opsawg
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

J. Zhao, Ed.
R. Pang, Ed.
W. Lv, Ed.
China Unicom
J. Dong, Ed.
Huawei Technologies
S. Zhang, Ed.
China Unicom

2 March 2026

Problem Statement for Network Resilience
draft-zhao-opsawg-network-resilience-ps-00

Abstract

This document defines the problem space and analyzes the limitations of current network architectures when dealing with complex, cascading, and unanticipated failures.

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 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

Traditional IP network reliability architectures are primarily built upon the principle of "Robustness." While static redundancy and deterministic topology convergence are mature enough to handle predictable single-point failures, modern networks exhibit significant survivability gaps as business logic complexity grows. Therefore, it is necessary to introduce resilience enhancement capabilities to improve the network's ability to adapt and maintain service continuity in complex environments.

The core drivers for this shift include:

* Evolution of Service Requirements: Critical services are shifting from simple "availability" to "deterministic survivability." This requires the network to maintain a baseline SLA even under extreme shocks, rather than accepting long-term interruptions.

* Complexity Surpassing Human Intervention: As analyzed in [RFC7276], traditional IP OAM mechanisms primarily focus on connectivity and continuity. However, they are increasingly insufficient for detecting implicit deterioration where the failure is not binary (up/down), especially in high-precision scenarios requiring millisecond-level awareness.

* Failure Modes Shifting from "Deterministic" to "Unanticipated": Existing robust designs focus on "all-or-nothing" failures. However, they show clear survivability deficiencies when handling cross-layer correlated risks, gray failures, and resource bottlenecks.

2. Problem Statement

The current vulnerability of networks is manifested in four deep failure modes:

2.1. Explicit Interruption

This refers to the direct offline status of physical links or nodes. While mechanisms like BFD and FRR are mature, issues persist in multi-point failure scenarios where backup paths may be exhausted or lead to "black holes" due to a lack of real-time capacity awareness.

2.2. Implicit Deterioration (Gray Failures)

* State Deception: Traditional heartbeats often fail to capture micro-burst deteriorations.

* Detection Gaps: While In-situ OAM (IOAM) as specified in [RFC9197] enables the collection of fine-grained, hop-by-hop telemetry data, it defines the data plane encapsulation rather than the operational logic for mitigation. Consequently, without an integrated automated response mechanism, traffic may remain on degraded links, leading to sustained SLA violations.

2.3. Common-Cause and Correlated Failures

Logical redundancies often have deep coupling at the physical or management layers, such as Shared Risk Link Groups (SRLG).

2.4. Resource-based Failures

Under extreme pressure (e.g., traffic surges or DDoS), the system hits resource bottlenecks, leading to loss of self-rescue capability; for example, when the control plane CPU is exhausted, the network loses its management entry point.

3. Root Cause Classification

Based on the process of failure evolution, the root causes of resilience deficiency are categorized into three stages:

3.1. Pre-event: Insufficient Prevention and Assessment

* Configuration and Specification Issues: Misconfigurations or non-standard networking practices are prevalent in current network deployments.

* Lack of Simulation/Prediction: Current networks lack the capability for integrated risk analysis and high-fidelity simulation across multi-vendor and multi-disciplinary complex environments.

3.2. In-event: Lack of Escape and Fault Tolerance Capacity

Issues include protocol defects and a lack of real-time resource awareness on escape paths.

* Protocol and Solution Defects: Bugs within protocols or improper coordination between solutions in complex scenarios (e.g., multi-solution stacking).

* Escape Path and Fault Tolerance Failure: Even when backup paths exist, they often fail to provide the intended relief. This is typically due to:

  - Resource Blindness: Traffic switches to backup paths that immediately collapse because they cannot handle the sudden load surge, stemming from a lack of real-time resource awareness.

  - Ineffective Design: The backup or escape schemes themselves are improperly designed (e.g., suboptimal path calculation or logical loops), resulting in a failure to achieve the intended "escape" effect and leaving the service in a degraded or interrupted state.

* Insufficient Cross-layer Coordination: The physical and network layers fail to collaborate, preventing rapid responses to cross-layer common-cause failures.

3.3. Post-event: Lagging Recovery and Self-Evolution

Recovery relies too heavily on manual intervention; while frameworks such as Service Assurance for IP-Based Networks (SAIN) [RFC9417] provide a foundation for modeling dependencies, fully automated "closed-loop" evolution remains in its infancy.

* Low Automation: Over-reliance on manual intervention leads to lack of automated self-healing logic.

* Lack of Closed-loop Learning: Systems cannot continuously learn from historical failures, leaving defense strategies static and unable to evolve with the changing network environment.

4. Technical Requirements for Resilience Enhancement

To address the aforementioned problems, a resilient architecture should satisfy:

* Proactive Risk Awareness: The ability to identify risk trends before failures occur based on multi-dimensional telemetry data.

* Elastic Resource Buffering: The ability to absorb instantaneous traffic shocks without changing topology through elastic scheduling, isolation, and resource decoupling.

* Deterministic Self-Healing: The ability to restore service performance to baseline SLA within a predefined time limit and maintain "inertial operation" of services.

* Closed-loop Immune Evolution: The ability to learn failure patterns through feedback loops and automatically upgrade defense strategies to raise the future anti-risk baseline.

TBD.

5. Security Considerations

Resilience mechanisms may introduce new attack vectors, such as injecting false telemetry data to trigger unnecessary path oscillations. Any framework must introduce identity-based authentication for all sensing data and policy updates.

TBD.

6. IANA Considerations

TBD.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

7.2. Informative References

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/info/rfc4272>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <https://www.rfc-editor.org/info/rfc7276>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/info/rfc9197>.

[RFC9417] Claise, B., Quilbeuf, J., Lopez, D., Voyer, D., and T. Arumugam, "Service Assurance for Intent-Based Networking Architecture", RFC 9417, DOI 10.17487/RFC9417, July 2023, <https://www.rfc-editor.org/info/rfc9417>.

Authors' Addresses

Jing Zhao (editor)
China Unicom
Beijing
China
Email: zhaoj501@chinaunicom.cn

Ran Pang (editor)
China Unicom
Beijing
China
Email: pangran@chinaunicom.cn

Wenxiang Lv (editor)
China Unicom
Beijing
China
Email: lvwx28@chinaunicom.cn

Jie Dong (editor)
Huawei Technologies
Beijing
China
Email: jie.dong@huawei.com

Shuai Zhang (editor)
China Unicom
Beijing
China
Email: zhangs366@chinaunicom.cn