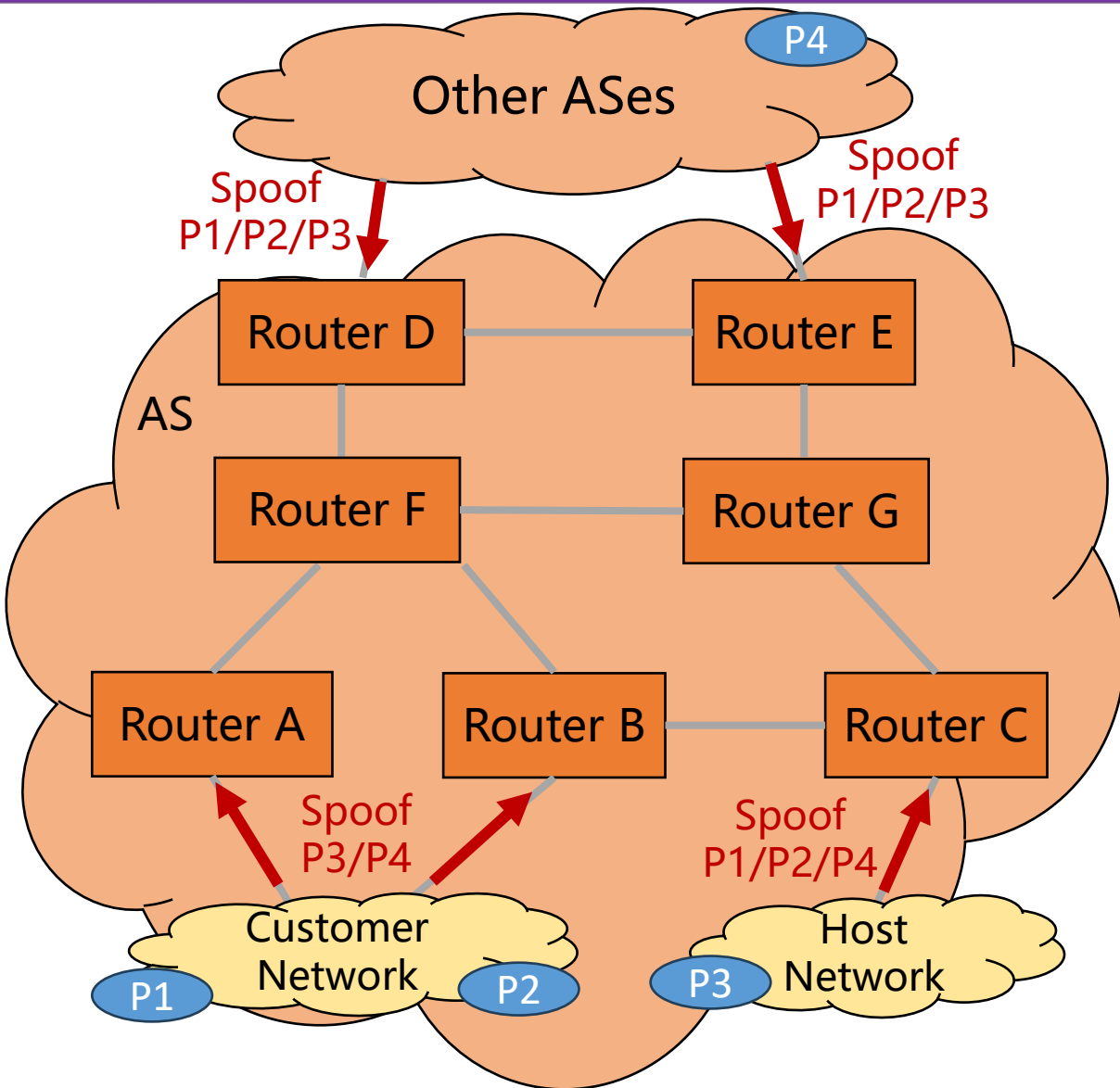


A Summary of Discussions on Intra-domain SAVNET Architecture

Dan Li, Jianping Wu, **Lancheng Qin**, Nan Geng, Li Chen

March, 2025

Goals of Intra-domain SAVNET



□ Goal #1:

- ◆ Avoid blocking legitimate traffic

□ Goal #2:

- ◆ Block spoofing traffic from a customer network or a host network that use a source address of another network

□ Goal #3:

- ◆ Block spoofing traffic from an external AS that use a source address of the local AS

Deployment Scope of Intra-domain SAV

□ Goal #1:

- ◆ Avoid blocking legitimate traffic

□ Goal #2:

- ◆ Block spoofing traffic from a customer network or a host network that use a source address of another network

□ Goal #3:

- ◆ Block spoofing traffic from an external AS that use a source address of the local AS

□ SAV on the edge (of the router network)

- ◆ Customer-facing routers perform SAV on interfaces facing a customer network
- ◆ Host-facing routers perform SAV on interfaces facing a host network
- ◆ AS border routers perform SAV on interfaces facing an external AS

□ SAV on inner routers

- ◆ Perform SAV on interfaces facing a neighboring router

➤ **Discussion: whether this case should be considered?**

Discussions on SAV on Inner Routers

- Since IETF 120, many people (including Gert^[1], Tony^[2], Yingzhen^[3], Mingqing^[4], etc.) have discussed the problems and considerations of SAV on inner routers on the Mailing List
 - ◆ **Common view: It is challenging to perform SAV on inner interfaces** for a generic topology with **IP FRR, Traffic Engineering Policy, or asymmetric routes inside the router network**
 - The computation of SAV rules would be complex and burdensome when considering these factors
- In IETF 121, we presented the revised architecture document to clarify the feasibility of SAV on the edge and the difficulty of SAV on inner routers
 - ◆ Peter: **Fully support the idea of moving the SAVNET function to the edge of the network.** It makes things much easier to deploy and implement
 - ◆ Joel: **Understand why edge deployments are much simpler.** The architecture document needs to clearly describe what do we get when only parts of the edge are covered
- After IETF 121, we continued the discussions on the SAVNET Mailing List and recommended that SAV on the edge should be preferred

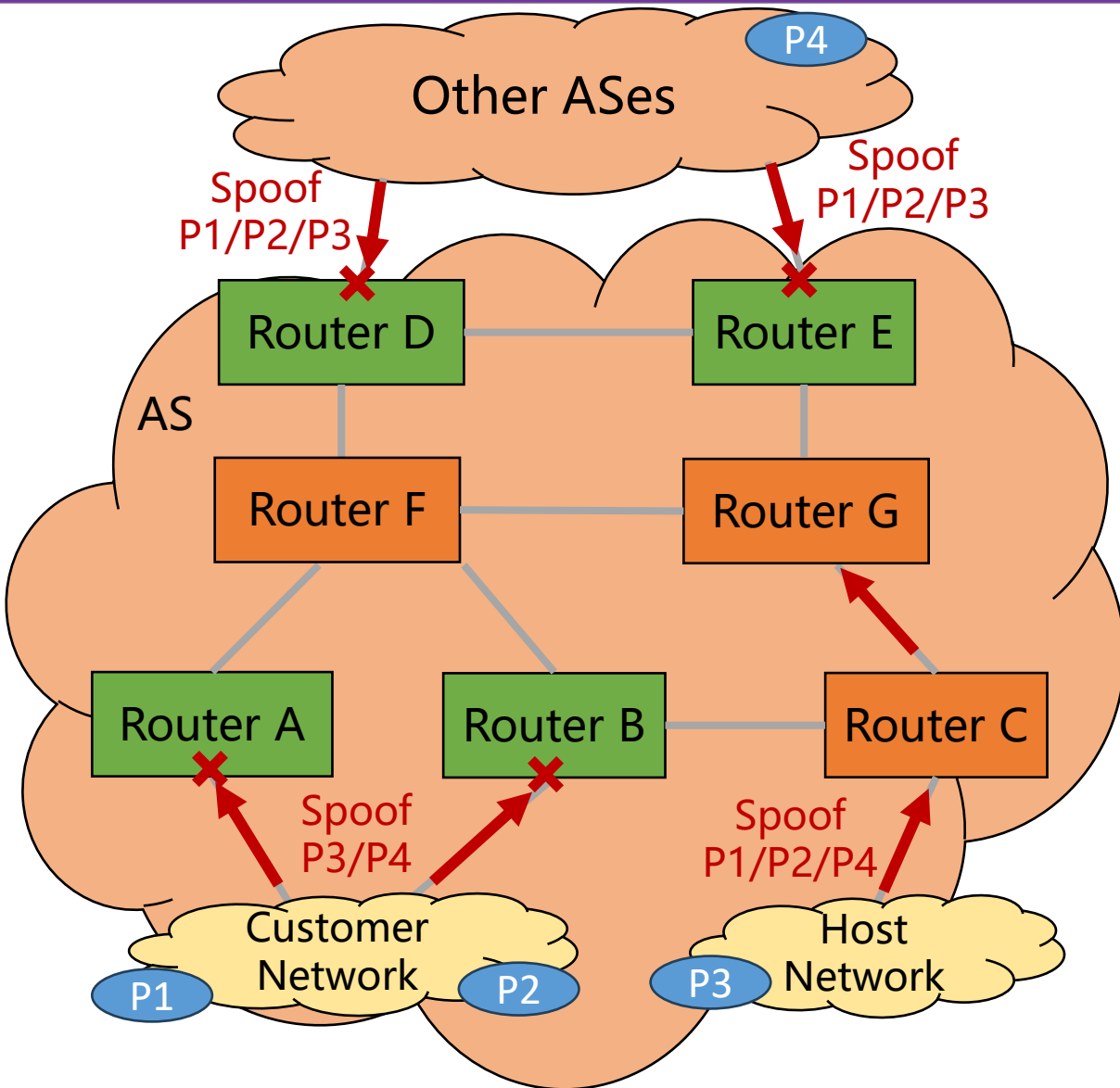
[1] Gert's comment: <https://mailarchive.ietf.org/arch/msg/savnet/ieTFdK4kJLYPyZA9bKxhhsWRxfU/>

