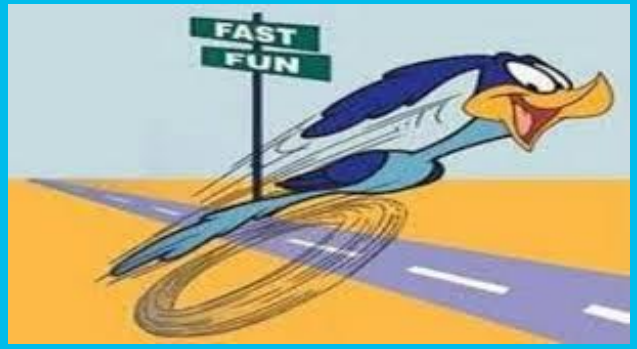


QUIC

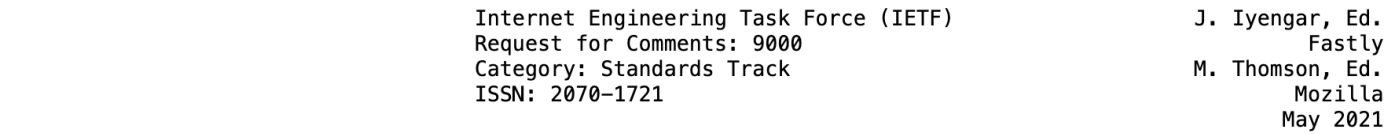
The New, Encrypted Protocol Stack @Internet & (How to Deal with it)

Dejan Jakšić, Cisco

1st NOGhr-meetup, 10.11.2022.

A bit of QUIC history

- In 2012, Google started working on QUIC (as alternative to TCP+TLS+HTTP/2)
- In 2014, Chrome started a wide-scale deployment of Google QUIC (gQUIC)
- In 2015, Google brought QUIC to the IETF
- In 2017, the IETF started creating versions of QUIC that diverged from Google QUIC (those new versions were then called IETF QUIC)
- In 2020, Chrome started wide-scale experiments with IETF QUIC
- In 2021, the IETF officially published QUIC as:
  - **RFC 9000** - UDP-Based Multiplexed and Secure Transport

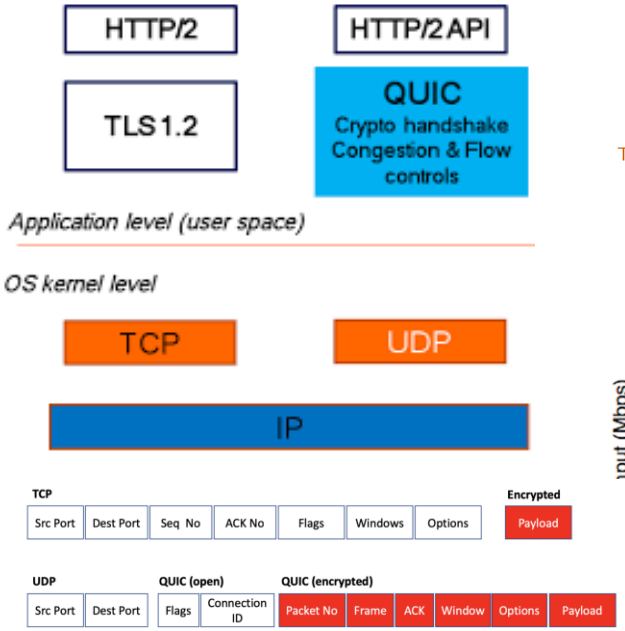


Internet Engineering Task Force (IETF) J. Iyengar, Ed.
Request for Comments: 9000 Fastly
Category: Standards Track M. Thomson, Ed.
ISSN: 2070-1721 Mozilla
May 2021

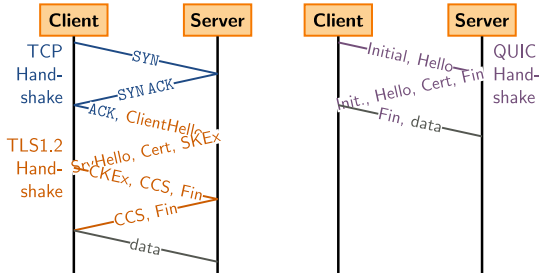
QUIC: A UDP-Based Multiplexed and Secure Transport

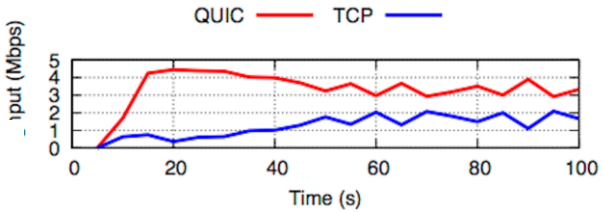
QUIC = Quick UDP Internet Connection

IETF RFC 9000 – The new “TCP”

