NASR
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

C. Liu
Huawei
M. Chen
China Mobile
M. Richardson
Sandelman Software Works
D. Lopez
Telefonica

3 March 2025

Network Attestation for Secured foRwarding (NASR) Architecture
draft-liu-nasr-architecture-02

Abstract

This document provides an architecture overview of NASR entities, interactive procedures and messages.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2025.

Copyright Notice

Table of Contents

1. Introduction

In the current network deployments, communicating entities implicitly rely on peer entities and use paths as determined by the control plane. These available path(s) are implicitly trusted. Communicating entities have very little information about the entities in the paths over which their traffic is carried, and have no available means to audit the entities and paths, beyond basic properties like latency, throughput, and congestion. However, increased demand in network security, privacy, and robustness makes tools for enabling visibility of the entities' security characteristics a necessity.

Path-agnostic traffic signing and encryption has been the primary method to ensure data confidentiality, integrity and authenticity today. However, with the increasing amount of attacks, and vulnerabilities, new emerging threats are imposing requirements that go beyond the data security currently provided. Vulnerable factors include:

* Unauthorized data duplication, caused by

- Routing/forwarding detour to unintended devices or areas
- Insecure network devices or unauthorized root access
- Middlebox decryption/inspection

* Capture-now-decrypt-later attacks, caused by
- Exploitation of vulnerable cryptographic engineering
- Post-Quantum attacks

* Pattern or behavioral analysis, etc.

With these additional security and privacy requirements, there is a need to provide enhanced or added services beyond the pure encryption-based data security; requiring better visibility of the security characteristics of the underlying network elements. Specifically, to satisfy the visibility of the network elements' security state, proof that data is traversed through network elements (devices, links and services) that satisfy security posture claims to avoid exposure of unqualified elements is needed.

The RATS (Remote ATtestation procedureS) working group has provided a framework and approaches to assess and establish the trustworthiness of a single device, hence offering an initial building block. However, a comprehensive framework that attests to a network -- meaning network-level elements' trustworthiness proofs and verification methods are lacking.

The Network Attestation for Secured foRwarding (NASR) working group is chartered to address the challenges associated with proving state and characteristics of a network path are compliant to a set of claims, so as to achieve predictable and verifiable forwarding behavior. The work will build as much as possible on existing standards and implementations, focusing on combining them in a clear and coherent manner to address secured forwarding use cases such as those identified and described in the NASR use cases and requirements document.

This document introduces the architecture, entities, interactive procedures, and messages sent between the entities, so to achieve the NASR objective.

2. Use Cases

Please refer to the use cases identified in [I-D.liu-nasr-requirements-01]

3. Terminology

Please refer to the terminologies identified in [I-D.richardson-nasr-terminology-01]. Terminology from RATS Architecture document [RFC9344] also applies.

NASR will leverage RATS implementations and specifications, including but not limited to [I-D.ietf-rats-ar4si-06][I-D.ietf-rats-corim-04].

