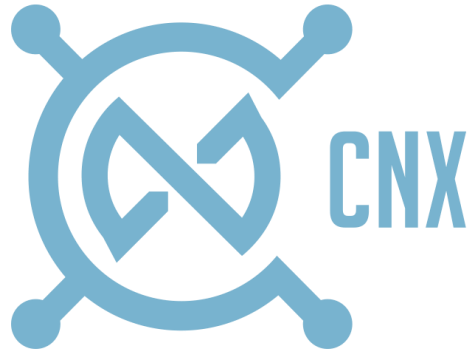
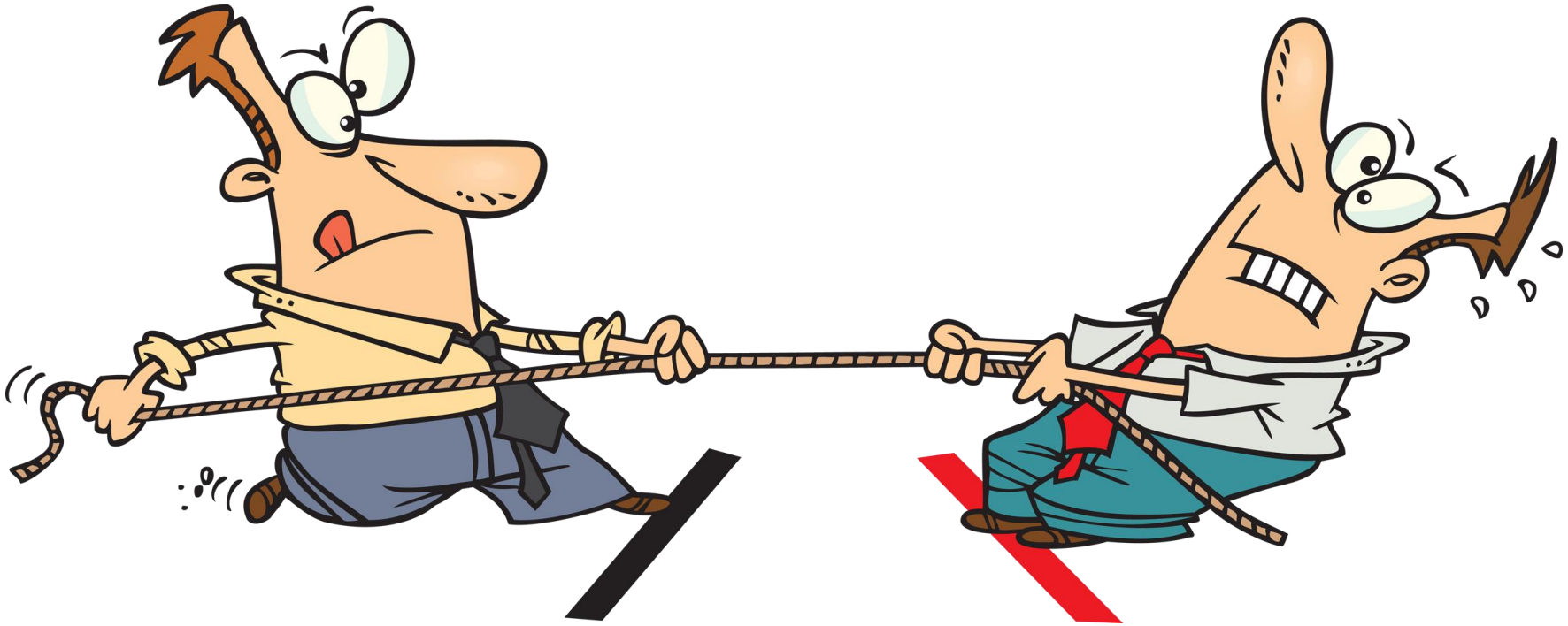


Who controls traffic?

Mike Gaertner (gaertner.mike@cnx.net.kh)

Flow control



Networks

Applications

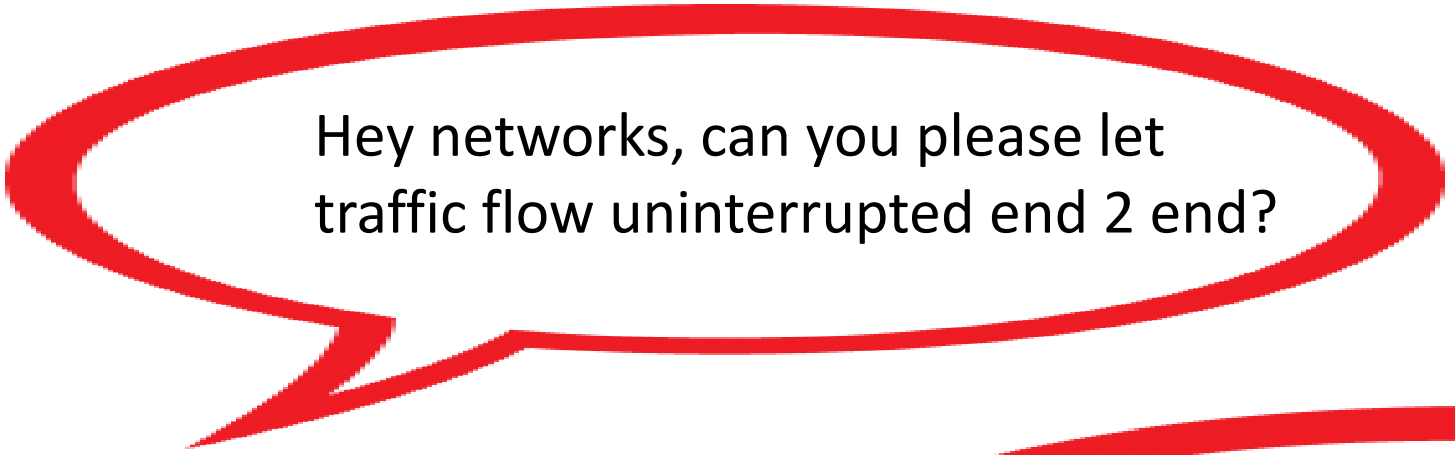
Networks be like ...

