Media OPerationS
Internet-Draft
Intended status: Informational
Expires: 8 January 2026

G. Deen
Comcast-NBCUniversal
S. Mishra
Verizon

7 July 2025

Network Overlay Impacts to Streaming Video
draft-ietf-mops-network-overlay-impacts-02

Abstract

This document examines the operational impacts to streaming video applications caused by changes to network policies by network overlays. The network policy changes include IP address assignment, transport protocols, routing, and DNS resolvers, which in turn affect a variety of important content delivery aspects such as latency, CDN cache selection, delivery path choices, traffic classification and content access controls.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ietf-wg-mops.github.io/draft-ietf-mops-network-overlay-impacts/draft-ietf--mops-network-overlay-impacts.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-mops-network-overlay-impacts/.

Discussion of this document takes place on the Media OPerationS Working Group mailing list (mailto:mops@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/mops/. Subscribe at https://www.ietf.org/mailman/listinfo/mops/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-mops/draft-ietf-mops-network-overlay-impacts.

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/.

Copyright Notice

Table of Contents

1. Introduction

Enhancing the privacy of Internet users has a been significant focus of the IETF since the Snowden revelations and the publication of [RFC7258]. [RFC7264] explored in greater detail the technical threats identified in RFC7258 along with high level descriptions of mitigations. Since then the various working groups at the IETF have endeavored to address the specific threats to their respective area and have produced a long list of new RFCs with privacy enhancements deliberately and consciously included. Protocols like QUIC [RFC9000] are examples of the new generation of IETF protocols with privacy enhancements such as always enabled encryption built directly into their design.

At the same time that the IETF has been diligently enhancing Internet privacy, Internet video streaming has become a part of daily life for billions of viewers with streaming being for many their primary way of watching sports, entertainment, user generated content (UGC) and news. This has grown to become the primary data by volume traversing the Internet with an hour of HD video consisting of roughly 1.5-2.5GB of data and streaming is estimated to account for 80-85% of current global Internet traffic.

The Operational Considerations for Streaming Media [RFC9317] provides a good introduction to the various engineering aspects encountered by streaming platforms in engineering and operating the infrastructure used to meet the global growth in video streaming.

While early streaming efforts were satisfied with being able to stream a video to a device successfully without consideration for efficiency or scale, the rapid growth in viewership has pushed platforms to develop sophisticated architectures and designs.

For video that is prerecorded, such as Video On Demand (VOD) TV and Movie content ans User Generated Content (UGC) distributing the recorded and encoded content using Content Delivery Network (CDN) caches is a common technique to meet demand at scale. The IETF CDNi working group has done significant work on this and SVTA OpenCaching (svta.org) extends upon CDNi to create a robust implementation of CDN architecture for VOD scaling. VOD and UCG streaming typically place a focus on selecting the best CDN cache with the best responsiveness, the shortest network path and fewest hops to avoid congestion and bandwidth limitations that might limit the quality of the video being delivered.

The newest frontier in streaming is live streaming, primarily around sports events. Live streaming, like VOD has significant capacity demands with events that can have viewership levels ranging from tens of thousands to 10-50 million live viewers. The day of hundreds of millions of live viewers for a single event such as a major global sporting event is on the near horizon as a normal occurence, with no limit in sight on how far growth can go. Perhaps, one day a significant portion of the global population will live view an event over the Internet.

Even today, the current viewer levels for large events are pushing the boundaries of video streaming techniques. Live also comes with new challenges; CDN caching is still used to meet scaling challenges for live events, but unlike VOD it can’t be prerecorded and prepositioned on CDN caches ahead of the event. Live sports streaming also has important low latency requirements - viewers don’t want a big goal spoiled by alerts on their phones, or cheering the street before they see it on their own screen. The video pipeline used to deliver live streamed events with low latency and at high quality is highly optimized and as a result is very sensitive to interference from unexpected network behaviors and conditions.

The delivery pipelines of VOD, UGC and Live have each been enginered and optimized to deliver the highest quality, in the most efficient manner over the Internet from platform to viewers. However, increasingly as consumer products have added responses to [RFC7258] and [RFC7264] to consumer devices and services, they have occasionally introduced unexpected and sometimes non-easily detectable changes to the network behavior and the video pipeline in ways that can interfere with and undermine the efficiencies, scaling and low latency engineering that video platforms have spent considerable time, money and talent developing and deploying to meet user video experience expectations.