4. Architectural Overview

4.1. Single client - single operator (An Oversimplification)

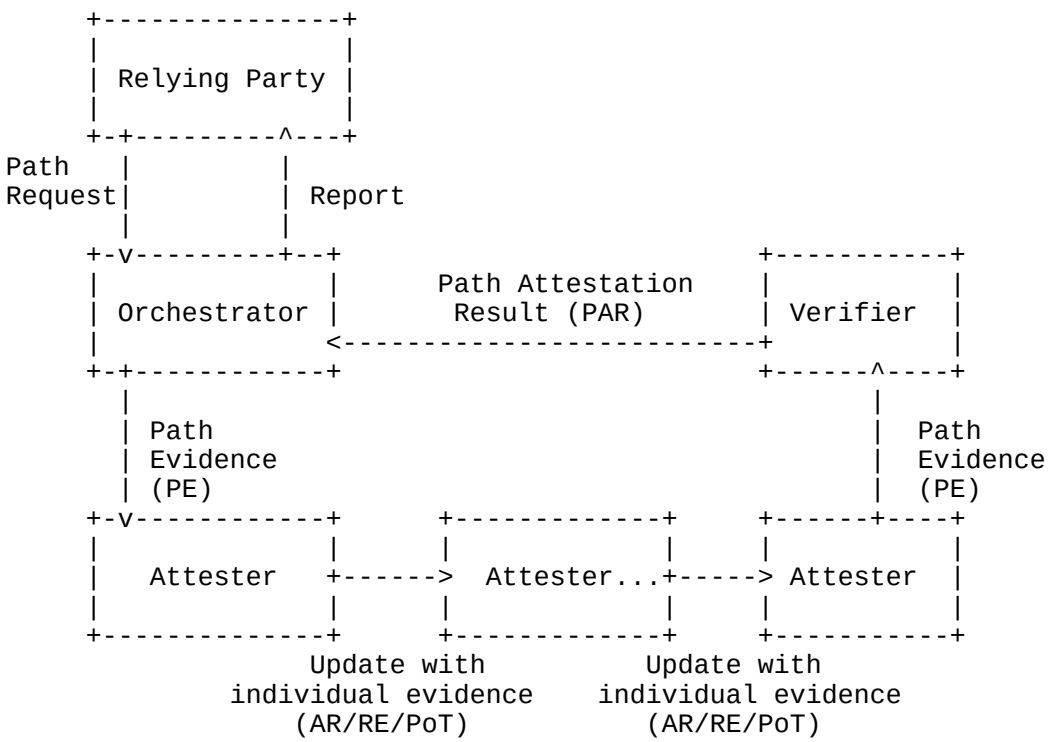


Figure 1. NASR Architecture-- Oversimplified (a data plane/BGP-LS example)

Fig. 1 is an oversimplification to ease understanding of the concept. In a single client - single operator scenario, a client (Relying Party) sends a Path Request containing his security or trustworthiness requirements of a connectivity service. The Orchestrator, run by the operator, would choose qualifying devices (Attesters) and send out an empty Path Evidence inquiry (using data

plane protocol like BGP-LS). The Attesters update the Path Evidence with its own Raw Evidence or Attestation Results one-by-one. The Verifier verifies the filled Path Evidence, produce a Path Attestation Result (PAR), and sends it back to the Relying Party. The Relying Party now have confidence over the trustworthiness of received network. After the end-to-end service is delivered, during service, Proof-of-Transits are also created by each Attester, being sent in-band accumulatively or out-of-band, to detect unexpected forwarding deviation.

Alternatively, the Path Evidence can be collected through management protocols like NETCONF/YANG. The orchestrator aggregates individual evidences of each attester device on the candidate path, then send the Path Evidence to the Path Verifier, who then produces a Path Attestation Result back to the Relying Party. When the attester devices are made by different vendors, multiple verifiers may be needed.