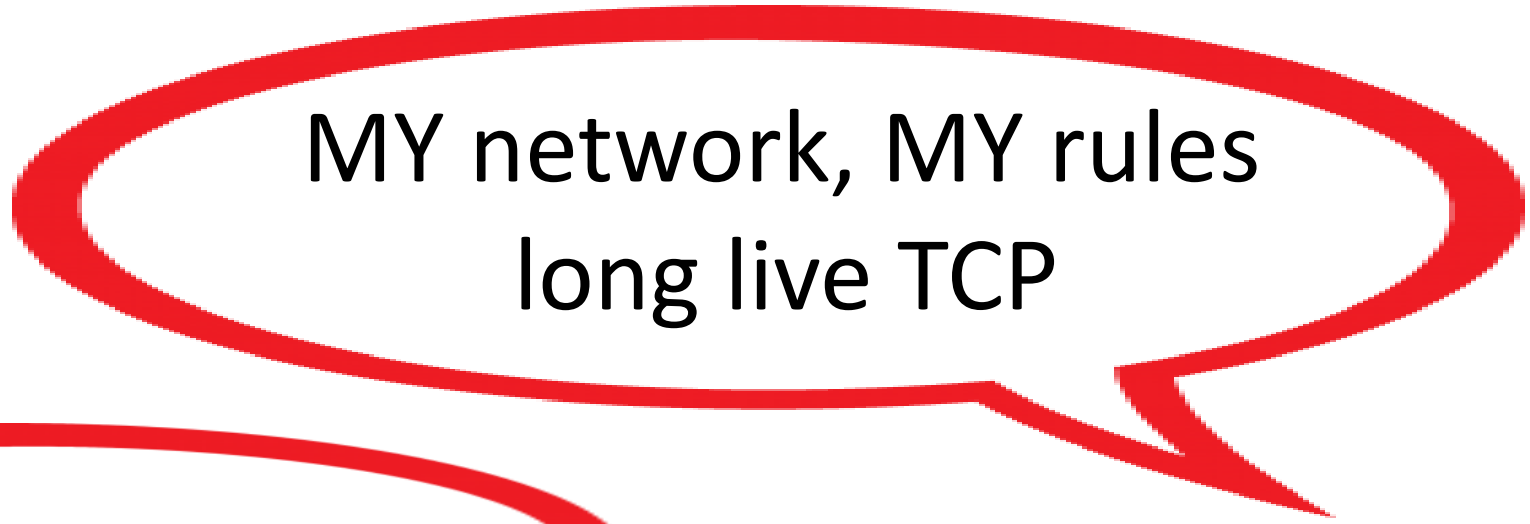
Networks friend TCP

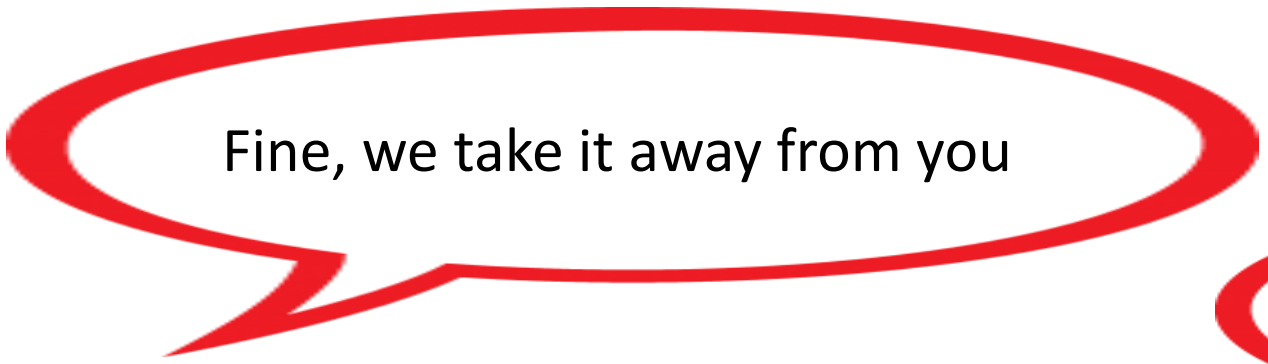
1. **Throttle Bandwidth:** ISPs can limit the rate at which data is transferred from or to a user.
2. **Prioritizes traffic :** ISPs can prioritize certain types of data over others. For example, they might prioritize video streaming or gaming data over less time-sensitive data types like emails or file downloads Quality of Service (QoS).
3. **Drop Packets:** When networks become congested, ISPs can selectively drop packets from users who are using a lot of bandwidth. This forces the TCP congestion control mechanism to reduce the rate at which data is sent, freeing up bandwidth for other users.

