Network Attestation for Secure Routing (draft-liu-nasr-requirements)

IETF 119

Brisbane, March 19, 2024

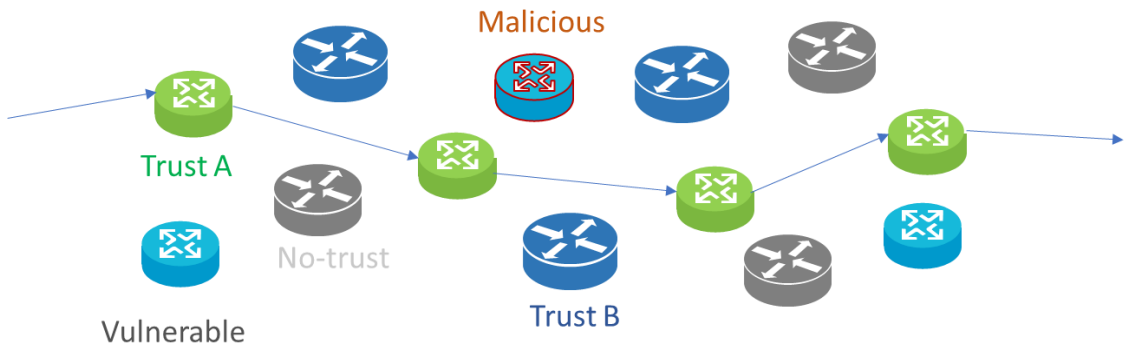
Chunchi (Peter) Liu

liuchunchi@huawei.com

Problem Statement

Traditional routing security and encryption does not suffice anymore!

- **Problem:** Traditional routing security does not guarantee predictability and auditability of forwarding behaviors.



- **Motivation:** Security-sensitive clients want their sensitive data forward only via trusted devices, with no data leakage or deviation from these predictable paths.

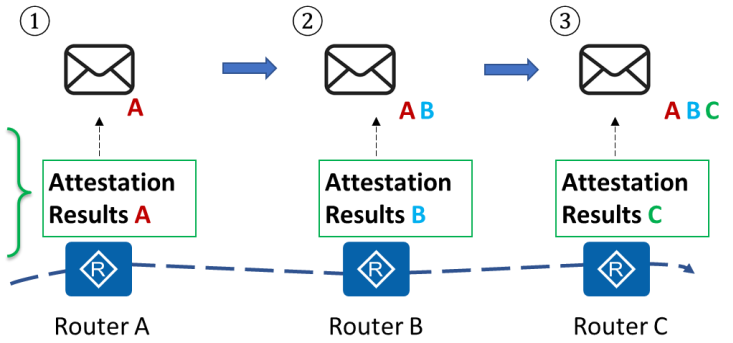
How to solve?

Reuse IETF work, build on solid IETF grounds, no disruption!

1. **Orchestrate a path that consists only of trusted devices, trusted operation environments, and trusted services; produce attestation evidence**
   - A dedicated packet collects all devices' "security proofs" along the path, produce a path-level security proof!

draft-ietf-rats-ar4si

"Security proof" of a device, existing work at **RATS WG**!



2. **Verify the actual forwarding complies to the above attestation**
   - Proof of Transit! (In-band or out-of-band)

Use Cases

- **Service Function Chains:** Operators can use Service Function Chaining (SFC) to provide packaged security services or compliance services. Committing to a sfc path, ensuring ordered traversal of these SFs and provide verifiable proofs of transit can help assure security performance and service delivery.
- **Secure Leased Lines:** Operator clients want a dedicated line consists only of devices/services that has certain trust attributes, with no vulnerable or unqualified device in between.
- **Customized Quality of Trust:** The secure line could be dynamically orchestrated based on path-level trust preferences (achieved collectively by device attributes) like deployed geolocation (geofencing), security level (RATS-ed, SBOM…), vendor, …
- **Forwarding integrity:** Operator clients (specifically security-sensitive industry clients, like financial institutions, government) want their sensitive data stay on top of this secure line ONLY. No deviation, no data leakage.

Current Scope

- **NASR Goal:** Protect data security by ensuring data transits only on trusted devices, trusted operating environments or trusted services.
- **NASR:** Establish a level of confidence in the trustworthiness of the routing path by appraisal, attestation and verification.

