BGP Prefix origin validation

draft-pmohapat-sidr-pfx-validate-04
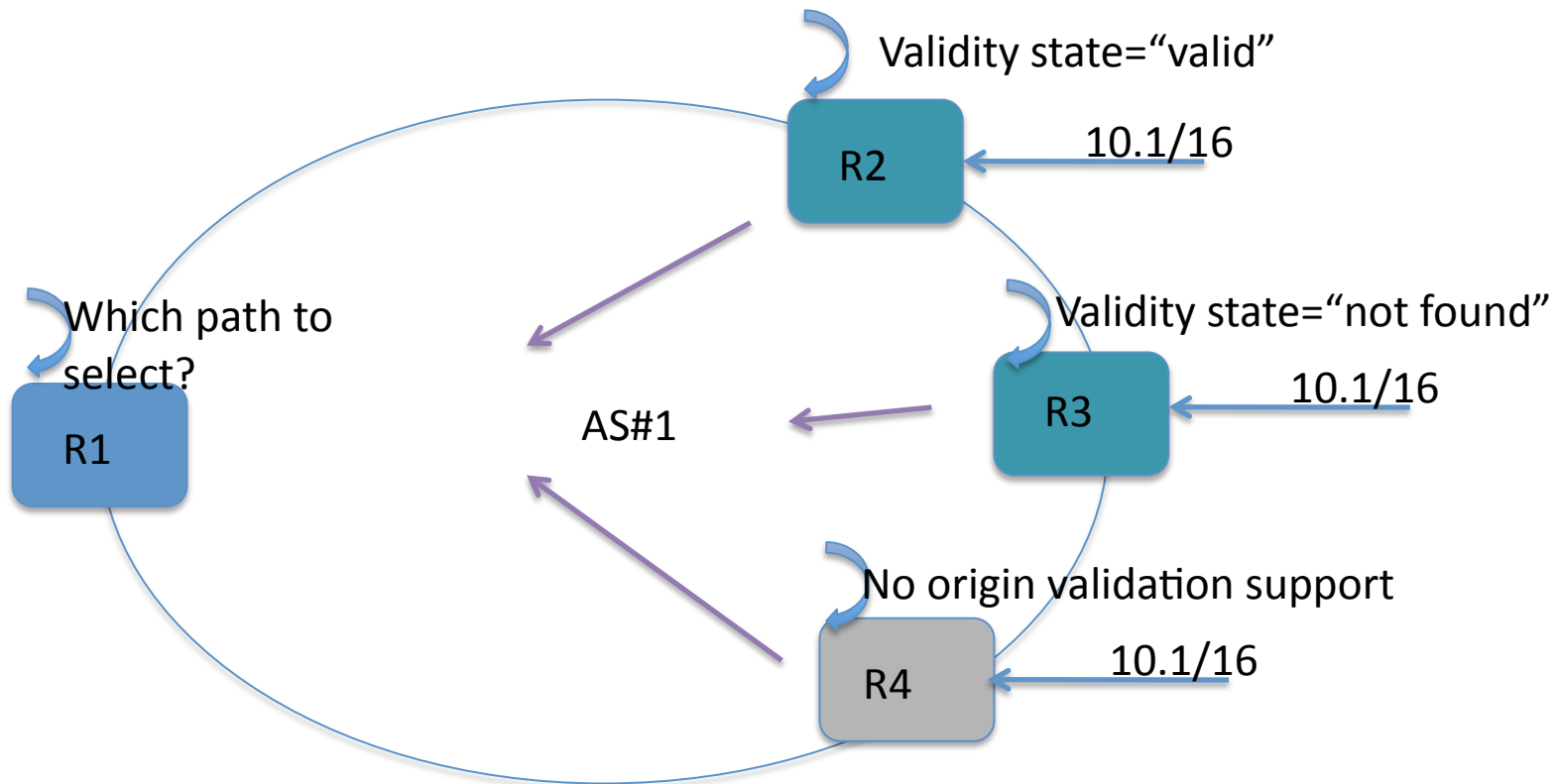
IETF 77, March 2010, Anaheim, California

Recap

- "In-router" maintenance of origin database (derived from RPKI data and result of cache-to-router exchange)

- Validity state marking per path (VALID, INVALID, NOT-FOUND)

- Best-path selection changes (first tie-breaking rule before LOCPREF; VALID > NOT-FOUND > INVALID)

- Various policy knobs

Status

- Prototype code in both Cisco IOS and IOS-XR
  - cache-to-router protocol (*draft-ymbk-rpki-rtr-protocol*)
  - BGP prefix validation (*draft-pmohapat-sidr-pfx-validate*)
- Testing in progress at multiple locations
- Draft (-04 version) updated to include pseudo-code and other details from implementation experience

IBGP behavior – Problem

Validity state="valid"

10.1/16

R2

Which path to select?

