
  - However, it cannot determine whether the traffic represents a problem or is just spoofed noise.

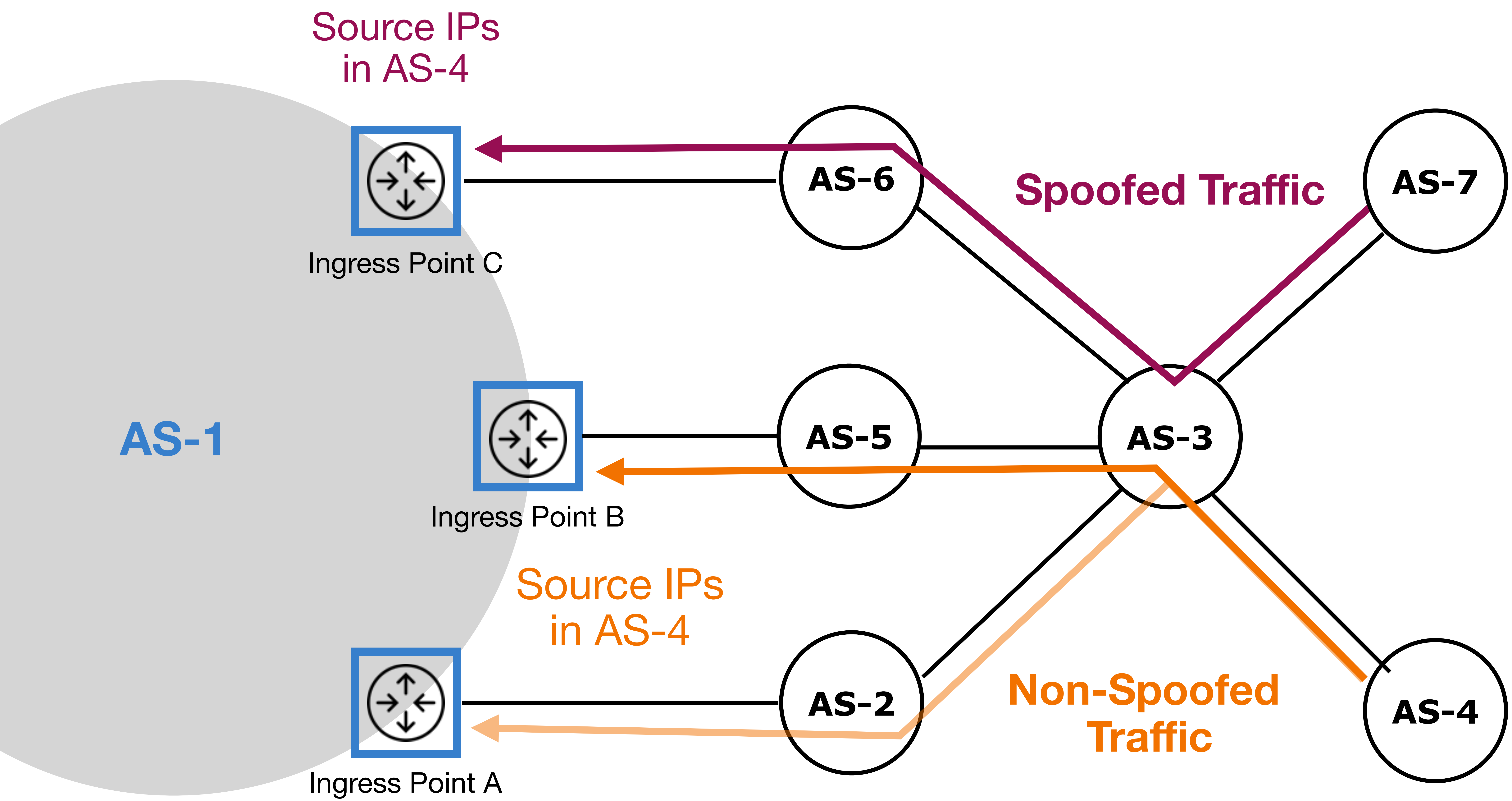
- **ISPs lack the capability to distinguish non-spoofed traffic in real-time.**

- Detecting non-spoofed traffic at an unexpected ingress point helps identify:
  (i) misconfigurations, (ii) sub-optimal routing policies,
  (iii) commercial agreement violations and (iv) hijacks.

