Signaling BGPsec Validation State

draft-sidrops-bgpsec-validation-signaling

O. Borchert, D. Montgomery – NIST

D. Kopp – DE-CIX

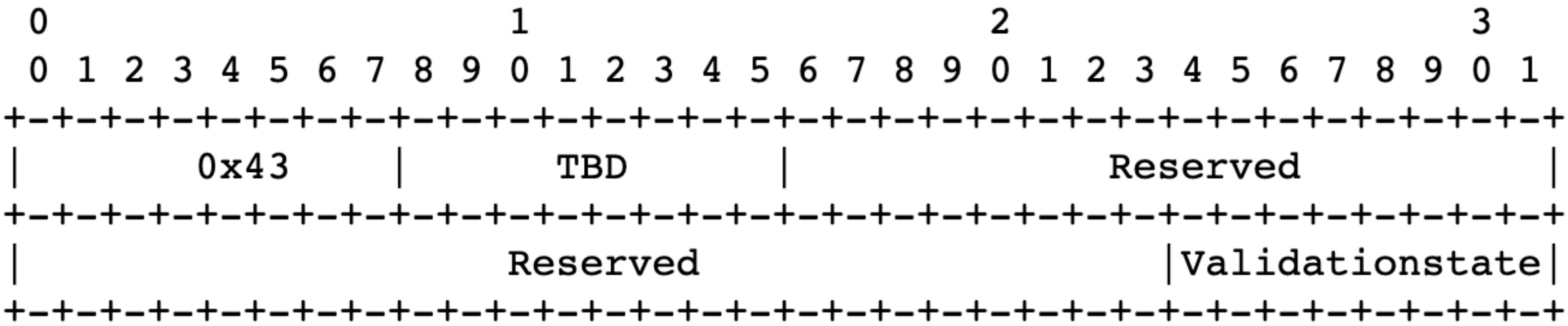
SIDROPS Meeting
IETF 108

Update since last presentation

- Removed Origin Validation State from draft
  - Removed any proposed modifications to RFC 8097
    - Reason:

      Concern from Vendors regarding backwards compatibility
  - Reverted to original proposed attribute structure.
- Added wording to assure non transitivity
- Reworded peer signaling

Extended Community Specification:

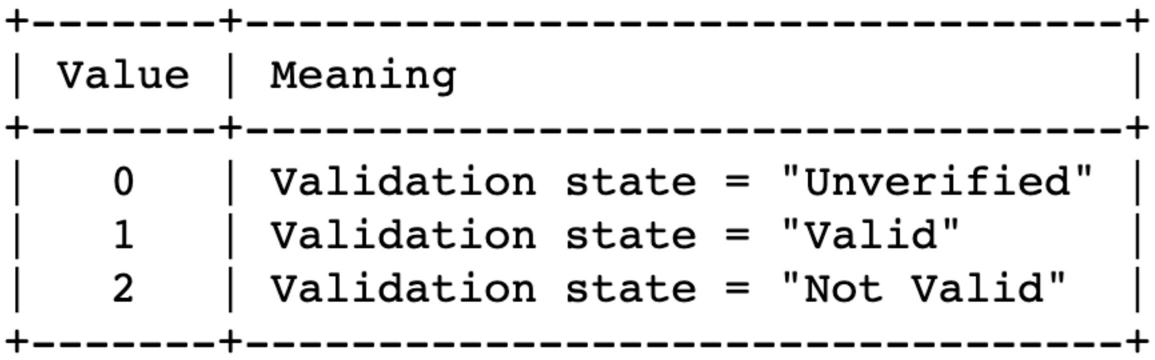


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0x43    |      TBD      |             Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Reserved                   |Validationstate|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- We need IANA to assign a new value from the ”BGP Opaque Extended Community” type registry from the non-transitive range, to be called:

“BGPsec Path Validation State Community”

Validation State Values



Value	Meaning
0	Validation state = "Unverified"
1	Validation state = "Valid"
2	Validation state = "Not Valid"

- Valid / Not Valid:
  - Specified in RFC 8205
- Unverified:
  - The sending router did not perform local BGPsec path validation on the UPDATE.

Assure Non-Transitivity

- The draft requires to set the value “Unverified” to UPDATES that were not explicitly validated at this router.

> Note, if a BGPsec speaker attaches this community to an UPDATE that was not explicitly validated at this router, the signaled validation state MUST be set to "Unverified".

  - This prevents the router from forwarding any BGPsec validation results “Valid / Not Valid” generated by peer routers.

Peer signaling

- Provide configuration to enable / disable sending and receiving on a per peer basis.
- Enable by default on iBGP sessions
- Disable by default on eBGP sessions.

> Implementations MUST provide a configuration mechanism to allow the use of this community (both sending and receiving) to be disabled on a per peer basis. By default, routers SHOULD enable use of this community on all iBGP sessions and routers SHOULD disable the use of this community on all eBGP sessions. Implementations MUST NOT send more than one instance of the origin validation state extended community and MUST drop (without processing) the BGPsec path validation state extended community if received over an External BGP (eBGP) peering session that has not be explicitly configured to enable processing.

Error Handling

- Implementation MUST disregard all instances of this attribute in case…
  - … more than one “BGPsec Validation State attribute” is attached
  - … the validation state is outside the specified values.

> If more than one instance of the extended community is received, or if the value received is greater than the largest specified value above (Section 3), then the implementation MUST disregard all instances and MUST apply a strategy similar to attribute discard [RFC7606] by discarding the erroneous community and logging the error for further analysis.

Questions?