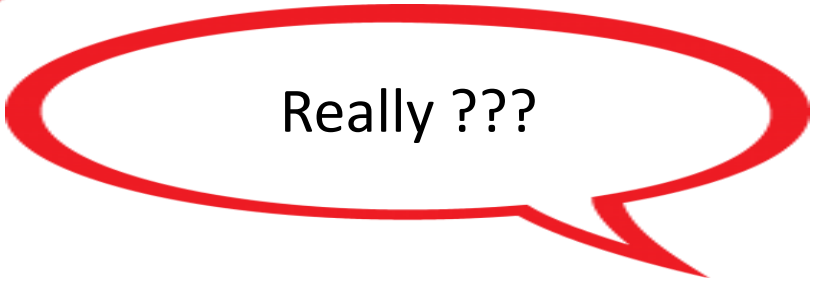
Applications be like …

A 20 YEAR CONVERSATION IN 10 SECONDS







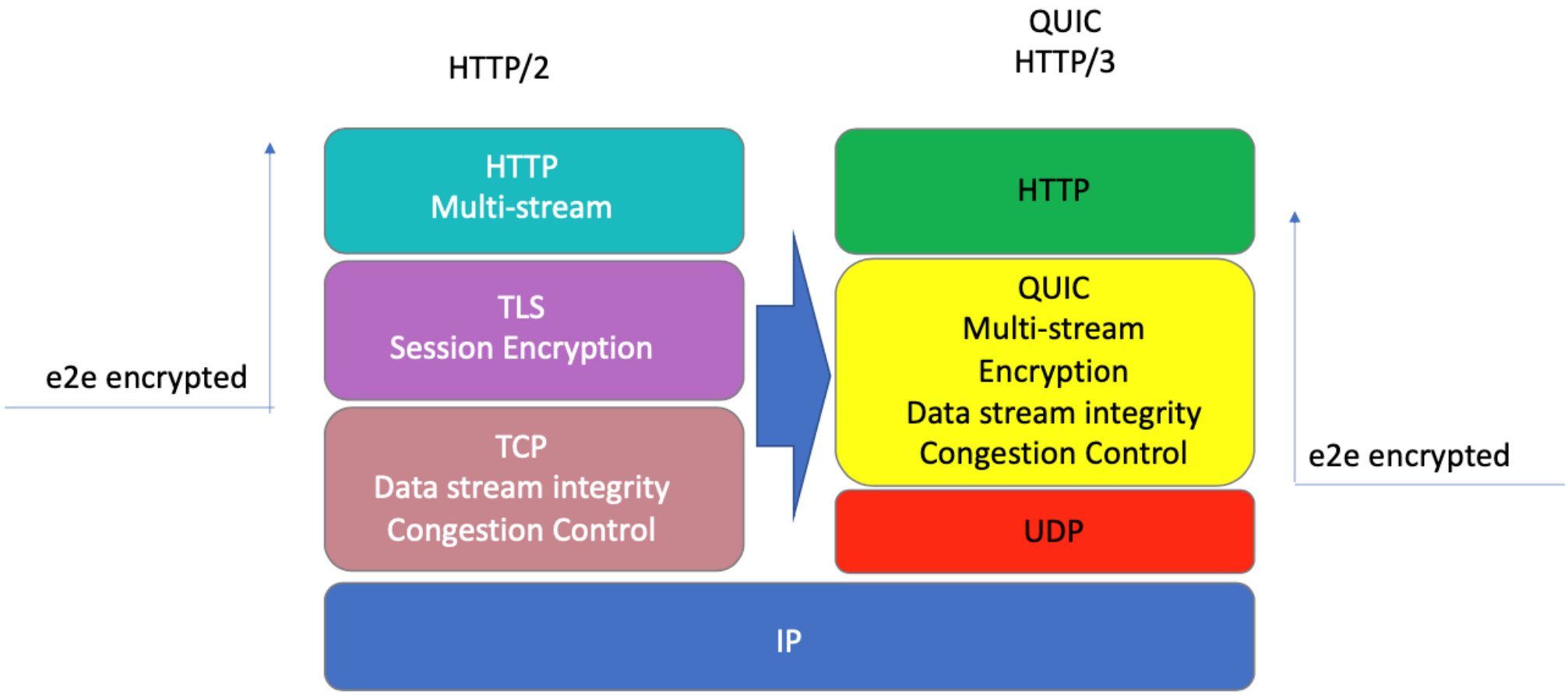


Quic 2012

1. Reduce Latency: One of the primary objectives was to reduce connection establishment time. QUIC aims for **zero-latency connection establishment** in the best case.
2. Improved Congestion Control: QUIC uses **advanced congestion control mechanisms** to adapt well in different internet conditions.
3. QUIC allows **multiple streams with simultaneous transmission**, ensuring that a lost packet in one stream does not affect the others.
4. Forward Error Correction: QUIC adds redundancy to **avoid retransmission of lost packets**, this prevents delays due to packet loss.
5. Secure and Encrypted: QUIC is designed to have a secure and encrypted communication. The aim was to make it **infeasible for any middle-man to tamper with the communication.**
6. Connection Migration: QUIC is designed to seamlessly support migration of connections to new client IP addresses, **helping mobile devices that switch from Wi-Fi networks to cellular** networks and vice-versa.
7. Quick & Efficient Updates: The QUIC protocol is equipped to transition quickly to newer versions and implement feature updates efficiently whenever it is required.

