

BGP Extensions for Source Address Validation Networks (BGP SAVNET)

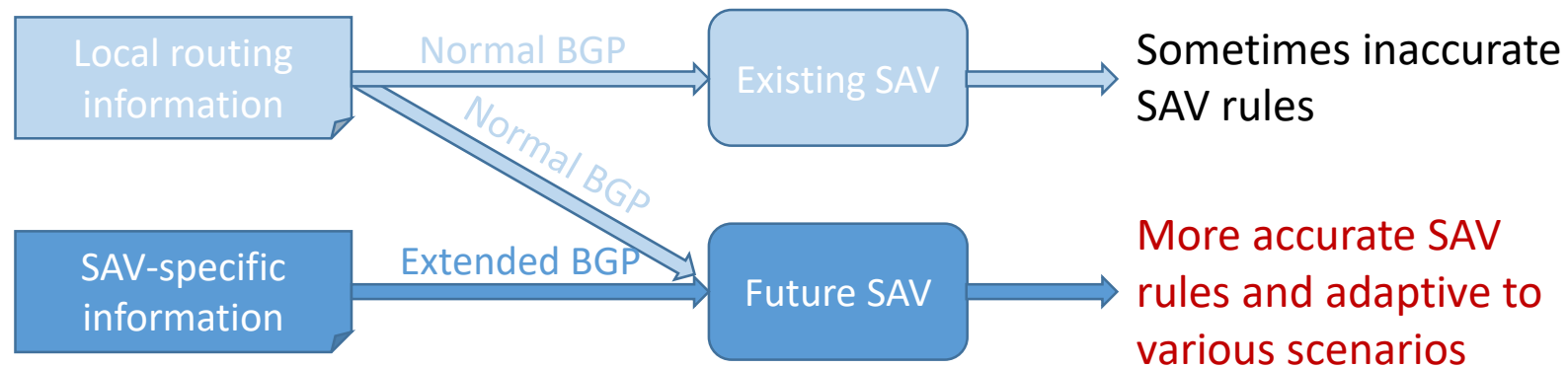
[draft-geng-idr-bgp-savnet-03](#)

