# SAVNET标准进展

秦澜城

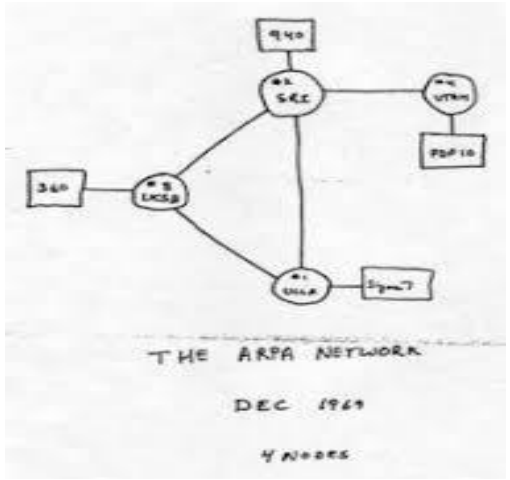
清华大学

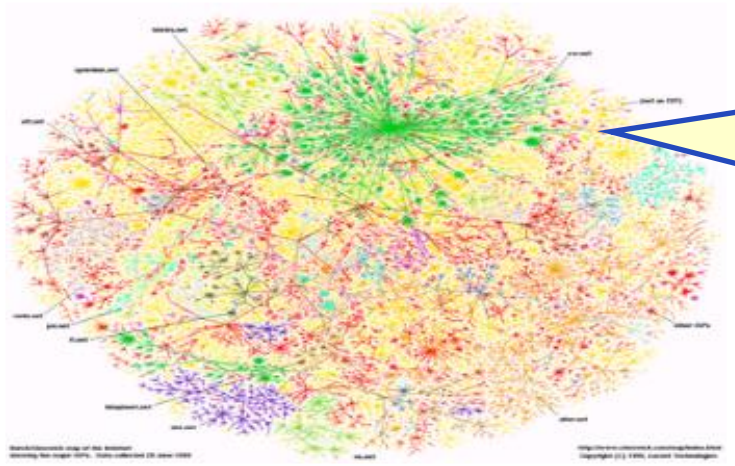
# 互联网已经逐步发展成为网络空间

## 互联网普及率逐年增加


## 互联网用户数量持续增长


- 截至2021年3月，全球互联网用户数量达到51.69亿人，占世界人口的比重达到65.6% (IWS)
- 其中，亚洲地区互联网用户数量最多，达43.27亿人，占全球的比重为54.94% (IWS)

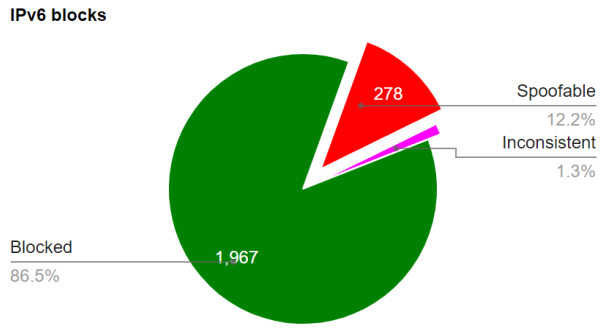


互联网经过50年的发展，成为人类社会的重要基础设施，成为继陆、海、空和太空之后的人类第五疆域：网络空间(Cyberspace)

# 当前互联网体系结构缺乏源地址验证

CAIDA近半年测试结果显示全球有12.2%的IPv6地址块可以被伪造




基于源地址伪造的反射放大攻击是最主要的DDoS攻击类型

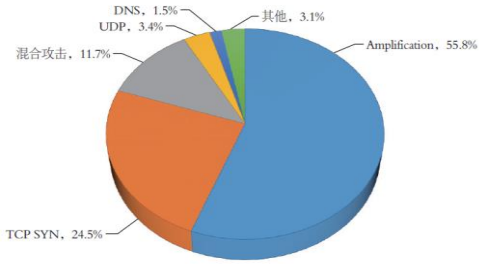



图 6-29　2020 年 DDoS 攻击次数占比按攻击类型分布
（来源：中国电信集团云网安全科技有限公司）

2020年我国境内共遭受152,538次DDoS攻击

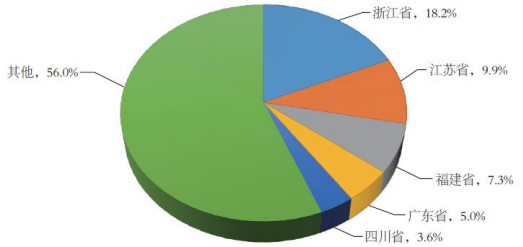



图 6-30　2020 年我国遭受 DDoS 攻击次数占比按地区分布
（来源：中国电信集团云网安全科技有限公司）

源地址伪造

- 恶意攻击难抵挡
- 非法用户难追溯
- 资源盗用难管控

- 当前互联网体系结构缺乏真实可信安全机制，不做源地址验证，使得假冒源地址横行
- 借助伪造源地址实施的反射放大攻击成为当今互联网最重要的安全隐患之一

# MANRS路由安全相互协议规范

## ◘Mutually Agreed Norms for Routing Security (MANRS)

◆MANRS由国际互联网协会（ISOC）发起，是一项由行业驱动的倡议，旨在维护网络空间安全，发展网络安全治理的集体责任文化

◆通过建立一个由“网络安全意识强”的机构组成的“社区”，构建更加安全的网络环境

## ◘MANRS 计划包括


◆运营商计划、IXP 计划、CDN&Cloud 供应商计划、设备商计划

## ◘反源地址欺骗是MANRS倡导的核心行动之一

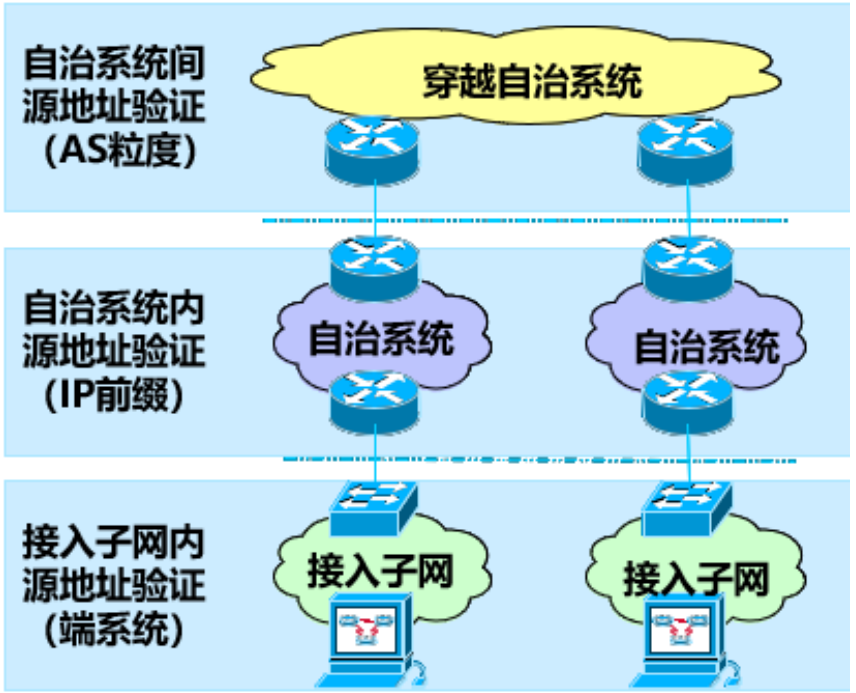
◆部署源地址验证，防止伪造源IP地址的报文进入或离开网络

◆为了使源地址验证尽可能有效，要在尽可能靠近源的位置部署源地址验证

# SAVA源地址验证体系结构

真实源地址验证体系结构SAVA将源地址验证划分为接入网内、域内、域间三个层次：

- 接入网内源地址验证
  - 部署于接入网内部，保证主机粒度的地址可信
  - 最佳实践：SAVI [RFC7039]
- 自治域内源地址验证
  - 部署于自治域内部，保证子网粒度的地址可信
  - 最佳实践：Ingress filtering [RFC2827] [RFC3704]
- 自治域间源地址验证
  - 部署于自治域之间，保证自治域粒度的地址可信
  - 最佳实践：EFP-uRPF [RFC8704]，Loose uRPF [RFC37[illegible]]




