

# ROAs and Detecting “Bad” Originations

Geoff Huston

SIDR WG

IETF 74

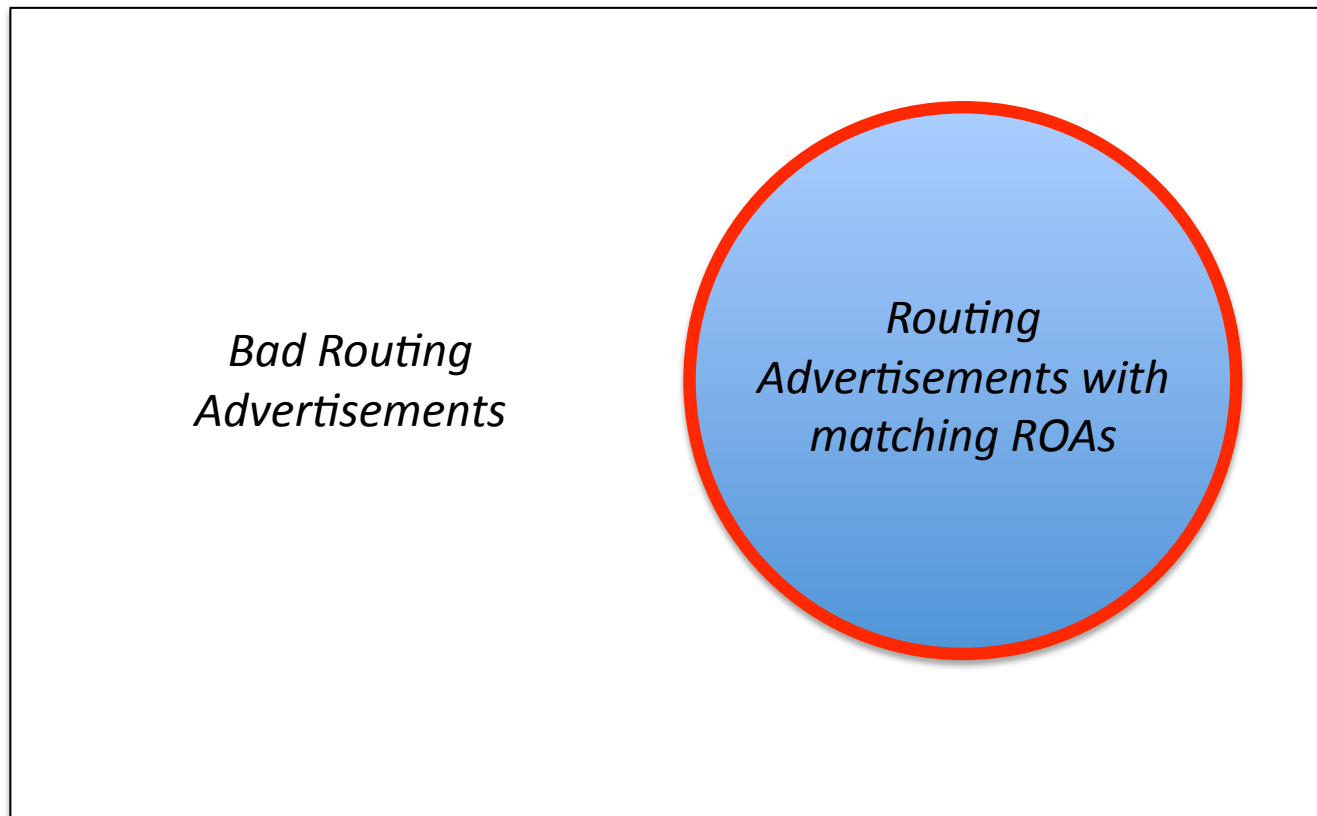
# What's the Problem ?

- Assumption that the aim of the SIDR work is to allow the identification of “bad” routing information
  - What forms of routing information is “bad”?
    - We are not (yet) working on the integrity of AS path and hop-by-hop attributes in the routing system
  - Lets restrict the question a little: What forms of *origination information* in routing is “bad”?