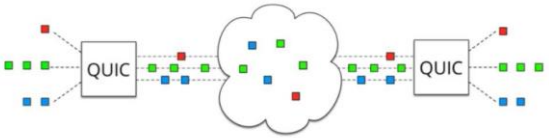


User Space
TLS 1.3 Encrypted

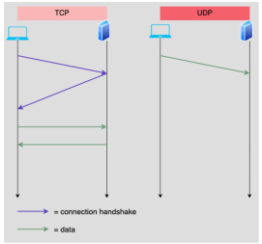




Fast and furious



Deliver at all cost with multi-stream (Multiplex, no-HOL)



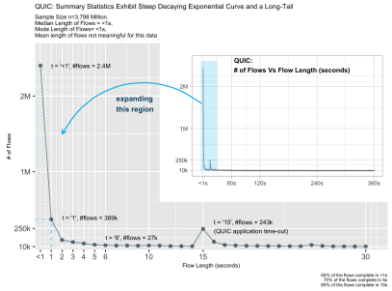
UDP is ”fire and forget”
App controls the rest

[A look at QUIC Use]

HOL = Head Of Line blocking

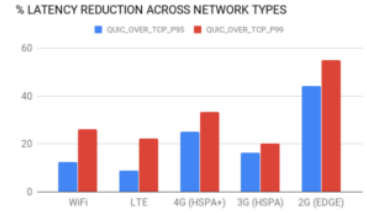
Moves Control of the User Experience to the App

Apps do not play nice – they will deliver over everyone else

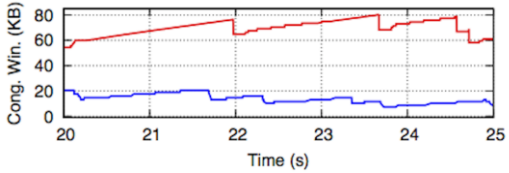


70% of interactions complete in <5s**

Scenario	Flow	Avg. throughput (std. dev.)
QUIC vs. TCP	QUIC	2.71 (0.46)
	TCP	1.62 (1.27)
QUIC vs. TCPx2	QUIC	2.8 (1.16)
	TCP 1	0.7 (0.21)
	TCP 2	0.96 (0.3)
QUIC vs. TCPx4	QUIC	2.75 (1.2)
	TCP 1	0.45 (0.14)
	TCP 2	0.36 (0.09)
	TCP 3	0.41 (0.11)
	TCP 4	0.45 (0.13)

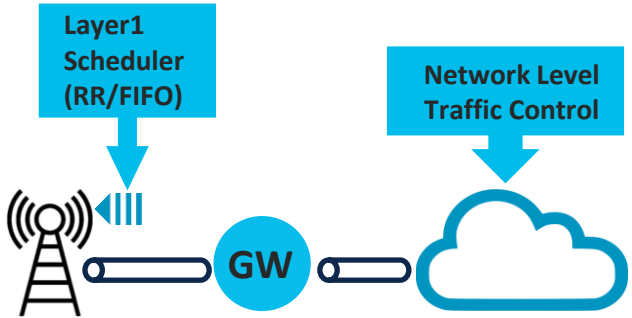


The poorer the network, the better the improvement*



QUIC is "Unfair"* - grab what you can – remember BitTorrent?**

Impacted Areas (fixed networks also)



QUIC goal = application performance!

*Uber engineering;**Cisco Analysis, cust.data;***APNIC study

Trigerring QUIC

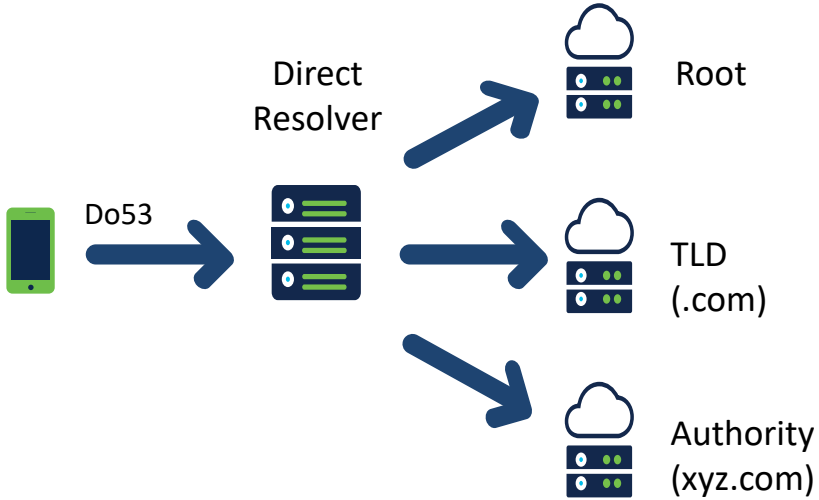
- Two mechanisms available for server to signal to the client:
- **What?**
  - Ability to support HTTP/3 session using QUIC
- **How?**
  - An Alternative Service directive in the HTTP content header, namely: Alt-Svc: h3=":443" (eg. Chrome)
  - A URL domain name with a defined HTTPS RR Type which value is: alpn="h3" (eg. Safari)
- Check APNIC lab study