**很难要求所有接入网同时部署SAVI，因此域内和域间源地址验证十分必要**

# 目前域内和域间源地址验证的最佳实践

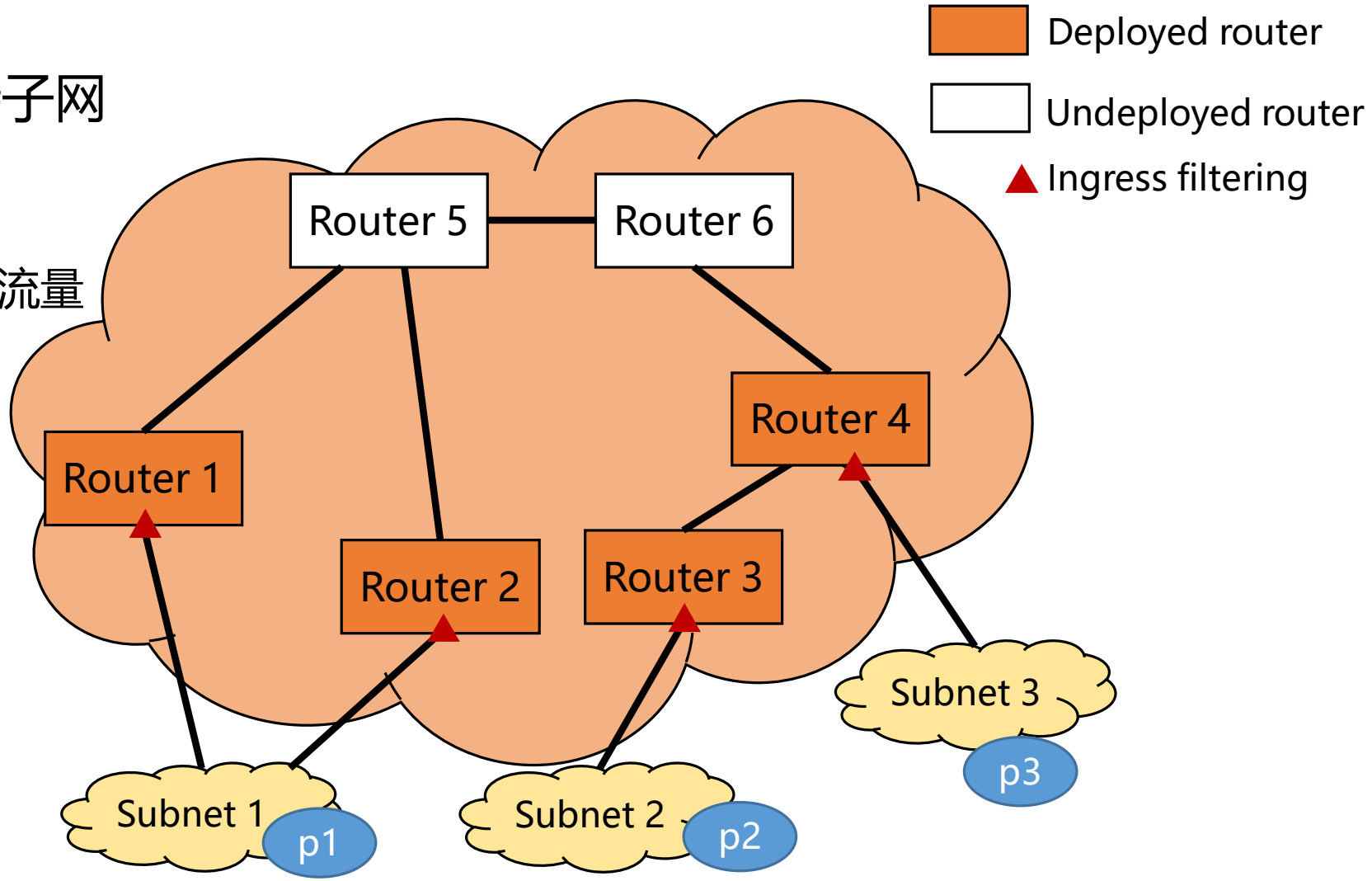
RFC8704 总结了目前域内和域间源地址验证机制的部署建议:

- 域内源地址验证最佳实践：Ingress filtering [RFC2827] [RFC3704]
  - ACL-based SAV 在设备上人工配置过滤规则，定义合法的源前缀列表
  - Strict uRPF 反向查询FIB，严格要求转发接口和入接口保持一致
- 域间源地址验证最佳实践：EFP-uRPF [RFC8704] + Loose uRPF [RFC3704]
  - EFP-uRPF 在customer接口上自动生成RPF(Reverse Path Filter) list，定义合法的源前缀列表
  - Loose uRPF 部署在provider和peer接口，仅要求源地址存在于FIB