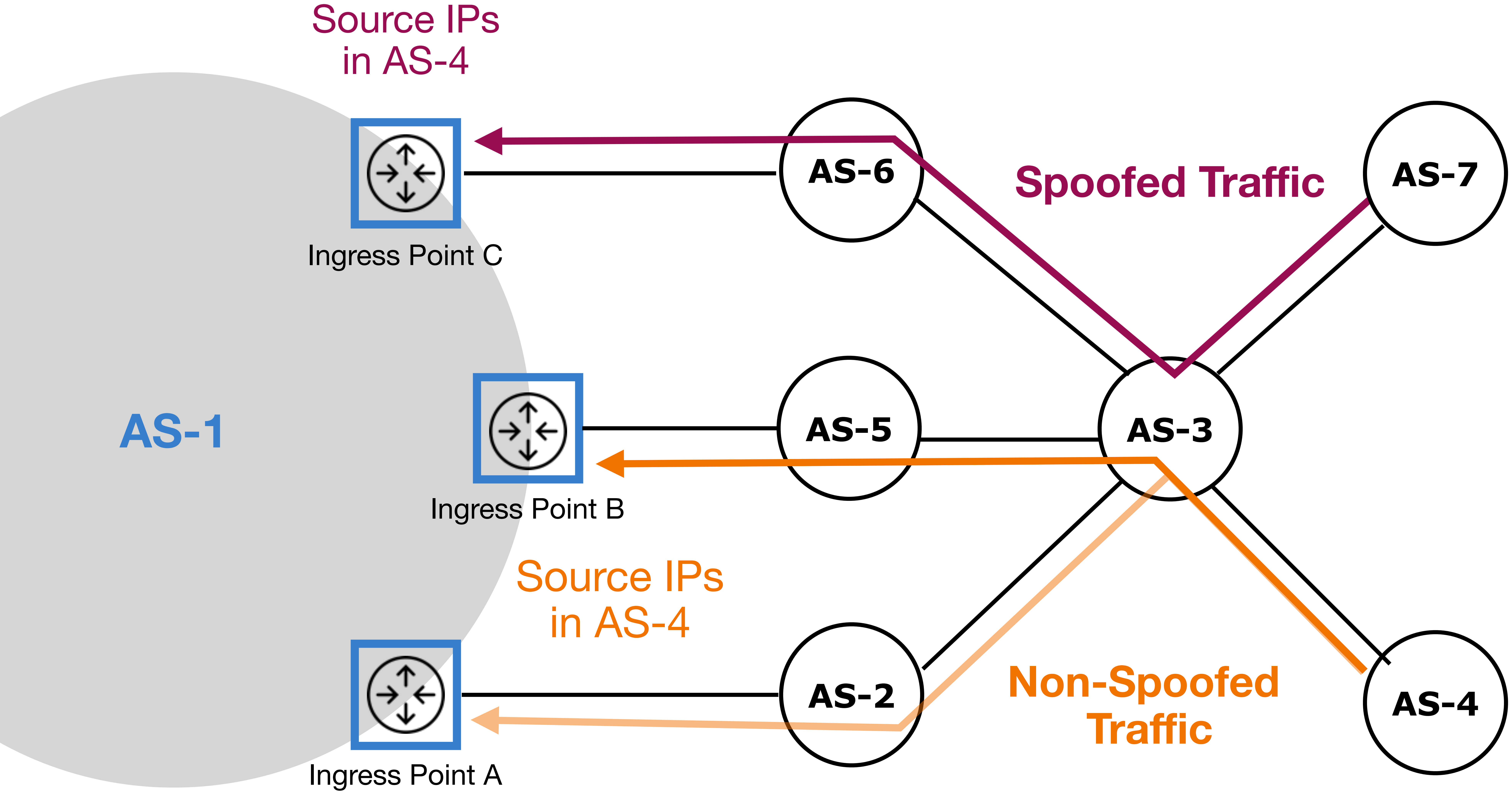

AS-1
Ingress Point C
Ingress Point B
Ingress Point A
AS-6
AS-5
AS-2
AS-3
AS-7
AS-4


AS-1
Ingress Point C
Ingress Point B
Ingress Point A
AS-6
AS-7
AS-5
AS-3
AS-2
AS-4
Source IPs
in AS-4
Non-Spoofed
Traffic


AS-6
AS-7
AS-1
Ingress Point C
AS-5
AS-3
Ingress Point B
Source IPs
in AS-4
AS-2
Non-Spoofed
Traffic
AS-4
Ingress Point A