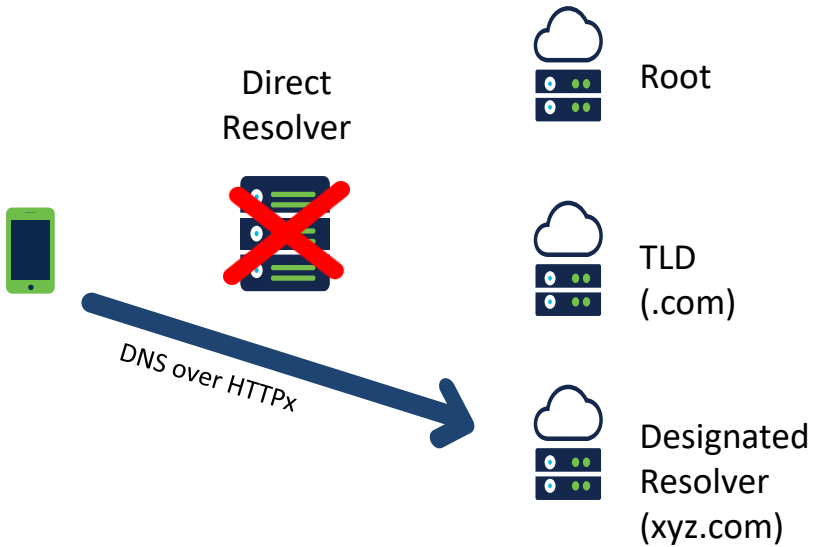
Check support:
https://http3check.net/

ALPN = Application layer Potocol Negotiation

Secure DNS – Directory lookup Privacy by default

DoH - RFC8484 is becoming mainstream





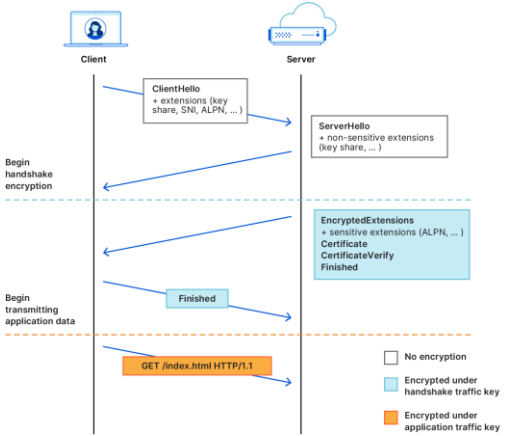
From: DNS Hierarchy + cleartext fields

To: DNS (direct) Connect + ciphered fields

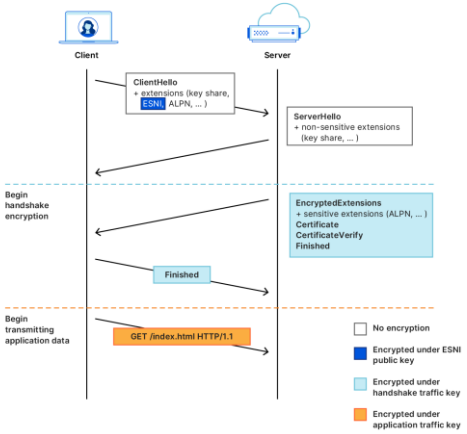
+ DNS is controlled by Applications

Hiding the destination completely - eSNI & ECH