**然而，目前域内和域间源地址验证机制存在准确性、验证方向性、激励性等局限**

# 域内源地址验证机制的典型部署场景

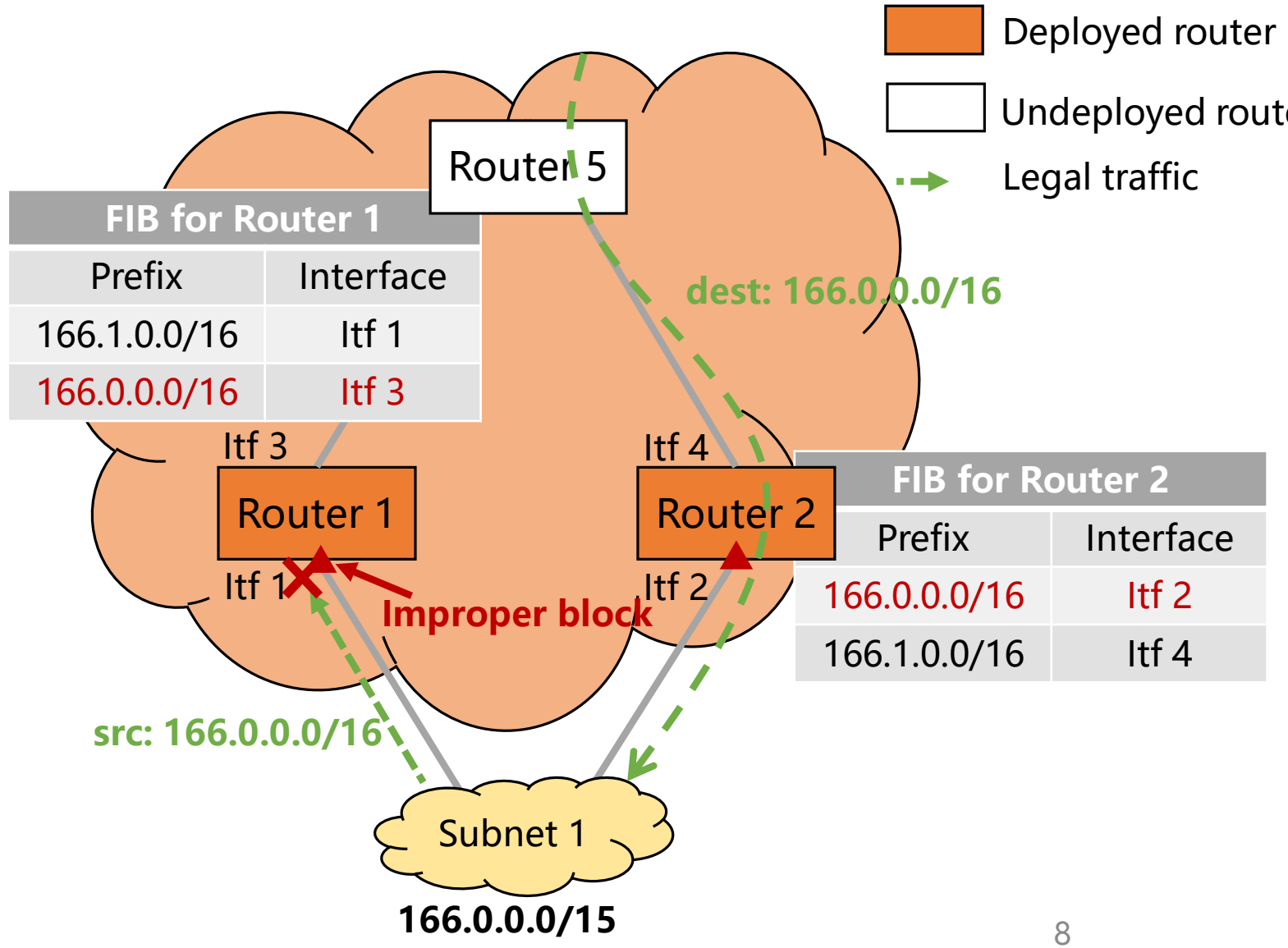
- Ingress filtering 部署在连接子网的域内边界路由器上
  - ◆阻断来自直连子网的伪造源地址流量



# 域内源地址验证机制局限#1: 误阻断

- **场景 1: 多接入子网**
  - Router 1 只从Subnet 1学到 166.1.0.0/16 的路由
  - Router 2只从Subnet 1学到 166.0.0.0/16 的路由

