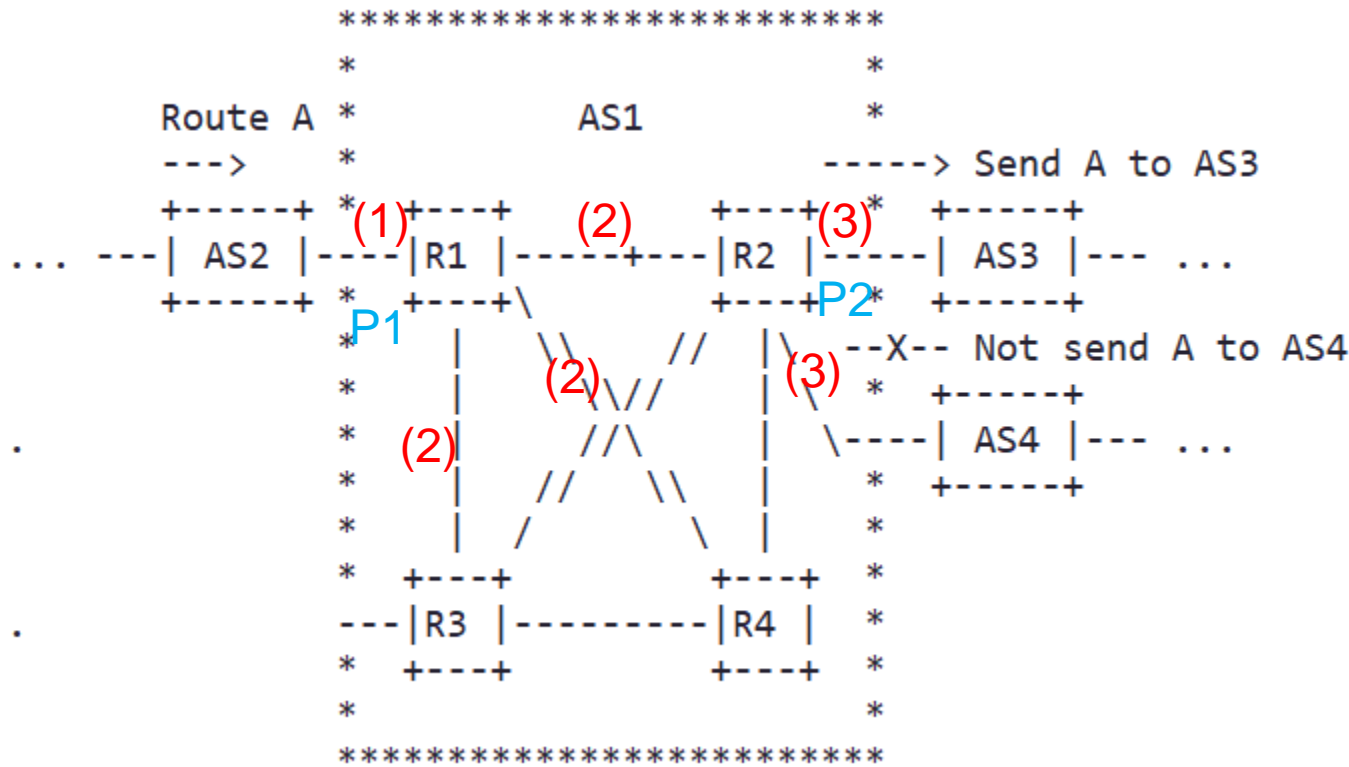# BMP for BGP Route Leak Detection

draft-gu-grow-bmp-route-leak-detection-00

Yunan Gu

Shunwan Zhuang

Introduction

- **This draft proposes a method for detecting BGP route leaks using BMP.**
- **We mainly identified the requirements and concerns for the route leak detection, such as:**
  - ✓ Implementation dependency on other ISPs
  - ✓ Detection accuracy and so on

- **We feel that BMP might be a good choice for the detection information collection with minor extension work while meeting these requirements.**
  - ✓ Do not change BGP protocol
  - ✓ Not put heavy impact on BGP processes
  - ✓ Singe-ISP-Available solution