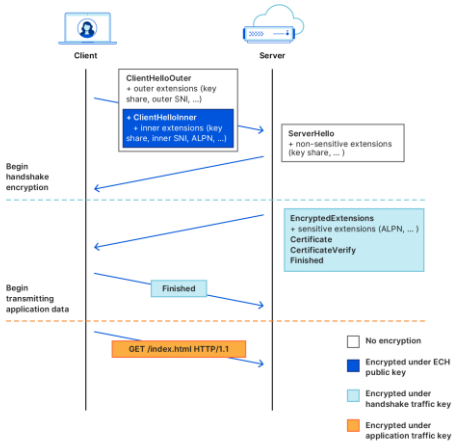
RFC6066



RFC8744



draft-ietf-tls-esni-14



Classic SNI**

Destination & Capabilities in the clear

eSNI

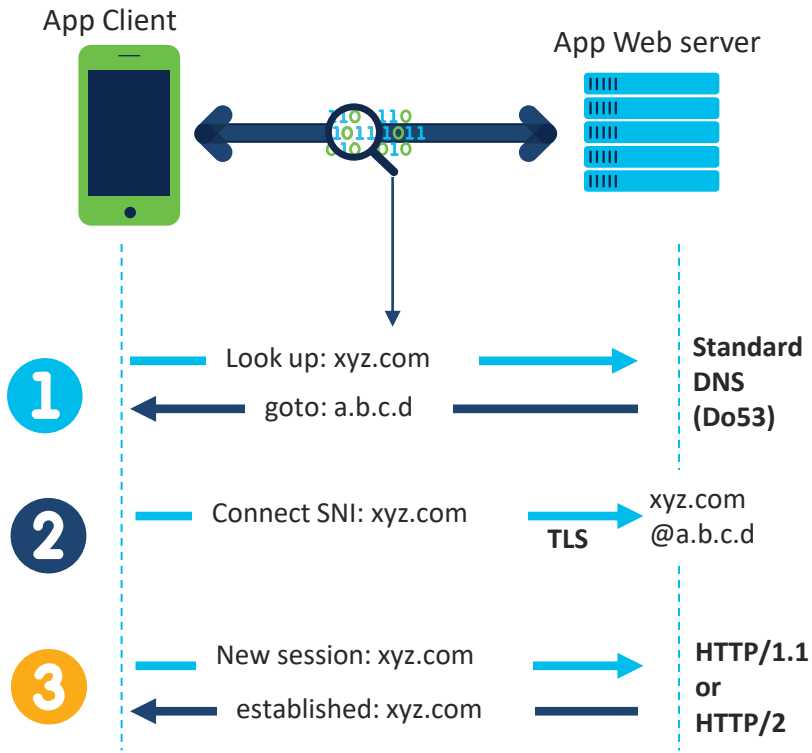
Destination leaked via DNS
ALPN still in the clear*

ECH***

Only CDN address visible – DoH
SNI & Capabilities fully encrypted

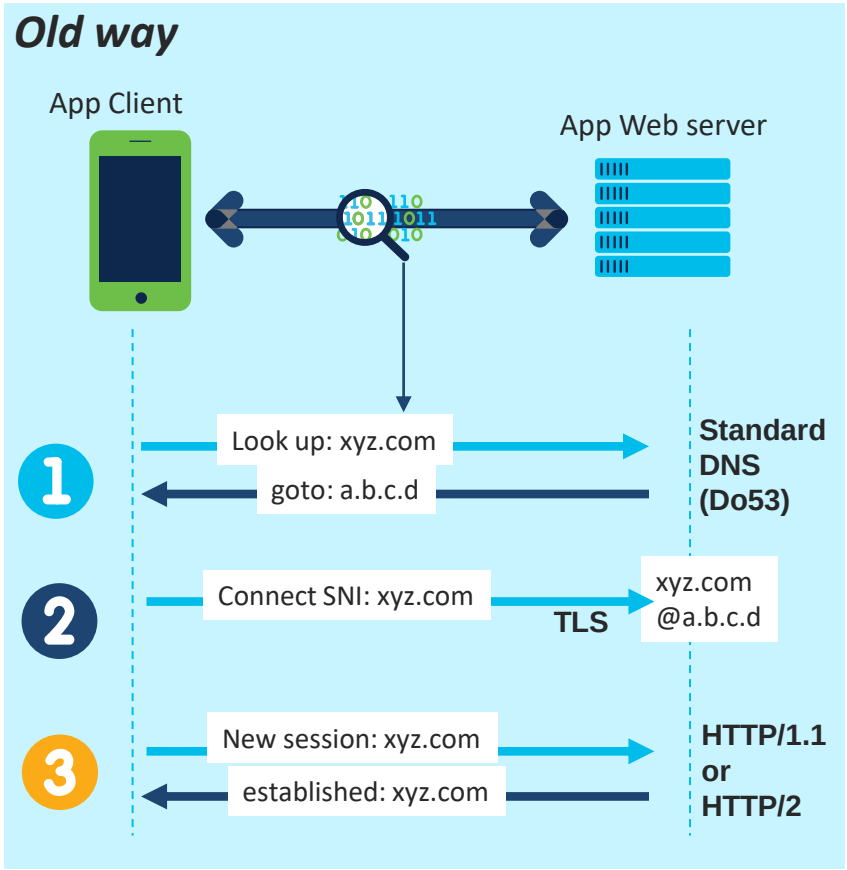
*ALPN = Application layer Potocol Negotiation **SNI = Server Name Indication, ***ECH = Encrypted Client Hello