The authors readily acknowledge the many challenges and difficulties in improving Internet privacy in an area as complex as the Internet while also maintaining compatibility with the wildly varied applications and uses of the Internet on which users rely upon daily in their lives. This is hard stuff and it's very natural for there to be operational considerations that must be understood and folded back into architectural designs and consumer products.

This document is intended to document the various impacts that have been observed by streaming applications from a streaming platform operational perspective on the impacts of certain enhanced privacy architecture approaches that have been pursued at the IETF.

2. Internet Privacy Enhancements

The IETF's work to enhance the privacy of Internet and defend against pervasive monitoring as described in [RFC7258] has employed as series of techniques starting with encrypting network data flows, typically using TLS. Other approaches, involve changing things at a policy level such as changing routing, DNS resolver choices so as to further obfuscate and isolate the network and data flows from the underlying base network as means of interfering with pervasive monitoring.

[RFC7258] from the IAB examines various pervasive montoring approaches while [RFC7624] discusses responses that enhance privacy. [RFC9000] itself is an excellent example of the applied design approaches and introduces the QUIC transport protocol that is always encrypted.

2.1. Network Overlays

The IETF's privacy enhancement work to address [RFC72558] covers a lot of design choices and policies such as the approach of always-on encryption as shown in the design of QUIC [RFC9000]. Many of these do not affect video streaming, however those that do impact streaming fall into a class of design choices that can be described as creating a new network overlay, operating as an overlay on top of the underlying native network, but following one or more different policies than the underlying network or the streaming application would follow on their own.

The Network Overlays that have been found by video platform operators to impact streaming operations are those that make policy changes in ways that are not directly visible, selectable, or detectable by the video streaming application or streaming platform. These changes, when made under the covers and out of visibiltiy to the streaming application, often can make unexpected changes to the streaming pipeline in ways that undermine the architecture choices of the streaming application and platform engineers.

Network Overlay's that cause network connection behavior and properties to differ from what the application expects can lead to situations where the application user and operator assume one set of behaviors of the network data flow to be true while in reality one or more different behaviors may occur. This in turn can lead to unanticipated outcomes that can have operational impacts.

Protocols such as MASQUE [RFC9484] and services built on it such as Apple's iCloud Private Relay (https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF) are examples of Privacy Enhancing Network Overlays that involve making a number of network policy changes from the open Internet for the connections passed through them.

2.1.1. Emerging Operational Issues with Network Overlay Policy Changes

Streaming video applications and the streaming platforms delivering content are starting to encounter various operational challenges related to Network Overlays. Typically the primary problems are encountered when the network overlay has made policy changes that are either unexpected, are difficult or impossible for the streaming platform to detect, or the changes are inconsistently applied.

There are a variety of impacts but a few common classes of issues have been observed:

2.2. Policy Changes

Changing the encryption policy from that expected by the streaming application, for example changing HTTP urls in manifests into HTTPS connections can disrupt architectures which involve the network being able to detect video flows.

Changing routing policy from what is expected by the streaming application can break CDN cache selection logic, resulting in a farther away cache delivering lower quality video at higher latency than the closer cache that would be selected by the CDN cache selection logic might.

A routing policy change example is illustrated in figure 1 of different policies for a network overlay vs the underlying base network which changes the traffic path from the Network Overlay having a different routing policy from that of the underlying native base network.

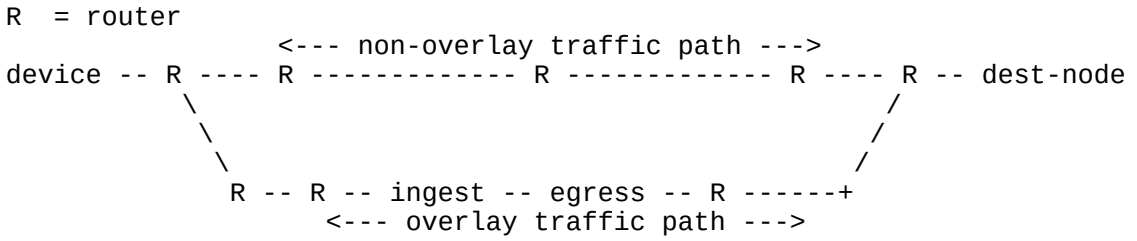

Figure 1: Network Overlay routing selects traffic via an alternate path

2.2.1. Partitioning

Network Overlay policy changes include an alternate routing policy since a fundamental aspect of this design is the tunneling of connections through alternate paths to enhance privacy. The reasons for this approach are discussed in the IAB document Partitioning as an Architecture for Privacy (https://datatracker.ietf.org/doc/draft-iab-privacy-partitioning/).

