Origin Validation Policy Considerations for Dropping Invalid Routes

Study of
"Drop Invalid if Still Routable (DISR)" Policy

draft-sriram-sidrops-drop-invalid-policy

K. Sriram, Oliver Borchert, Doug Montgomery (NIST), and Job Snijders (NTT)

Special thanks to Lilia Hannachi (NIST) for Routeviews / ROA Data Analysis

March 2018

Acknowledgements: Thanks to Jeff Haas and Saku Ytti for discussions related to implementation issues. Thanks also due to many who offered feedback and comments on the SIDROPS mailing list.

Question: How to utilize Origin Validation (OV) state in route selection policy?

- 'Valid' -- obviously raises no concerns
- 'NotFound' – not penalized during partial deployment
- 'Invalid' – questions
  - Always drop Invalid?
    - Answer: Perhaps not. Network operators would like reachability not be compromised during incremental deployment / transient conditions.
    - Unconditionally dropping Invalid -- only in mature RPKI adoption state.
  - **Incremental deployment state -- Should 'Invalid' route be dropped only if a less specific route exists that is 'Valid' or 'NotFound'?**

Why DISR?

What is DISR:

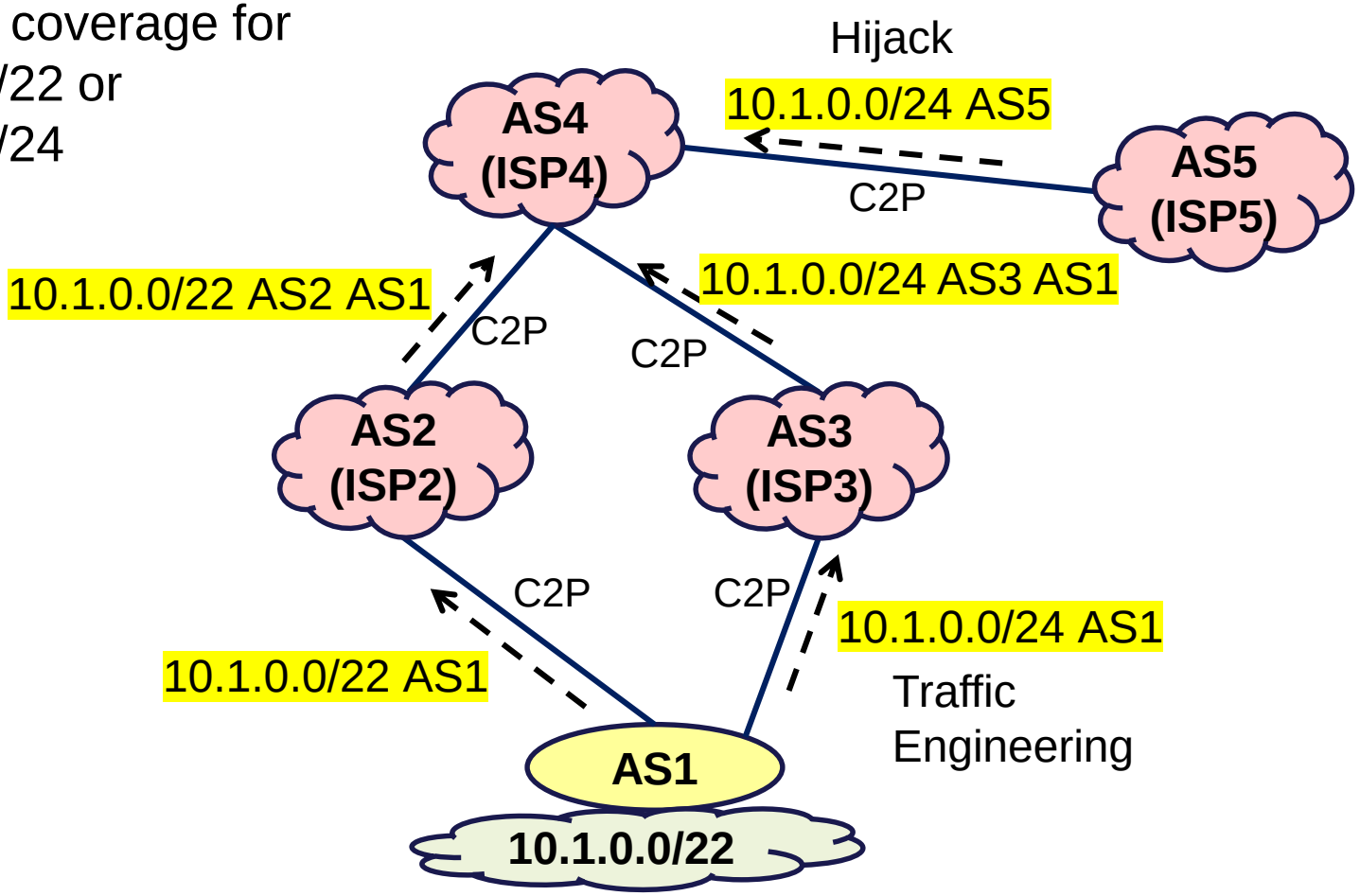
- DISR = Drop Invalid if Still Routable
  - Drop Invalid if a Valid or NotFound less specific route exists

Why DISR:

- If ROA for subsuming less specific prefix exists but there is no ROA for the more specific that you announce, then
  - DISR (working in ASes elsewhere) ensures that traffic for the more specific prefix still reaches you - correct destination (possibly via suboptimal / non-TE path)
  - Invalid announcements of your more specific prefix (by you or others) are rejected