- 如果部署 strict uRPF
  - 误阻断合法流量
- 如果部署 ACL-based SAV
  - 依赖人工配置更新ACL规则

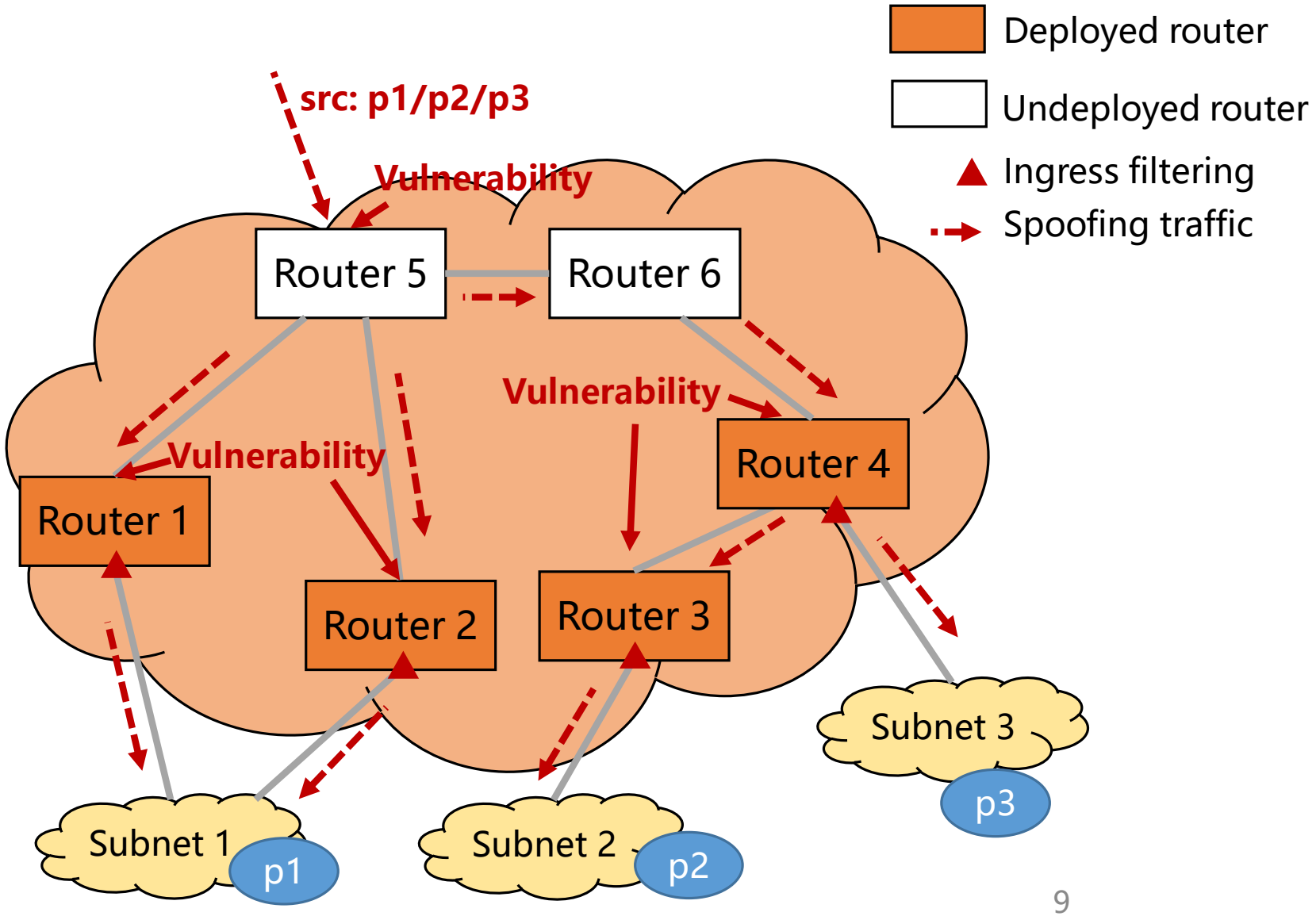


# 域内源地址验证机制局限#2: 缺乏网络侧入流量验证

## ◘ 场景 2: 域外假冒源地址入流量

◘ Ingress filtering 不支持网络侧入流量的源地址验证

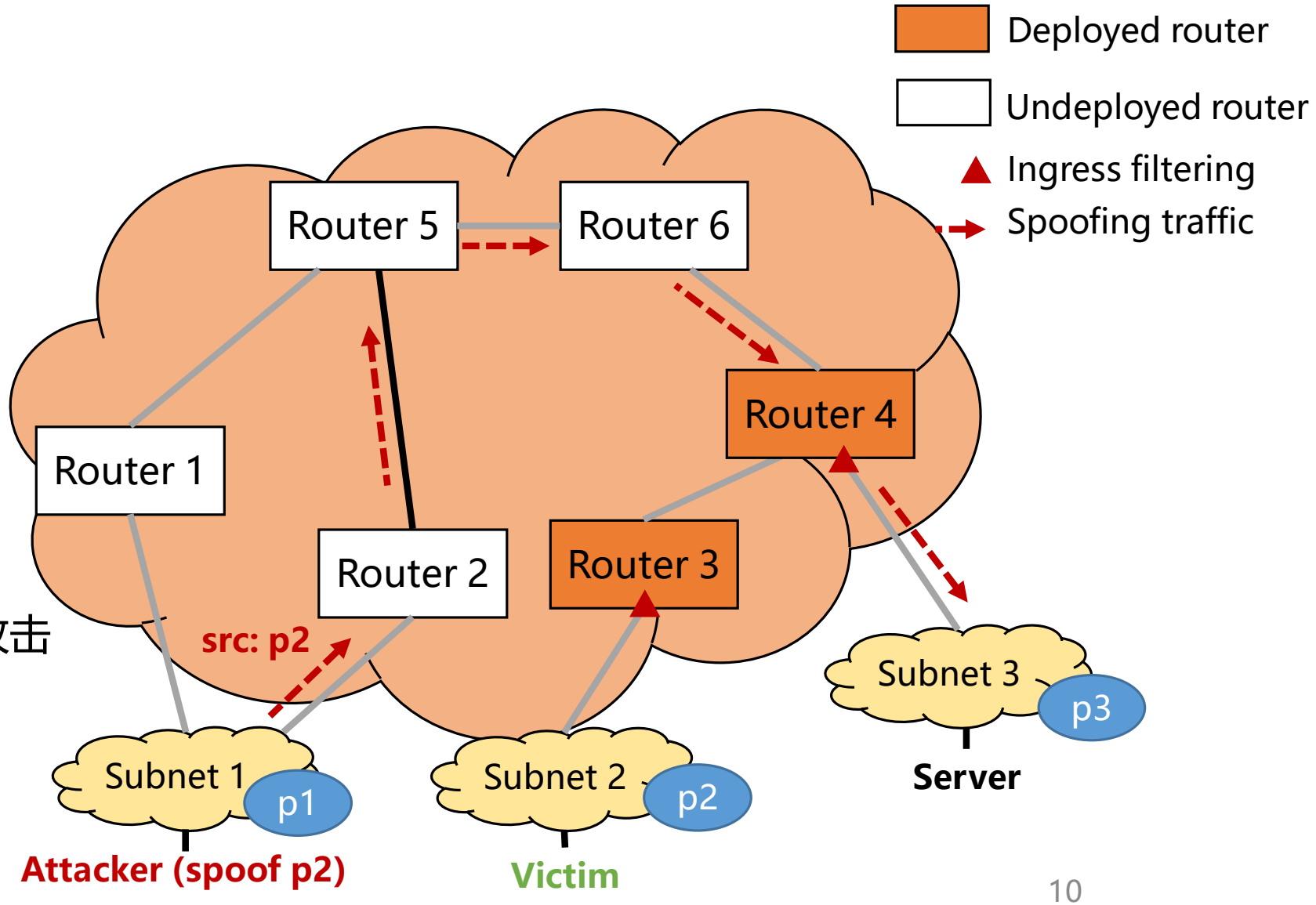
◆伪造域内源地址的流量可以从域外流入子网



# 域内源地址验证机制局限#2: 缺乏网络侧入流量验证

- **场景 3: 域内反射放大攻击**
  - ◆攻击者: Subnet 1
  - ◆受害者: Subnet 2
  - ◆反射器: Subnet 3

- 域内源地址验证**部分部署**时:
  - ◆已部署Subnet无法伪造源地址
  - ◆未部署Subnet可以伪造其他 Subnet源地址来实施反射放大攻击



# 域内源地址验证机制需求

| | |
|---|---|
| **准确源地址验证** | • **确定源到本地的真实入方向（与数据平面真实转发路径保持一致）** |
| **全方向保护** | • **支持对任意入方向流量的源地址验证**<br>• **在尽可能靠近源的位置阻断伪造源地址流量** |
| **开销可接受** | • **不能引入过多的开销** |