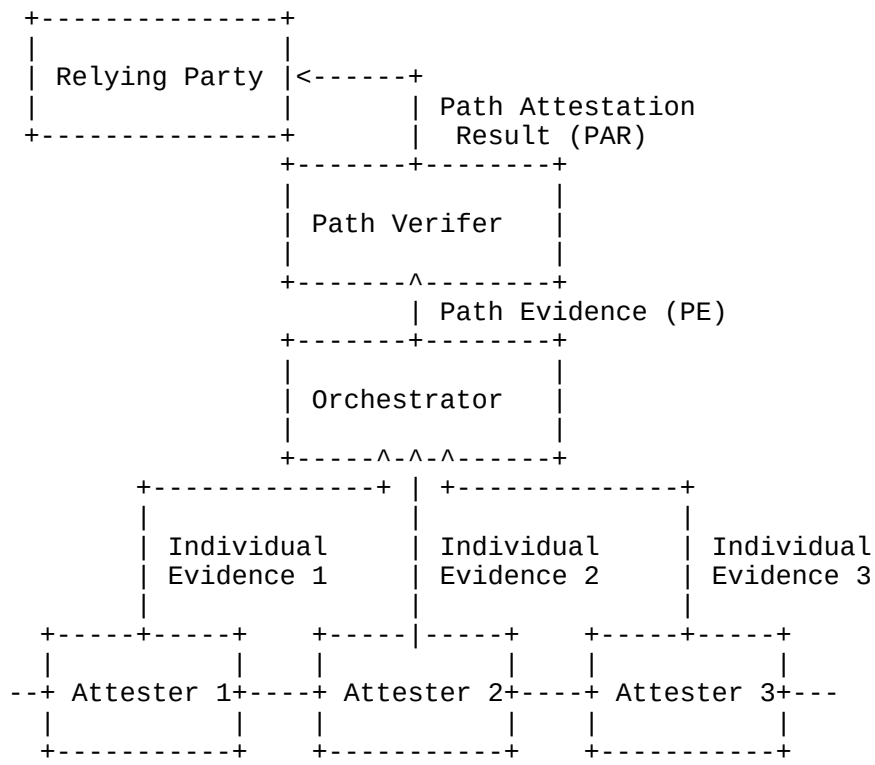


Figure 1.1. NASR Architecture-- Oversimplified (a management plane/ YANG example)