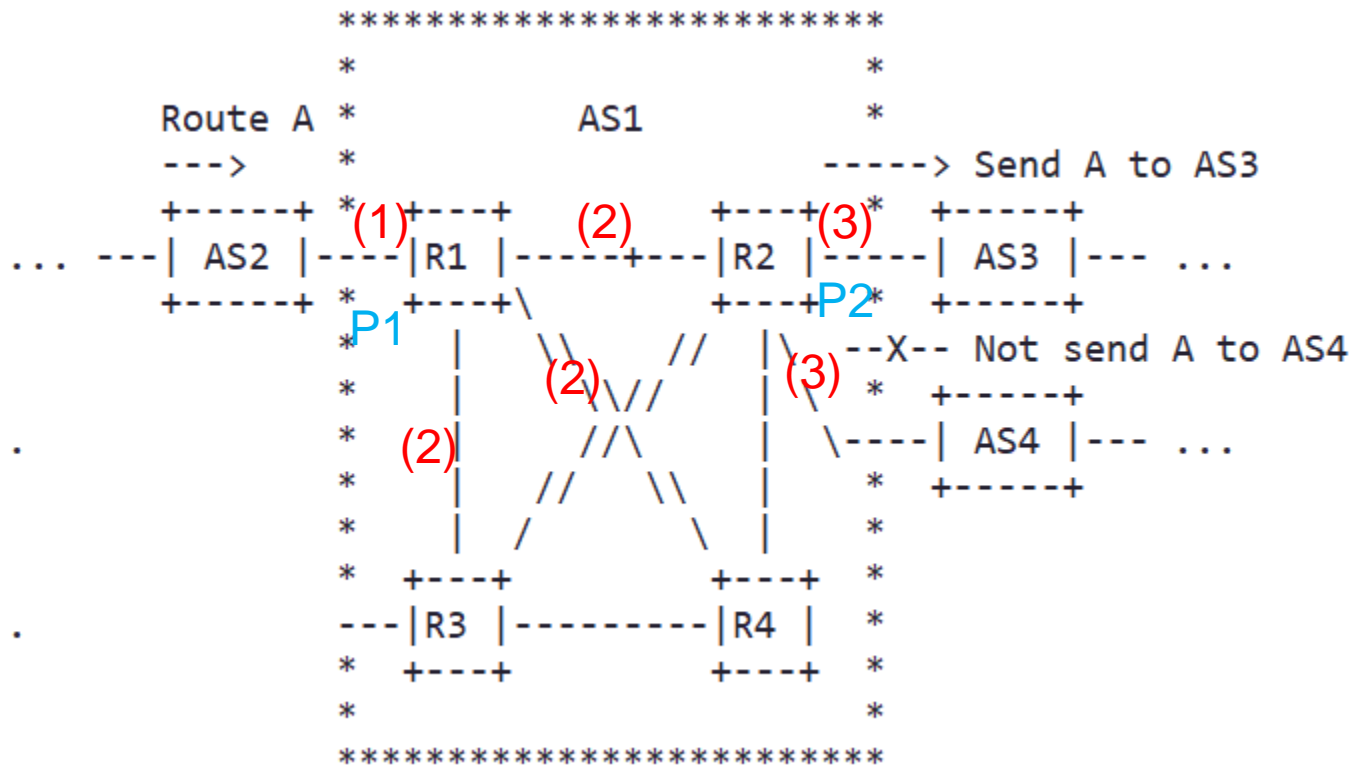# Legacy Solutions – Heavily depending on correct configurations, Lacking Verifications

```
                  ****************************
                  *                          *
  Route A         *           AS1            *
  --->            *                          *        -----> Send A to AS3
  +-----+       *(1)+---+       (2)     +---+(3)*  +-----+
... ---| AS2 |----|R1 |-----+---|R2 |------| AS3 |--- ...
  +-----+       *  +---+\              +---+P2*  +-----+
           *P1       |    \\    //   | \   --X-- Not send A to AS4
                  *       |  (2)\//   |  (3) *  +-----+
                  *    (2)|     //\    |  \   \----| AS4 |--- ...
                  *       |    //  \\  |      *  +-----+
                  *       |   /      \ |      *
                  *     +---+        +---+    *
                  ---|R3 |--------|R4 |   *
                  *     +---+        +---+    *
                  *                          *
                  ****************************
```

□ Pre-configured routing policies：

✓ P1: Configure Inbound Policies on R1 for eBGP neighbor in AS2；

✓ P2: Configure Outbound Policies on R2 for eBGP neighbors in AS3 AND AS4

□ Routing between multi-AS:

  (1) R1 receives Route A from AS2, Sets ISP-Specific community per the business relation between AS1 and AS2;

  (2) R1 sends Route A to the other border routers (e.g. R2);

  (3) Per the ISP-Specific community in Route A and the business relation between AS1 and AS3/4, R2 can control the route advertisement, e.g., Send A to AS3, Not send A to AS4

draft-ietf-idr-bgp-open-policy-03 Solution - Intra-AS route leak protection/avoidance

```
                  ***************************
                  *                         *
   Route A        *          AS1            *
   --->           *                         *     -----> Send A to AS3
   +-----+      *(1)+---+    (2)      +---+(3)*   +-----+
...---| AS2 |----|R1 |-----+---|R2 |-----| AS3 |--- ...
   +-----+      * P1+---+\         +---+P2*   +-----+
                  *   |    \\   //   |\   --X-- Not send A to AS4
                  *   |   (2)\ //    |(3)*   +-----+
                  *   |      //\     |   \----| AS4 |--- ...
                  *  (2)|    // \\    |   *   +-----+
                  *   | //     \\ |   *
                  *   |/         \|   *
                  *  +---+     +---+  *
                  ---|R3 |---------|R4 |  *
                  *  +---+     +---+  *
                  *                    *
                  ***************************
```

☐ **Motivation**
- ✓ "route tagging which relies on operator maintained policy configuration is too easily and too often misconfigured"
- ✓ A means to "standardize" the route marking procedures for route leak avoidance