2.2.2. Protocol Policy Changes

Network overlays have been seen to make application and transport protocol changes from what is expected. Changes such as HTTP2/tcp into HTTP3/QUIC and HTTP2 into HTTPS2+TLS are performed by some privacy enhancing approaches, converting what is considered an undesirable protocol choice into what is considered a better alternative, hidden under the covers from the application.

One impact occurs when the protocol change alters the network as seen by the video application. For instance, a video application may make a test fetch of video in order measure network conditions which will be used to make streaming decisions for the actual content being accessed. If the application test probe uses HTTP2/tcp to test, but the actual content access request over HTTP2/tcp is converted to HTTP3/QUIC then the video platform does not have accurate results from its test probe which can directly lead to erroneous non-optimal choices by the video player algorithm.

2.2.3. Encryption Policy

Changing the encryption policy applied to video streams either adding where it wasn’t originally used or removing if it was originally specified can cause a wide range of operational problems.

2.2.3.1. Forced Encryption Upgrade

Changing unencrypted HTTP2 to encrypted HTTP2+TLS connects will prohibit streaming workflows that involve content detection as part of the network delivery. This can result in video traffic not being correctly identified and the incorrect network policies being applied to it. This is particularly problematic in environments using multicast and in mobile environments.

2.2.3.2. Forced Encryption Downgrade

Equally so, the removal of encryption applied to the transport stream by a streaming platform would be significantly problematic as such encryption may be part of a content protection and content integrity protections architecture.

2.2.4. Address Policy Changes

IP address changes such as converting from IPv4 to IPv6 or IPv6 to IPv4, done unexpectantly unexpectedlyor done invisibly to the application can cause both routing and cache selection issues, as well as cause problems in debugging situations causing engineers to not be using the correct address when examining logs, doing their own test probes etc.

Source IP Address assignment changes, again when done invisibly to the application can cause significant disruption. Platform authentication gateways that associate session authorizations with the session’s device’s IP address can result in service access denial when associated addresses change unexpectedly. For example, when the device address as seen by the video application is different from the device address seen by the associated streaming platform, this can result in the platform rejecting logins, content access and other service functions from the device.

2.2.5. DNS Policy Changes

Network overlays that change DNS settings have long been an issue for CDN architectures that use DNS as part of their load balancing architecture.

2.2.5.1. DNS0

DNS0 extension information was specifically designed to help CDN cache selection logic by providing more information to the decision making algorithms, so a policy change that changes the DNS resolver for an application to a different resolver that does not support DNS0 can have quite a significant impact to a video application.

2.2.6. Log Data Changes

Logging is often the first tool used to find and diagnose problems. Network overlays which change policies that result in unexpected and non-understandable log entries on either the user device or the video platform can greatly undermine the use of logs in problem determination and resolution.

2.2.7. Geo Location & Identification

Network Overlays that change the apparent location of devices can result in platforms not being able to properly identify the geospatial location of the user. It is very common for CDN caches to apply IP address level geolocation to determine in broad terms, such as identifying the country the user is in. If an overlay changes the apparent origin addresses of video device to one outside the of the address blocks mapped by location providers, then geolocation can fail and users can be denied access to content they otherwise are able to access.

2.2.8. CDN interconnection troubleshooting

In a CDN interconnection when two CDN domains have to localize a point of failure, they first determine the delivery path and a point of observation where to take measurements. Then they proceed by dichotomy to determine the domain where the point of failure is. The issue with overlay networking is the following: CDNs use their request routing information to determine a point of observation on the delivery path where to do the measurement, as their delivery path is overwritten by the re-routing of the overlay networking, the flow can’t be observed at the observation point.

2.2.9. Routing Changes

Routing changes which cause connections between video applications and the infrastructure services they use can create a large number of problems.

2.2.9.1. End to End Problem Discovery

A common issue in video delivery is locating where along the delivery path the video transport is encountering problems. Often such problems are more complex than the connection not working at but instead involve identifying bottlenecks, lost packets, and congestion issues. When the routing changes from what is expected or visible to support tools it becomes an operational trouble spot for users and platform suport to locate and determine the source of the problems.

