SCONE PRO

Securely
COmmunicating
NEtwork PROperties

PLUS++

...THE SEQUEL IS ALWAYS BETTER THAN THE ORIGINAL

NOTE WELL

This is a reminder of IETF policies.

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam if you have questions or concerns about this.

Definitive information on these policies:

- Internet Standards Process
- Working Group processes
- Anti-Harassment Procedures
- Code of Conduct
- Copyright
- Patents, Participation
- Privacy Policy

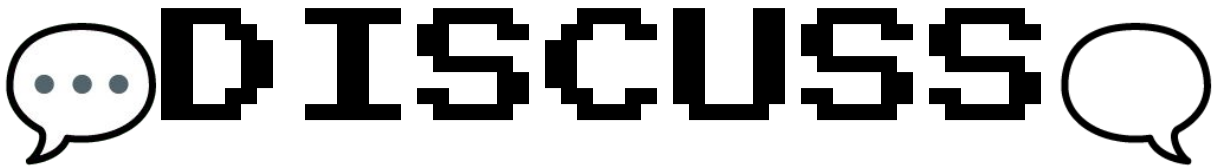
For advice, please talk to WG chairs or ADs.

Agenda

Introduction	Chairs	10m
Traffic policing in networks: goals, methods, and shortcomings	Marcus Ihlar	15m
Solution space and trials	Matt Joras	20m
Lessons from IETF history	Brian Trammell	10m
Discussion on use case and scope	Everyone	55m
Conclusions	Chairs	10m

Reminder: BoF Objectives

1. Is there a problem to be solved?
2. Do we understand that problem enough to engineer a solution?
3. Are enough people interested enough to do the work?


DISCUSS

Backup Slides

Charter 1/8

Video traffic is already 70% of the overall traffic volume on the Internet and is expected to grow to 80% by 2028. Across developed and emerging markets video traffic forms 50-80% of traffic volume on mobile networks. New formats like short form videos have seen tremendous growth in recent years. These growth trends are likely to increase with new populations coming online on mobile-first markets.

Charter 2/8

Mobile network operators continuously invest in network resources, including deployment of new generations or new bands of spectrum. Since spectrum is a limited and expensive resource, operators often make use of flow-based traffic handling such as shaping of video traffic, especially when the network is highly loaded. Operators cannot explicitly measure the degradation that shaping causes to end user quality of experience (QoE), making this approach open loop.

Charter 3/8

Video traffic usually employs adaptive bitrate (ABR) schemes to dynamically adjust the video quality (and thus the data rate) in response to changing network conditions. In the presence of traffic shaping, the ABR scheme should ideally adapt the quality and converge on a bitrate sustainable by the shaper. In practice this is extremely difficult to achieve while maintaining a good user experience. Application providers are even designing algorithms to detect the presence of such traffic shapers and estimate the targeted shaping rate, however, these algorithms are likely to be both inaccurate and complex. Instead, it would be beneficial, for both the application provider and network operator, to signal the shaper rate to the application to self-adapt their video traffic to conform to the specified characteristics. The application provider has the ability to measure end user QoE and therefore can self-adapt with QoE feedback.

Charter 4/8

The Secure Communication of Network Properties (SCONEPRO) Working Group's primary objective is to specify an on-path protocol for securely communicating network properties to clients relevant to a given application, such as the maximum achievable bandwidth for a video.

Charter 5/8

- The working group will initially focus on a solution that communicates the maximum achievable bandwidth for a video delivered from a server to a client, using QUIC connections carrying the application signaling traffic.
- Work to support TCP or other transport protocols may be considered later in the working group, however, these considerations shouldn't distract from support for video over QUIC.
- Further use cases may be considered later in the working group, however, it is not assumed that future use cases must or can be addressed by the same protocol. In essence, any protocol specified by the working group should be tailored to solve a specific use case.

Charter 6/8

The properties of this mechanism are as follows:

1. Associativity with an application. The network properties must be associated with a given application traversing the network, for example a video playback.
2. Client initiation. The communication channel is initiated by a client device, just as the end to end application flows are also typically initiated by a client.
3. Network properties sent from the network. The network provides the properties to the client. The client might communicate with the network, but won't be providing network properties.

Charter 7/8

4. On-path establishment. That is, no off-path element is needed to establish the communication channel between the entity communicating the properties and the client.
5. Optionality. The communication channel is strictly optional for the functioning of application flows. A client's application flow must function even if the client does not establish the channel.
6. Properties are not directives. A client is not mandated to act on properties received from the network, and the network is not mandated to act in conformance with the properties.

Charter 8/8

7. Resilient to NAT rebinding. The mechanism will allow the communication channel to be resilient to NAT rebinding, as long as the client is still served by the same logical Communication Service Provider (CSP).

8. Scalability. The mechanism must be scalable and implementable by Internet infrastructure as it exists today, for example mobile network packet cores.

9. Security. The mechanism must ensure the confidentiality, integrity, and authenticity of the communication. The mechanism must have an independent security context from the application's security context. The group must not define new security mechanisms for this purpose.