N. Geng, Z. Li, Z. Tan, M. Liu, D. Li, F. Gao

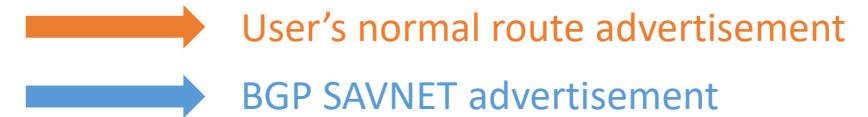
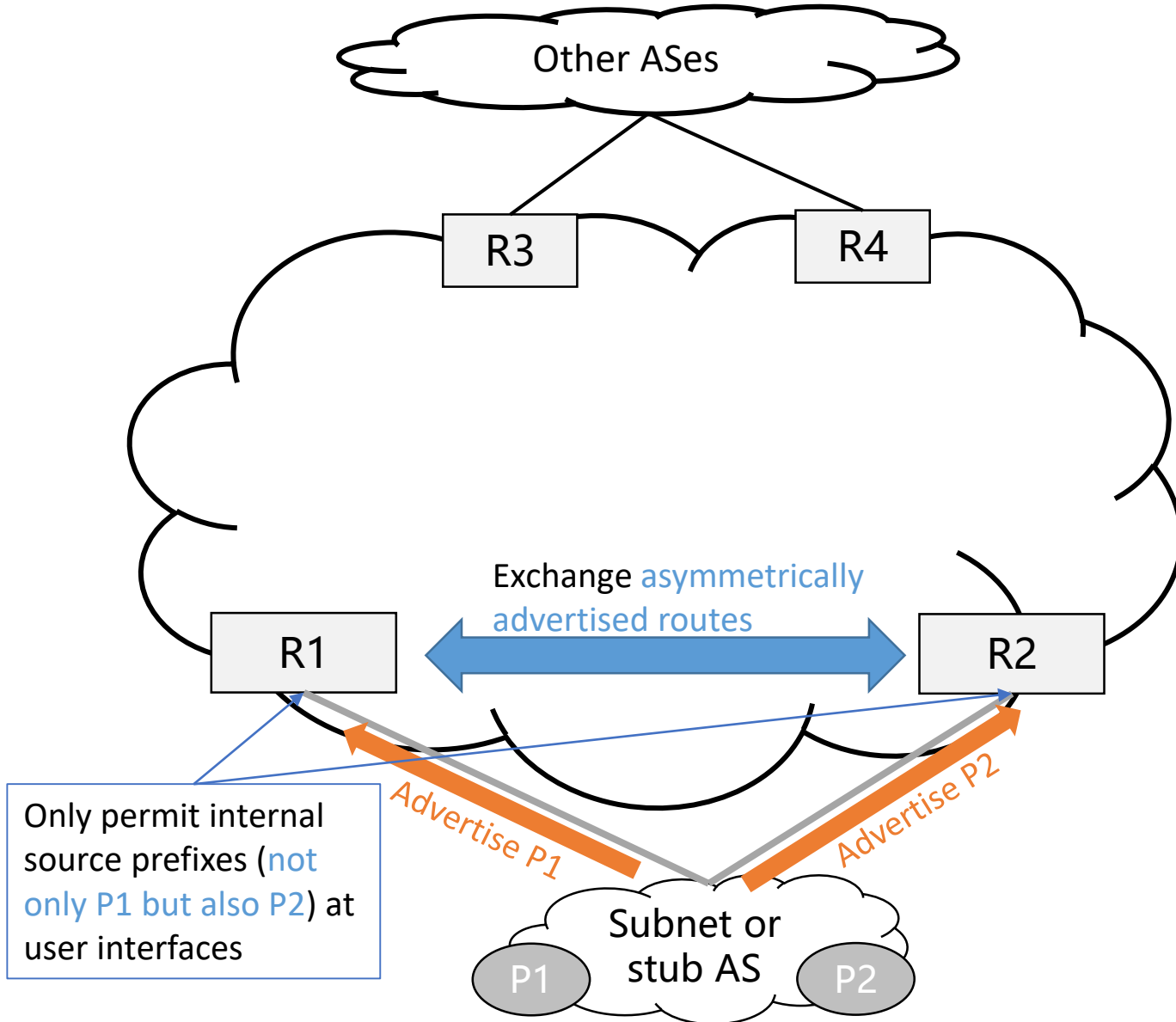
March 2024

BGP SAVNET Helps Construct the Validation Boundary for a Network

- Extend BGP protocols to advertise **SAV-specific information** between **edge/border routers** of **one or multiple ASes** (Follow the intra- and inter-domain architectures)
- Assist **edge/border routers on the network boundary** to generate SAV rules
 - ◆ Edge routers connected to subnets or stub customer AS generate rules for validating packets from users
 - ◆ Border routers connected to other ASes generate rules for validating packets from other ASes