[2] Tony's comment: <https://mailarchive.ietf.org/arch/msg/savnet/l9gNA7DISwjic35IFKvJQ94PMo/>

[3] Yingzhen's comment: https://mailarchive.ietf.org/arch/msg/savnet/yCSEvF3SY_XfacQPwe1L2GKdnW8/

[4] Mingqing's comment: <https://mailarchive.ietf.org/arch/msg/savnet/qhKDFmrEWTkzrLx7yfvMjOvthIA/>

Incremental Benefits of SAV on the Edge



- ❑ When only parts of the edge have deployed SAV, it provides incremental benefits
 - ◆ Routers that deploy SAV can block spoofing traffic from the facing network
 - ◆ The AS is only vulnerable to spoofing traffic entering from parts of the edge where SAV has not been deployed
- ❑ For example, if only Routers A, B, D, and E deploy SAV on the edge
 - ◆ Spoofing traffic from the customer network and other ASes will be checked and blocked
 - ◆ Only the host network connected to Router C can send the spoofing traffic
- ❑ By understanding the incremental benefits, network operators can plan the incremental edge deployments

Summary

□ SAV on the edge (of the router network)

◆ Advantage

- **Feasibility:** Edge implementations and deployments are simpler
- **Effectiveness:** To be as effective as possible, SAV should be applied as close to the source as possible

◆ Issue

- It takes time to achieve full deployment if there are many edge routers in an AS
- Discussions:
 - ✓ SAV on the edge can provide incremental benefits
 - ✓ The deployment complexity depends on the design and implementation of the new solution

□ SAV on inner routers

◆ Advantage

- By performing SAV on certain inner routers, it would help block more spoofing traffic when only parts of the edge have deployed SAV^[1]

◆ Issue

- **Difficulty:** IP FRR, TE, and many other factors that affect the accuracy of SAV on inner routers are difficult to address

[1] Aijun's comment: <https://mailarchive.ietf.org/arch/msg/savnet/1CVwGkhKyFPD6E51eeElI8ij-yE/>

Recommendations

We plan to provide the following recommendations on how intra-domain SAVNET should be deployed to ensure the desired goals are fulfilled

- SAV on the edge of the router network MUST be considered to ensure the goals of intra-domain SAV can be fulfilled
 - ◆ SAV on the edge is simpler, more practical, and more effective for a generic topology
- SAV on inner routers can be considered, but is not required
 - ◆ Factors that may affect the accuracy of SAV on inner interfaces need to be taken into account
 - Including IP FRR, TE policy, and asymmetric routes inside the network

Comments are welcome!