# What's the Problem?

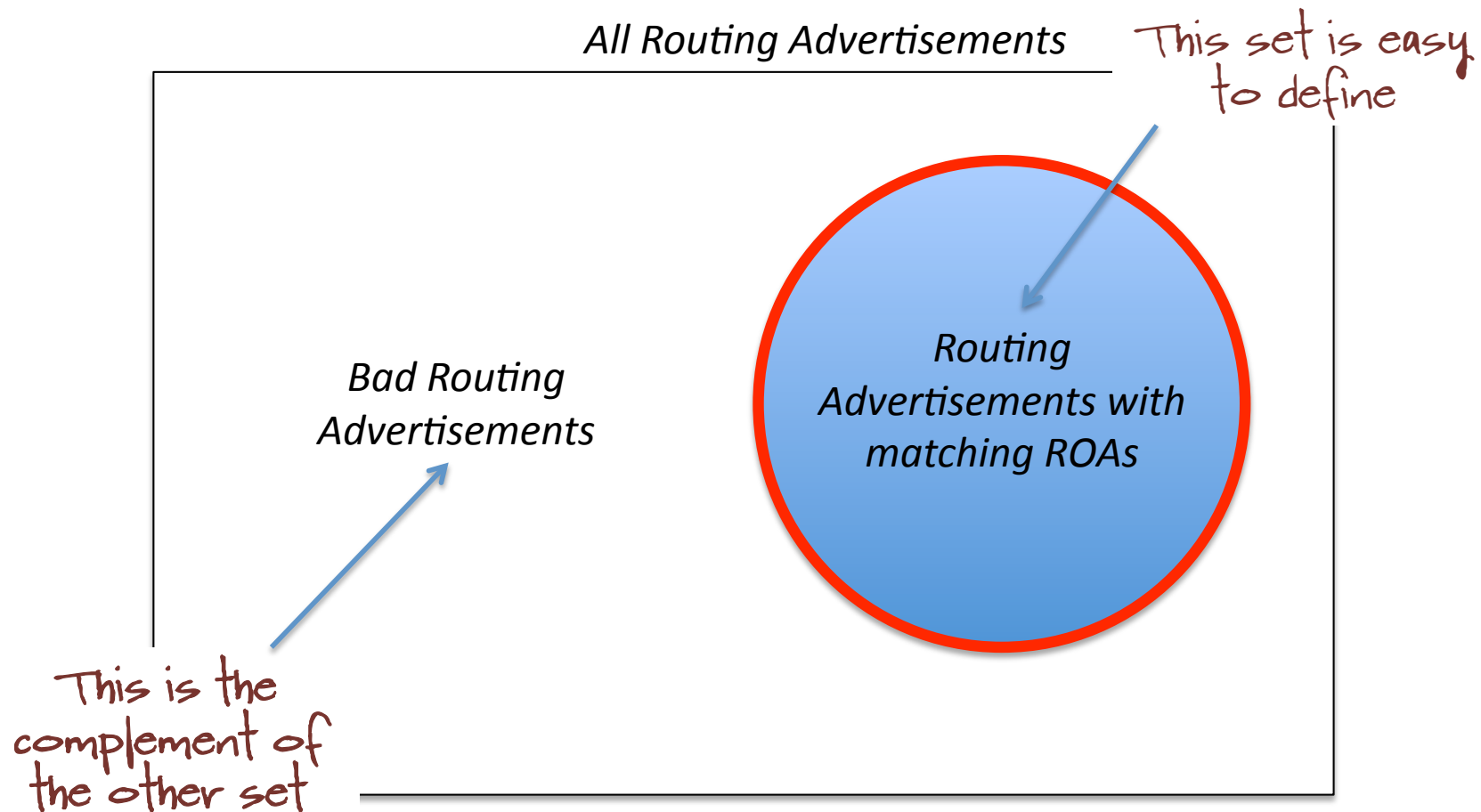
## Scenario A: Comprehensive Use of ROAs