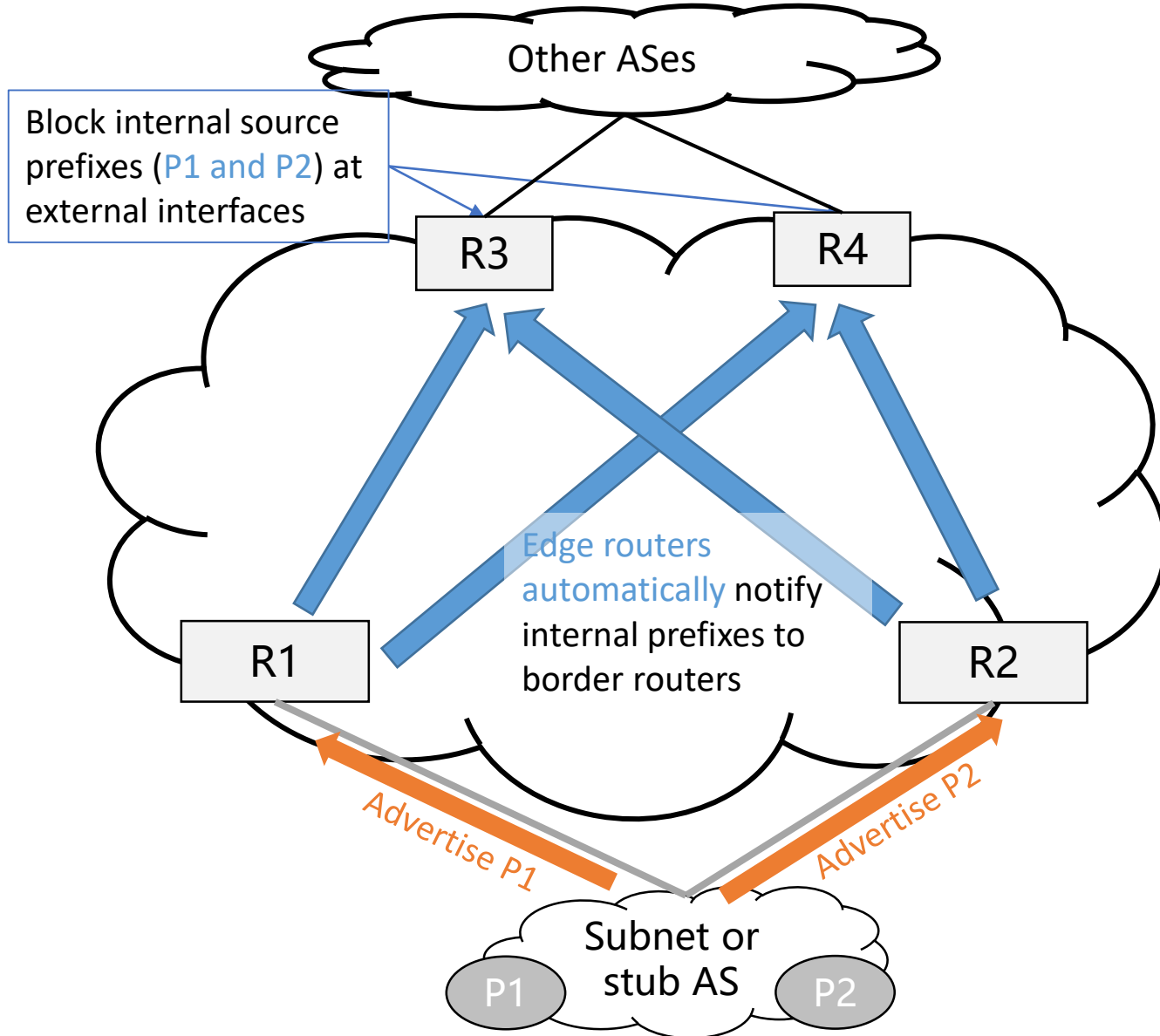
BGP SAVNET for Protecting Internal Prefixes



Outbound protection:

- Edge routers can exchange asymmetrically advertised routes and avoids improper block of strict uRPF.

