IRS19

AS4PATH confed-set/-sequence問題と Optional Transitive Attributeの扱いについて

18 Feb. 2009

河野 美也, Miya Kohno (mkohno@juniper.net)

Agenda

- そもそもの問題
- To reset or not to reset, that is a question
- 今後の方向性

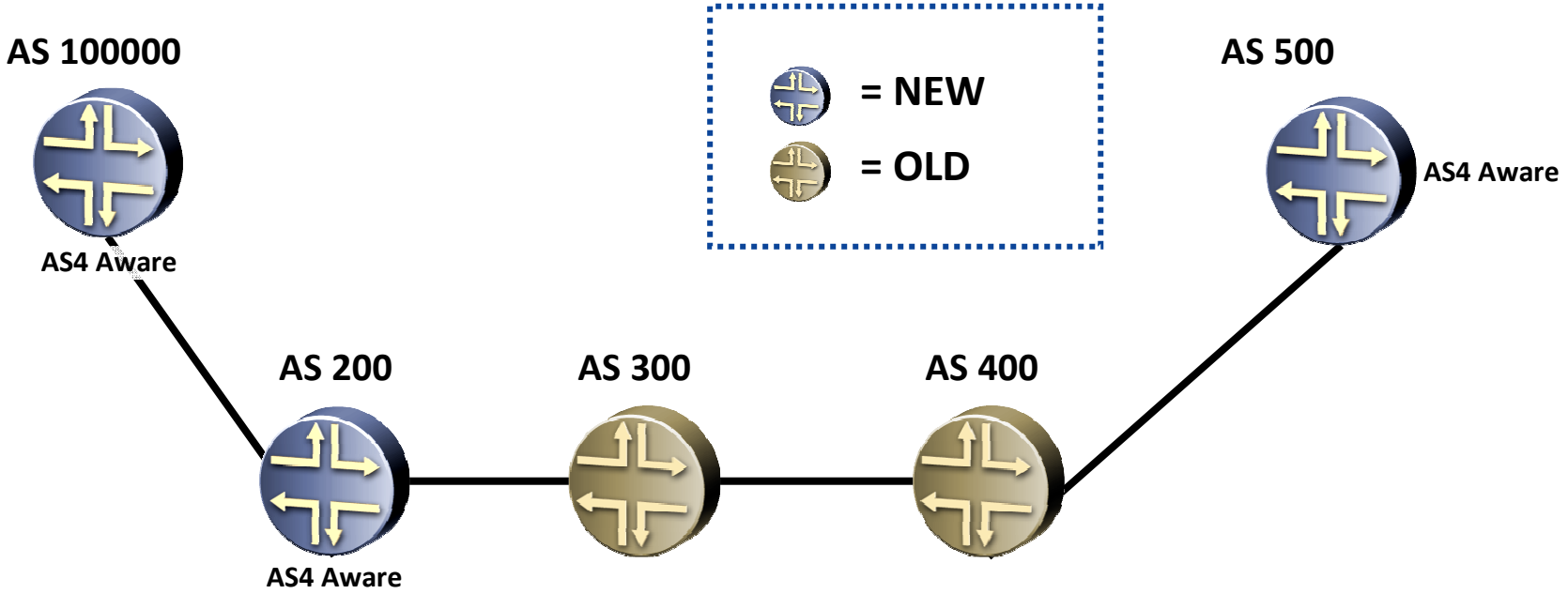
そもそもの問題

- 4 byte AS対応JunOS(R9.1以降)において、
  - Confederation使用時 AND
  - NEW to OLD 変換時
  - AS4_PATH attributeに、confed-segment {CONFED_AS_SET / CONFED_AS_SEQUENCE} を付けたまま出してしまう