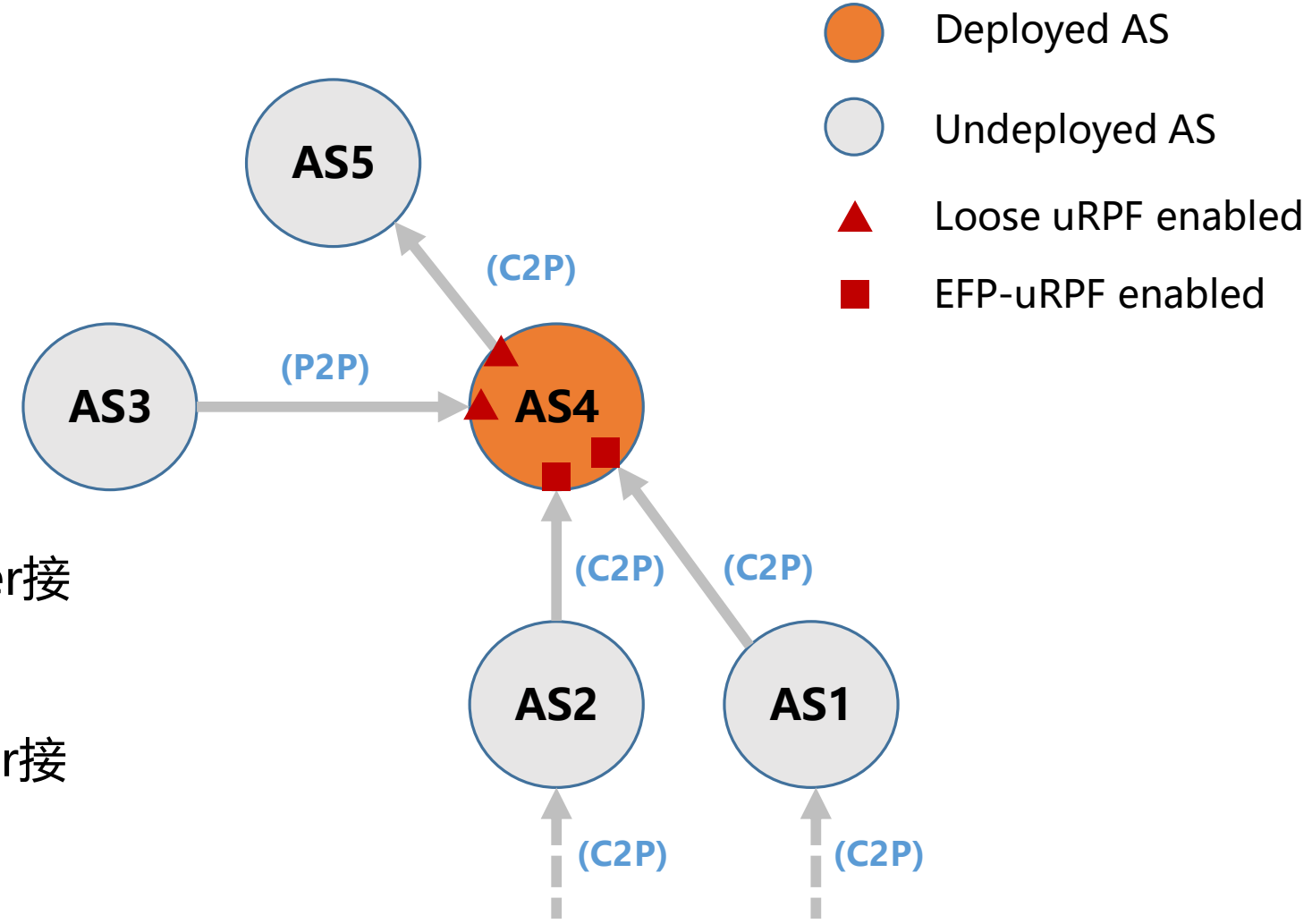
# 域间源地址验证机制的典型部署场景

## Loose uRPF

- 工作在 provider/peer 接口
  - ◆允许所有在FIB的源地址

## EFP-uRPF

- 工作在 customer 接口
  - ◆EFP uRPF Algorithm A: 每个customer接口生成单独的过滤表
  - ◆EFP uRPF Algorithm B: 所有customer接口生成同样的过滤表