Scenario 1

No ROA coverage for
10.1.0.0/22 or
10.1.0.0/24

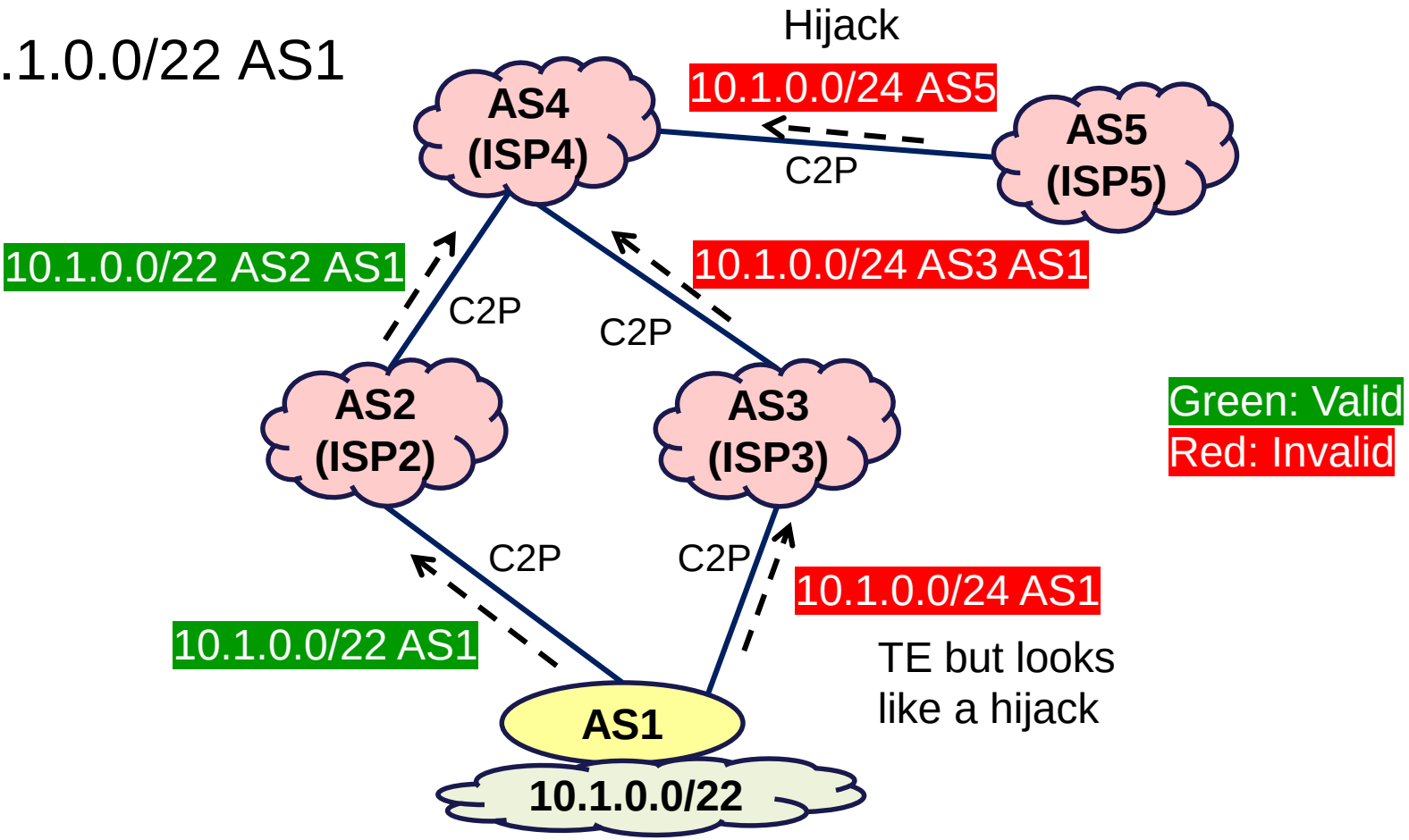


Yellow: Not Found

- AS4 performs OV
- Hijack succeeds because of lack of ROAs

Scenario 2

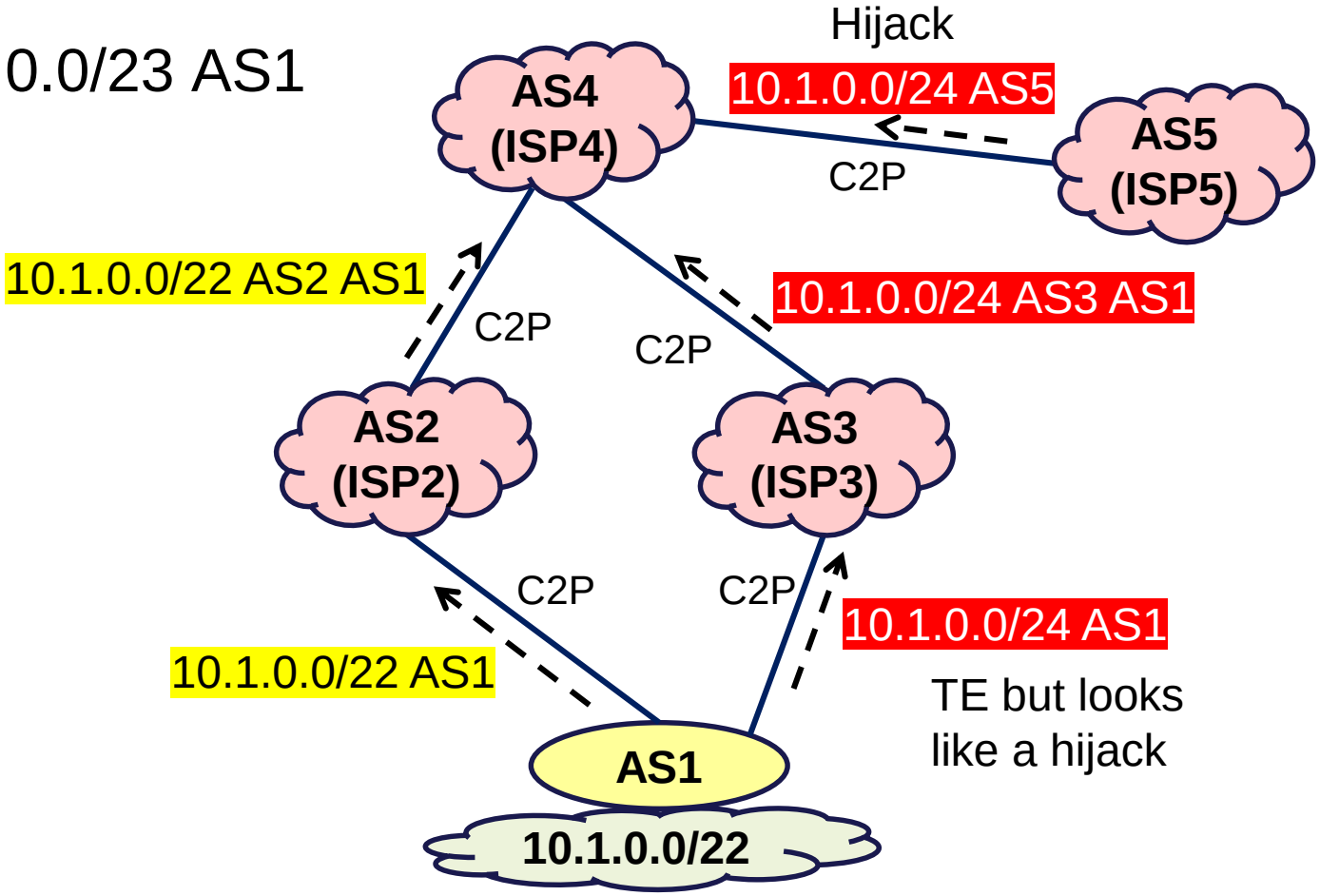
ROA: 10.1.0.0/22 AS1



- AS4 performs OV & DISR, but AS 3 does not.
- Drop Invalid if Still Routable (DISR) policy at AS4 prevents hijack from AS5; it also disrupts the TE intended by AS1