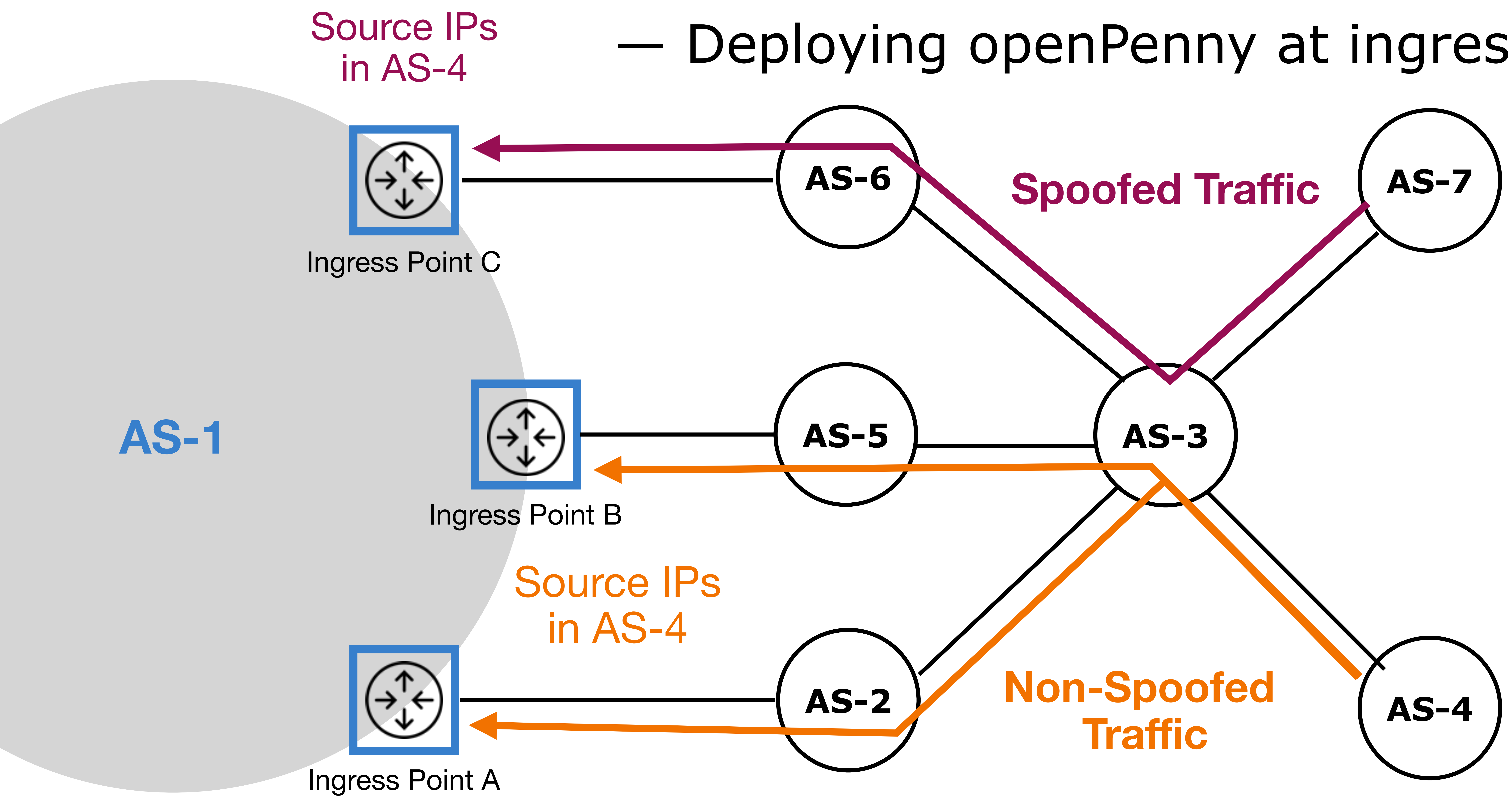

Source IPs in AS-4
Ingress Point C
AS-6
Spoofed Traffic
AS-7
AS-1
Ingress Point B
AS-5
AS-3
Source IPs in AS-4
Ingress Point A
AS-2
Non-Spoofed Traffic
AS-4