actual picture of the developer

The birth of QUIC 2012



Quick UDP Internet Connections

H3 QUIC/TLS/DoH/eSNI
THE NEW NORMAL

Content Delivery Security Privacy Loadbalancing App Infrastructure App Experience

QUIC in 3 bullet points

- **End-to-End Flow Control**: Unlike TCP, which allows ISPs to manipulate the flow of data, QUIC proposes end-to-end flow control. This means only the sender and the receiver – **not any of the ISPs in between** – can control the data flow
- **Improved Speed**: QUIC reduces the time needed to make a connection, decreasing latency. This is especially beneficial in **mobile connections**, where high packet loss and high latency are commonplace.
- **Encrypted Traffic**: QUIC's encryption provides more privacy to users and makes it harder for ISPs to analyze packets and manage traffic based on what they carry. **All QUIC traffic is encrypted, so ISPs cannot throttle the flow based on its content**.

TLS 1.3

1. **Encryption**: TLS 1.3 provides enhanced end-to-end security by encrypting the data transmitted between two devices. It ensures that any communication between a client and a server remains confidential and tamper-proof.
2. **Authentication**: TLS 1.3 verifies the identity of the parties involved in communication. It uses digital certificates to validate the authenticity of a website or server, which helps prevent phishing attacks and potential misinterpretations of identity.
3. **Performance**: TLS 1.3 has made **significant improvements in terms of performance**. It requires fewer round trips to establish a secure connection, resulting in faster fully encrypted connections.
4. **Forward Secrecy**: Unlike the previous versions, TLS 1.3 supports forward secrecy by default. This means that even if a session key is compromised, the attacker **cannot decrypt past session data**.
5. **Simplified Protocol**: TLS 1.3 has removed some of the older, less secure cryptographic features and algorithms, making it less complicated and reducing the chances of implementing it incorrectly.
6. **Improved Privacy**: TLS 1.3 **encrypts more of the negotiation handshake** to protect it from eavesdroppers. This includes the "finished" message that verifies the key exchange and authentication succeeded.

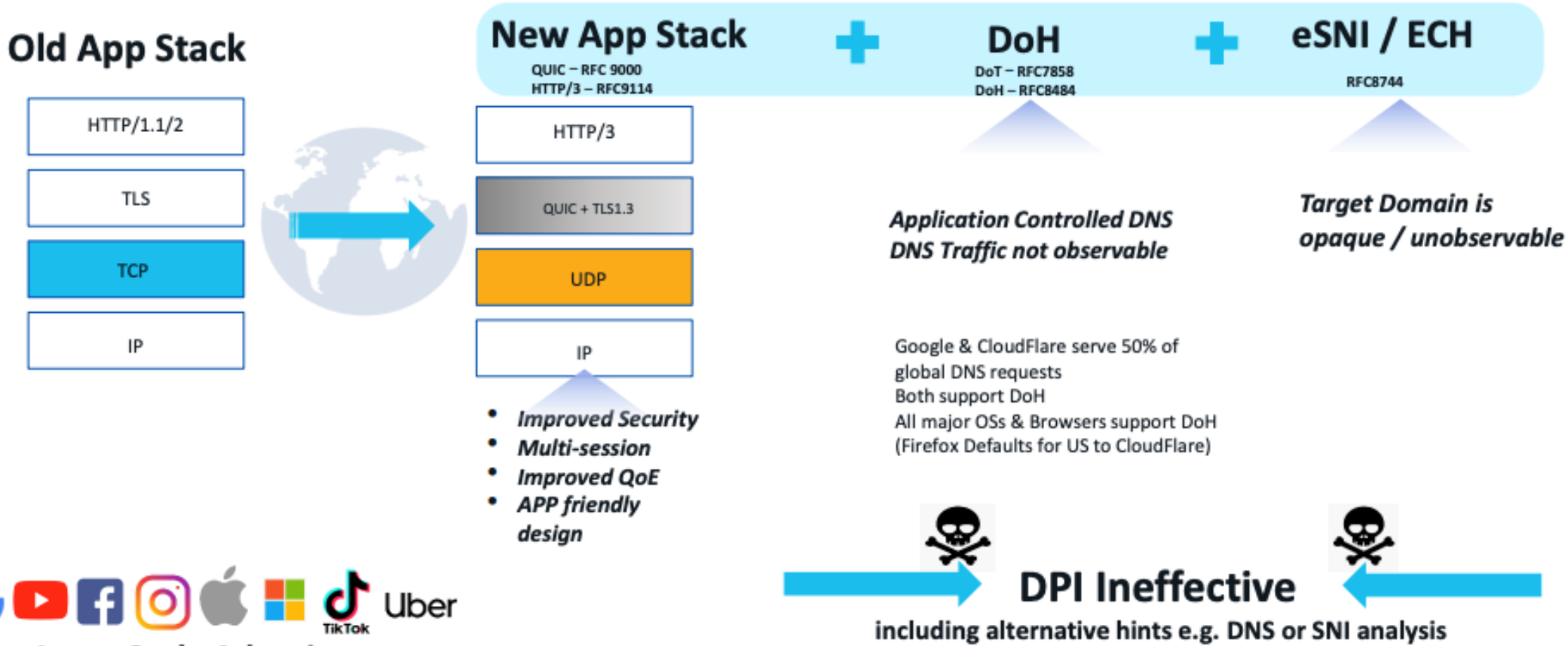
DNS over HTTPS (DoH)

- DNS over HTTPS (DoH) is a protocol that encrypts and secures communication between a user's computer and a DNS server, using HTTPS to increase privacy and security.
- DoH works by sending DNS requests over an encrypted HTTPS connection to a DoH-capable DNS server (a DoH resolver). This means that third parties, such as internet service providers (ISPs), can't see which websites a user is visiting.
- It serves two main purposes
  1. Privacy: It prevents internet service providers and potential eavesdroppers from viewing your DNS queries and thus your browsing history.
  2. Security: It helps prevent DNS spoofing attacks, where an attacker hijacks DNS queries and redirects the user to a malicious website.