- However, all traffic for 10.1.0.0/24 reaches the correct destination albeit via a non-optimal / non-TE path.

Scenario 3

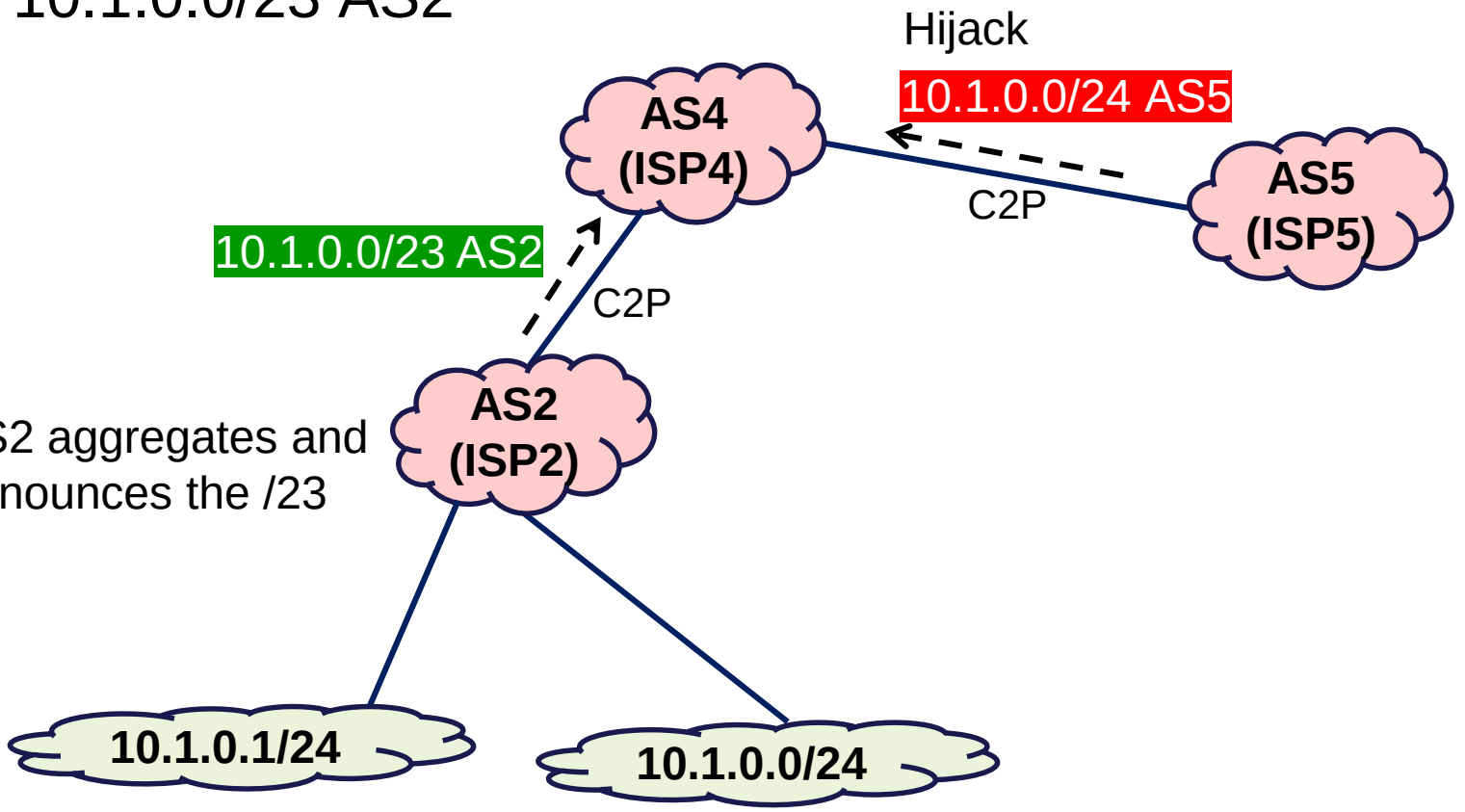
ROA: 10.1.0.0/23 AS1



- AS4 performs OV & DISR, but AS 3 does not.
- DISR policy at AS4 prevents hijack from AS5; it also disrupts the TE intended by AS1
- However, all traffic for 10.1.0.0/24 reaches the correct destination albeit via a non-optimal / non-TE path.