# How can we distinguish which case we are in?

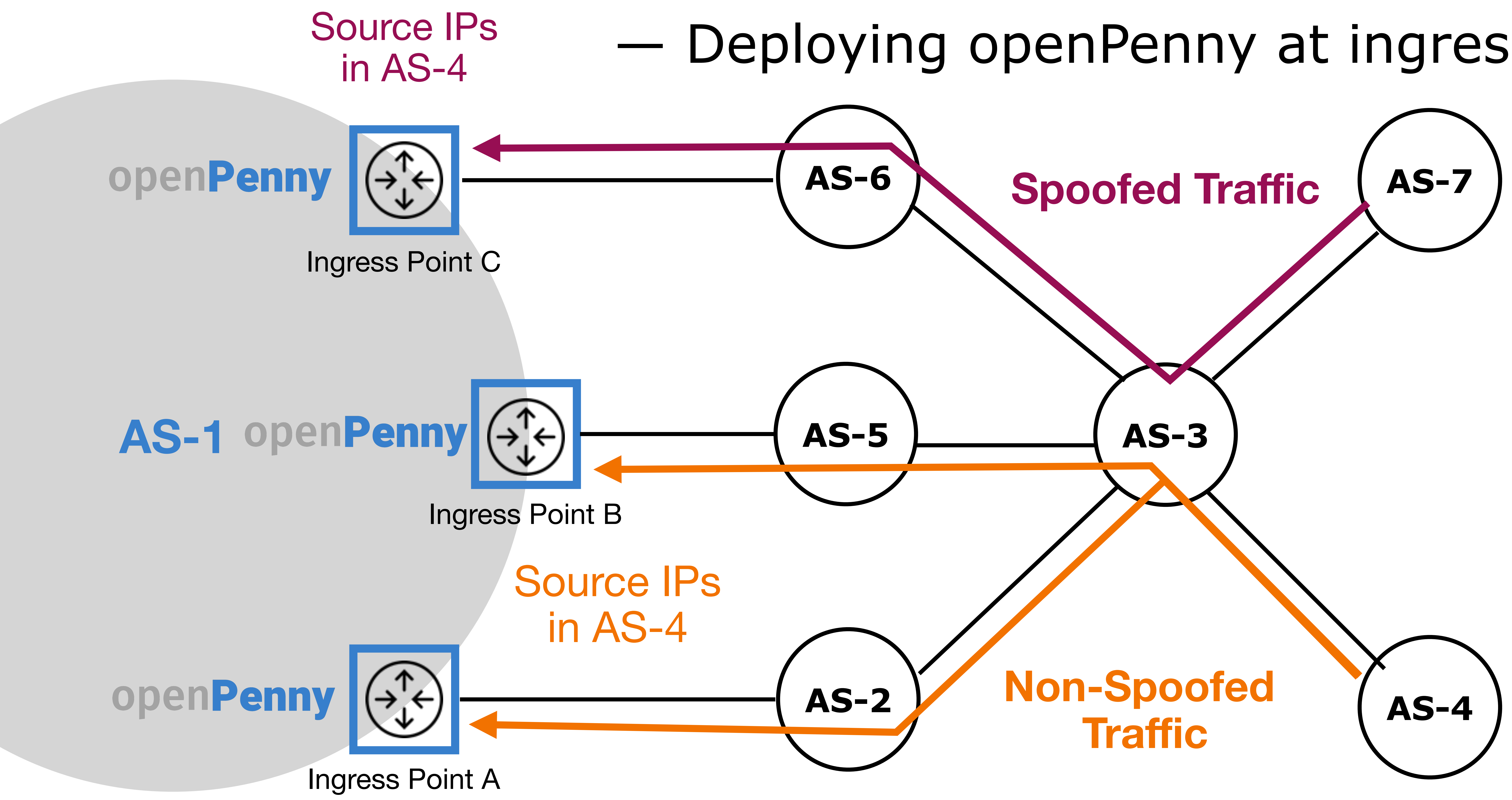


openPenny

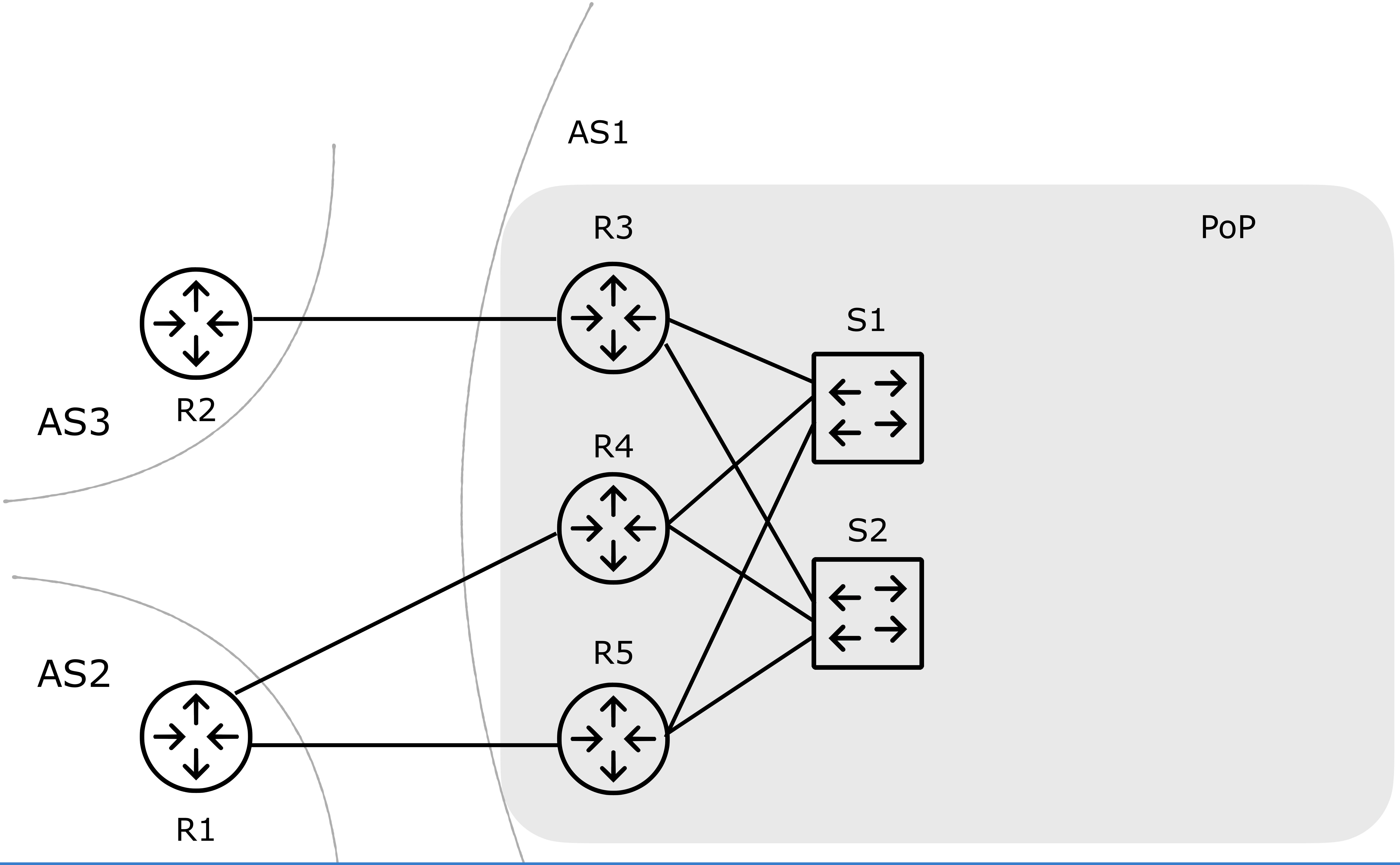
# How can we distinguish which case we are in?
# — Deploying openPenny at ingress points.