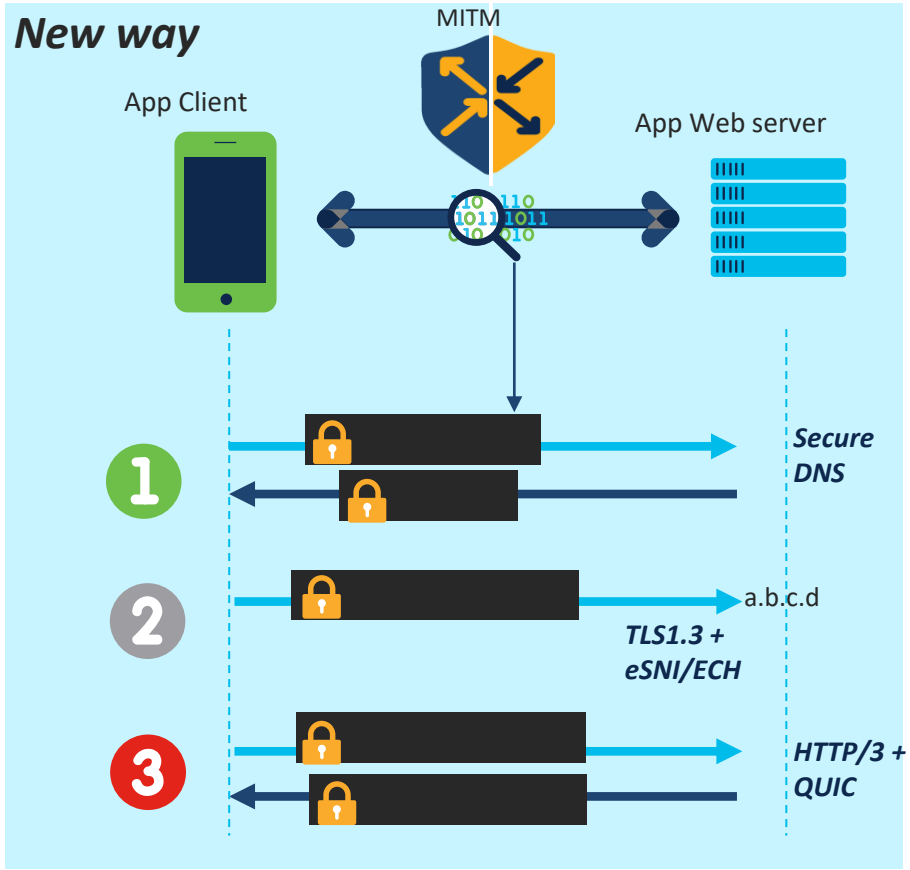
Bringing this all together – well known…



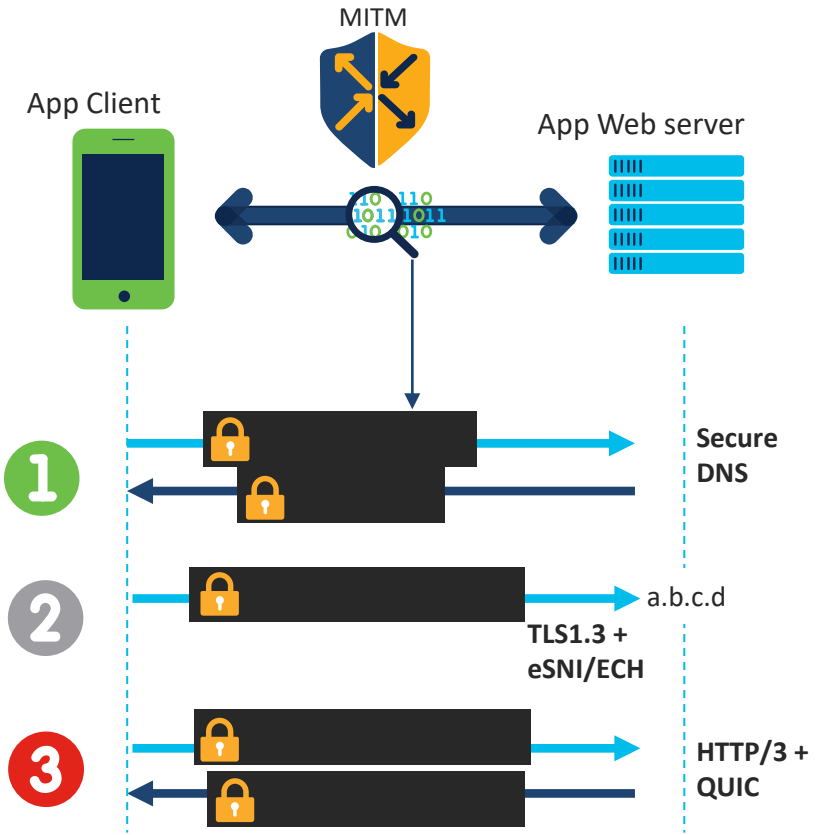
- ✔ Well-understood protocol stack
- ✔ Foundation of **all** web traffic
- ✔ Adopted by Applications
- ✔ Globally scaled