Scenario 4

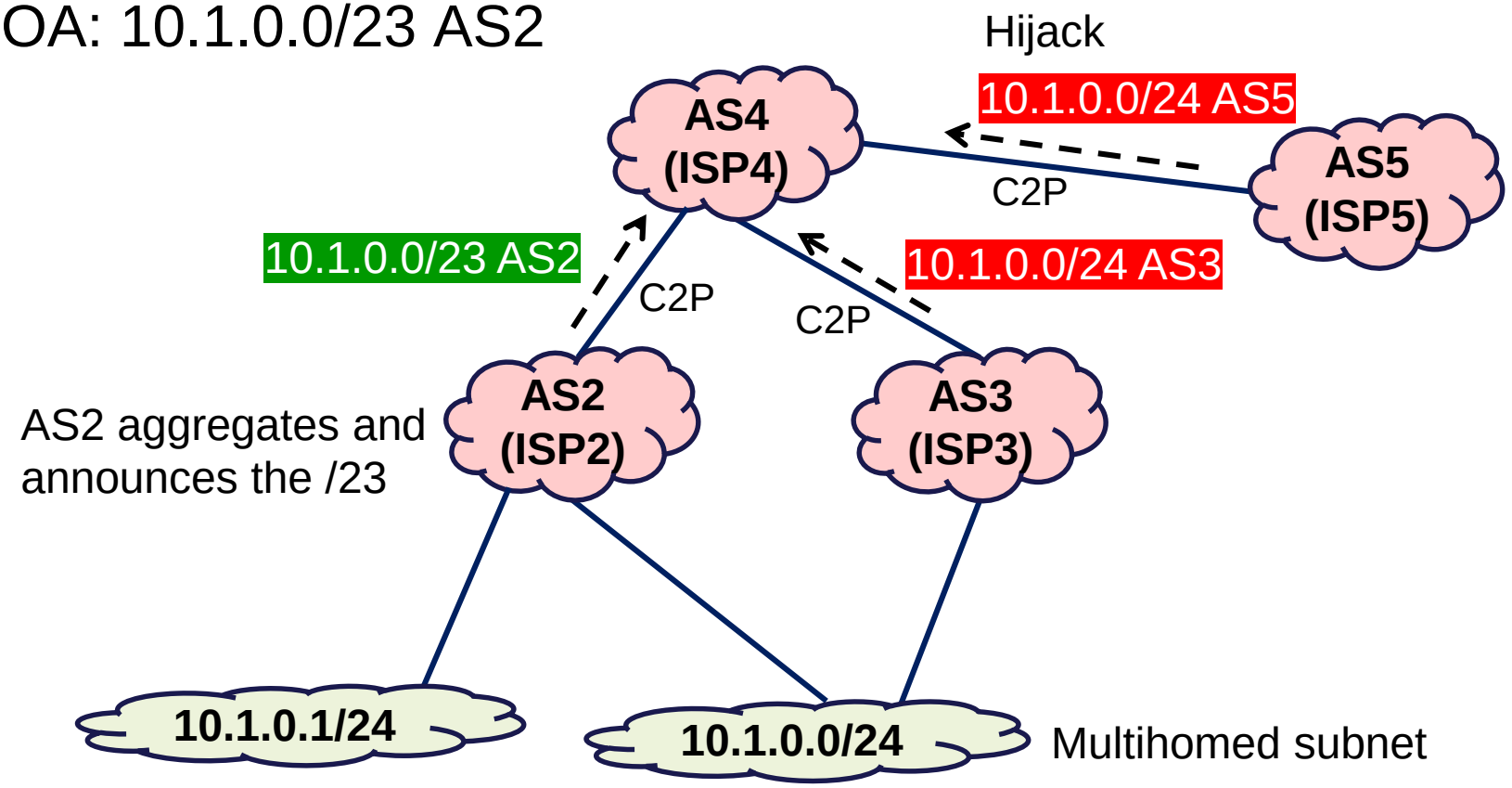
ROA: 10.1.0.0/23 AS2



- AS4 performs OV & DISR
- DISR policy at AS4 prevents hijack from AS5

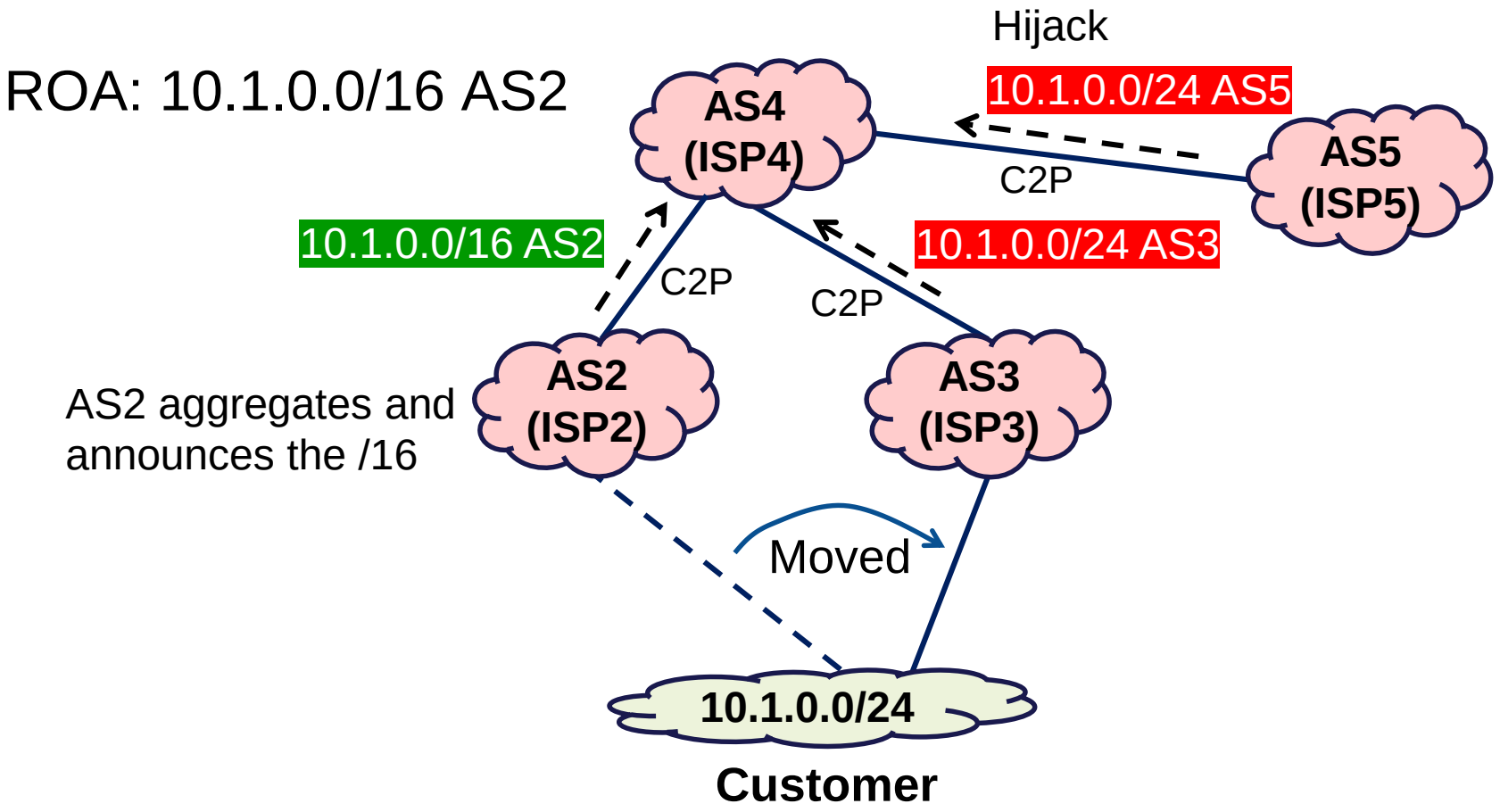
Scenario 5

ROA: 10.1.0.0/23 AS2