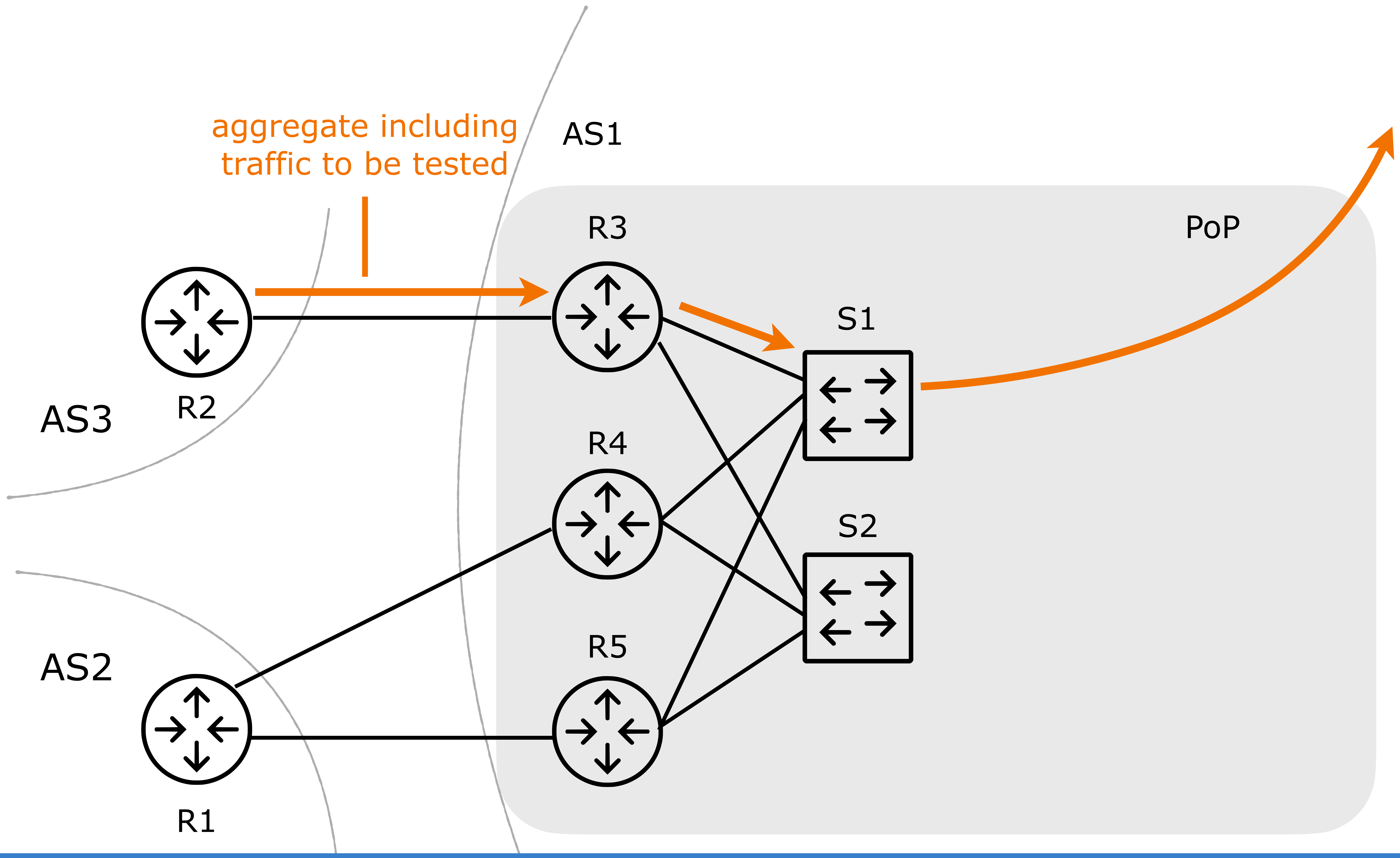
# How can we distinguish which case we are in?
# — Deploying openPenny at ingress points.



