Network overlay impacts to streaming

Glenn Deen – Comcast-NBCUniversal

Sanjay Mishra - Verizon

IETF123 MOPs WG

July 21st 2025

-02 version of submitted ahead of IETF 123

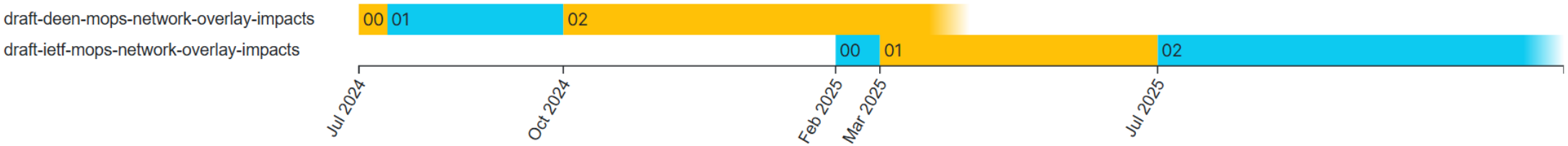
Network Overlay Impacts to Streaming Video

draft-ietf-mops-network-overlay-impacts-02

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

00 01 02



Many Thanks to Jay Robertson for the review of -01 and submitting a PR

https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/

Network Overlays

Network Overlays that make changes to network policies such as routing, DNS resolvers, IP Address assignment etc. are often intended to enhance privacy are causing operational problems for Streaming video platforms

Network Overlays make policy changes: IP Assignment , DNS Resolvers, Routing etc.

The problem begins when the application workflow isn’t expecting it

… and it can get worse from there

https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/

Example of changed network policies

- Alternate network policies to the underlying ”native” network
  - Routing changes
    - Alternate Ingress/Egress paths
  - Protocol /Application Specific Routing changes
  - DNS changes
    - DNS Resolver choice: 1.1.1.1 -> 8.8.8.8
    - DNS Protocol Choice: DNS/53 -> DoH
    - Changed DNS policies: DNS Query Results different than expected
  - Changed Address Assignment
    - IPv4 to IPv6 (or IPv6 to IPv4)
    - Changed address block

https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/

What changed from v1?

- Tidying up the document; fixing typos and other inconsistent text throughout the document
- Added a new section (sec 2.2.10) – Unintended Content Blocking (partial text below for context)
  - A strongly undesirable unintended side-effect of network policy changes is the blocking of content to the viewer. This may be the primary content URLs access which are blocked, or possibly advertising fetched from a second URL from the main video content. This can be due to policy changes altering device IP addresses, or changes to routing that run afoul of enforced traffic routing policies.

Table of Contents

1. Introduction 3
2. Internet Privacy Enhancements 5
2.1. Network Overlays 5
2.1.1. Emerging Operational Issues with Network Overlay Policy Changes 6
2.2. Policy Changes 6
2.2.1. Partitioning 7
2.2.2. Protocol Policy Changes 7
2.2.3. Encryption Policy 8
2.2.4. Address Policy Changes 8
2.2.5. DNS Policy Changes 8
2.2.6. Log Data Changes 9
2.2.7. Geo Location & Identification 9
2.2.8. CDN interconnection troubleshooting 9
2.2.9. Routing Changes 9
2.2.10. Unintended Content Blocking 11

https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/

Survey to gather operational impacts

Issued questionnaire to the SVTA members seeking input on observed impacts to the network due to network overly:

- https://forms.gle/DFzCsJehWhP87oas8

GitHub:

- https://github.com/gitnnelg/NetworkOverlays

https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/

Moving the draft forward to WG LC

This draft is a problem statement, once we decide on the problem we will later create another draft to capture Best practices, mitigations, alternatives…..

Completing the work of capturing the problem:

IETF122: We want MOPS WG comments and other contributions of observed operational impacts

IETF123: draft will be updated to include the impacts and operational description

Done

IETF124: WG LC?

After WG LC – next New I-D submission to MOPS: draft-??-proposed-mitigation-for-network-overlays

https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/

Thank you