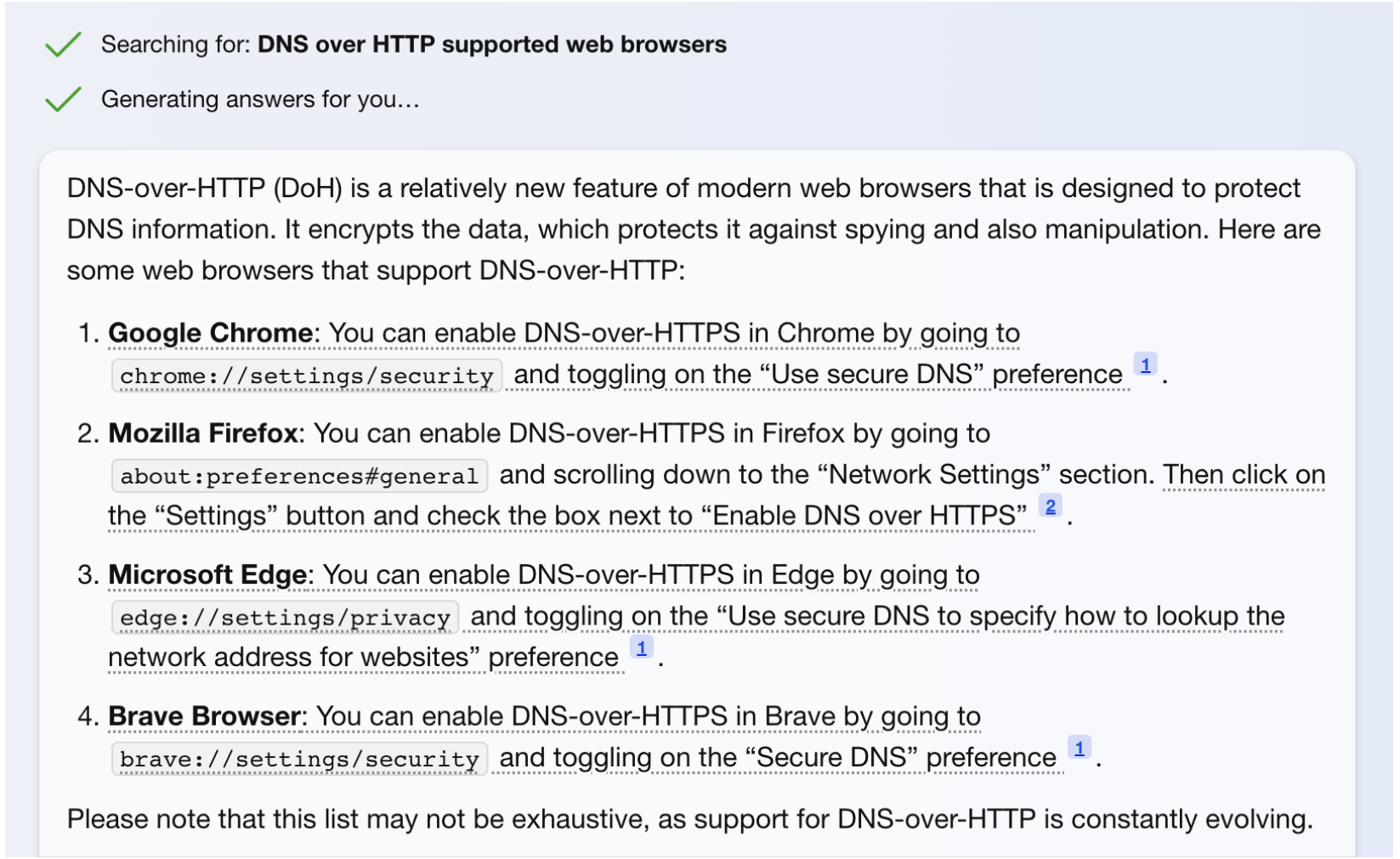
eSNI

- Extended Server Name Indication (eSNI) is a mechanism that allows a server to **present multiple certificates on the same IP address and TCP port number**. It is an extension to the existing Server Name Indication (SNI), a protocol for indicating what hostname the client is attempting to connect to during handshaking process.
- eSNI enhances the privacy and security level of users by keeping their online activities private from unwanted scrutiny or attacks. In the **original** SNI mechanism, **the hostname is sent in plaintex**t which could be easily seen and exploited.
- eSNI helps to address this issue by encrypting the SNI information, making the browsing activities of users less visible to those monitoring network traffic.

HTTP/3 = QUIC + TLS + DoH + eSNI



Bing, in which web browser is DNS over HTTP supported?