Step 1: What to attest

- How: Connect and consume RATS outputs (and other security proofs) to commit to a path

- [PS] Path-level trust attribute definition (objective)
- [PS] Secure configurations
- [I] Path trustworthiness appraisal methods, trust levels (subjective)
- …

Step 2: How to attest

- How: Dedicated OAM dial-test protocol, output attestation result/proof

- [PS] TPR+POT
- [PS] Attestation Result Format
- [I] Architecture, procedures
- …

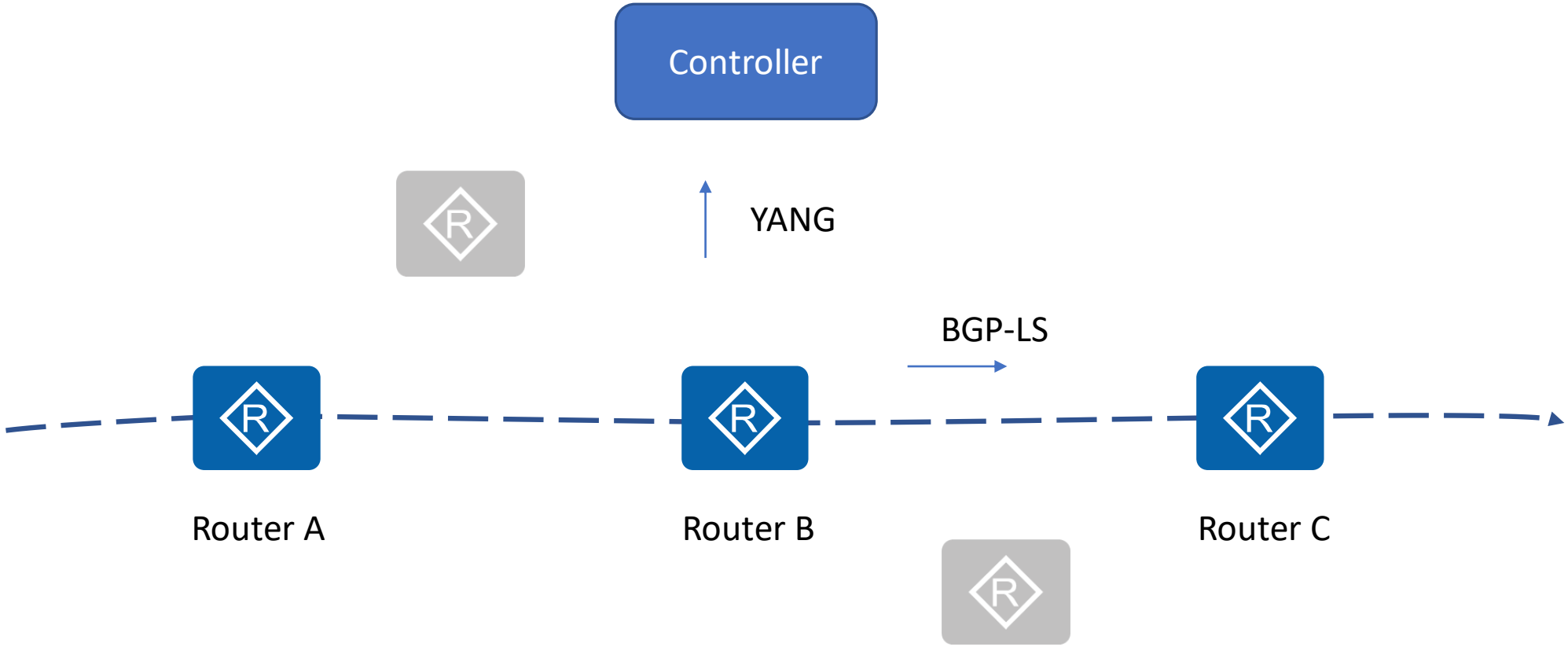
Step 3: How to verify

- How: In-band or out-of-band verification of compliance

- [I] Proof-of-Transit
- [PS] Management plane protocol data field extension
- [PS] in-situ OAM data field extension
- [BCP] Ingress/ Egress Filtering
- …