…Today - Visibility is lost





HTTP/3 and QUIC multi-session technology



The Internet Reality – around 2020

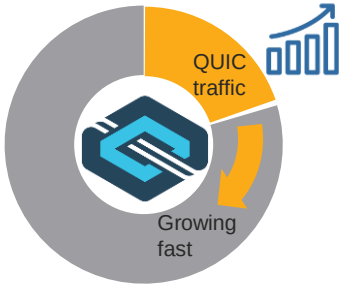
>90% of Volume encrypted

>70% of volume To Cloud

10 Cloud sites
"Elephant destinations" not "Elephant flows"

~50% of Flows DNS

>20% of Traffic QUIC



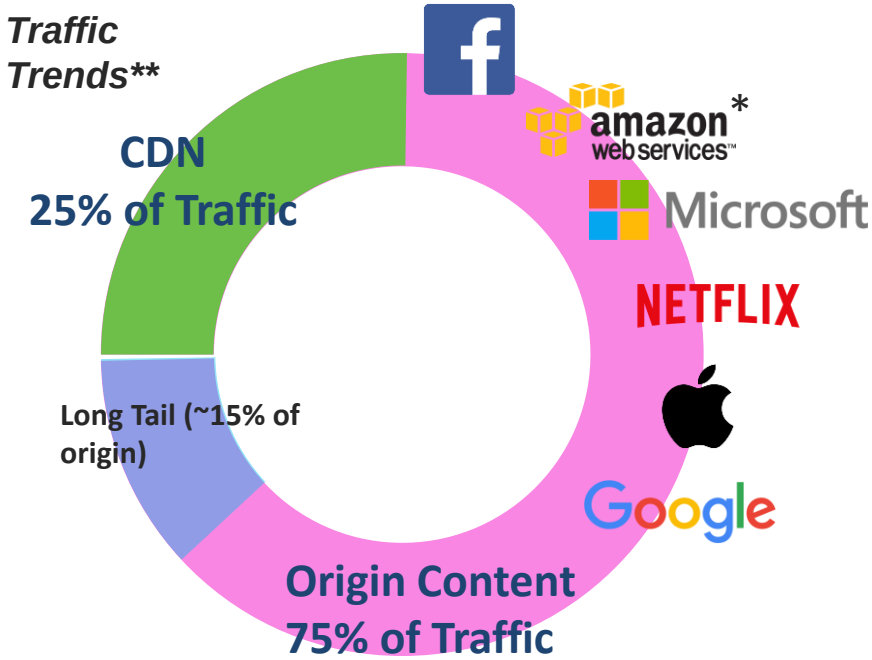
Many small flows
Micro-sessions

- **Destination:** all-encrypted world
- **Cloud:** concentrating the Internet

- **Content:** DNS is the load-balancer
- **QUIC:** Future Protocol of choice

The Internet is converging on a new normal

In 2021 HTTP/3 became “rocket fuel”



- **10 of 12 Cloud Domains Are implementing HTTP/3 + QUIC plans**
- **6 of 12 Cloud Origin Content Domains have their own CDNs and/or Secure DNS plans**
- **12 Cloud Domains = >80% of the Volume**
- **130 Primary Domains = 95% of the Internet**

Widespread Impact :
Architecture, Network, Devices, Standards *and* Value-chain

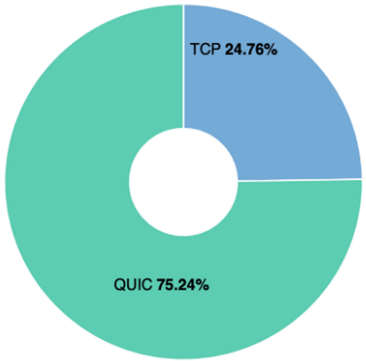
**Consumer Traffic Analysis

* Amazon own ~1% of public IPv4

Fast forward 18 months - Tier-1 Mobile Carrier

YouTube

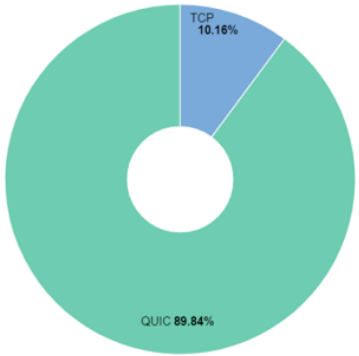
volume



QUIC is "default"