✓ Searching for: **DNS over HTTP supported web browsers**

✓ Generating answers for you…

DNS-over-HTTP (DoH) is a relatively new feature of modern web browsers that is designed to protect DNS information. It encrypts the data, which protects it against spying and also manipulation. Here are some web browsers that support DNS-over-HTTP:

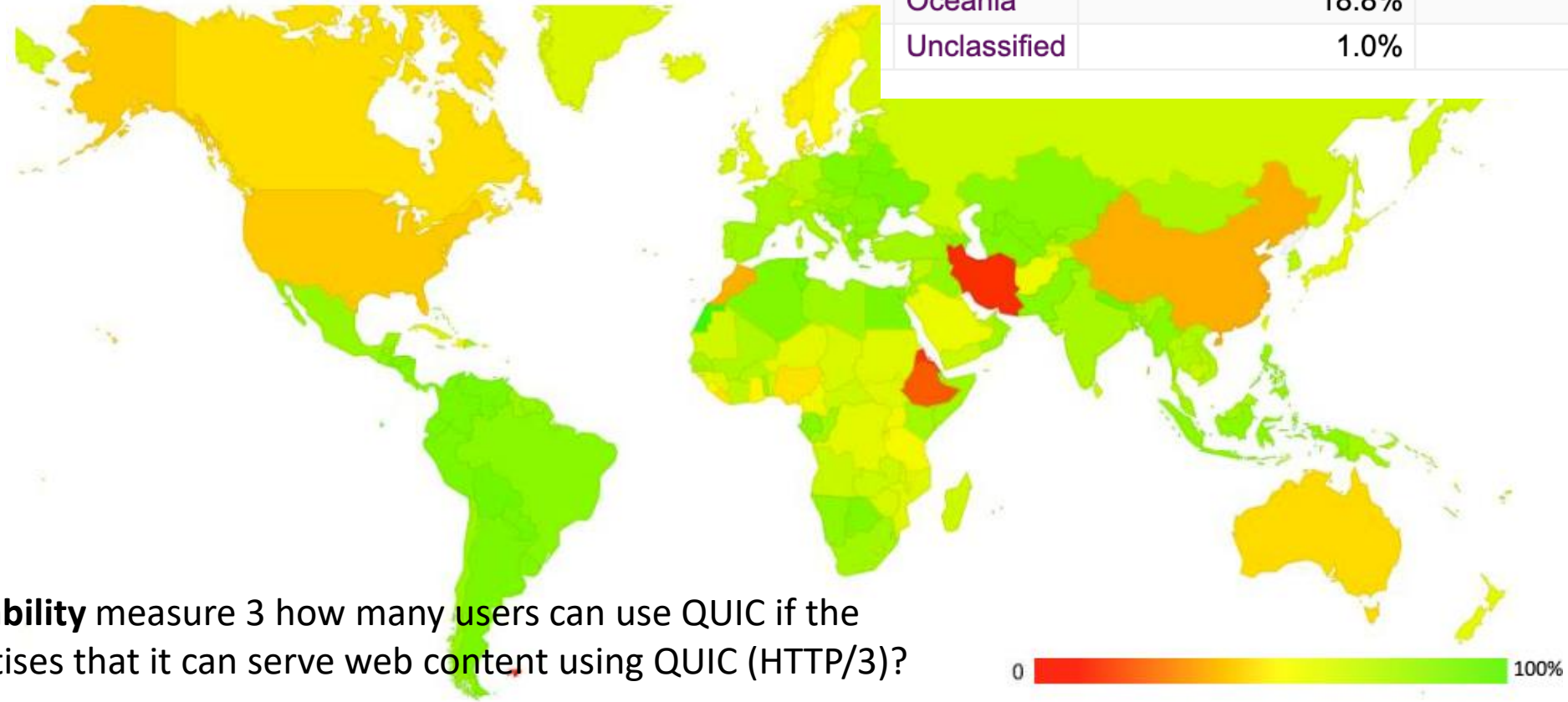
1. **Google Chrome**: You can enable DNS-over-HTTPS in Chrome by going to `chrome://settings/security` and toggling on the "Use secure DNS" preference [1].
2. **Mozilla Firefox**: You can enable DNS-over-HTTPS in Firefox by going to `about:preferences#general` and scrolling down to the "Network Settings" section. Then click on the "Settings" button and check the box next to "Enable DNS over HTTPS" [2].
3. **Microsoft Edge**: You can enable DNS-over-HTTPS in Edge by going to `edge://settings/privacy` and toggling on the "Use secure DNS to specify how to lookup the network address for websites" preference [1].
4. **Brave Browser**: You can enable DNS-over-HTTPS in Brave by going to `brave://settings/security` and toggling on the "Secure DNS" preference [1].

Please note that this list may not be exhaustive, as support for DNS-over-HTTP is constantly evolving.