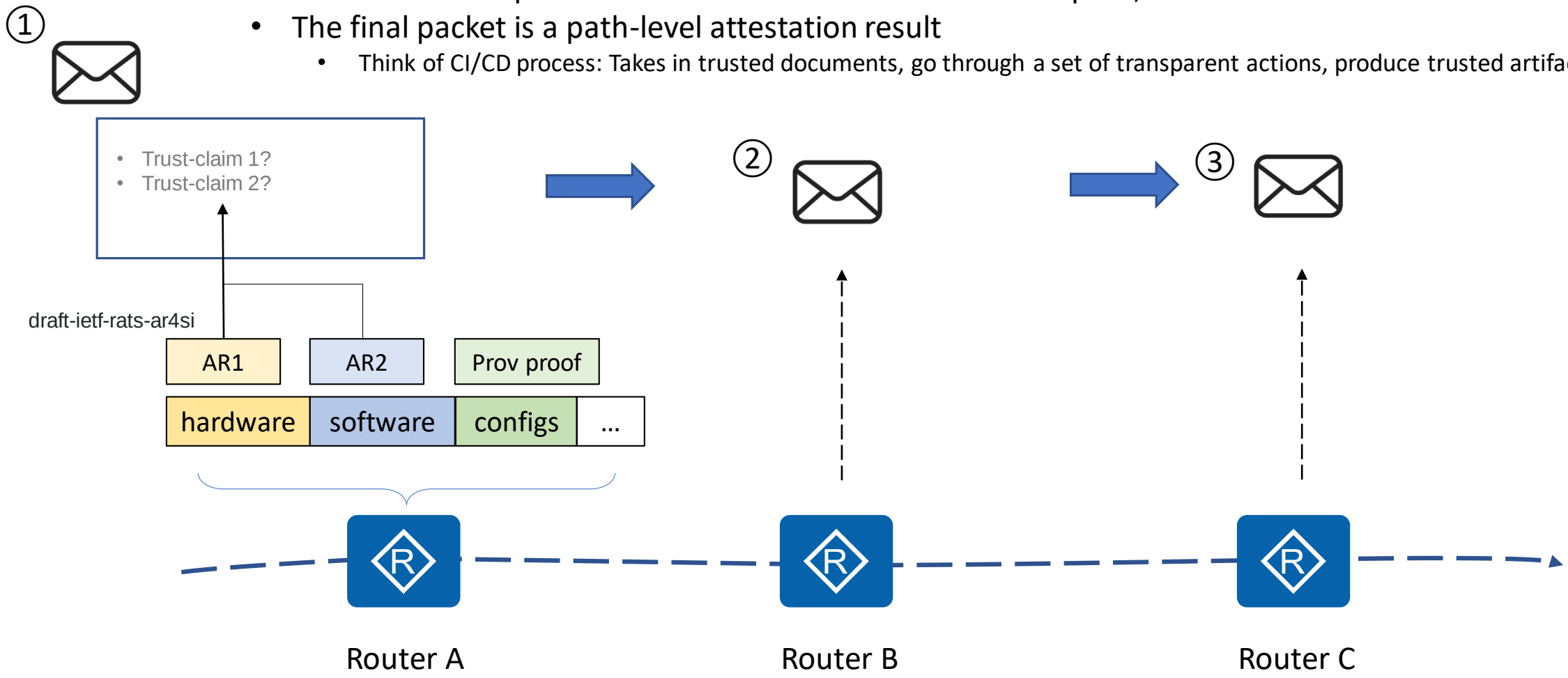
How to achieve– graphical illustration

- Step 1:
  - Orchestrate a path, where devices may have common trust attributes
  - May require a controller or state-inquiring protocols