# How does openPenny Work?



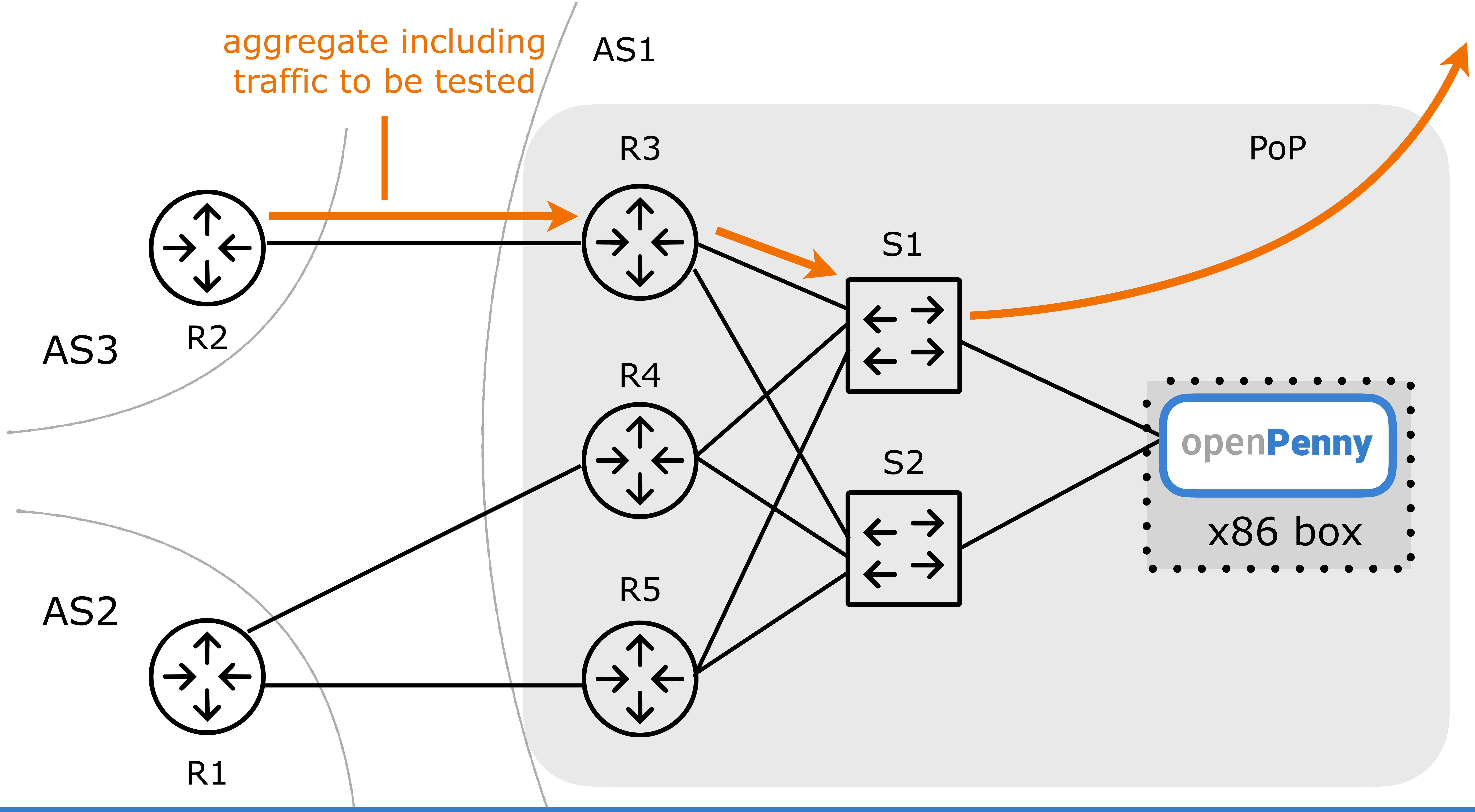
# How does openPenny Work?



openPenny

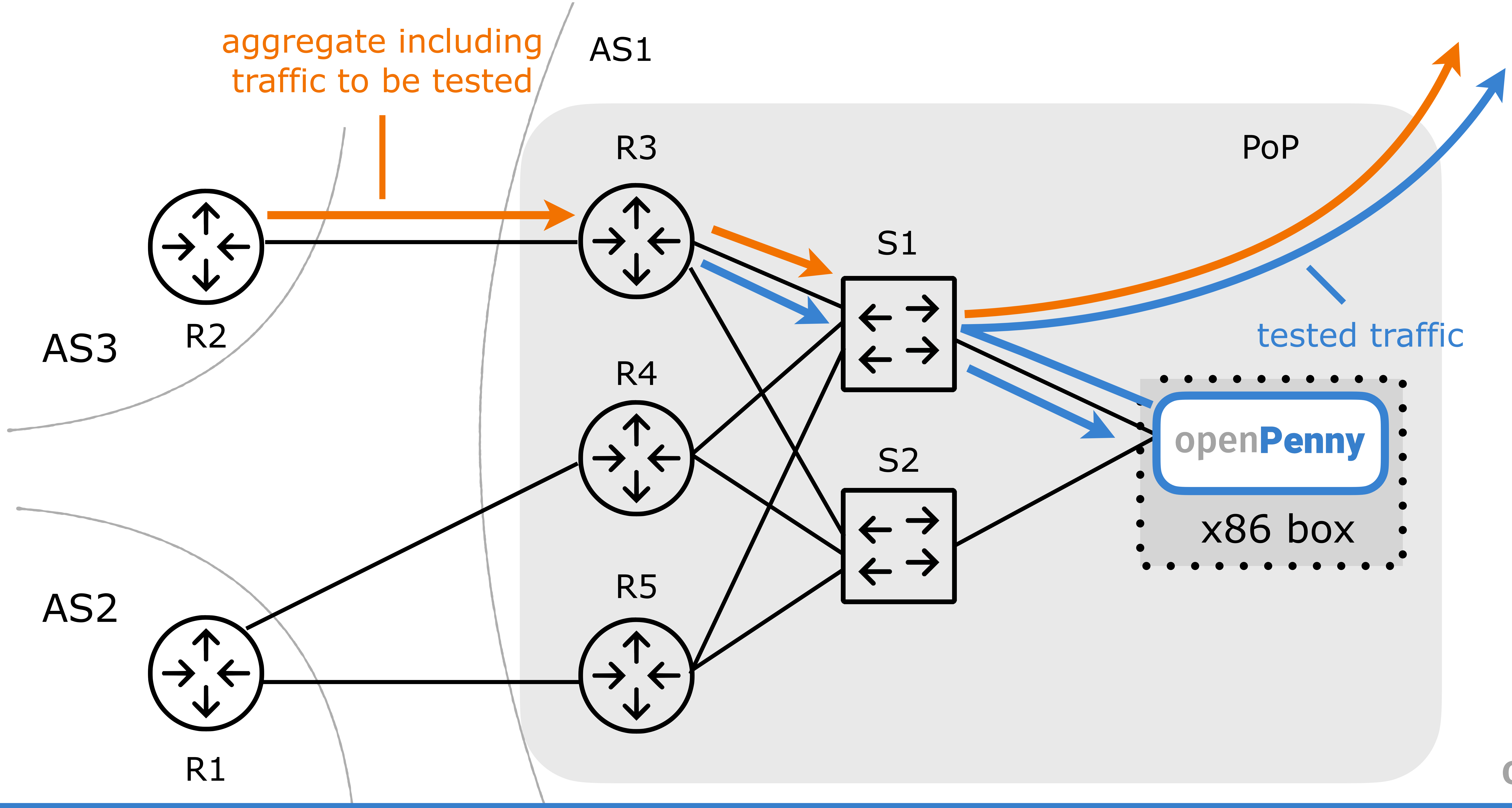
# How does openPenny Work?

