IETF 100

Singapore 2017

Extending RFC 8208

Adding private-use algorithm IDs for experimentation / documentation

What?

- Declare fixed range of PRIVATE-USE algorithm IDs
  - To be used for documentation and experimentation
  - Allows software developers to generate unit tests for processing multi signature blocks etc.

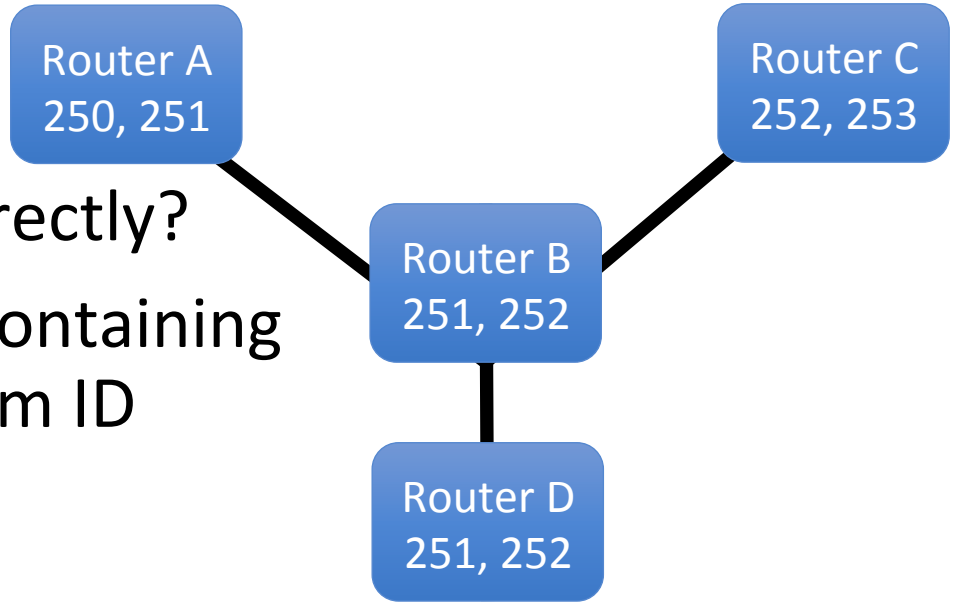
- Assign 4 private-use algorithm IDs that range from 251-254 (0xFB-0xFE)
  - The algorithm IDs are for private-use ONLY.
  - Production systems MUST (???) ignore signature blocks that use algorithm IDs within this range in addition to the already reserved IDs 0 (0x00) and 255 (0xFF)

Why?

- This allows to safely use algorithm IDs in general documentation
  - E.g.: Future best practice implementation guides
- Should/must (upper case ???) be ignored in the real world (production systems)
- Allow generation of test vectors for testing both signature blocks within BGPsec (RFC8205) without real world interference
  - E.g.: Internal testing (software testing)
- Generated test vectors for implementers will not interfere with future algorithm assignments
  - There are only a limited number of algorithm IDs available and having a reserved set for private-use is a good idea

Example Scenario

- Test the correct behavior of an implementation with multiple signature blocks.
- The test specifies a mapping of the specified algorithm (ID=1) to algorithm IDs 250, 251, 252, and 253
- Does each router process the updates correctly?
- Is each signature block containing an unsupported algorithm ID correctly removed?



Next Step…

- Requesting the range of private-use IDs (250-254) with IANA
- ?? Extending RFC 8208 -> 8208-bis
  - Adding the new algorithm IDs to RFC
  - Adding one or two paragraphs explaining the what, (what not), and why
- ?? New Document to Update RFC 8208
- Other…

Questions?