*All Routing Advertisements*



# What's the Problem?

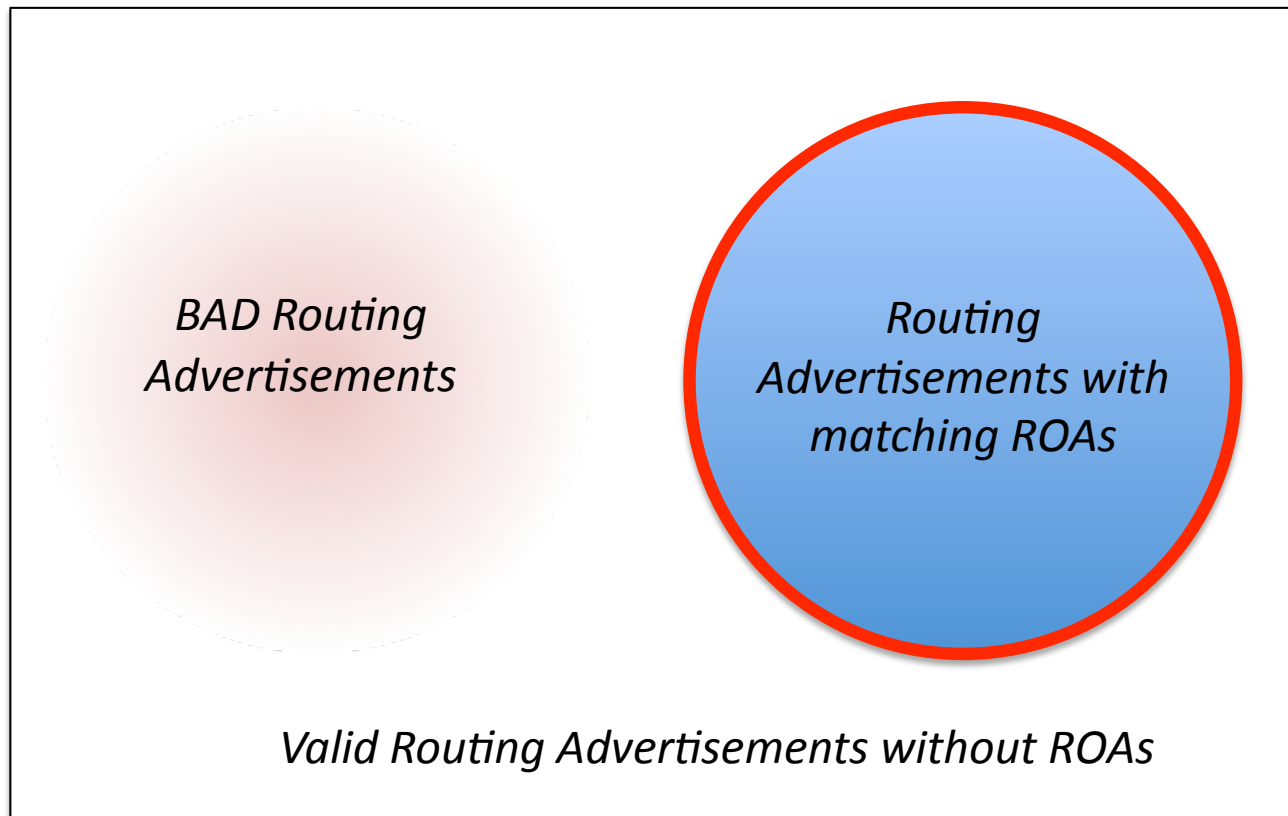
## Scenario A: Comprehensive Use of ROAs