2.2.9.2. CDN Edge Cache Selection due to Routing

A significant, and often overlooked problem is the addition of network latency compared to edge CDN caches or access network peering connections. Routing changes which cause bypassing edge CDN caches and instead choosing less optimal caches

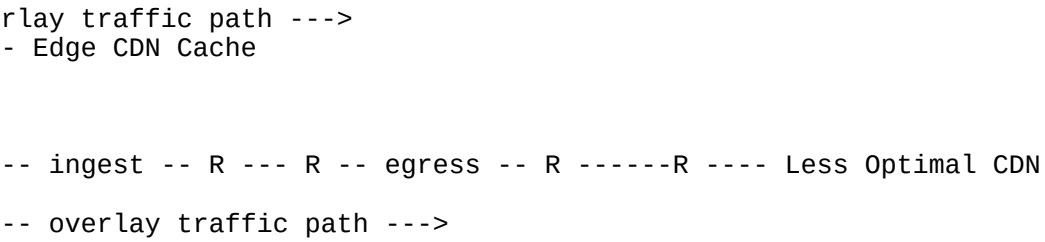

Figure: Routing Changes altering CDN Cache selection

2.2.9.3. Performance and Problem determination

Network overlays often interfere with the tools used in performance and problem determination. This is due to either the tool and protocols not being able to traverse the alternative route tunnel impacting service's ability to diagnose connection and performance problems, or the network overlay itself not supporting the tool and not supporting or carrying the tools functions.

2.2.9.4. Impact of Changing Network Routing and other Policies

The problem for streaming applications occurs when the underlying network properties and policies change from what is expected by the streaming application. In particular when such changes are either hidden or not visible to the streaming application.

While the open Internet is a dynamic environment, changing of basic network behavior and policies from what is expected as seen from the streaming application, deviates unexpectedly from what the streaming application expects. This behavior disrupts the optimized streaming

delivery architecture for the end-user device. Changes to Network Policies such as routing, source IP address assigned to the streaming application traffic, DNS resolver choice etc influences this behavior.

Having a reliable understanding of the delivery path is essential for streaming operators and the introduction of network overlays like those based on technologies such as MASQUE especially when designed to be undetectable by the applications using them has introduced new technical challenges for streaming operators and network operators as well as for their viewers.

The core problem occurs when changes to network policies are made often without notification or visibility to applications and without clear methods of probing to determine and test changed behaviors that affect the streaming application’s content delivery path resulting in increased latency, changes of IP address for the application as seen by either the application or the streaming service connection, changes to DNS resolvers being queried and the results returned by DNS, and changes to application transports such as adding or removing outer layer encryption are all problems that have been observed in production streaming platforms.

2.2.10. Unintended Content Blocking

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.

Such blocking may be connected to restrictions built upon data feeds used for geofiltering and georestuctions, for example restriction which block delivery to networks identified as either commercial data-centers or other CDNs service network addresses. Essentially, running afoul of configurations possibly used to combat security threats that expect streaming viewers to be on home or possibly mobile networks, but not in commercial data centersor CDN content networks and so block delivery to IP addresses in those unexpected network blocks. This is more likely to occur in network overlays that shift egress traffic to commeerical or CDN blocks.

This is a particularly troublesome problem to determine as it may appear inconsistently from one streaming session to another. Small changes in URLs in manifests from on session to another, especially on streaming platforms that make use of multi-CDN delivery and may encounter different delivery and security protection policies from the different multi-CDN operators invovled.

3. Policy Changes Hidden from Applications

One of the central recurring issues with streaming applications running on devices or networks with changed policies due to network overlays is that the changes are often hidden from the applications.

Applications often find it difficult or even impossible to detect when network policy changes will be active and what they are changing. For example, a device may have a designated default DNS resolver for the device, but may have a different resolver selected depending on how the streaming application queries the DNS.

Likewise, a streaming application might find that one application transport protocol such as HTTP queries will have one set of routing policies applied to it but a different application transport like HTTPS may have a different set of routing policies applied.

Streaming applications that cannot determine the exact behavior to be expected can prevent the streaming application from making good content source decisions and can prevent applications from being able to provide reliable feedback and logs when problems are encountered.

4. Making It Easy (for Users) by Working Under the Covers

Historically, incorporating privacy features into consumer-facing products has been complex. This challenge arises from the need to address a wide range of use cases while also offering users easy access to advanced privacy frameworks and taxonomies. Many attempts have been made and very few have achieved finding success with end users.