BGP SAVNET for Protecting Internal Prefixes



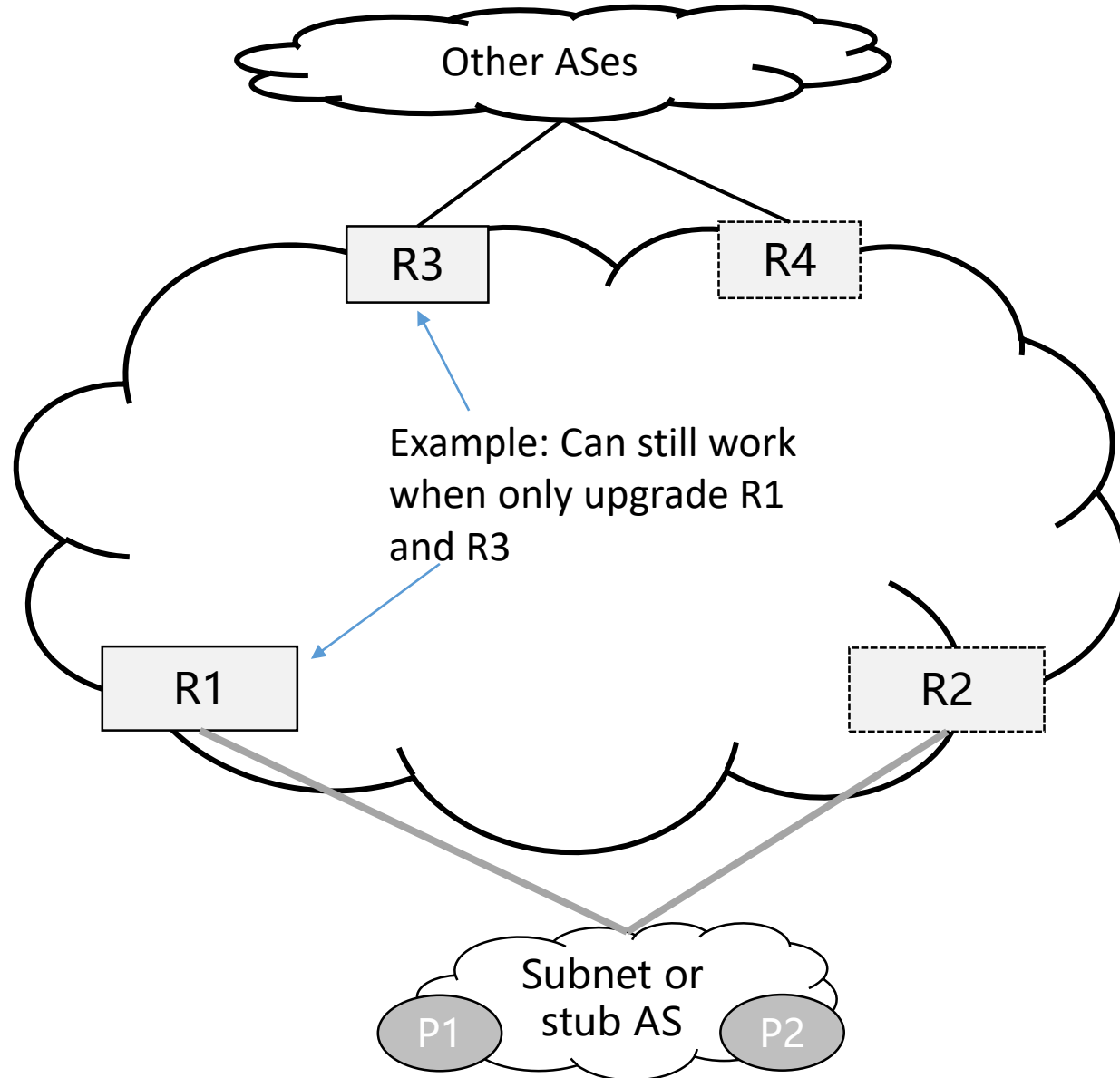
➔ User's normal route advertisement

➔ BGP SAVNET advertisement

Inbound protection:

- Border routers can automatically collect internal prefixes and simplifies operations compared to manually configuring ACL rules.