— openPenny runs within an x86 box.



# How does openPenny Work?

— openPenny runs within an x86 box.



# From ***Penny*** to openPenny

What is ***Penny***?

- Checker for non-spoofed TCP flows.
- Drops a few TCP packets and checks for retransmissions.
- **Simple idea, but complex in practice:** Must handle TCP quirks, external losses, user impact, and resilience against tool-aware spoofers.

***Penny*** *ACM SIGCOMM'24.* → openPenny

# From ***Penny*** to openPenny

***Penny*** *ACM SIGCOMM'24.*

openPenny

# From ***Penny*** to open**Penny**

| | ***Penny*** *ACM SIGCOMM’24.* | open**Penny** |
|---|---|---|
| ***Modes:*** | Active | Active + Passive |

# From ***Penny*** to openPenny

| | ***Penny*** *ACM SIGCOMM'24.* | openPenny |
|---|---|---|
| ***Modes:*** | Active | Active + Passive |
| ***Metrics:*** | Non-spoofed | Non-spoofed, load-balancing, abruptly terminated flows, … |

# From ***Penny*** to openPenny

| | ***Penny*** *ACM SIGCOMM'24.* | openPenny |
|---|---|---|
| ***Modes:*** | Active | Active + Passive |
| ***Metrics:*** | Non-spoofed | Non-spoofed, load-balancing, abruptly terminated flows, … |
| ***Implementation:*** | NS-3 (Prototype) | Real-world (Production) |

# From ***Penny*** to openPenny

| | ***Penny*** *ACM SIGCOMM'24.* | openPenny |
|---|---|---|
| ***Modes:*** | Active | Active + Passive |
| ***Metrics:*** | Non-spoofed | Non-spoofed, load-balancing, abruptly terminated flows, … |
| ***Implementation:*** | NS-3 (Prototype) | Real-world (Production) |
| ***Evaluation:*** | Simulations | Real traffic in a controlled lab testbed |