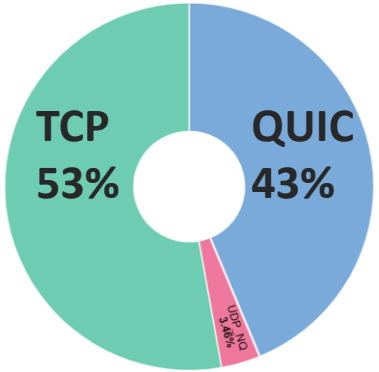
Meta

Volume



Meta is going full QUIC

Overall Volume

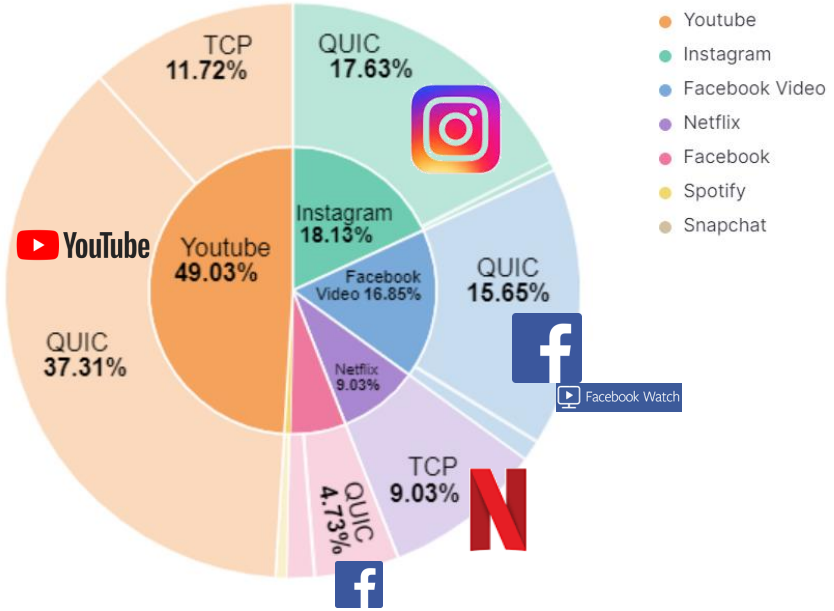


QUIC has doubled in 18 months

QUIC is 43% of total and rising

(snapshot 11/2/2022)

Top 5 Apps – QUIC is dominant
80/20 rule now

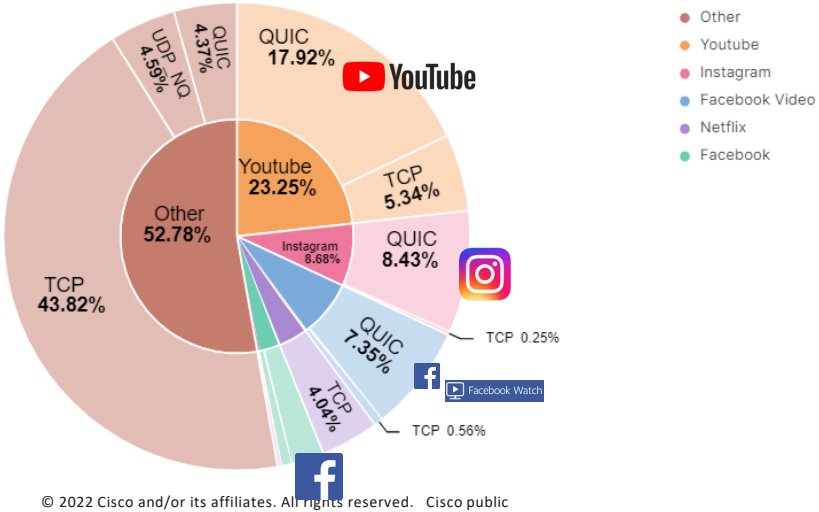


April 10 2022

Network Traffic by Volume and Flows

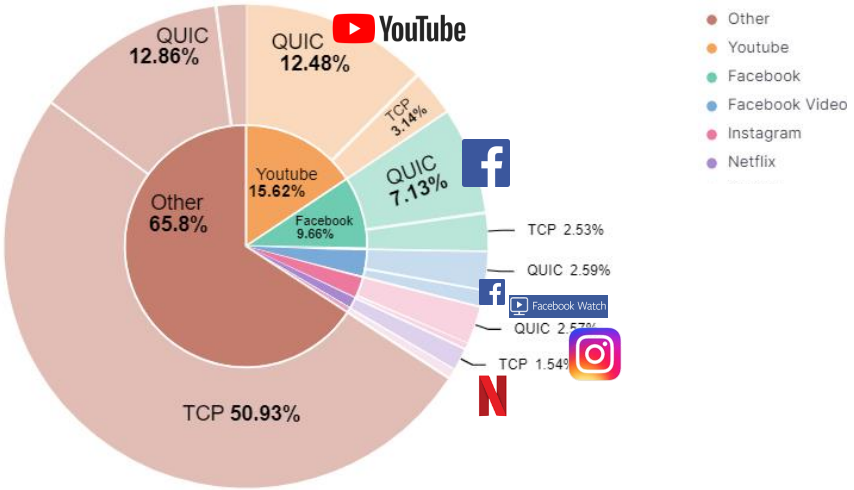
Overall Volume by Apps

Big 5 is 48% of traffic
QUIC is 40% of traffic
"other traffic" still largely TCP, QUIC now visible (4.3%).