# What's the Problem?

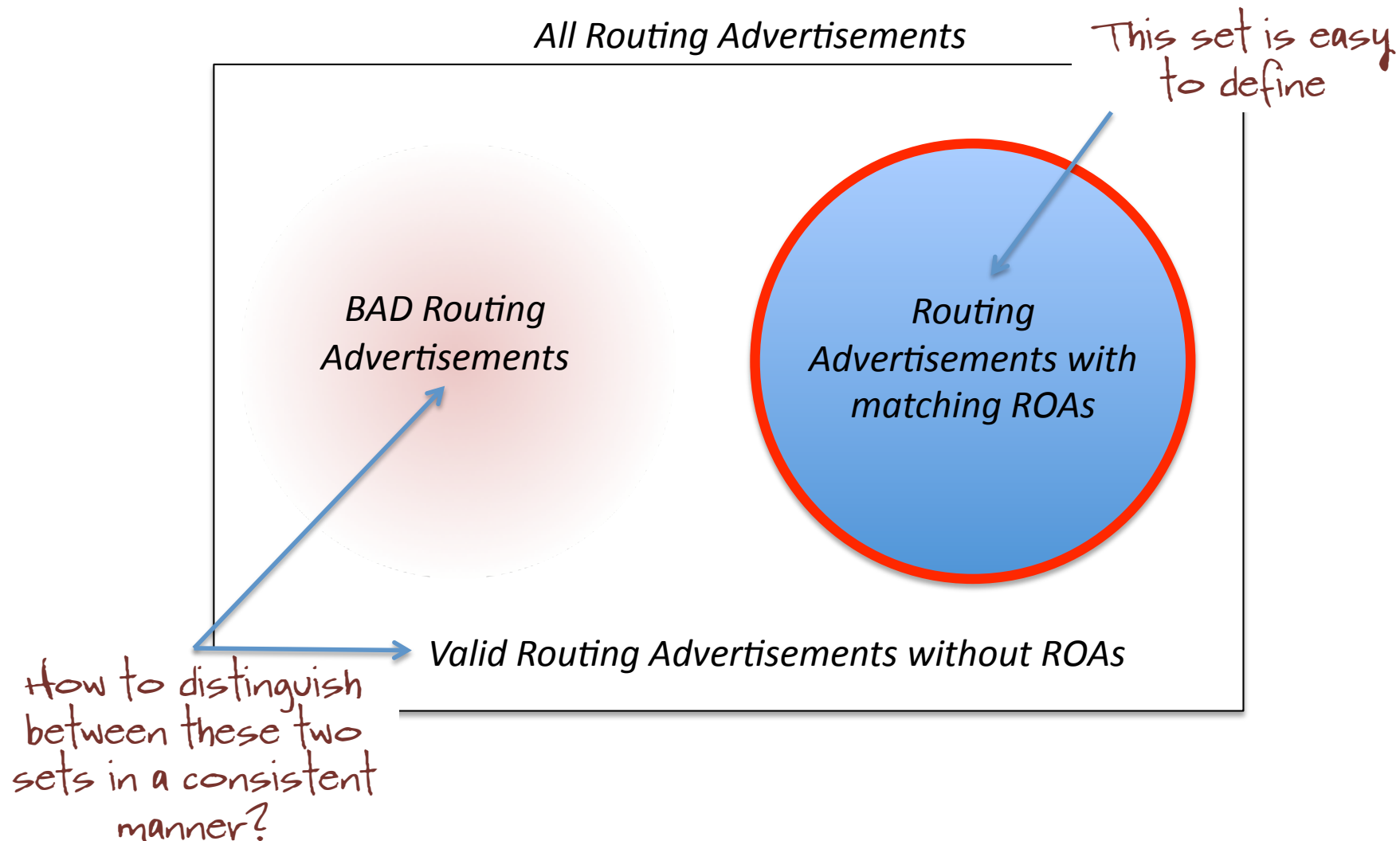
## Scenario B: Piecemeal Use of ROAs

*All Routing Advertisements*



# What's the Problem?

## Scenario B: Piecemeal Use of ROAs



# “Bad” Originations

## No ROA

- Use of a prefix that is not currently allocated for public use
- Use of an AS that is not currently allocated for public use

## A valid ROA exists, but...

- Use of a prefix (address and mask) that is **more specific than authorized** by the prefix holder
- Use of a prefix (address and mask) that is an **aggregate of what is authorized** by the prefix holder
- Use of a prefix (address and mask) by an AS that is **not authorized** by the prefix holder