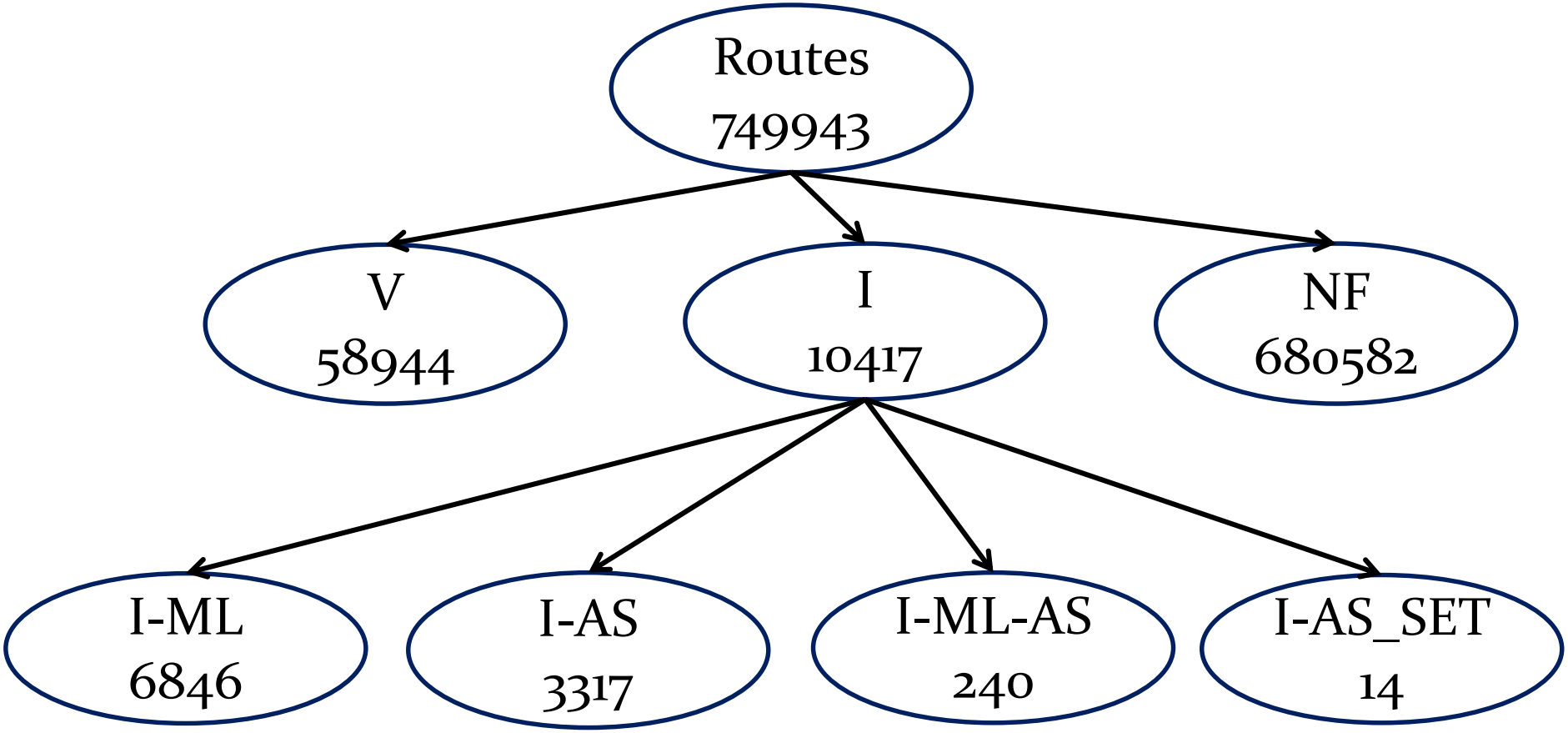
- AS4 performs OV & DISR
- DISR policy at AS4 prevents hijack from AS5
- All traffic for 10.1.0.0/24 reaches the correct destination but possibly via a non-optimal / non-TE path.

Rogue Customer (Jeff Haas' concern)