4.2. Multi Client - Multi Operator

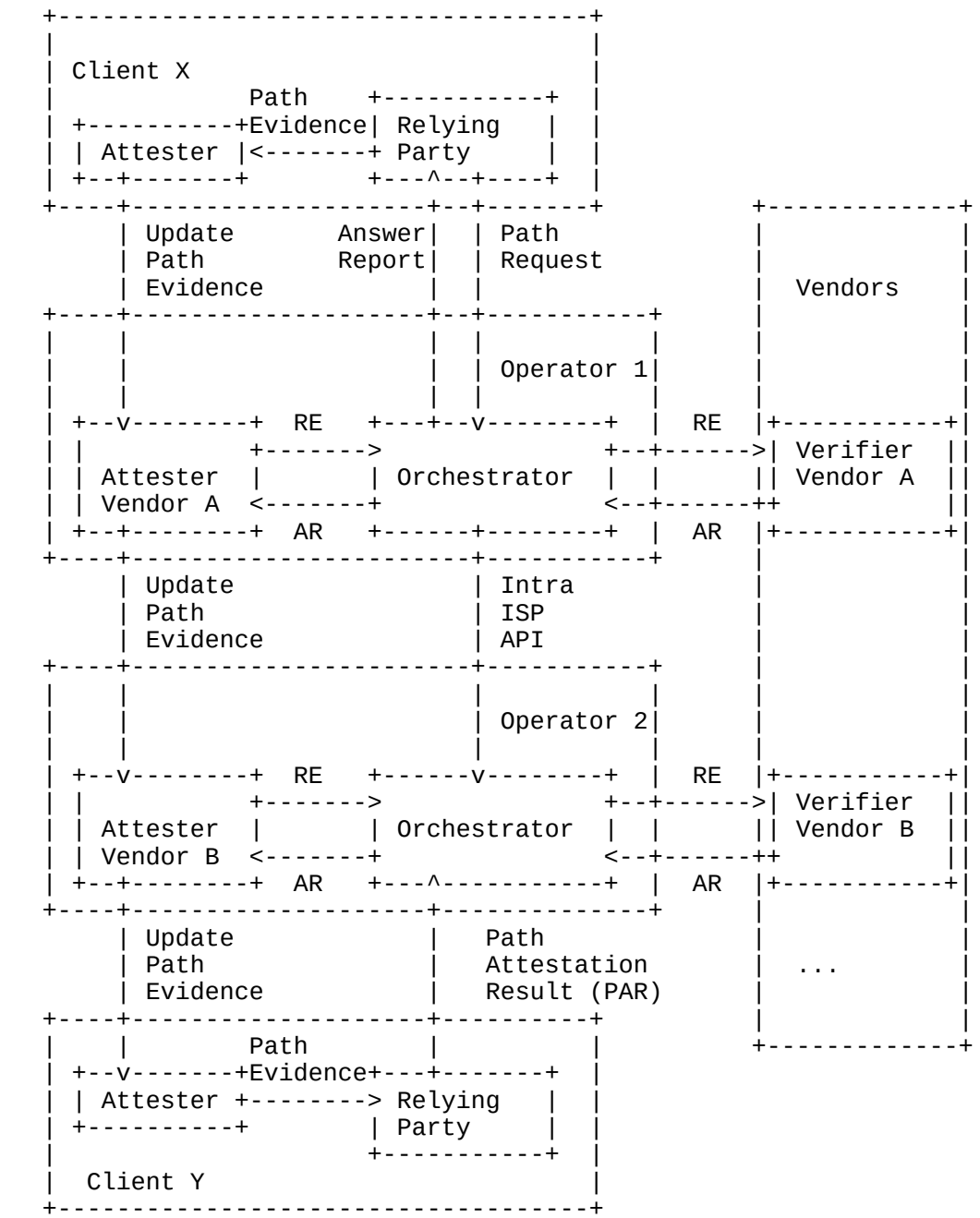


Figure 2. NASR Architecture

In a more generalized scenario, due to geographic distances, a single operator cannot span across a long distance to deliver an end-to-end service-- multiple operators collaborate to deliver it. The Customer A would send the Path Request to the Operator nearest to him (Operator 1). Operator 1 pass down the Path Request to the collaborating operators, through an intra-ISP API. Operators of different domains choose qualifying devices to altogether orchestrate the path.

Relying Party (customer) then sends the Path Evidence inquiry to check and attest to this path. Following the same procedure, the client of other side would return the Path Attestation Result back, through the operators. The Operator 1 would send back a comprehensive answer/report to the Client.

Also, the operators may have heterogeneous network devices from different vendors. Since vendors provide Verifier software/hardware and Reference Values, Verifiers can be deployed either outside the operators (Fig 2) or inside of the operators (Fig 3).