Perhaps learning from the lessons of offering too many options, the recent trend in privacy enhancements has steered toward either a very simple "Privacy On or Off" switch or in other cases automatically enabling or "upgrading" to enhance privacy. Apple’s iCloud Private Relay can be easily turned on with a single settings switch, while privacy features such as Encrypted DNS over HTTP and upgrade from HTTP to HTTPS connections have had a number of deployments that automatically enable them for users when possible.

Keeping with the motto of "Keep It Simple", users are generally not provided with granular Network Overlay controls permitting the user to select what applications, or what network connections the Network Overlay policies can apply to.

Adhering to the "Keep It Simple" approach the application itself has very little connection to privacy enhancing Network Overlays. Applications generally do not have a means to detect when networking policy changes are active. Applications generally do not have a means to access policy change settings or to interact to change them.

5. Streaming Video

Streaming Video, while just one of the many different Internet applications does standout from other uses in a number of significant ways that perhaps merit some amount of special consideration in understanding and addressing the impacts caused by particular privacy enhancing design and service offering choices.

Firstly, Streaming video operates at a hard to imagine scale - streaming video is served globally to more than 2 billion user daily currently and continuing to grow in leaps and bounds.

Secondly, the content types delivered through streaming has evolved from the pre-recorded low-resolution, low-bit rate, latency tolerant video-on-demand movies, live or pre-recorded TV shows, and user generated videos delivered by pioneering streaming platforms to now including low-latency 4K and 8K live sports events, while also evolving the pre-recorded content with high-bit rate such as 4K and 8K cinema quality and High Dynamic Range (HDR) lighting.

Finally, the expectations of streaming video viewers have significantly evolved from the days of settling for being able to watch a movie in a PC browser. Viewers expect to watch on any device type they want ranging from low-end-streaming sticks that plug into a USB port, to 4K and HDR capable laptops, 4K and 8K HDR TV screens, gaming consoles, smart phones and many more choices. Viewers also expect to have the same great viewing experience while at home connected via high-speed wired Internet, high-speed WiFi, or mobile cellular 5G and even satellite Internet connections.

To meet the growth to billions of users, the growth in content type, quality and speed expectations, and on-any-device anywhere that I am over any-network-connection expectations of users the Streaming Video technology infrastructure has had to itself evolve significantly. This video streaming evolution work is being done in the IETF and in the Streaming Video Technology Alliance (SVTA) (https://www.svta.org/), and in a number of other technical and industry groups.

It’s hard to overstate just how much the growth of streaming video has contributed to the growth of the Internet. Internet connections of multiples of hundreds of megabits and gigabits speeds today are because of the needs of video streaming, the ongoing work on low-latency networking and ultra-low-latency video delivery are both driven by the use of streaming video.

5.1. Advances in Streaming Video Architecture

Internet streaming has greatly matured and diversified from its early days of viewers watching pre-recorded 320x240, 640x480 standard definition 480p movies to wired PCs connected to the Internet via high-latency, low-bandwidth DSL as early DOCSIS modems.

Streaming has grown to the extent that it has become a daily go-to video source worldwide for billions of viewers and has expanded from pre-recorded movies to encompass every type of video content imaginable. This growth to billions of viewers and the addition of low latency sensitive content and new connectivity options like WiFi, Cellular and Satellite in addition to high-speed DOCSIS and fiber is the world streaming platforms now provide service in.

With the large user base and its usage, the Streaming platforms also have significant technical challenges to meet viewer expectations:

* (1) Delivery scales that commonly range from hundreds of thousands to many millions of viewers simultaneously, with billions of views globally daily;

* (2) Low latency demands from live sports, live events and live streamed content;

* (3) content resolutions and corresponding formats which have jumped from the days of SD-480p to 4K (3840x2160) and 8K (7680x4320) along with bit rates which can had data needs of 10-24+ Mbps for 4K with 8K demanding 40 Mbps under extreme compression and 150-300 Mbps for high quality such as cinema;

* (4) devices with very diverse capabilities low-cost streaming sticks, to Smart TVs, tablets, phones, and game consoles

* (5) broad range of connectivity choices including WiFi, Gig speed-low latency DOCSIS, Fiber, satellite, and 5G cellular networks;

* (6) application transport protocols including MPEG DASH, HLS, HTTP2/TCP, HTTP3/QUIC, WebRTC, Media over QUIC (MoQ) and specialty application transports such as SRT, HESP etc.

