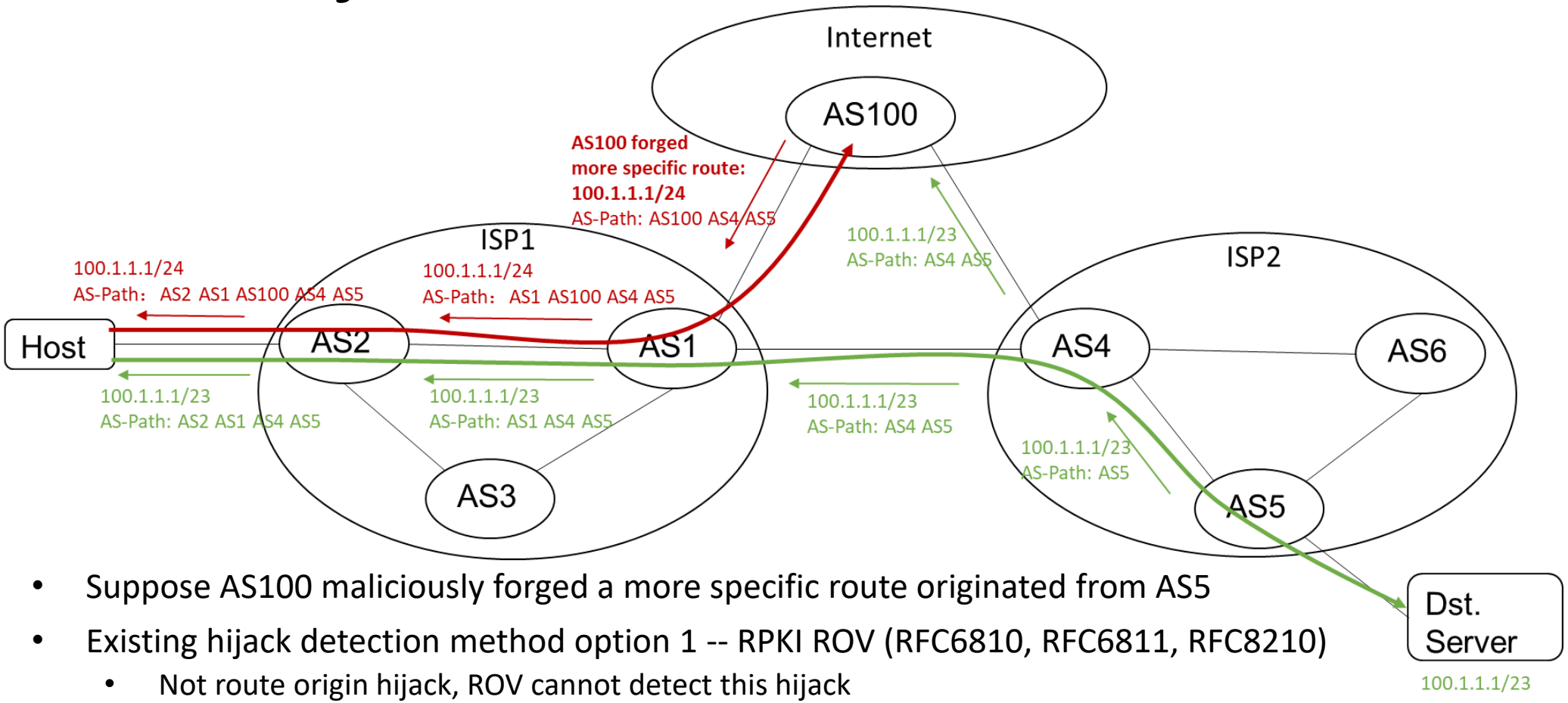
BGP Routing Security: Region-based Trust Alliance (ReTA) Route Hijack Validation

Presenter: Yunan Gu, Huawei

Email: guyunan@Huawei.com

2020-09-09

Route Hijack Case



- Suppose AS100 maliciously forged a more specific route originated from AS5
- Existing hijack detection method option 1 -- RPKI ROV (RFC6810, RFC6811, RFC8210)
  - Not route origin hijack, ROV cannot detect this hijack
- Existing hijack detection method option 2 -- RPKI ASPA
  - There exists (AS1, AS100) (AS4, AS100) ASPA profiles, so ASPA cannot detect this hijack

Either ROV or ASPA can not detect hijacks, where the way of AS-path manipulation does not violate RPKI ROA/ASPA profiles.