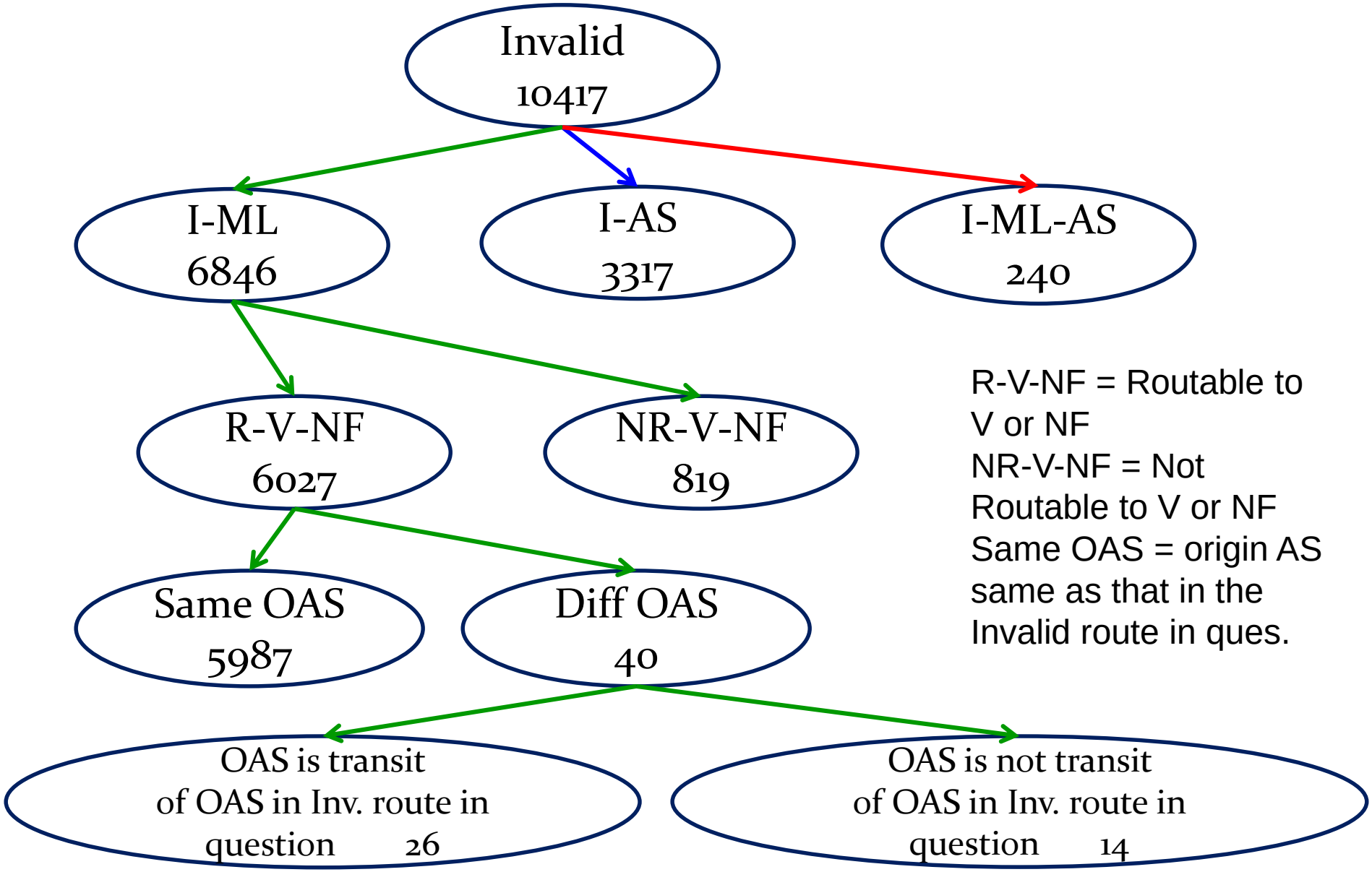
- Observation: If ISP2 (AS2) still cares about customer's connectivity, they should create a ROA for the /24 with AS3.

Routeviews / ROA Data Analysis



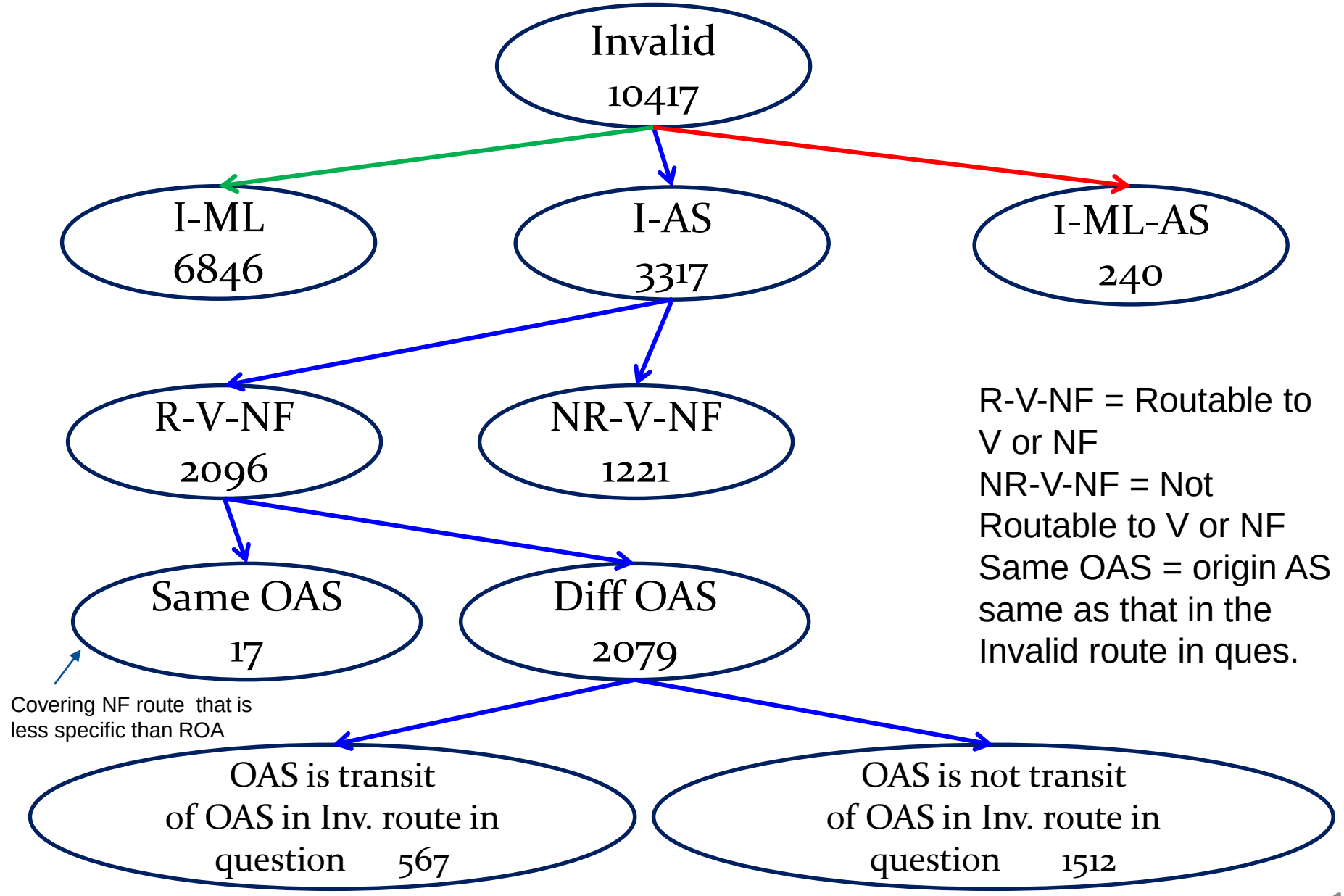
- NIST RPKI and OV analysis
- # Routeviews collectors used = 7