BGP SAVNET for Protecting Internal Prefixes



➔ User's normal route advertisement

➔ BGP SAVNET advertisement

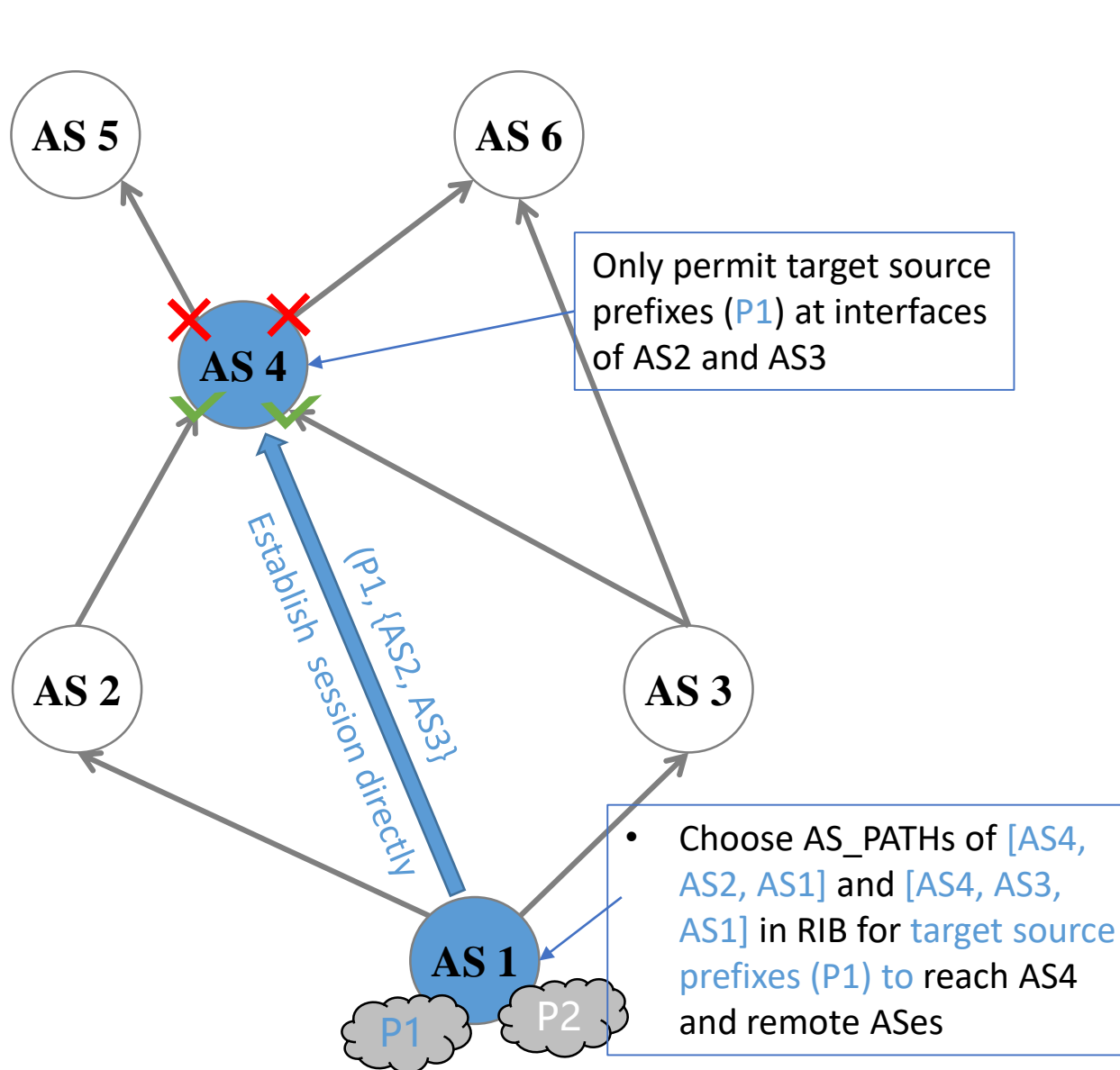
Deployability:

- Upgrading part of routers can also work well.
- Examples: 1) only upgrade R1 and R2; 2) only upgrade R1 and R3.