Browser support

https://stats.labs.apnic.net/quic

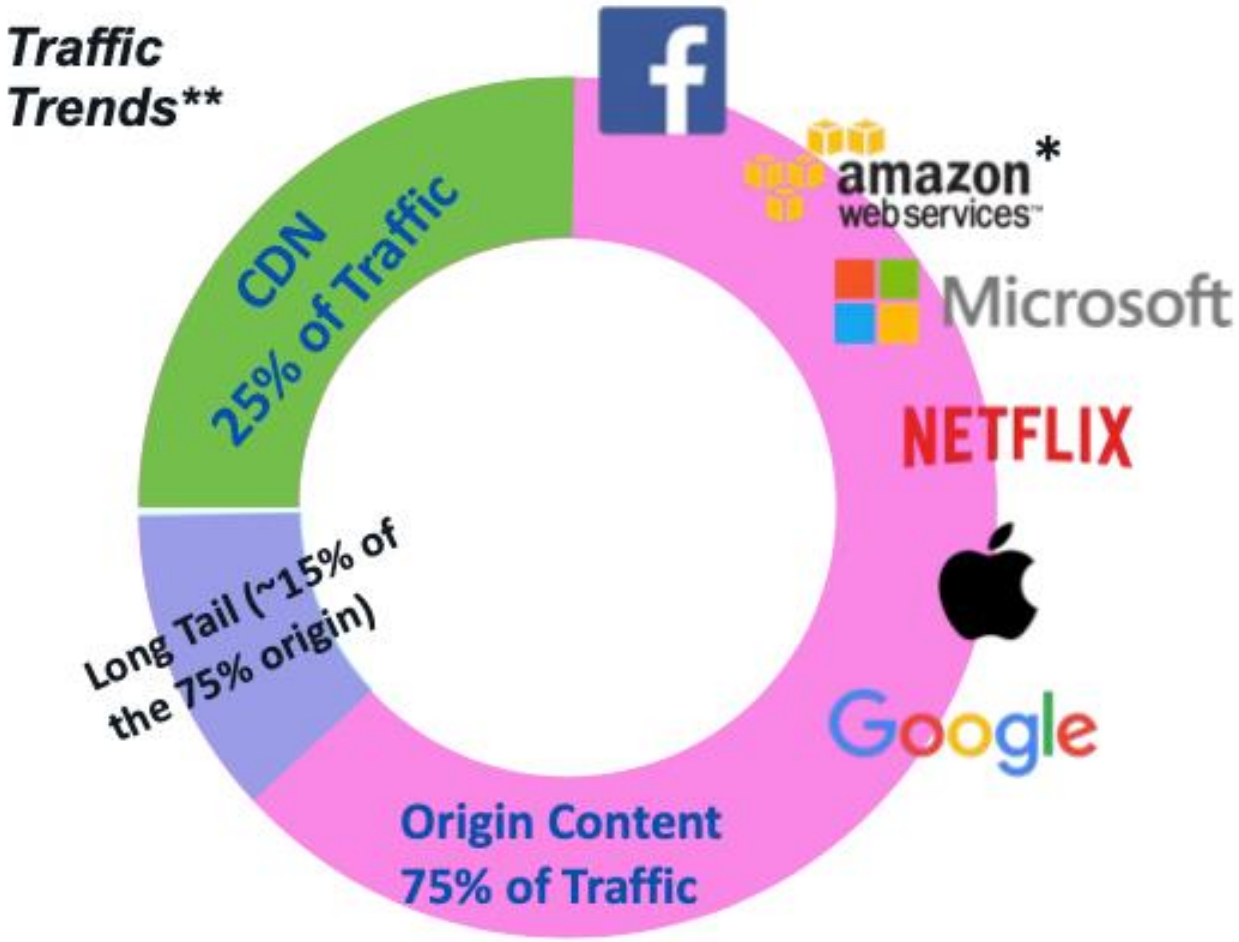
Region	HTTP/3 on First Query	HTTP/3 on Second Query
World	6.1%	62.1%
Africa	3.8%	68.4%
Americas	11.5%	68.6%
Asia	3.8%	56.0%
Europe	10.2%	76.6%
Oceania	18.8%	51.0%
Unclassified	1.0%	34.7%



This is a **capability** measure 3 how many users can use QUIC if the server advertises that it can serve web content using QUIC (HTTP/3)?

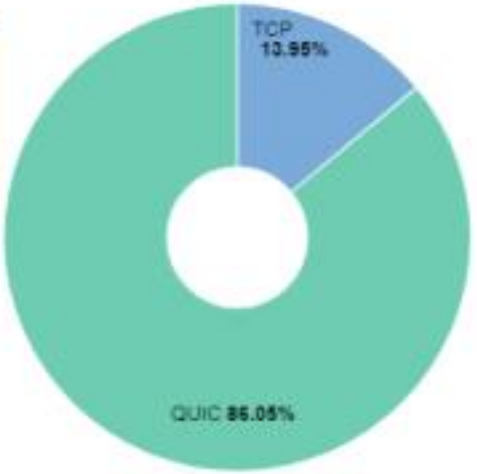
QUIC THE NEW NORMAL

- 12 Cloud Domains
  = >80% of the Volume
- 6 of 12 Cloud Origin Content Domains have their own CDNs and/or Secure DNS plans
- 10 of 12 Cloud Domains
  Are implementing HTTP/3 + QUIC plans