☐ Pre-requirements: BGP Open Message (extension for route leak protection capability) exchange before peering set up;
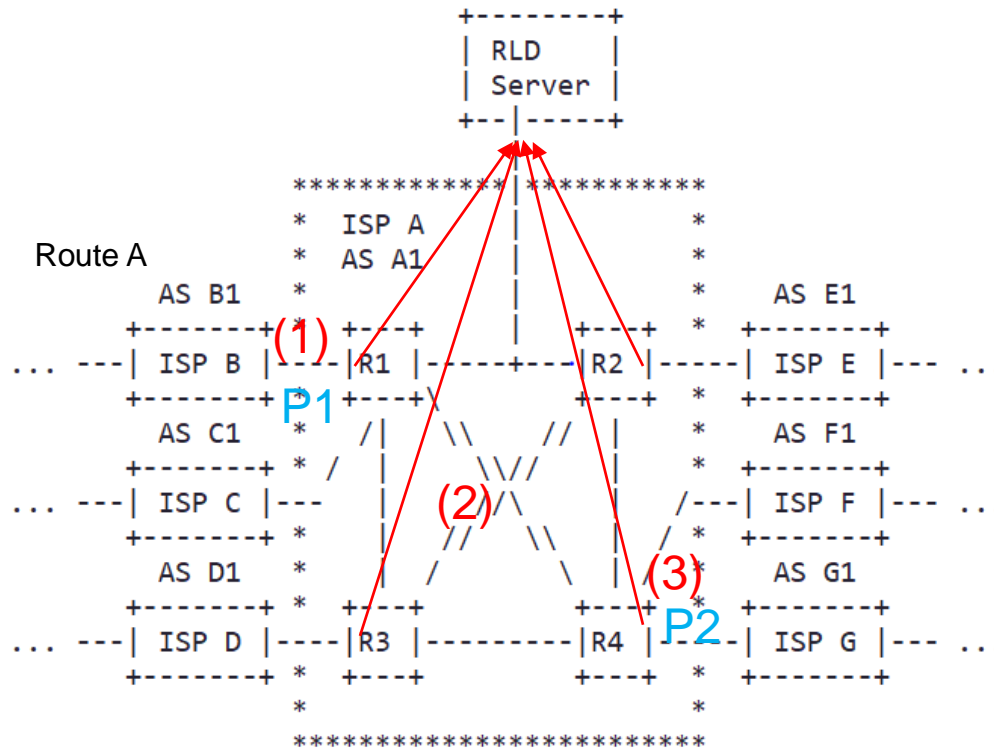
☐ Routing between multi-AS:

(1) R1 receives Route A from AS2, set the Internal Only To Customer (iOTC) attribute per the business relation exchanged through Open message exchange between R1 and AS2;

(2) R1 sends Route A to the other border routers (e.g. R2);

(3) Per the iOTC attribute in Route A and the business relation exchanged between R2 and AS3/4, R2 make the route advertisement decision, e.g., Send A to AS3, Not send A to AS4

Proposed Solution –Intra-AS route leak detection

```
                    +--------+
                    | RLD    |
                    | Server |
                    +--|-----+
          ***********|*|*********
          *   ISP A    |        *
Route A   *   AS A1     |        *
   AS B1  *            |         *        AS E1
  +-------+ (1) +----+  |  +--+   *      +-------+
...---| ISP B |----|R1 |----+---|R2 |-----| ISP E |--- ...
  +-------+ P1 +---+\       +--+  *      +-------+
   AS C1   * /|    \\    //  |   *        AS F1
  +-------+ * /  |   \\//    |    *      +-------+
...---| ISP C |---    |   (2)/\    |   /---| ISP F |--- ...
  +-------+ *    |   //  \\   |  / *     +-------+
   AS D1   *     |  /      \  | /  *   (3)  AS G1
  +-------+ * +--+  /        \ | /  *      +-------+
...---| ISP D |----|R3 |---------|R4 |P2--| ISP G |--- ...
  +-------+ * +---+         +---+ *      +-------+
          *                        *
          ************************
```

☐ Pre-configuration options：
1. Legacy ISP-specific policy-based approach；
2. BGP open policy approach;
☐ Our approach can be an ISP route leak self-checking method:
   1. No dependency on third-party ISP；
   2. No BGP extension required.

☐ Routing between multi-AS:
(1) R1 receives Route A from AS B1, Sets ISP-Specific community per the business relation between AS A1 and AS B1; R1 sets business relation to the BMP Route-Monitoring message that including Route A within the message, and sends the BMP Route-Monitoring message to RLD Server;
(2) R1 sends Route A to the other border routers (e.g. R4);
(3) Per the ISP-Specific community in Route A and the business relation between AS A1 and AS F1/G1, R4 can control the route advertisement, e.g., Send A to AS F1, Not send A to AS G1. R4 sets business relation to the BMP Route-Monitoring message that including Route A within the message if Route A been sent to AS F1/G1, and sends the BMP Route-Monitoring message to RLD Server;
(4) RLD Server doing route-leak verifications using the BMP information collecting from R1 & R4.

Any comment?