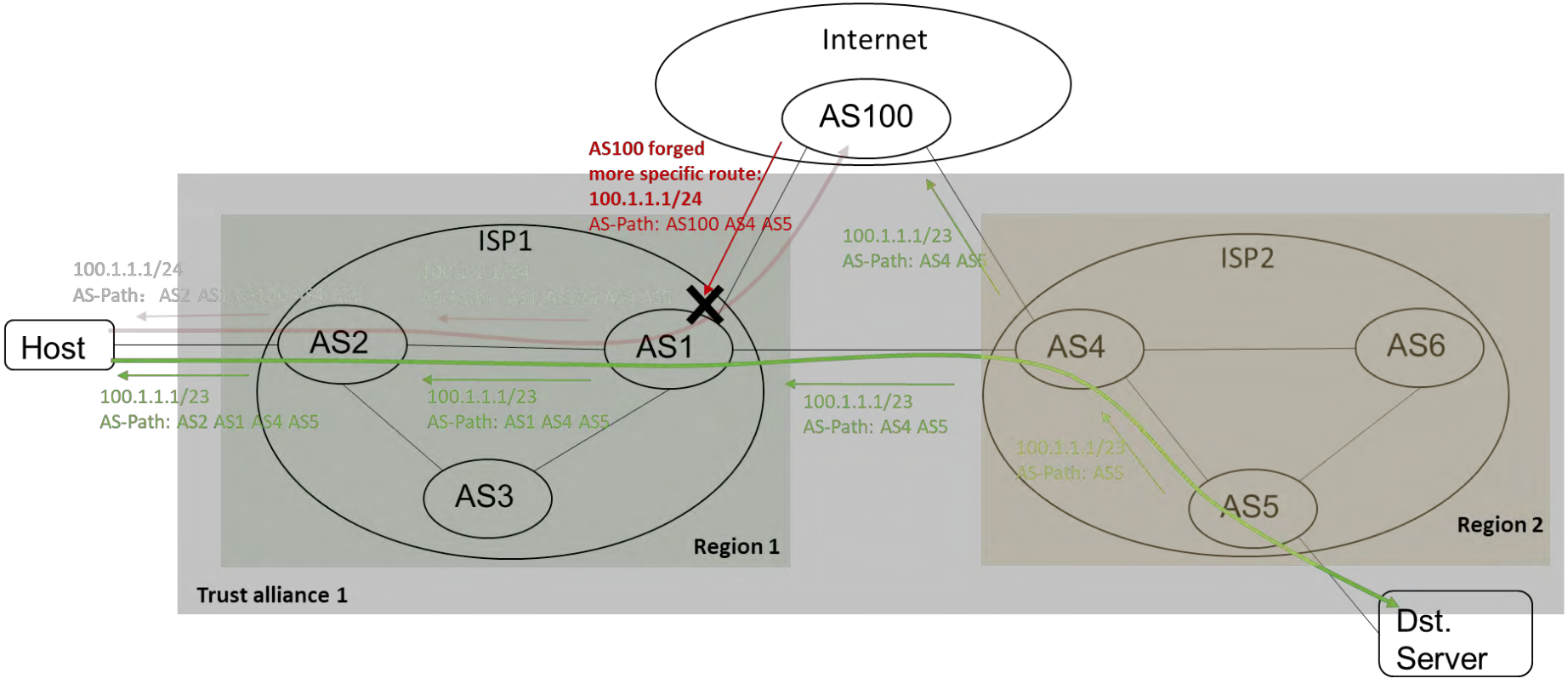
Proposal: Region-based Trust Alliance (ReTA) Validation Design Principles

