NASR Side Meeting

Opening

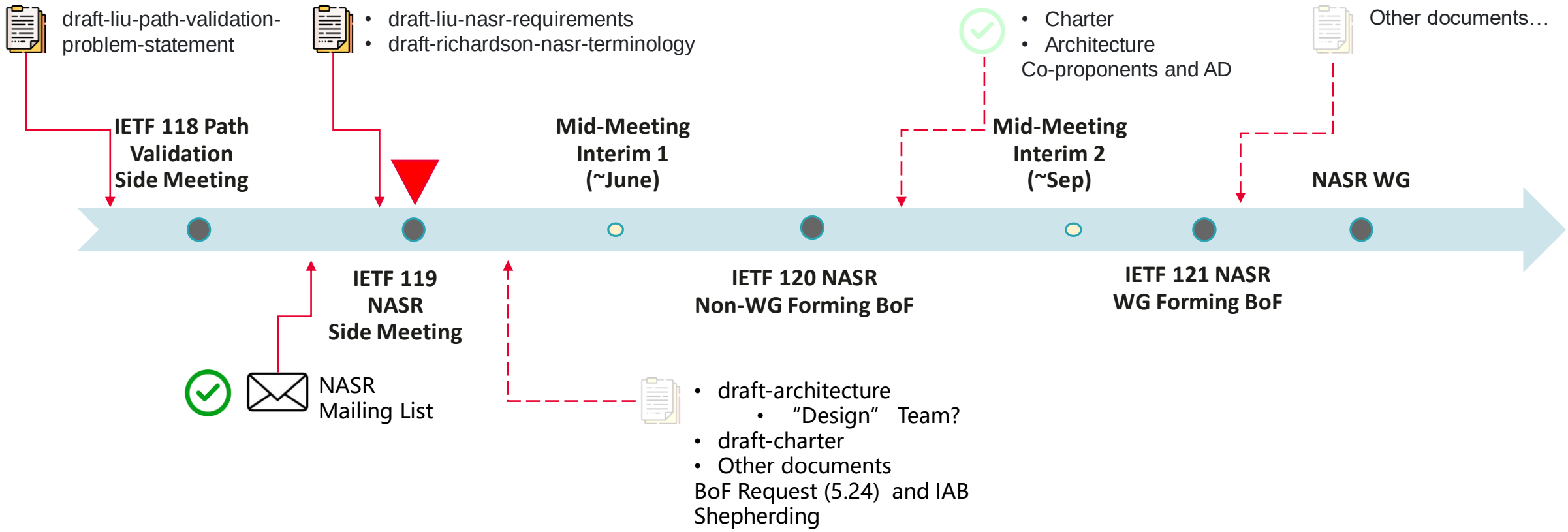
IETF 119

Chunchi (Peter) Liu

Before Started

- Can we agree on goals for this meeting?
  - Summarize past NASR list discussions and align consensus
  - Align key information and documents that facilitate the next successful BoF and formation of NASR WG
- Can we agree on non-goals for this meeting?
  - Do not discuss non-relevant topics that may deviate from the purpose of facilitating a successful BoF
- Trivia
  - IETF Note Well
  - We are being recorded– if you object, please volunteer to take minutes!

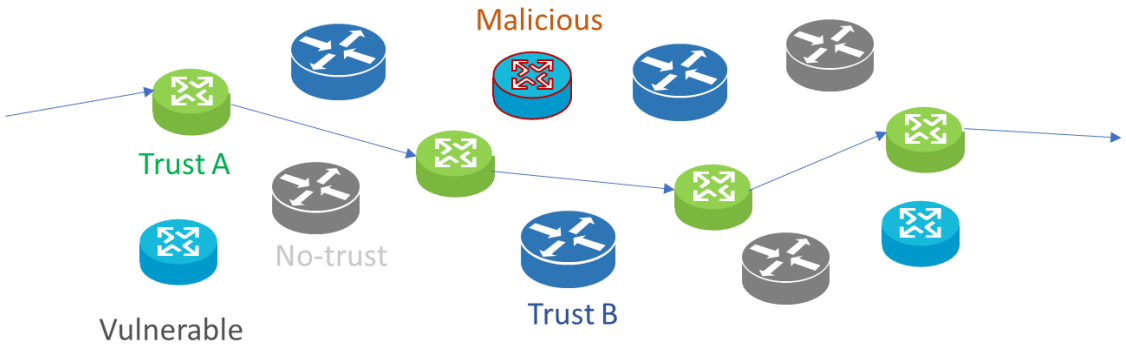
Timeline


draft-liu-path-validation-problem-statement
• draft-liu-nasr-requirements
• draft-richardson-nasr-terminology
• Charter
• Architecture
Co-proponents and AD
Other documents…
IETF 118 Path Validation Side Meeting
Mid-Meeting Interim 1 (~June)
Mid-Meeting Interim 2 (~Sep)
NASR WG
IETF 119 NASR Side Meeting
IETF 120 NASR Non-WG Forming BoF
IETF 121 NASR WG Forming BoF
NASR Mailing List
• draft-architecture
• "Design" Team?
• draft-charter
• Other documents
BoF Request (5.24) and IAB Shepherding

Recapping Problem Statement

Traditional routing security and traffic 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.

Recapping 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.

Documents Status

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

Terminology Status

- draft-richardson-nasr-terminology-00
  - **Secure routing (NASR Goal):**
    - Protect data security by ensuring data transits only on trusted devices, trusted links, trusted operating environments or trusted services.
  - **Routing Security (traditional):**
    - Achieving correct reachability within and across networks by ensuring authentic and truthful distribution of routing information
  - **Proof of Transit:**
    - Secure and verifiable logs or evidence of a packet's transit path in the data plane.

- draft-liu-nasr-requirements-01
  - See the scope next page

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
- …

Agenda

- Opening, List Discussion Recap – Huawei (5 min)
- Current Scope—CMCC (10 min)
- Architecture Proposal – Telefonica (15 min)
- Trusted Enhanced Path Routing— Pengcheng Lab (10min)
- POT Mechanisms Survey/Benchmark— Huawei France (10 min)

- QA, Open Discussion, Related Pointers (30 min)
- Wrap up, Next Steps

Opening ends

Q&A and Discussion:

The floor is open for discussion.

Questions
Question 1: Do you agree on the current goal of NASR? • Protect data security by ensuring data transits only on trusted devices, trusted operating environments or trusted services.
Question 2: Do you agree on the current 3-stage scopes and directions? Any comments?
Question 3: Do you agree our next steps should include: • Establish **design team** for architecture and charter • One **interim meeting** to review architecture and charter
Question 4: Who will volunteer to join the NASR-architecture design/virtual/architecture team? Frequency? Who will join the interim meeting?
Question 5: Any other pointers? Related documents from other SDOs?

Don’t forget to subscribe to NASR Mailing List!