Routeviews / ROA Data Analysis



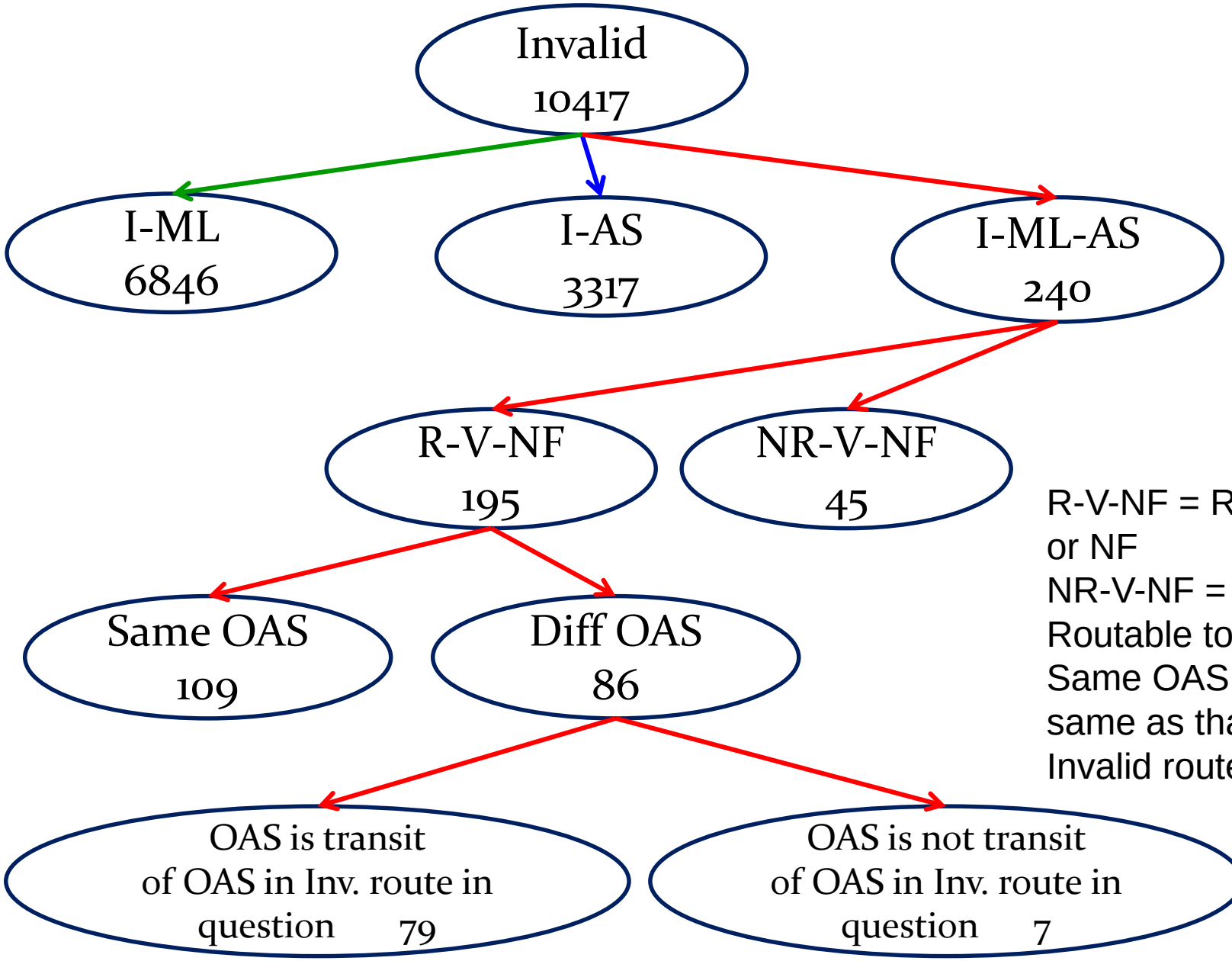
R-V-NF = Routable to V or NF
NR-V-NF = Not Routable to V or NF
Same OAS = origin AS same as that in the Invalid route in ques.

Routeviews / ROA Data Analysis



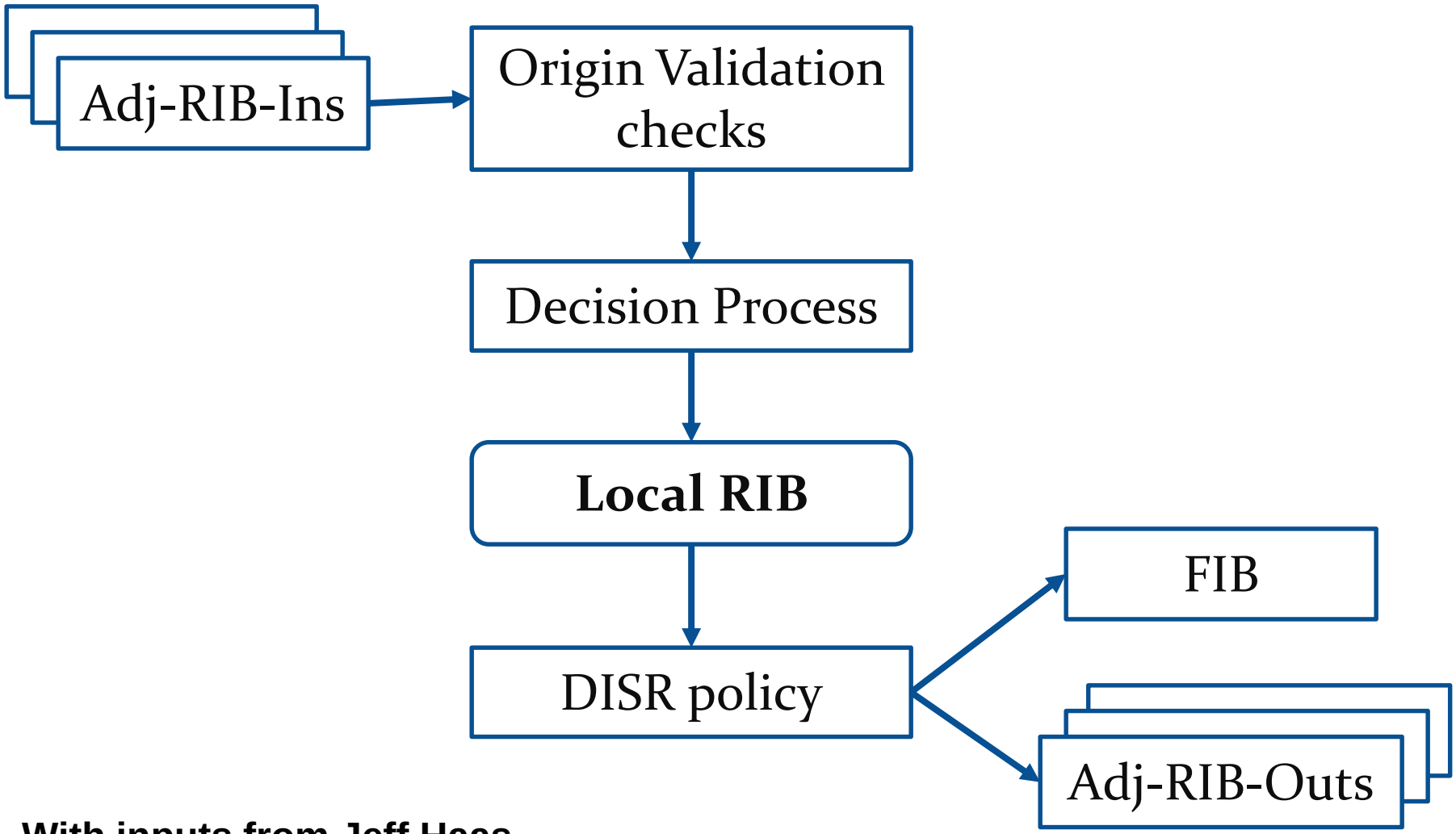
R-V-NF = Routable to V or NF
NR-V-NF = Not Routable to V or NF
Same OAS = origin AS same as that in the Invalid route in ques.

