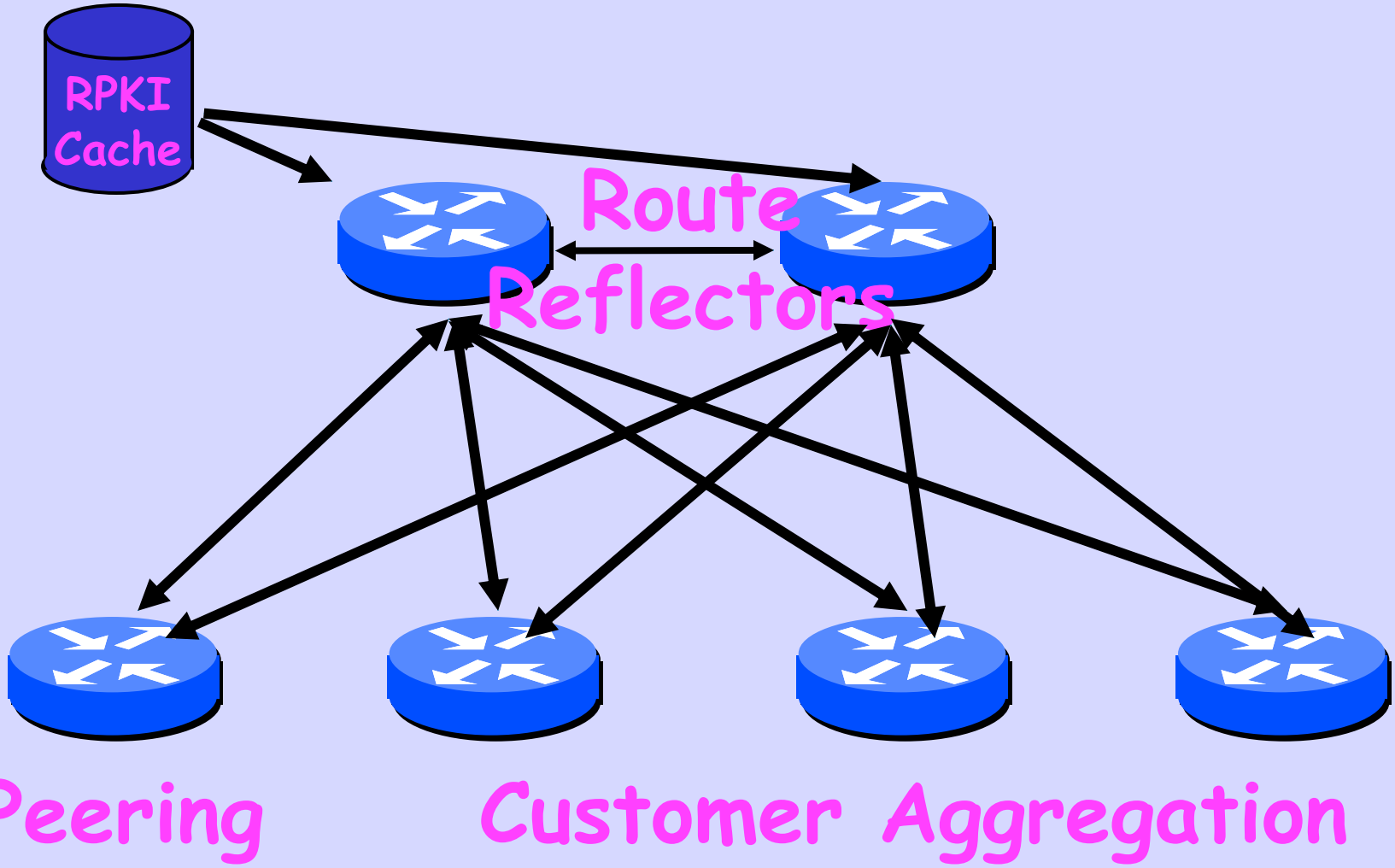
Origin Validation Signaling

draft-ymbk-sidrops-ov-signal-01

Use Case

Within a routing trust boundary, e.g. a PoP, it may not be desirable or necessary for all routers to perform Origin Validation using the RPKI per [RFC6811]. A good example is route reflectors.



Terminology

Evaluator - a device receiving routing announcements from *senders*, applying RPKI-based Origin Validation, and possibly signaling route Invalidity back to the *sender*.

The Hack

An *Evaluator*, SHOULD signal receipt of an **Invalid** route back to the sender by announcing that route back to the sender marked with the BGP Prefix Origin Validation State Extended Community as defined in [RFC8097]

A sender receiving the returned prefix announcement so marked MUST treat it the way it would treat an Invalid origin that it itself detected. It should withdraw all routes it had announced to that prefix with the Invalid origin AS. This includes withdrawing any instances of additional paths with that origin AS advertised under [RFC7911].

Capability

- The router sending the Invalid announcement is not normally expecting to receive it back
- So a BGP Capability exchange is needed to agree on the capability

Isn't This Outsourcing Security?

No

- It is "remote decision making"
- Not letting a third party make the decision; it is simply doing it on a different computer -- smb
- Similar to a PoP having a single RPKI Cache, with all trust is vested in it

As with all communities which cause semantic change, this use of the community may be abused as an attack vector. Therefore the operator MUST configure their incoming external border to strip the community.

Drive Safely