    → rfc4893 violation

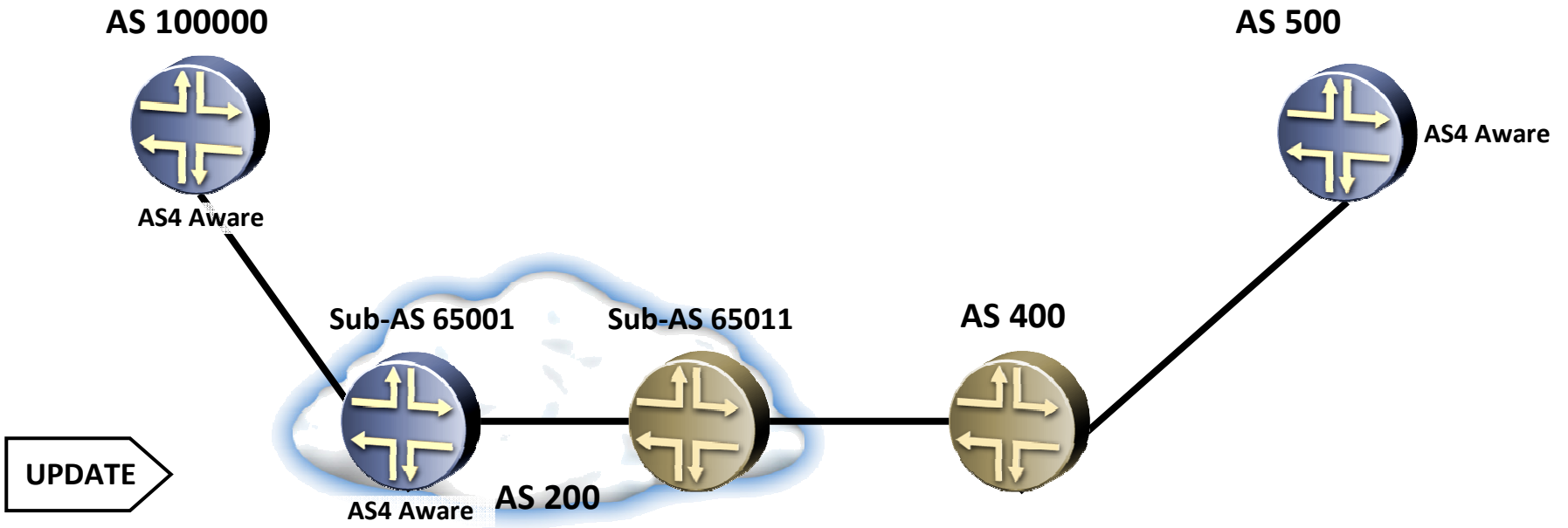
    “To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC3065] are declared invalid for the AS4_PATH attribute. “
  - PR417046
    - 9.1R4, 9.2R4, 9.3R3, 9.4R2, 9.4R1, 9.4R1.3 にて修正済み