Routeviews / ROA Data Analysis



R-V-NF = Routable to V or NF
NR-V-NF = Not Routable to V or NF
Same OAS = origin AS same as that in the Invalid route in ques.

Conceptual Implementation of DISR
(Part 1 of 2)



With inputs from Jeff Haas

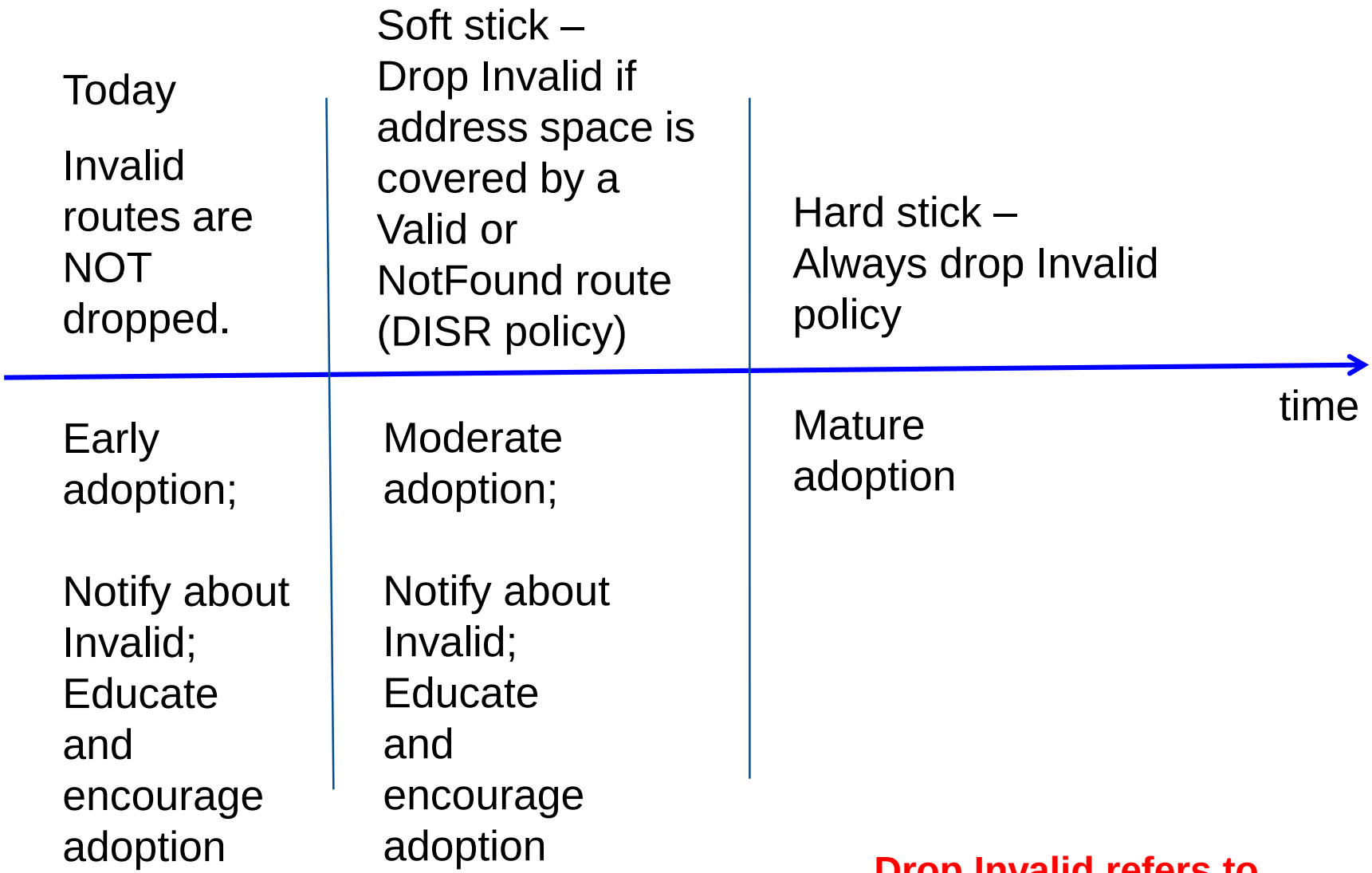
Conceptual Implementation of DISR
(Part 2 of 2)

When a Valid/NotFound route is added, check if there are any more specific prefixes in FIB / Adj-RIB-Outs subsumed by the route prefix; If such more specific prefix route is Invalid, then remove it from FIB / Adj-RIB-Outs.

When a Valid/NotFound route is withdrawn, check if there are any more specifics prefixes subsumed by the route prefix; If such more specific prefix route is Invalid, then rerun the route selection decision and DISR policy for it.

When router is notified of RPKI state change, then list all the prefixes effected by it. Rerun route selection decision and DISR policy for those prefixes.

Gradual Hardening of the ‘Stick’



Drop Invalid refers to filtering it in route selection.