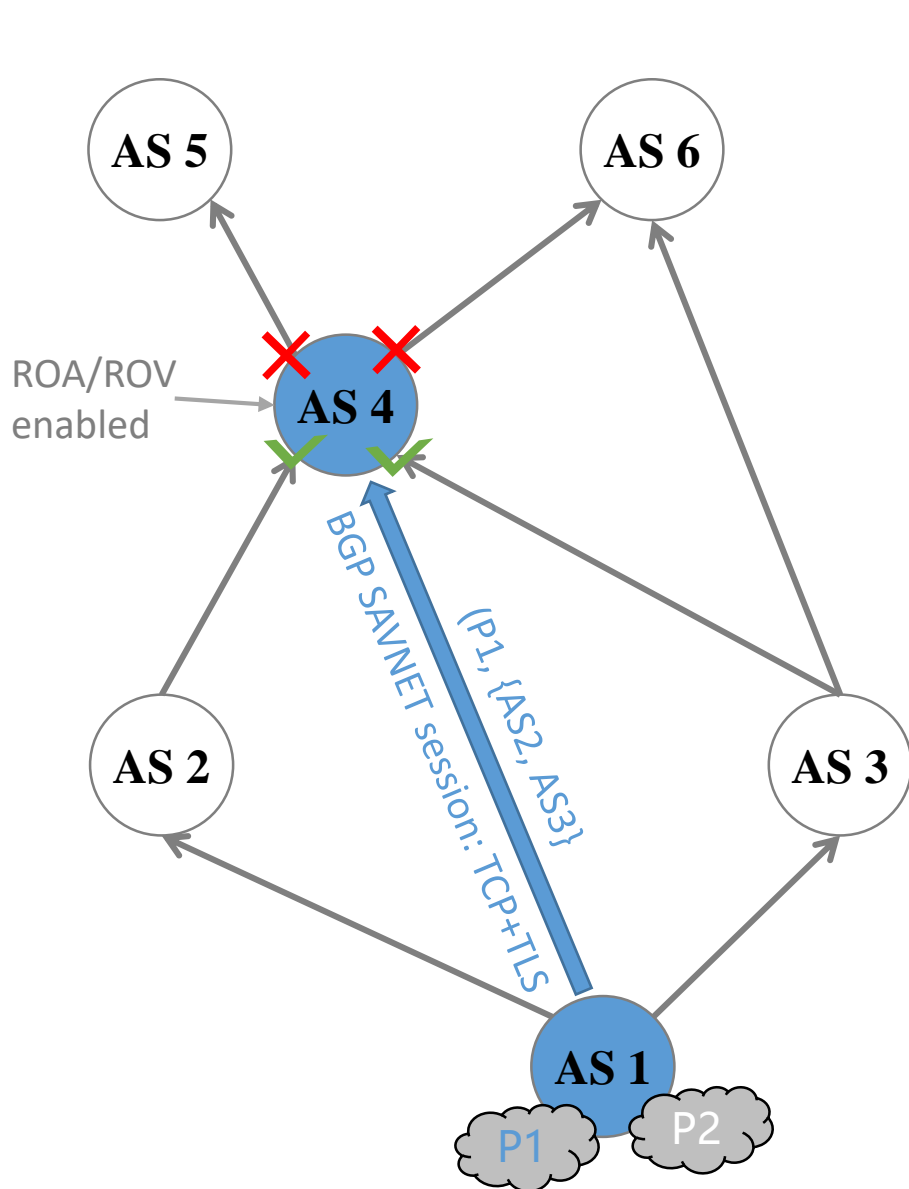
Convergence:

- 1) similar propagation speed to route.
- 2) support independent and incremental update (no need to wait for complete information).

BGP SAVNET for Protecting Remote Prefixes



BGP SAVNET for Protecting Remote Prefixes



Deployability:

- Any pair of upgraded ASes can work well.

Convergence:

- 1) similar propagation speed to route.
- 2) support independent and incremental update (no need to wait for complete information).
- 3) Direct session reduces delay during propagation.

Security:

- Target prefixes should be covered by ROAs that support ROV at Validation AS.
- Validation AS can also directly get target prefixes by RPKI data for protection.
- BGP session can be protected by TLS.

Conclusion

- Share some preliminary ideas. Will improve design continuously, especially the inter-domain SAVNET design.
 - ◆ Added more descriptions in the updated draft to response to the comments from David Lamparter, Antoin Verschuren, and Keyur Patel during IETF 118.
 - ◆ Issues are tracked in <https://github.com/XiaoTianCan/BGP-SAVNET/issues>

- Comments are welcome. Offline talks are welcome.

Thanks!

Contacts: gengnan@huawei.com