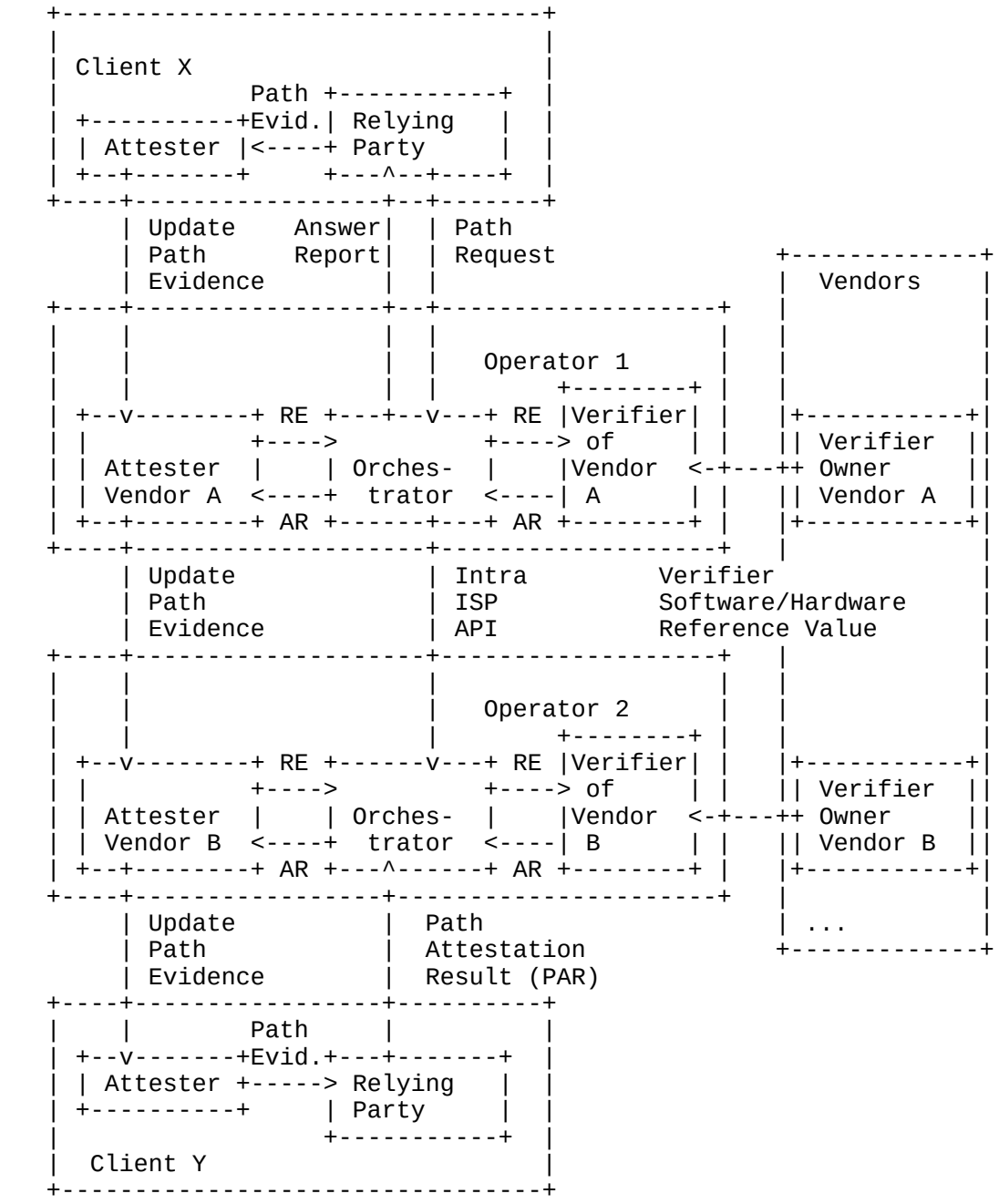


Figure 3. Verifier deployed in operators

5. Roles

The existing roles from RATS Architecture document [RFC9344] applies.

* Attester: The definition in [RFC9344] applies. Additionally, it can be performed by either a physical device or a virtual function. The Attester can update Path Evidence with his Attestation Result/Raw Evidence/Proof of Transit.

  - Produces: (updated) Path Evidence

* Relying Party: The definition in [RFC9344] applies. Additionally, it creates Path Request to the Orchestrator, and receive Reports from Orchestrator as an auditable result, comparing the actually received network service versus the requested PR attributes.

  - Produces: Path Request

  - Consumes: Report

In the case where an Attester is deployed in the customer premises, the Relying Party could also start the unfilled Path Evidence inquiry at his side.

New role(s) are defined below.

* Orchestrator: A role performed by an entity (typically a controller or a special device) that performs two functions: path orchestration and path attestation. The input and output of different functions are different.

  - Path Orchestration: The Orchestrator receives a Path Request from the Relying Party. After path computation/orchestration, he creates configurations to be distributed to the Attesters/ devices.

    o Consumes: Path Request

    o Produces: Configurations

  - Path Attestation: The Orchestrator receives a Path Request from the Relying Party, send unfilled Path Evidence (PE) inquiry to Attesters, collects Path Attestation Result (PAR) from the Verifier, and send PAR back to the Relying Party.

    o Consumes: Path Request, Path Attestation Result

    o Produces: (unfilled) Path Evidence

* Verifier: A role performed by an entity that appraises the validity of filled Path Evidence about a set of Attesters and produces Path Attestation Results to be used by an Orchestrator.

  - Consumes: (filled) Path Evidence

  - Produces: Path Attestation Results

6. Conceptual Messages

The existing artifacts from RATS Architecture document [RFC9344] applies. New conceptual message(s) are defined here.

* Path Request: A set of claims, describing the properties of a network path that a Relying Party requested.

