

BGP Prefix Origin Validation

draft-ietf-sidr-pfx-validate-03

John Scudder

<jgs@juniper.net>

SIDR, IETF-82

Clarifications

- Rewrote section 2 to be Even Clearer
- Newly defined terminology:
 - Covered: a ROA covers a route prefix if it matches it in the usual CIDR prefix match way
 - Matched: A ROA matches a route prefix if it *covers* it *and* the maxlength of the ROA is \geq the route prefix length
- Clarify that the criterion for “invalid” is “covered, not matched”
 - This was a cause of confusion

Validity States

- Not Found: No ROA *covers* the route prefix.
- Valid: At least one ROA *matches* the route prefix.
- Invalid: At least one ROA *covers* the route prefix, but no ROA *matches* it.

Example

- ROA set:
 - 10/8 maxlength 16 origin AS 690
 - (and nothing else, this is an example!)
- Route to be matched:
 - 10.0.0/24 origin AS 42
- Some readers believed that in this example the route validation state should be “not found”
- Hopefully it is now clear it is “invalid”

Other Changes

- Fixed some bugs in pseudo-code

Pending for -04

- Default validation states for routes that don't have one explicitly assigned
 - Proposed default is “not found”
- 03 and earlier restrict validation lookup step to EBGP routes.
 - Use cases exist for doing validation on IBGP and locally-originated routes
 - Thus, relax previous restriction

Discussion, possibly for -04

- If we are going to allow validation to be run against local routes...
- ... we have to think about what “local” means.
- This is less obvious than it might seem
 - Private ASNs for peering with stubs
 - Confederations
 - Local-AS
 - ...

Next Steps

- Several implementations
- Authors feel we're about done
- Spin -04, then WGLC?