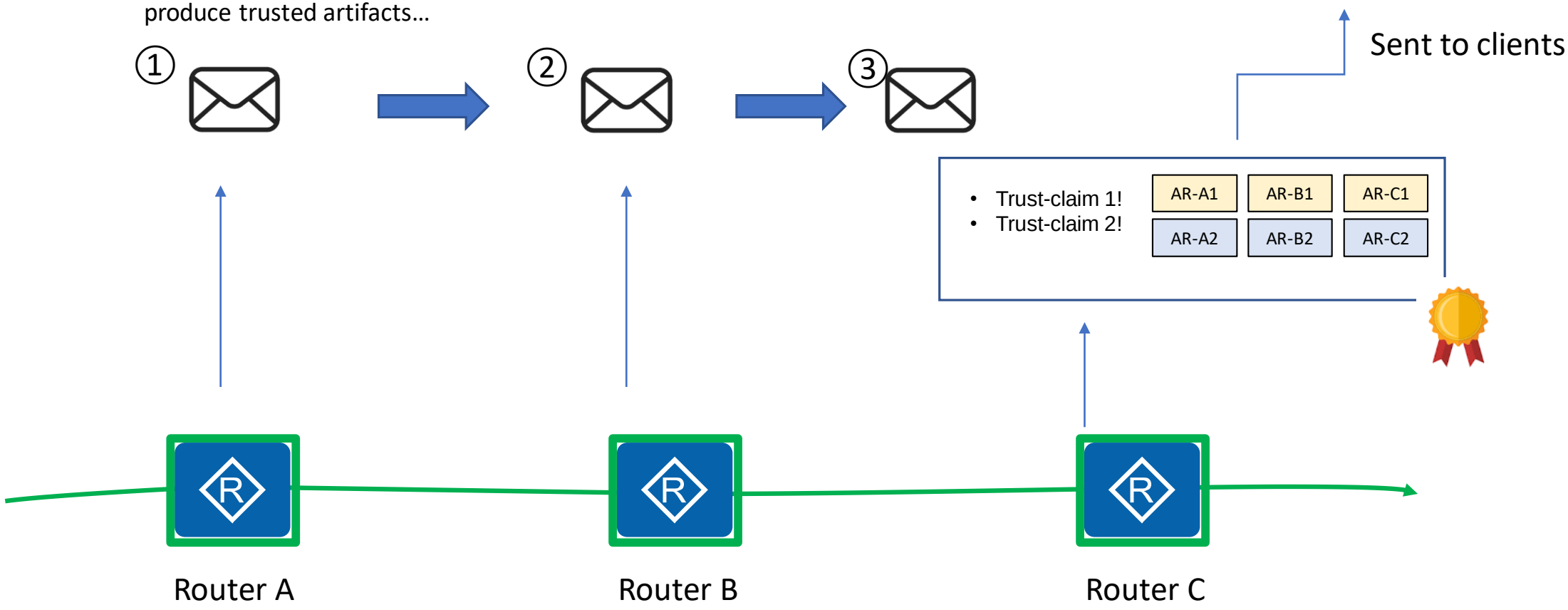
How to achieve– graphical illustration

- Step 2:
  - Dedicated OAM packet traverse an orchestrated network path, consumes attestation results along the way
  - The final packet is a path-level attestation result
    - Think of CI/CD process: Takes in trusted documents, go through a set of transparent actions, produce trusted artifacts…