- The concept of Region and Trust Alliance (TA)
  - Region: consists of ASes from one ISP (e.g.,)
  - TA: consists of regions, where each region must be connected to all other regions within the TA through BGP
- Assumption
  - Routers within the same Region are trust-worthy (no hijacking)
  - Routers within the same TA are trust-worthy (no hijacking)
- Benefit
  - Protect routes, that originated within the same Region/TA, from being hijacked by non-trusted Region/TA routers
- Prerequisite of ReTA – RPKI ROA/ROV
  - ROA/ROV provides the mapping of: routes <--> origin AS, thus provides mapping of: routes <--> origin Region/TA
- Validation rules:
  - REJECT routes, that are originated within the same Region but are received from an eBGP peer outside the same Region
  - REJECT routes, that are originated within the same TA (not the same Region) but are received from an eBGP peer outside the same TA

Proposal: Region-based Trust Alliance (ReTA) Validation Steps

- Step 0: region and trust alliance division
  - Mutual agreement reached between cooperative ISPs
- Step 1: ISPs register their own RPKI ReTA profile (to be defined) :
  - <TA#, region#, AS#>
- Step 2: routers download ReTA profiles from RPKI RP server, use the ReTA profiles to decide the eBGP peer roles
  - Decide if an eBGP peer (using its AS# to correlate with the ReTA profile) is within the same Region or within the same TA (not the same Region)
- Step 3: routers execute ROV
  - If the prefix ROV returns “unknown” or “valid”, we assume that the route is originated from the origin AS in the AS-path, and thus deciding if the route is originated from the same Region/TA
- Step 4: routers execute ReTA hijack validation
  - If the route is originated within the same Region, but the eBGP peer is not within the same Region, then reject
  - If the route is originated within the same TA (not the same Region), but the eBGP peer is not within the same TA, then reject

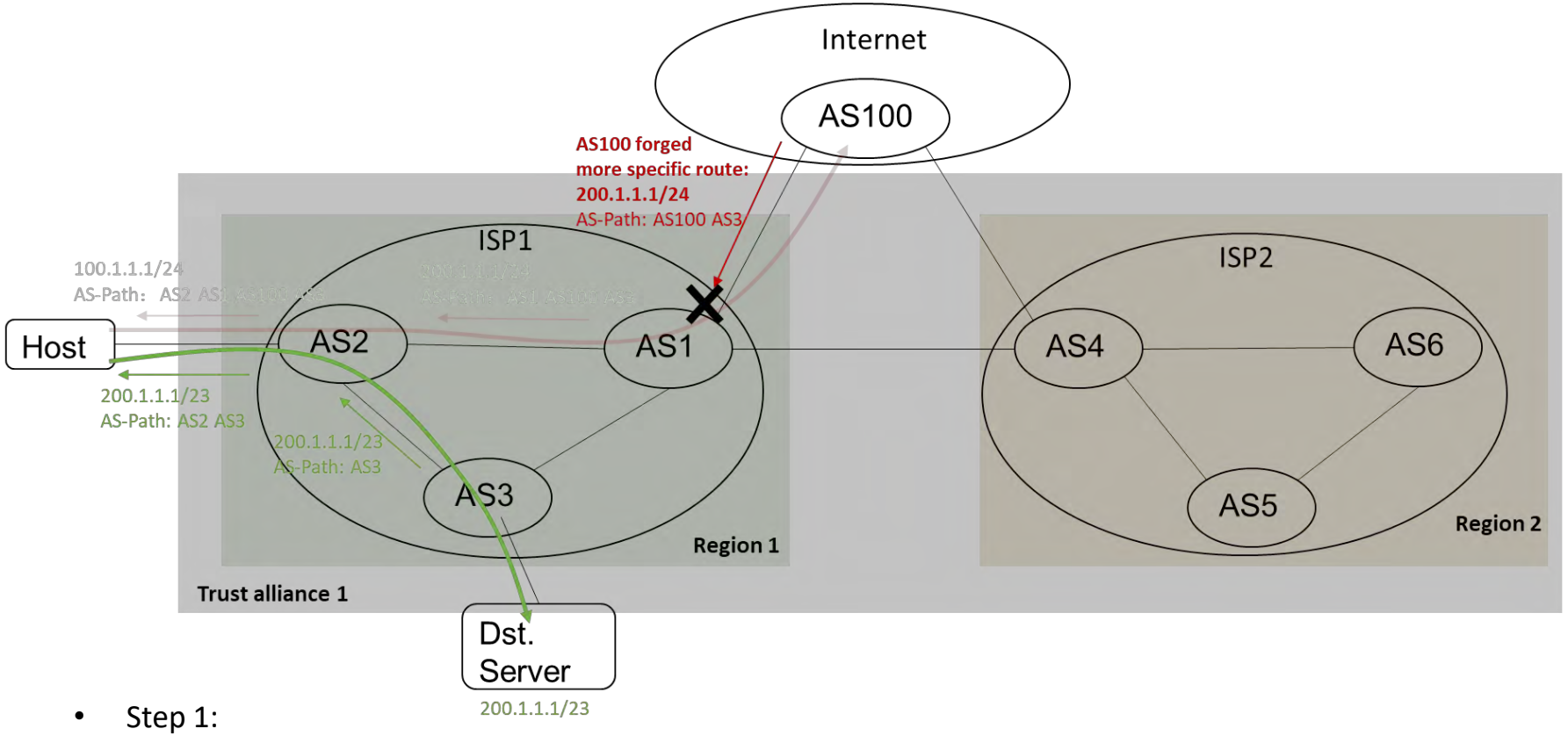
Application Scenario 1: Hijack Protect for routes originated within the same TA but not the same Region