# From ***Penny*** to openPenny

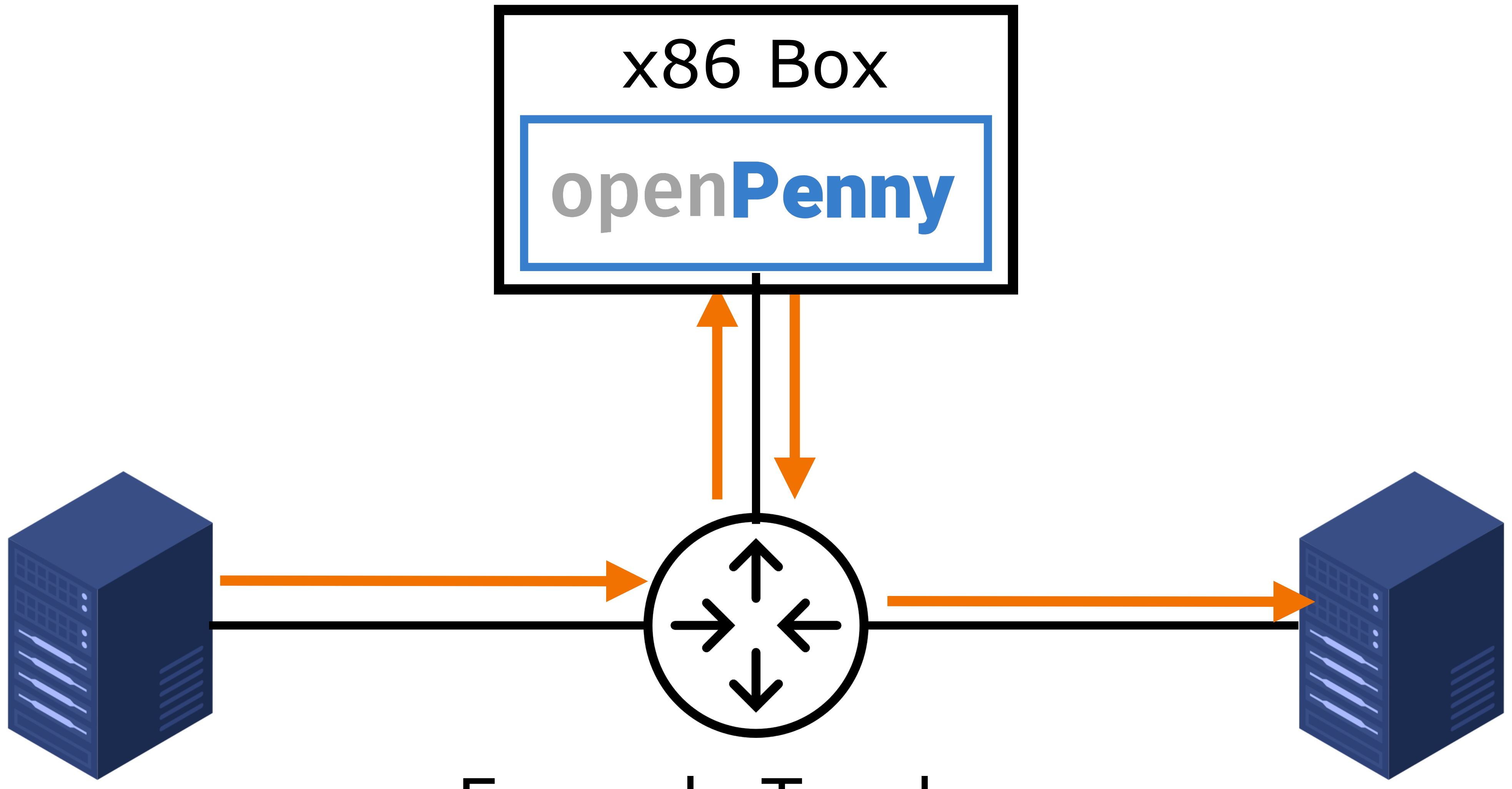
- All uses cases of Penny apply to openPenny.
  — (i) misconfigurations, (ii) sub-optimal routing policies,
  — (iii) commercial agreement violations and (iv) Hijacks.

- RIPE 89 operator feedback on Penny suggested adding a passive mode.
  - Detect route flaps and per-packet load balancing.
  - Detect abruptly interrupted TCP flows.

- To make openPenny useful for operators, we will engage them via mailing lists and meetings.
  - We will seek volunteer networks for early deployment.
  - Feel free to reach out if you're interested in running openPenny in the future.

# Experimental Testbed Lab

- Set up a testbed at UCL using real switches and routers.
- Replicate a diverse range of network settings (e.g., bandwidth, latency, and topology).
- Deployment Scenarios:
  Single vs. multi-core testing box.
- Explore the efficiency of traffic redirection techniques in commercial routers.



Example Topology

# Project Roadmap

# Project Roadmap

- **Initial Testbed & Prototype Adaptation:** Set up the testbed and adapt the current prototype for real-device interaction.

# Project Roadmap

- **Initial Testbed & Prototype Adaptation:** Set up the testbed and adapt the current prototype for real-device interaction.
- **Fully Fledged Implementation:** Ensure scalability and realistic traffic handling and testing with various traffic patterns.

# Project Roadmap

- **Initial Testbed & Prototype Adaptation:** Set up the testbed and adapt the current prototype for real-device interaction.
- **Fully Fledged Implementation:** Ensure scalability and realistic traffic handling and testing with various traffic patterns.
- **Use Case Exploration:** Identify and prioritise supported use cases while gathering feedback from the RIPE community.

# Project Roadmap

- **Initial Testbed & Prototype Adaptation:** Set up the testbed and adapt the current prototype for real-device interaction.
- **Fully Fledged Implementation:** Ensure scalability and realistic traffic handling and testing with various traffic patterns.
- **Use Case Exploration:** Identify and prioritise supported use cases while gathering feedback from the RIPE community.
- **Use Case Support & Integration:** Implement external components (e.g., result database) and develop example applications leveraging openPenny.

# Project Roadmap

- **Initial Testbed & Prototype Adaptation:** Set up the testbed and adapt the current prototype for real-device interaction.
- **Fully Fledged Implementation:** Ensure scalability and realistic traffic handling and testing with various traffic patterns.
- **Use Case Exploration:** Identify and prioritise supported use cases while gathering feedback from the RIPE community.
- **Use Case Support & Integration:** Implement external components (e.g., result database) and develop example applications leveraging openPenny.