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.

Streaming applications are part of an end-to-end architecture that is optimized around achieving the best experience including low latency video delivery to viewing devices. The open Internet can be unpredictable with temporary issues like packet loss, congestion and other conditions. However, streaming architecture is designed to handle these momentary problems as effectively as possible often through use of dynamic adaptive approaches designed into streaming protocols and platform components.

6. Middleboxes and learning from the past

The IETF has discussed this situation in the past, more than 20 years ago in 2002 Middleboxes: Taxonomy and Issues [RFC3234] was published capturing the issues with Middleboxes in the network and the effects of hidden changes occuring on the network between the sender and receiver.

7. Appendix A: Network Overlays are different than VPNs

While conceptually similar in many ways to VPN (Virtual Private Network) technology, the various network overlay technologies currently being deployed as well as new ones currently being designed by the IETF differ quite significantly from the older VPN approach they are replacing in a number of ways.

It is also worth noting that one reason why the issues discussed in this document have not been concern with regard to VPNs is that largely VPNs have not been a pervasive way to stream video. First, many VPNs have not had very good or consistent throughput compared to the direct open Internet and so provide a poor viewing experience. Second, many video platforms block or deny service to VPN connections due to the very common use of VPNs to bypass geofiltering restrictions.

Whatever the reason, it is worthlooking at how VPNs differ from the Network Overlays being discussed herein.

7.1. VPNs typically:

* (1) VPNs typically are detectable by both the video application and often by the streaming platform.

* (2) VPNs typically work at the network layer of a device, resulting in a wide-range (if not all) transports

* and protocols from the device flowing through the VPN

* (3) VPNs typically provide exception options allowing for exclusion from traversing via the VPN based on

* various criteria such as application, destination IP address, application protocol etc.

7.1.1. Network Overlays typically:

* (1) Network Overlays are often undetectable by video applications or by the streaming platform, when in use

* (2) Network Overlays often only apply to specific application transports such as HTTP2/TCP or HTTP3/QUIC while not applying to HTTP2/TCP+TLS on the same device.

* (3) Network Overlays often only apply to HTTP connections and do not support ICMP, non-HTTP versions of DNS, NTP etc, and various tools used for network measurement, problem determination, and network management that are not HTTP based.

* (4) Network Overlays do not expose to applications any means for the application to discover the policy changes the overlay will apply to the applications network connections.

* (5) Network Overlays do not expose mechanisms or APIs for applications to interact with them such as getting or setting options.

8. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

9. Security Considerations

TODO Security

10. IANA Considerations

This document has no IANA actions.

11. 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/rfc/rfc2119>.

[RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, DOI 10.17487/RFC3234, February 2002, <https://www.rfc-editor.org/rfc/rfc3234>.

[RFC72558] "*** BROKEN REFERENCE ***".

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/rfc/rfc7258>.

[RFC7264] Zong, N., Jiang, X., Even, R., and Y. Zhang, "An Extension to the REsource LOcation And Discovery (RELOAD) Protocol to Support Relay Peer Routing", RFC 7264, DOI 10.17487/RFC7264, June 2014, <https://www.rfc-editor.org/rfc/rfc7264>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/rfc/rfc7624>.

[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/rfc/rfc8174>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[RFC9317] Holland, J., Begen, A., and S. Dawkins, "Operational Considerations for Streaming Media", RFC 9317, DOI 10.17487/RFC9317, October 2022, <https://www.rfc-editor.org/rfc/rfc9317>.

[RFC9484] Pauly, T., Ed., Schinazi, D., Chernyakhovsky, A., K端hlewind, M., and M. Westerlund, "Proxying IP in HTTP", RFC 9484, DOI 10.17487/RFC9484, October 2023, <https://www.rfc-editor.org/rfc/rfc9484>.

Acknowledgments

The authors would like to acknowledge the contributions from the Streaming Video Technology Alliance (SVTA) based on their work studying the impacts of network overlays on the streaming platforms. In particular, contributions from Brian Paxton have been very helpful.

Authors' Addresses

Glenn Deen
Comcast-NBCUniversal
Email: glenn_deen@comcast.com

Sanjay Mishra
Verizon
Email: sanjay.mishra@verizon.com