R1

AS#1

Validity state="not found"

10.1/16

R3

No origin validation support

10.1/16

R4

Characterizing the problem…

- Need to carry the validity state marking of routes in IBGP for debugging purposes
- Need for policy extensions to provide operators with an ability to influence decision process
- Need for a protocol mechanism to get the "desired" behavior automatically in the IBGP network (e.g. valid > not-found > invalid)

Solution choices

- Policy
  - Route policy extensions to match on "validity state" and set an attribute value (LOC_PREF, MED, community, …) to influence best path decision
  - No standardization required

- Well-known community
  - Attach a well-known community value based on the result of origin validation at the border routers (receivers map the community back to the validity state)

- New attribute
  - Define a new attribute for carrying the validity state intra-AS

Decision time

- Combination of "policy" and "well-known community"
- Default behavior
  - Border router
    - Mark routes based on origin database lookup
    - Allow policy extensions to match based on validity state & set various attributes
  - IBGP receiver
    - Base BGP behavior. No changes.
- Automatic-validation-ON knob
  - Border router
    - Mark routes based on origin database lookup
    - Allow policy extensions to match based on validity state & set various attributes
    - Best path selected based on valid > not-found > invalid
    - Tag well-known community based on validity state on IBGP advertisements
  - IBGP receiver
    - Map well-known community to route's validity state
    - Best path selected based on valid > not-found > invalid
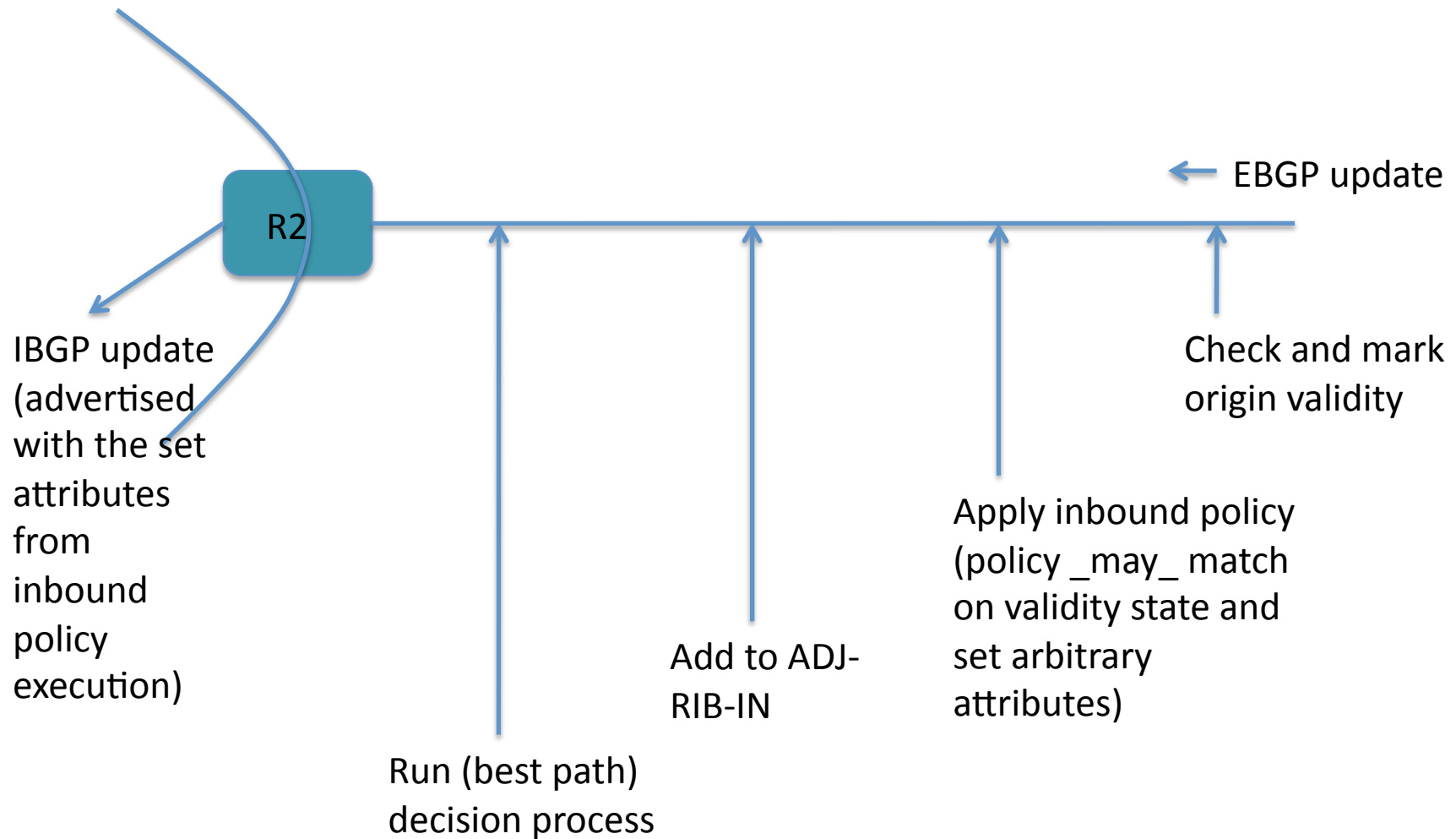
Well-known community

- Provides an automated (protocol) mechanism to get the "desired" behavior
  - No configuration required. No extra policy steps.
- Supports OLD routers (partial migration)
  - Match on a community to set something is a base policy support

Policy examples

```
route-map validity-0
  match state valid
  set local-preference 100
route-map validity-1
  set local-preference 50

route-map validity-2
  match state valid
  set metric 100
route-map validity-3
  match state unknown
  set metric 50
route-map validity-4
  set metric 25
```

Policy execution

R2

EBGP update

IBGP update (advertised with the set attributes from inbound policy execution)

Run (best path) decision process

Add to ADJ-RIB-IN

Apply inbound policy (policy _may_ match on validity state and set arbitrary attributes)

Check and mark origin validity

Document Status

- Feedback Please!
  - To authors or SIDR mailing list
- Request for WG adoption