  - Consumed By: Orchestrator

  - Produced By: Relying Party

* Path Attestation Result: The output generated by a Verifier, including information about a set of Attesters, where the Verifier vouches for the validity of the results.

  - Consumed By: Relying Party

  - Produced By: Verifier

* Path Evidence: The output generated by the Orchestrator and a set of Attesters, to be appraised by a Verifier. Path Evidence may include each Attester’s raw Evidence [RFC9344], Attestation Results, Proof-of-Transit, or other proof suggesting correctness of functioning of each Attester.

  - Consumed By: Verifier

  - Created By: Orchestrator

  - Updated By: Attester(s)

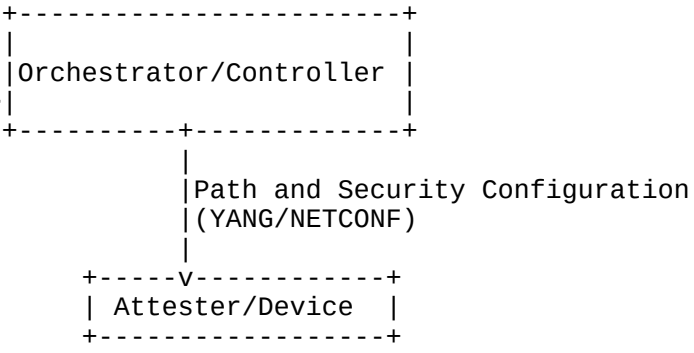
* Report: An auditable result that compares the actually received network service versus the requested PR attributes.

  - Created By: Orchestrator

  - Consumed By: Relying Party

7. Orchestration

The orchestration process collects client's path requests and output configurations. The Orchestrator/Controller then distribute them to the attester/device using NETCONF/YANG or other control plane protocols. In the first case, a new YANG module needs to be defined.



8. Security Considerations

TODO Security

9. IANA Considerations

This document has no IANA actions.

10. Informative References

[RFC9344] Asaeda, H., Ooka, A., and X. Shao, "CCNinfo: Discovering Content and Network Information in Content-Centric Networks", RFC 9344, DOI 10.17487/RFC9344, February 2023, <https://www.rfc-editor.org/rfc/rfc9344>.

[I-D.liu-nasr-requirements-01] Liu, P. C., Iannone, L., Lopez, D., Pastor, A., Chen, M., and L. Su, "NASR Use Case and Requirements", Work in Progress, Internet-Draft, draft-liu-nasr-requirements-01, 3 March 2024, <https://datatracker.ietf.org/doc/html/draft-liu-nasr-requirements-01>.

[I-D.richardson-nasr-terminology-01] Richardson, M. and P. C. Liu, "Terminology and Use cases for Secured Routing Infrastructure", Work in Progress, Internet-Draft, draft-richardson-nasr-terminology-01, 20 May 2024, <https://datatracker.ietf.org/doc/html/draft-richardson-nasr-terminology-01>.

[I-D.ietf-rats-ar4si-06]
Voit, E., Birkholz, H., Hardjono, T., Fossati, T., and V. Scarlata, "Attestation Results for Secure Interactions", Work in Progress, Internet-Draft, draft-ietf-rats-ar4si-06, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-ar4si-06>.

[I-D.ietf-rats-corim-04]
Birkholz, H., Fossati, T., Deshpande, Y., Smith, N., and W. Pan, "Concise Reference Integrity Manifest", Work in Progress, Internet-Draft, draft-ietf-rats-corim-04, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-corim-04>.

Acknowledgments

We sincerely thank contribution from NASR mailing list.

Authors' Addresses

Chunchi Liu
Huawei
Email: liuchunchi@huawei.com

Meiling Chen
China Mobile
Email: chenmeiling@chinamobile.com

Michael Richardson
Sandelman Software Works
Email: mcr@sandelman.ca

Diego Lopez
Telefonica
Email: diego.r.lopez@telefonica.com