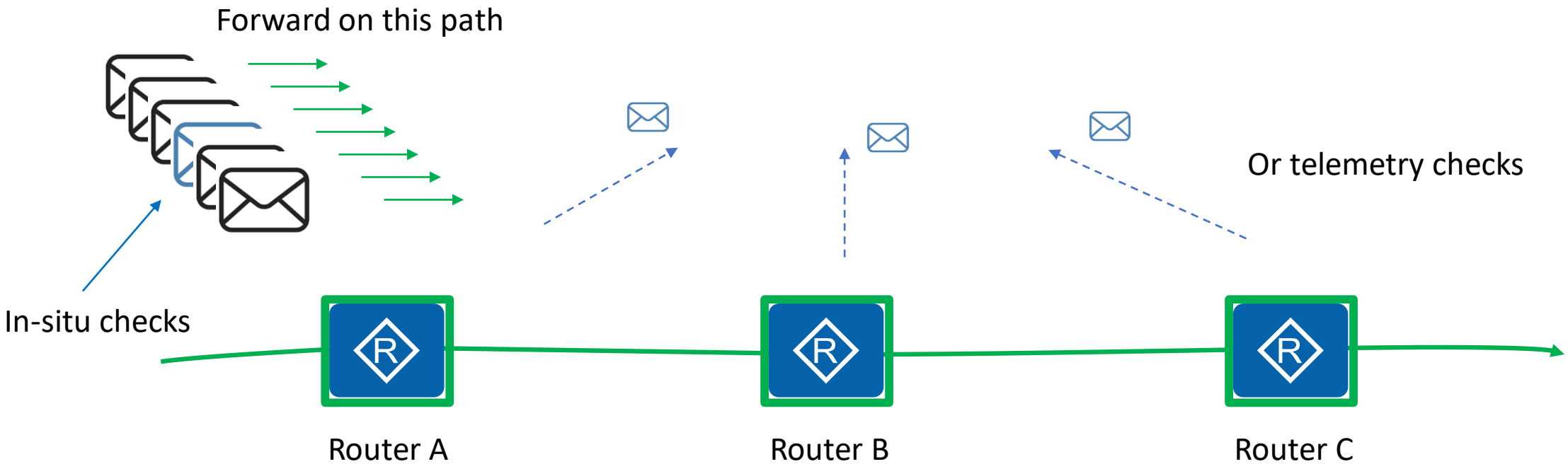
How to achieve– graphical illustration

- Step 2:
  - Dedicated OAM packet traverse an orchestrated network path, consumes attestation results along the way
  - The final packet is a path-level attestation result
    - Think of CI/CD process: Takes in trusted documents, go through a set of transparent actions, produce trusted artifacts…



How to achieve– graphical illustration

- Step 3:
  - After path-trust established, when using this path, **periodically do in-band or out-of-band proof-of-transit checks** to check if forwarding complies with attested path
- Ingress / Egress filtering BCPs…

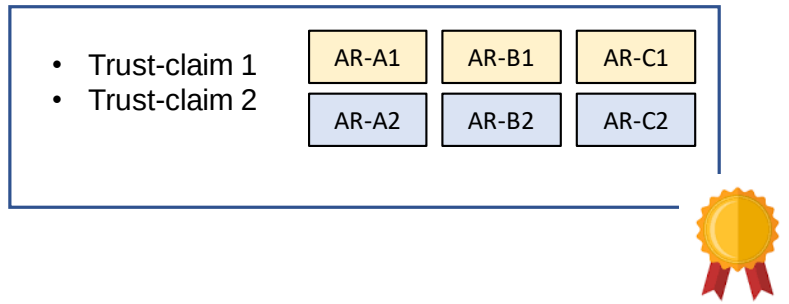


In RATS language…

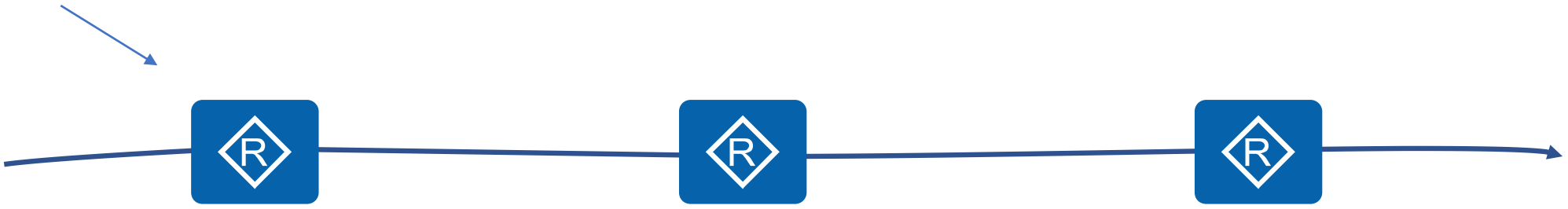
- Dedicated OAM packet traverse an orchestrated network path, collect attestation results along the way
- The final packet is a path-level attestation result

Relying party

- Client
- Operator



Attesters



Documents Status

- draft-richardson-nasr-terminology-00
- draft-liu-nasr-requirements-01
- draft-liu-path-validation-problem-statement-00

- draft-architecture
- draft-charter

Looking for guidance and collaboration

- Guidance, oversight from RATS
  - Dependencies— consume RATS outputs
  - Designs— similar logic, similar architecture and interactive procedures
- Collaboration
  - Design team (architecture, main protocols)
  - BoF co-proponents
- Plans
  - NASR Side Meeting at IETF 119
  - Non-WG Forming BoF at IETF 120
  - WG Forming BoF at IETF 121
    - Interims, design team meetings in between.

- Side meeting agenda and materials:
  - https://github.com/liuchunchi/nasr_side_meeting
- Side Meeting Wiki Page:
  - https://wiki.ietf.org/meeting/119/sidemeetings
- NASR Mailing List:
  - https://www.ietf.org/mailman/listinfo/nasr

liuchunchi@huawei.com