おさらい：OLD BGP speakerとNEW BGP Speaker

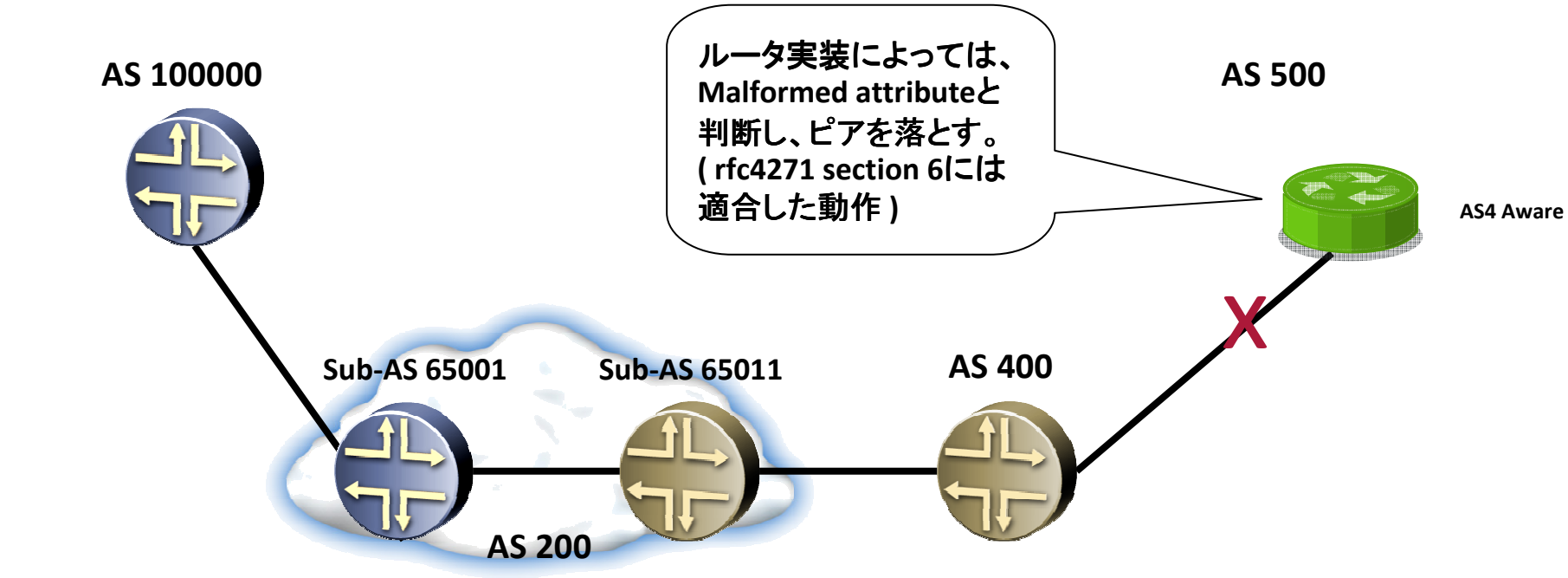


AS_PATH	100000	200 23456	300 200 23456	400 300 200 23456	500 400 300 200 100000
AS4_PATH		200 100000	200 100000	200 100000	

おさらい：Confederation時の正しい動作



PR417046修正前のJunOS動作と、遠隔ルータのピア断



To reset or not reset … Nanogでの議論

- http://www.merit.edu/mail.archives/nanog/msg14345.html
- http://www.merit.edu/mail.archives/nanog/msg14393.html

- http://www.nanog.org/meetings/nanog45/presentations/Monday/Davidson_asn4_breaks_light_N45.pdf

- Bugそのものというよりは、Peer Resetする動作の方が問題となった

- “we’re saved because vendors ignored the RFCs!”

To reset or not reset … Optional Transitiveの悩ましさ (1/2)

- Optional Transitive …
  - そもそも「認識しない」ときは、

    → partial bitをONにして、ただ通過させる

- Peerを切るのはrfc的には正しいが…
  - AS4対応、かつ、AS4PATH内容を厳しくチェックするルータのみがPeerを切る。AS対応ルータ自体が少ないし、対応していても、AS4PATHにconfed-segmentがあろうが、気にしないのがほとんど。

    → 殆どのルータが、ただ通過させる

- Peer切断の目的は …
  - 悪さをするルータを分離することにより、系全体の整合性を保つ。

    → しかしRemoteでのPeer resetは、remote attackになる。

To reset or not reset … Optional Transitiveの悩ましさ (2/2)

- では切らなければよいか？というと、そういう訳でもない…
  - 経路関連情報そのものが、PATH Attributeで運ばれる場合がある。(e.g. MP_REACH/ MP_UNREACH)

    → エラーが起こってもそのままにしておくと、経路不整合によりループやBlackholeの可能性もある。

    → 誤動作は、なるべく水際で防ぐのが鉄則。

- Malformedであっても、ゴミ情報か重要情報かで、エラーハンドリングを変えられるのがベスト
  - でも、どうやって識別するかが問題？

今後の方向性 … 1) rfc4893の改訂

- draft-chen-rfc4893bis
  - Optional Transitive Attribute (AS4_PATH attribute, AS4_AGGREGATOR) に対し、
    - エラー条件を明示
    - エラーが起こっても、UPDATEは継続するように明記

"A NEW BGP speaker that receives a malformed AS4_PATH attribute in an UPDATE message from an OLD BGP speaker MUST discard the attribute, and continue processing the UPDATE message. The error SHOULD be logged locally for analysis."

今後の方向性 … 2) optional transitive全般の扱い (1/2)

- **draft-scudder-idr-optional-transitive**
  - rfc4271 Section 6には次のように書かれているが、

    “When any of the conditions described here are detected, a NOTIFICATION message, with the indicated Error Code, Error Subcode, and Data fields, is sent, and the BGP connection is closed (unless it is explicitly stated that no NOTIFICATION message is to be sent and the BGP connection is not to be closed). “

  - 本draftでは、Optional Transitiveを別扱いにするように提案

今後の方向性 … 2) optional transitive全般の扱い (2/2)

- draft-scudder-idr-optional-transitive
  - Optional transitive attributeに関しては、そのattributeを定義する者が、エラーハンドリングについても定義すべし。
    1. Drop attribute
    2. Repair
    3. Ignore
    4. Withdraw
    5. Drop session (これは余程のことがない限り避ける)
  - DEBUG_SKIPPED Attributeの追加？
  - Local Contextに依存する場合が無いか?

Thanks

Comments/Questions are welcome !