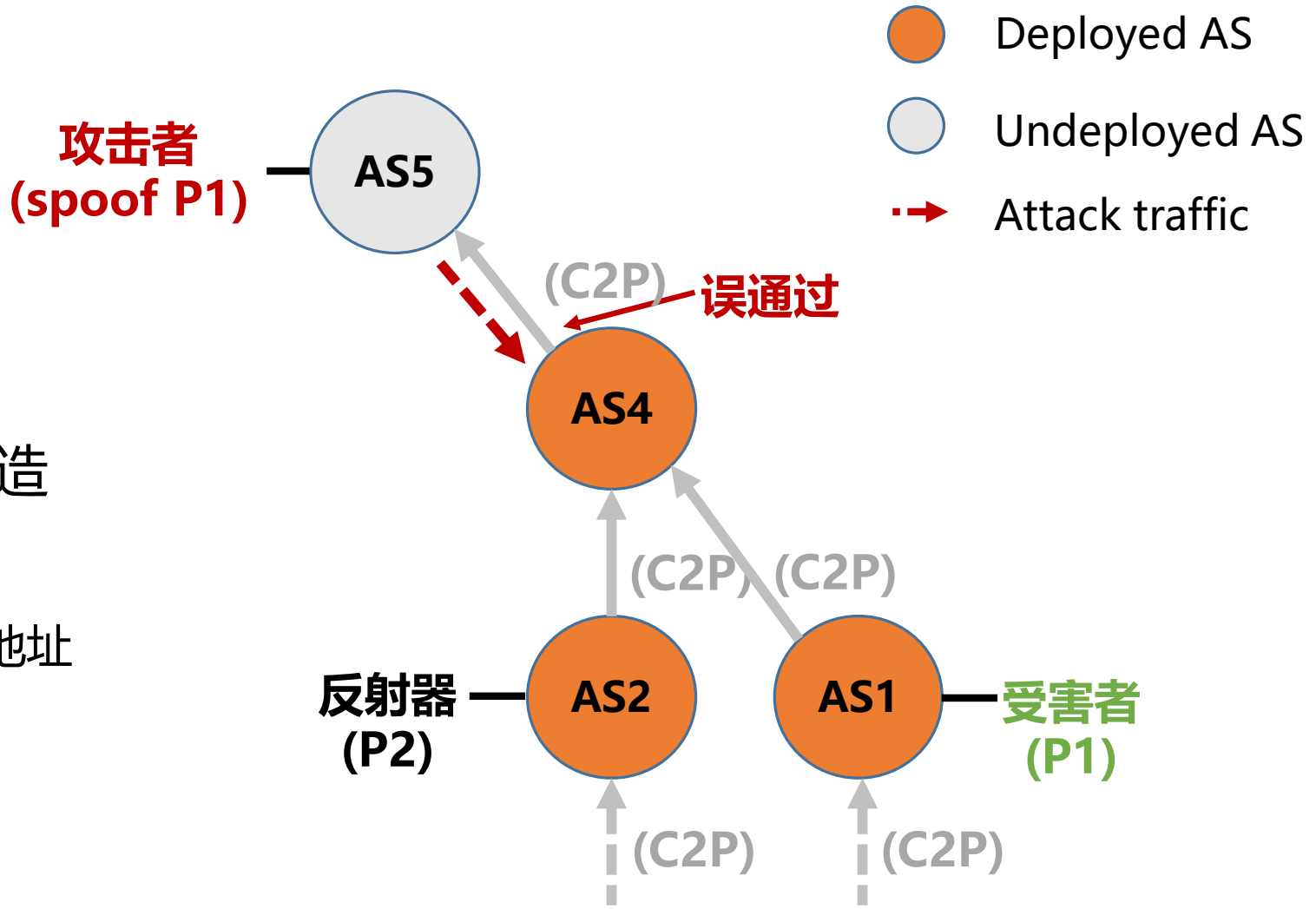
# 域间源地址验证机制局限#1: 误通过

## 场景 1: 反射放大攻击

- ◆攻击者: AS5
- ◆反射器: AS2
- ◆受害者: AS1

## AS4**误通过**来自AS5的源地址伪造流量

- ◆Loose uRPF 允许在FIB内的所有源地址

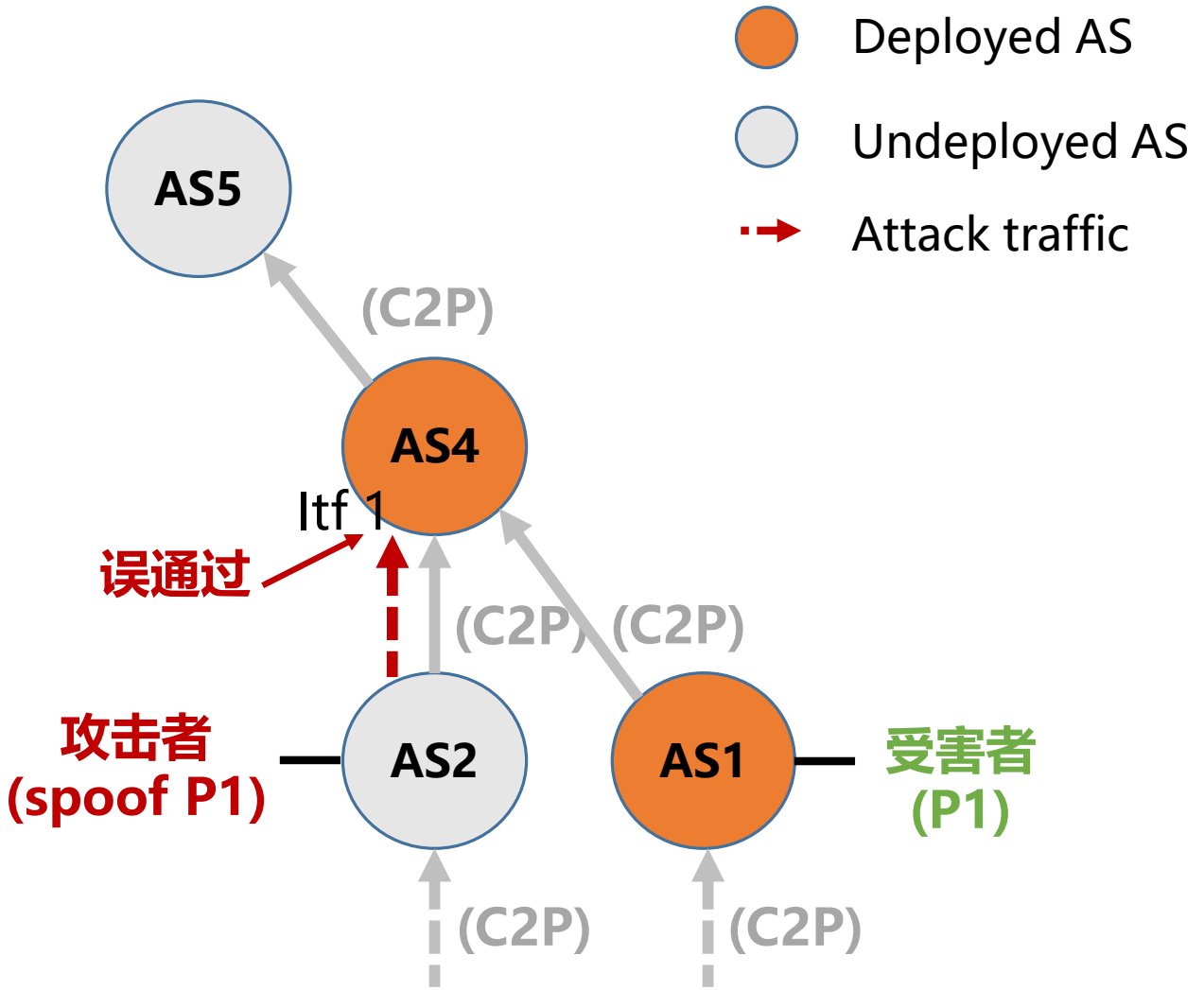



Scenario 1: Reflection attack

# 域间源地址验证机制局限#1: 误通过

- **场景 2: Customer cone内部的源地址伪造**

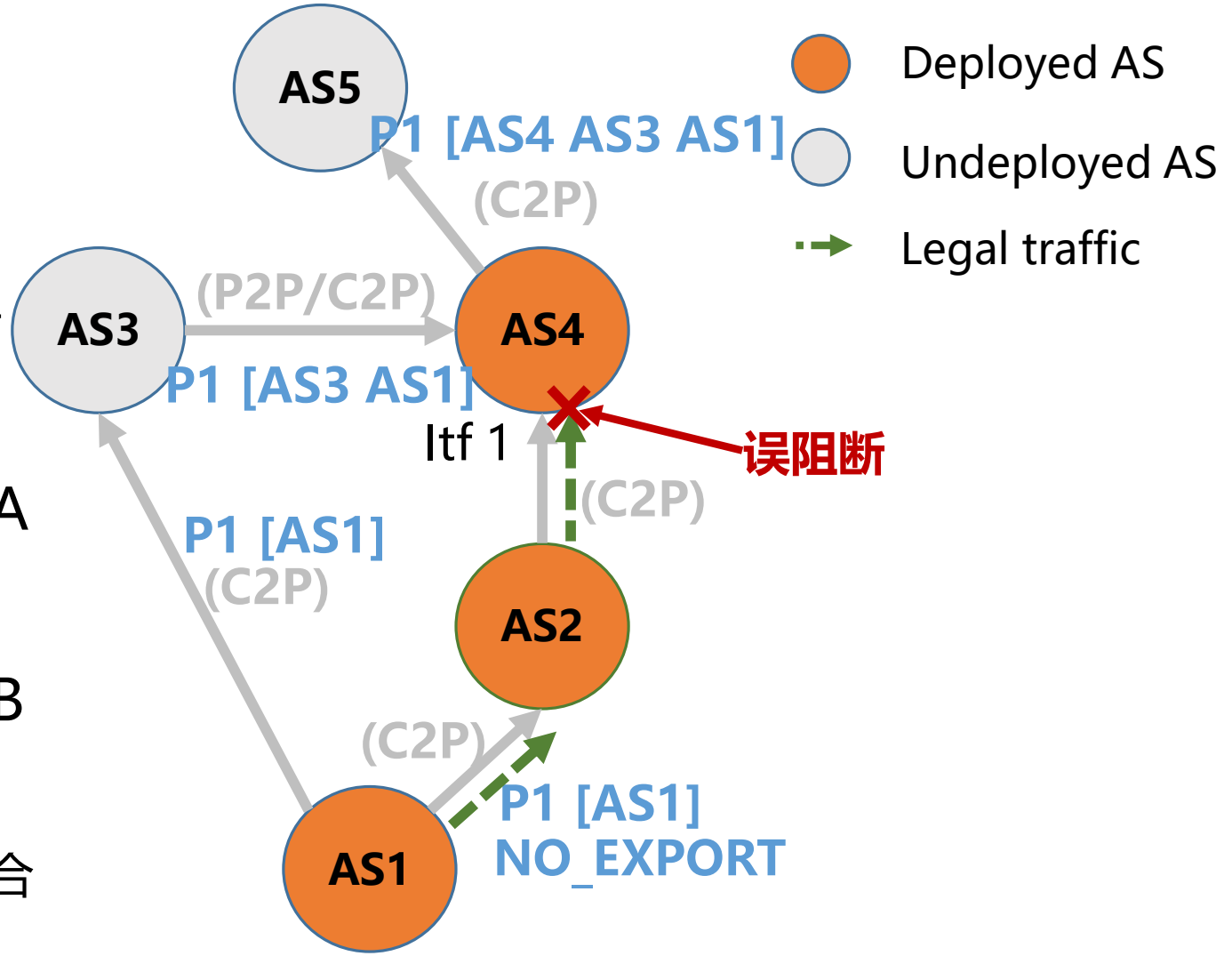
- 如果AS4部署 EFP-uRPF Algorithm A
  - ◆没有问题
- 如果AS4部署 EFP-uRPF Algorithm B
  - ◆误通过来自AS2的源地址伪造流量