# ROA Scope Considerations

## ROA: Prefix and Origin AS binding

ROA = prefix: 198.18.0.0/16 , maxlength: 20, origin: AS64500

### – More specific than ROA Prefix?

198.18.0.0/**24** , originated by AS64500

### – Aggregate Prefix?

198.18.0.0/**15** , originated by AS64500

### – Unauthorized Origin AS

198.18.0.0/16 , originated by **AS64501**



# Approaches (1)

A ROA implicitly defines its complete “anti-set”:

- The AS's listed in this ROA are authorized to originate a prefix in the range of this ROA and **no other AS's have this authority**, and **no more specific prefix may be used by any AS** (unless another ROA specifically authorizes such use)

# Approaches (2)

The AS 0 ROA (with maxlength=32<sub>v4</sub>, 128<sub>v6</sub>)

- A ROA authorizing AS 0 to originate a prefix is an explicit (and verifiable) declaration by the prefix holder that **NO AS should originate this prefix**, and **NO AS should originate any more specific prefix** (unless there is a ROA explicitly authorizing such use)
- This approach is a refinement of the “anti-set” interpretation of a ROA in so far as an AS 0 ROA authorizes NO use, so the AS 0 ROA has an anti-set interpretation that is intended to encompass ALL AS’s

# Approaches (3)

## The BOA

- A signed instrument with a similar (but not identical) structure to a ROA that asserts that set of prefixes (and their more specifics) AND the set of AS's listed in the instrument should not be used in a public routing context, unless there is a ROA explicitly authorizing such use.

# Some Open Issues

- In the AS 0 approach, do conventional ROAs include an implicit “anti-set” interpretation, or is this strictly limited to AS 0 ROAs?
- In the AS 0 approach, what is the interpretation of a ROA with an AS list that includes 0 with a maxlength less than 32 (128)?
- Should the anti-set be limited to the prefix up to maxlength and say nothing about more specifics?
- In the BOA approach, should ROAs carry an anti-set interpretation as well, or should all forms of authority ‘negation’ be performed by the BOA?

# Some Open Issues

- What, if any, authority framework would allow a route for, say, 192.0.0.0/8 to be flagged as invalid? (*invalid aggregate*)
- What authority framework would allow a route for 191.0.0.0/8 to be flagged as invalid? (*unallocated address*)
- Should AS 0 and/or BOAs include semantics that include aggregates?

# What is “partial deployment”?

- This uncertainty in validity stems from partial deployment of ROAs
- What scenarios should these ‘partial deployment’ approaches encompass?
  - Should a prefix holder be required to operate in an “all or none” mode with respect to ROA issuance?
    - once a prefix holder issues a ROA then ALL uses of the prefix and more specifics of that prefix that are not described by a ROA should be considered unauthorized?
    - What if the prefix holder wants to indicate that NO authority has been given to any AS?
  - Should the actions of a prefix holder in issuing a ROA force a more specific prefix holder to issue ROAs?
    - coerced ROA issuance for more specifics
  - Should the actions of a more specific prefix holder in issuing a BOA for the force the encompassing prefix holder to issue ROAs?
    - coerced ROA issuance for aggregates

# Yet More Open Issues

- In a world of partial deployment, where some valid routes do not have ROAs, how should ROAs (and BOAs) be interpreted?
  - Accept / Reject?
  - Relative local preference setting?
- In a relative local preference setting framework are some omissions or authority failures more serious than others? (i.e. how should the failure modes be compared relative to each other?)

# One possible way forward?

A ROA implicitly defines an AS “anti-set”:

- The AS’s listed in this ROA are authorized to originate a prefix in the range of this ROA and **no other AS’s have this authority**, ~~and no more specific prefix may be used by any AS~~ (unless another ROA specifically authorizes such use)

A ROA for AS0 with a maxlength=32<sub>v4</sub>, 128<sub>v6</sub> acts as a verifiable attestation in terms of an explicit denial capability