Region 1: AS1, AS2, AS3
Region 2: AS4, AS5, AS6
TA 1: region 1, region 2

- Step 1:
  - ISP 1 ReTA profile registration: <TA1, Region 1, AS1>, <TA1, Region 1, AS2>, <TA1, Region 1, AS3>
  - ISP 2 ReTA profile registration: <TA1, Region 2, AS4>, <TA1, Region 2, AS5>, <TA1, Region 2, AS6>
- Step 2:
  - AS1 (TA1, Region1) decides that the eBGP peers from AS100 (non-TA 1 member) are not within the same TA
- Step 3:
  - 100.1.1.1/24 received from AS100 is valid for ROV, and it is originated from TA1, Region 2
- Step 4:
  - Reject 100.1.1.1/24 (originated from TA1, Region2) received from AS100, since the eBGP peer from AS100 is not within TA1

Application Scenario 2: Hijack Protect for routes originated within the same Region



Region 1: AS1, AS2, AS3
Region 2: AS4, AS5, AS6
TA 1: region 1, region 2

- Step 1:
  - ISP 1 ReTA profile registration : <TA1, Region 1, AS1>, <TA1, Region 1, AS2>, <TA1, Region 1, AS3>
  - ISP 2 ReTA profile registration : <TA1, Region 2, AS4>, <TA1, Region 2, AS5>, <TA1, Region 2, AS6>
- Step 2:
  - AS1 (TA1, Region1) decides that the eBGP peers from AS100 (non-TA 1 member) are not within the same Region
- Step 3:
  - 200.1.1.1/24 received from AS100 is valid for ROV, and it is originated from TA1, Region 1
- Step 4:
  - Reject 200.1.1.1/24 (originated from TA1, Region1) received from AS100, since the eBGP peer from AS100 is not within TA1

Next steps

- Take the topic to IETF
  - Propose ReTA profile draft in SIDROPS WG in the near future
- Plan a demo
  - A simple demo was done last year by ourselves
  - Seeking participants from ISPs!
- Any questions or suggestions?
- How to reach us?
  - guyunan@Huawei.com

Thank you!