Scenario 2: Spoofing within a customer cone

# 域间源地址验证机制局限#2: 误阻断

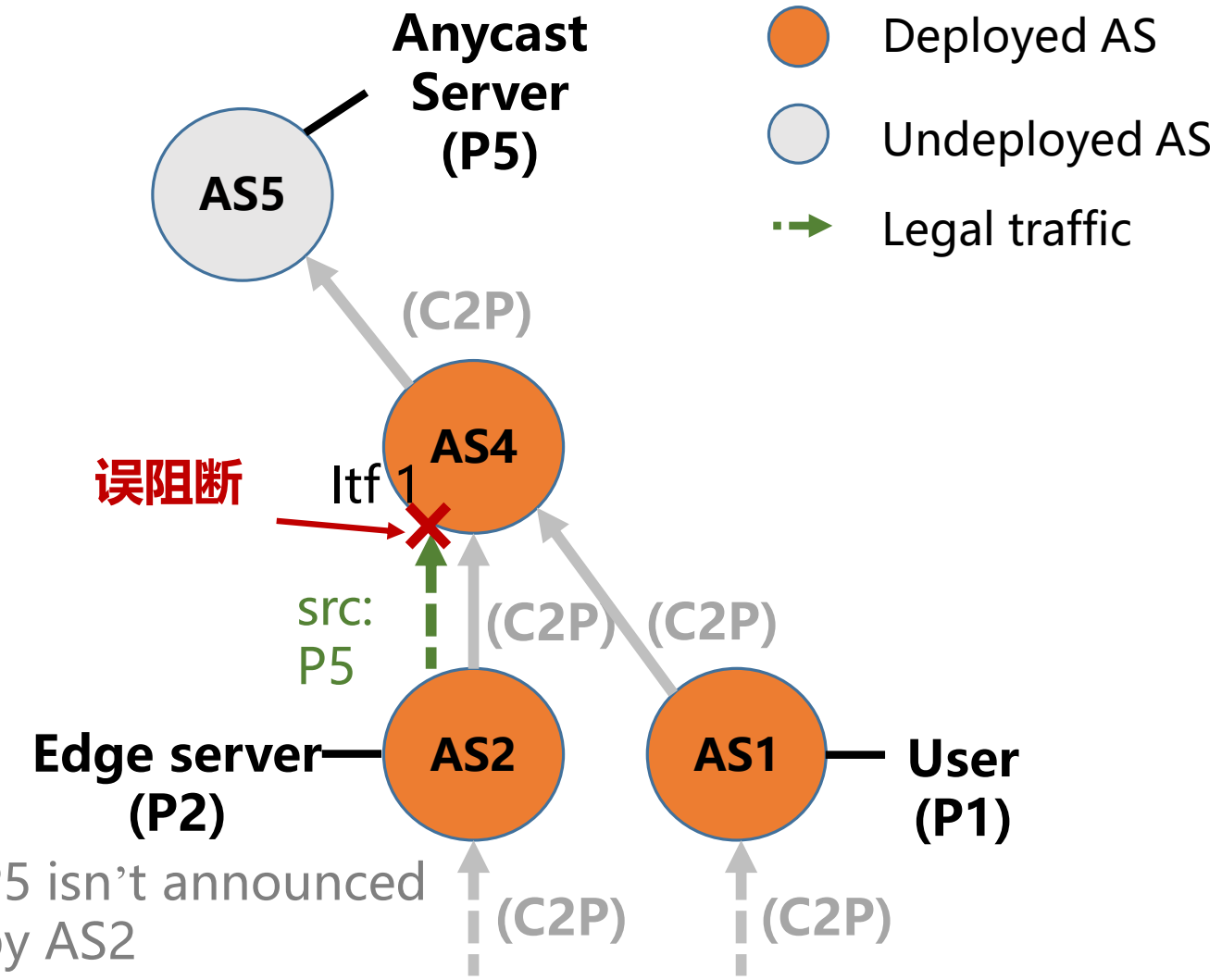
- **场景 3: NO_EXPORT in BGP Advertisement**
  - ◆AS4到AS1的转发路径：AS4->AS3->AS1
  - ◆AS1到AS4的转发路径：AS1->AS2->AS4
- 如果AS4部署 EFP-uRPF Algorithm A
  - ◆误阻断来自AS2的合法流量
- 如果AS4部署 EFP-uRPF Algorithm B
  - ◆如果AS3是AS4的customer: 没有问题
  - ◆如果AS3是AS4的peer: 误阻断来自AS2的合法流量



# 域间源地址验证机制局限#2: 误阻断

- **场景 4: Anycast/Edge Hybrid--Direct Server Return (DSR)**
  - Request path: AS1->AS4->AS5
  - Tunnel path: AS5->AS4->AS2
  - Response path: AS2->AS4->AS1

- 如果AS4部署 EFP-uRPF Algorithm A
  - 误阻断来自AS2的合法流量
- 如果AS4部署 EFP-uRPF Algorithm B
  - 误阻断来自AS2的合法流量