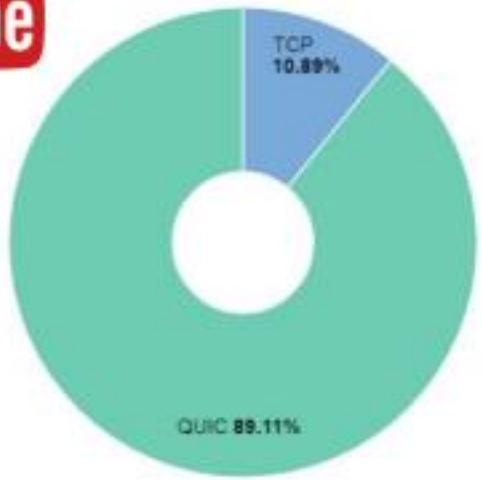
Top5 apps 4/5 are on QUIC

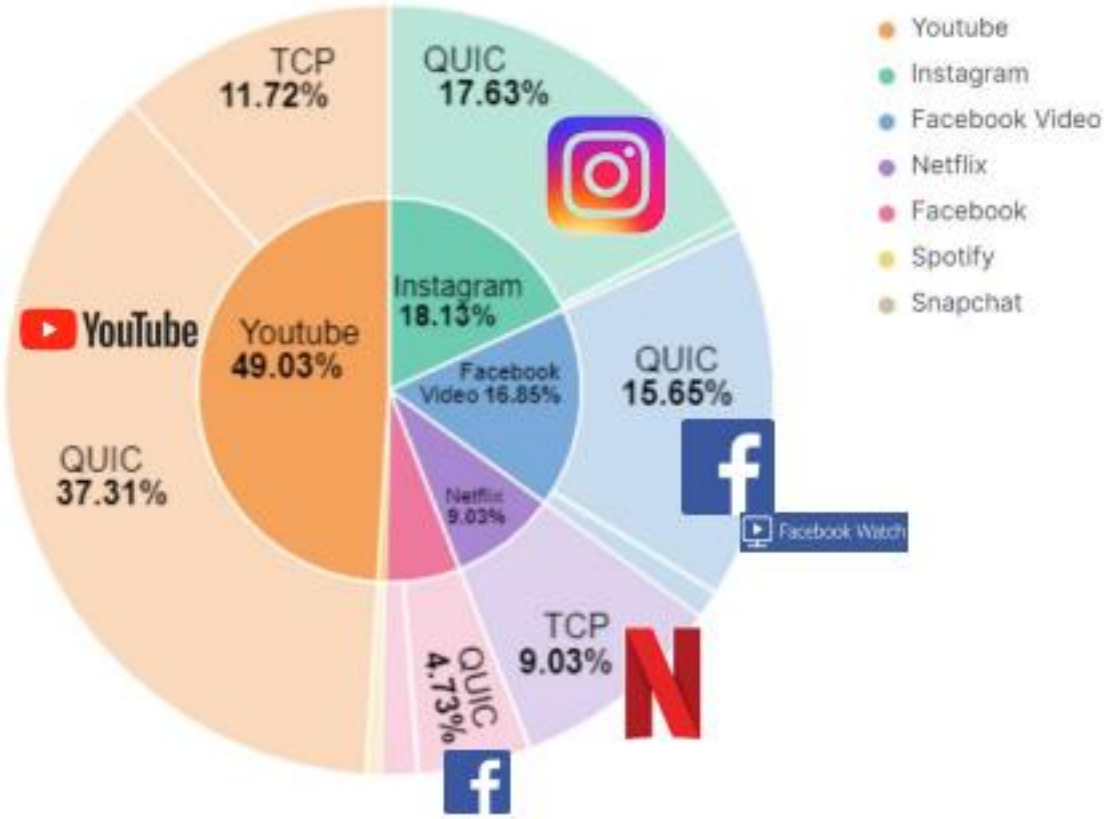
QUIC : 86%



YouTube

QUIC : 90%

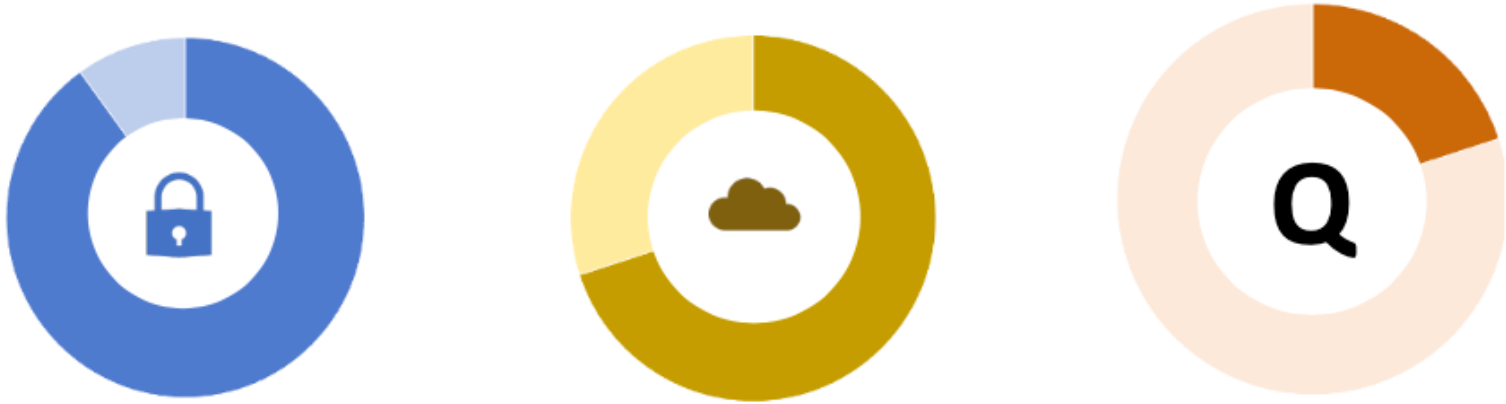




May 2023

The winner is ….

- More than 90% of all Internet traffic uses encrypted payloads
- More than 70% of all Internet traffic is sourced from Cloud servers
- More than 20% of all traffic by volume uses QUIC (2x in 18month)



we don't really need your permission networks

listen guys …

we got both ends …