Network overlay impacts to streaming

Glenn Deen – Comcast-NBCUniversal

Sanjay Mishra - Verizon

IETF122 MOPs WG

March 18th 2025

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

-01 version of adopted draft submitted

Network Overlay Impacts to Streaming Video

draft-ietf-mops-network-overlay-impacts-01

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

Versions:

00 01

Many Thanks to Jay Robertson for the review of -01 and submitting a PR. Will review the PR to pick up your changes

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

Evolution of viewing from broadcast to streaming

- Internet streaming has greatly matured and diversified and viewing on a daily basis far exceed billions of viewers and is a preferred choice
- Viewers expect network to provide
  - Low latency for live sports, live events and live streamed content
  - Support a myriad of devices with diverse capabilities including low-cost streaming sticks, to smart TVs, tablets, phones, and game consoles
  - Support Ultra-high definition, 4K, 8K and immersive experiences
- To meet these challenges streaming platforms have significantly invested in developing delivery architectures that are built with detailed understandings of each element in the content delivery pathway starting from the content capture all the way through to the screen of the viewer

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

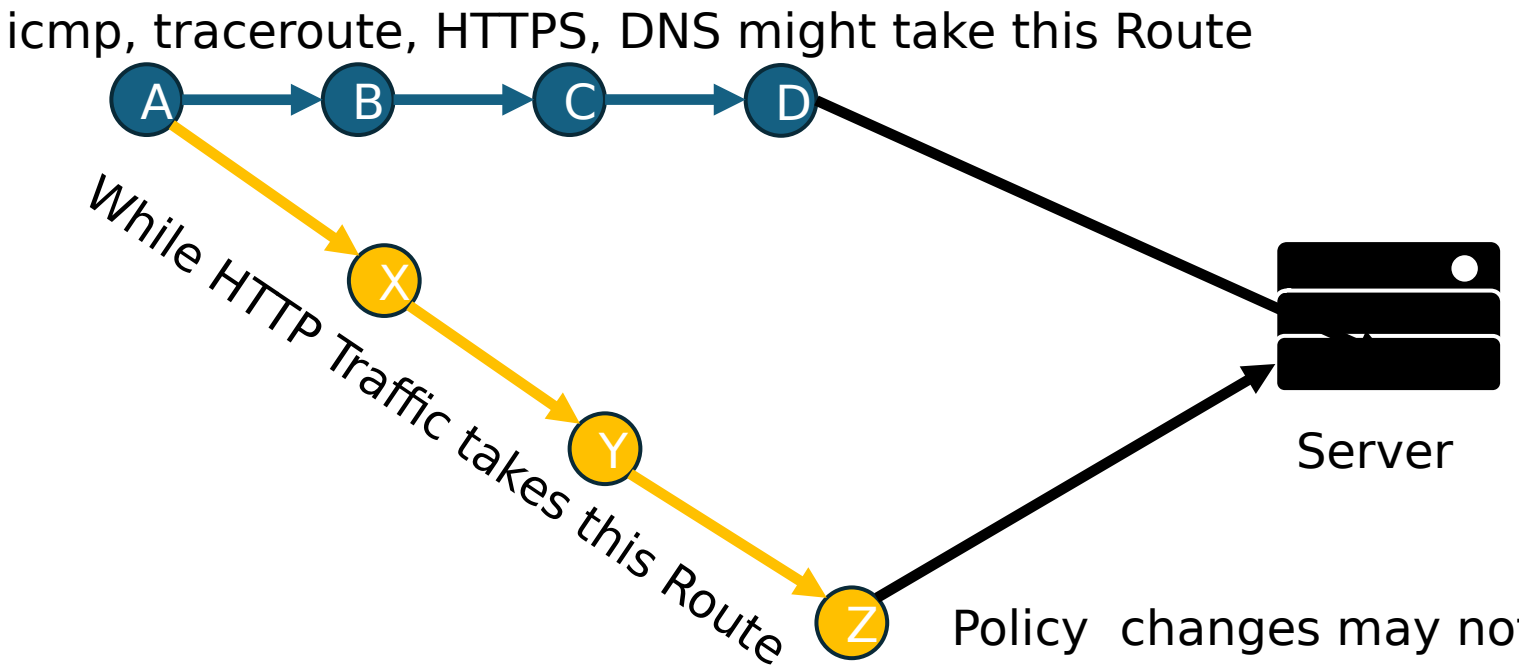
Example of changed network policies

- 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/

Network policies maybe different for different protocols

Different Protocols may take different routes:

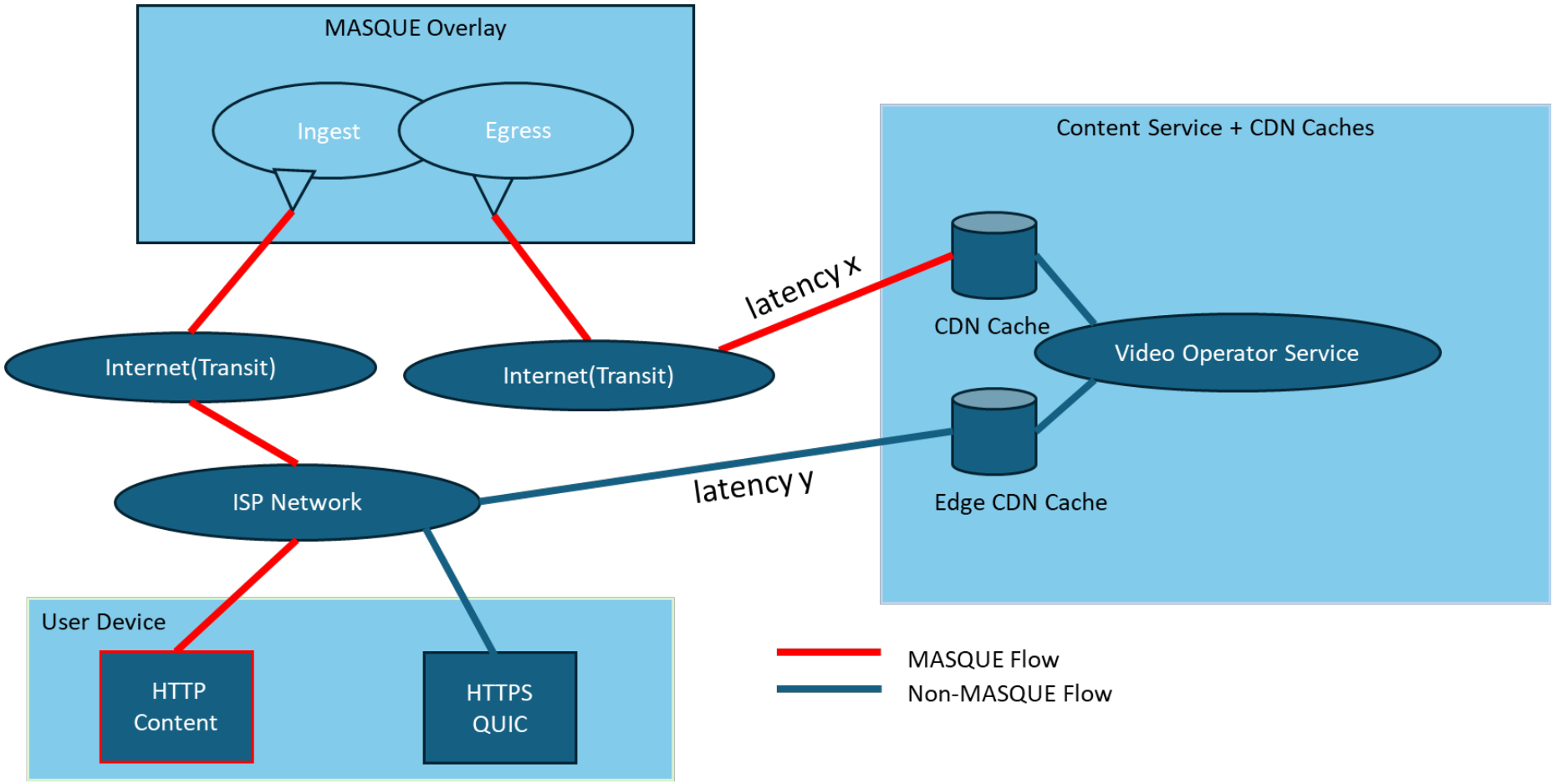


Policy changes may not to visible to Applications

Different Protocols see different perspectives of the network

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

Example impact: Different CDN cache selection, Different Latencies



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

Review: Identified Impacts & Get MOPS Input

olicy Elements of Interest in the I-D

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

2.2.1 IP Address Changes:

Network overlays often change the source IP address of connections, making it appear that traffic originates from a different location. This can disrupt geolocation-based services and CDN cache selection, as CDNs rely on IP addresses to route users to the nearest servers.

2.2.2 Transport Protocol Changes:

Overlays can alter the transport protocols used for connections, such as converting HTTP/2 to HTTP/3. This can impact performance and compatibility, as different protocols have varying characteristics.

2.2.3 Routing Changes:

Network overlays establish alternative routing paths, bypassing the traditional routing decisions of ISPs. This can lead to unpredictable latency and routing, affecting the performance of latency-sensitive applications like streaming video.

2.2.4 DNS Resolver Changes:

Overlays frequently change the DNS resolver used by connections, which can affect DNS-based load balancing and content delivery. This can result in users being directed to suboptimal servers or experiencing DNS resolution delays.

2.2.5 Encryption Policy Changes:

Overlays can enforce or modify encryption policies, which can impact the ability of applications to inspect or optimize traffic. This can hinder troubleshooting and performance optimization.

2.2.6 Traffic Classification Changes:

Network overlays can obscure or alter traffic classification, making it difficult for network operators to prioritize or manage traffic. This can lead to congestion and performance degradation for certain applications.

2.2.7 CDN Interconnection Changes:

Changes to IP addresses and routing can disrupt CDN interconnections, affecting the efficiency of content delivery. This can result in increased latency and reduced throughput for streaming video.

2.2.8 Multipath Changes:

Some overlays use multipath technologies, which can introduce complexity and unpredictability into network behavior. This can make it challenging to troubleshoot and optimize performance.

2.2.9 Other Policy Changes:

This section acknowledges that network overlays may introduce other policy changes beyond those listed, further complicating network behavior and application performance.

2.2.10 ?

Question: Did we miss a policy change?

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 capt
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

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

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