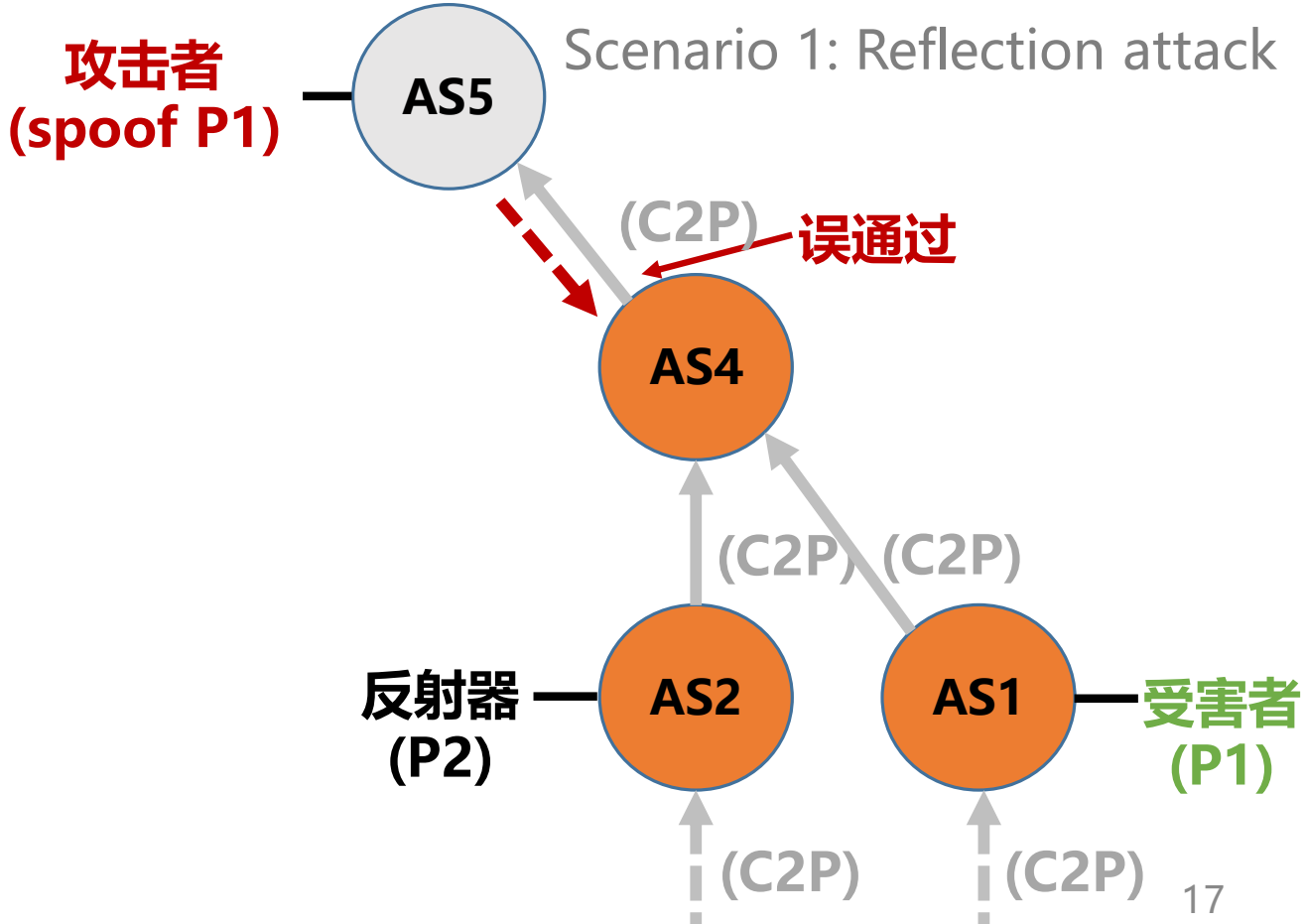


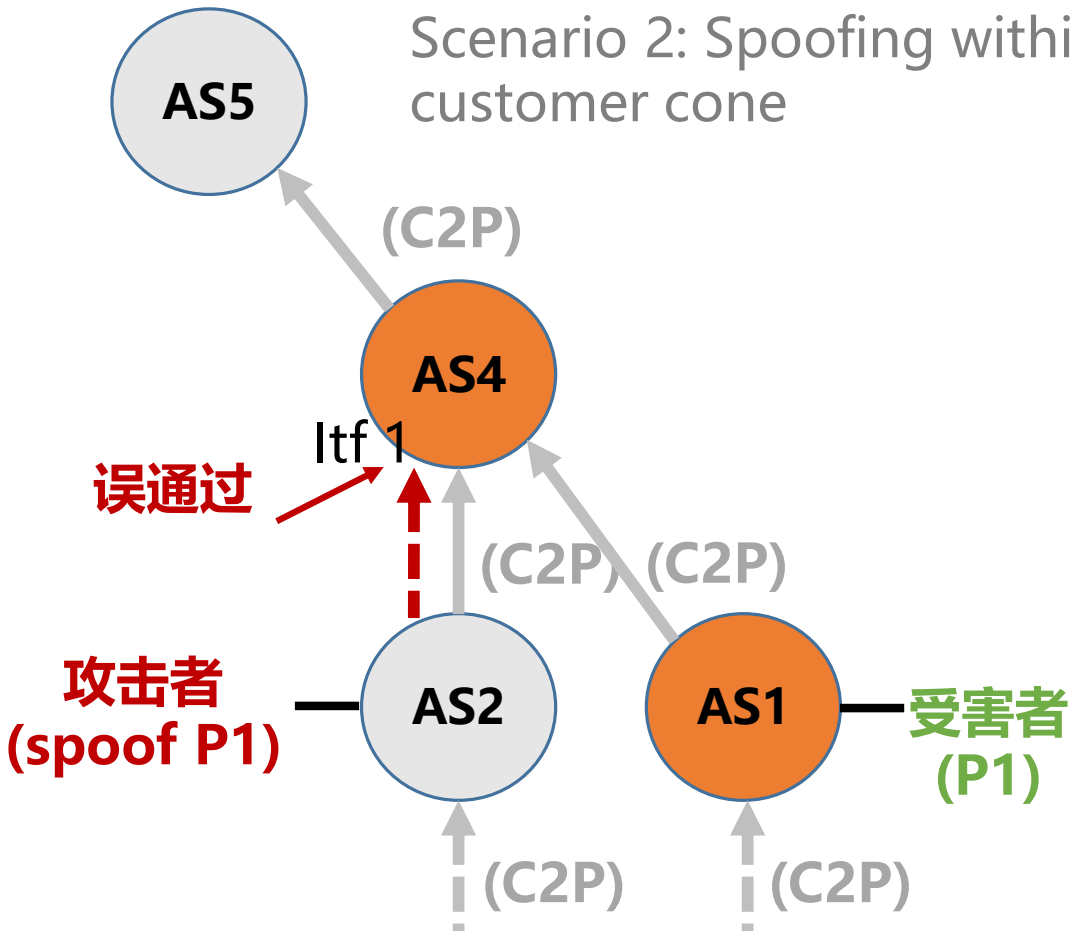



Scenario 4: Direct Server Return (DSR)

# 域间源地址验证机制局限#3: 激励错位

**受害者部署源地址验证，无法对防止自己的源地址被伪造提供额外帮助，仍然易受到反射放大攻击**



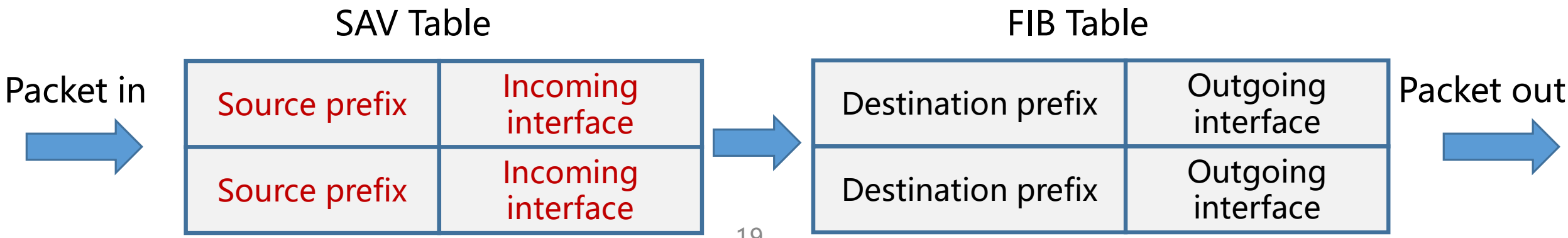



# 域间源地址验证机制需求

| | |
|---|---|
| **准确源地址验证** | • **确定源到本地的真实入方向（与数据平面真实转发路径保持一致）** |
| **直接激励** | • **为已部署网络提供直接激励** |
| **支持部分部署** | • **部分部署时可以有效防止源地址假冒** |
| **开销可接受** | • **不能引入过多的开销** |

# SAVNET技术思路

- 独立的源地址验证表生成
  - 通过逐跳前缀通告的方式，发现源的真实转发路径，并在沿途的路由器上生成源地址验证表
    - 源地址验证**准确**
    - 源地址**全方向验证**
    - 协议**低开销**
    - 部署**直接激励**
  - SAVNET分为域内源地址验证机制和域间源地址验证机制，域内和域间机制基本思路一致，实现略有不同
- 基于源地址验证表的源地址验证



# IETF SAVNET WG

- SAVNET BOF, IETF 113, Mar 24, 2022
  - Proponent: Dan Li (Tsinghua University), Jianping Wu (Tsinghua University), Mingqing Huang (Huawei), etc.
  - Presenter: Dan Li (Tsinghua University), Lancheng Qin (Tsinghua University), 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

# SAVNET WG Meeting

- First SAVNET WG meeting, IETF 114, July 25, 2022
  - 域内和域间源地址验证机制问题陈述
    - Source Address Validation in Intra-domain Networks (Intra-domain SAVNET) Gap Analysis, Problem Statement and Requirements
    - Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) Gap Analysis, Problem Statement, and Requirements
- Second SAVNET WG meeting, IETF 115, Nov 11, 2022
  - 域内和域间源地址验证机制问题陈述（更新版本）
  - SAVNET域内源地址验证机制设计框架
    - Intra-domain Source Address Validation (SAVNET) Architecture
  - SAVNET域间源地址验证机制设计框架
    - Inter-domain Source Address Validation (SAVNET) Architecture

谢谢！