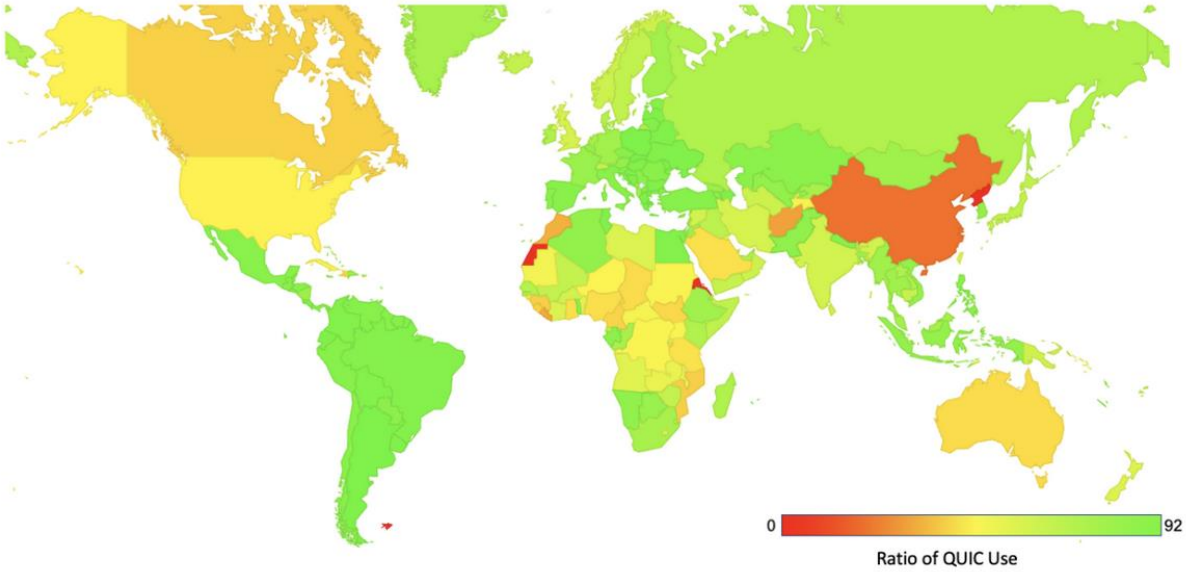
Total Flows by Apps

Lots of TCP sessions (likely IOT related, transactional related)
Big 5 QUIC sessions are very targetted and high efficiency (video related behaviour)



HTTP/3 use by country

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



1.95 s
260 ms
18 ms
15 ms
14 ms
17 ms
345 ms
24 ms
24 ms
24 ms
25 ms
24 ms
21 ms
21 ms
21 ms

Figure 5 — QUIC use per economy, August 2022.

QUIC/H3/DOH stack is in business

Content Delivery **Security** **Privacy** **Loadbalancing** **App Infrastructure** **App Experience**

An application driven global transition

HTTP/3 Stack = UDP+QUIC+TLS

Large Scale Adoption

Old App Stack

- HTTP/1.1/2
- TLS
- TCP
- IP

New App Stack

QUIC – RFC 9000
HTTP/3 – RFC9114

- HTTP/3
- QUIC + TLS1.3
- UDP
- IP

- ***Improved Security***
- ***Multi-session***
- ***Improved QoE***
- ***APP friendly design***

DoH

DoT – RFC7858
DoH – RFC8484

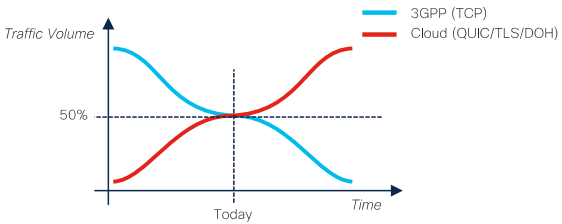
Application Controlled DNS
DNS Traffic not observable

Google & CloudFlare serve 50% of global DNS requests
Both support DoH*
All major OSs & Browsers support DoH (Firefox Defaults for US to CloudFlare)

eSNI / ECH

RFC8744

Target Domain is opaque / unobservable



DPI Ineffective

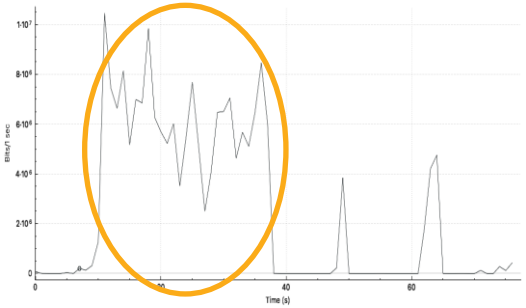
including alternative hints e.g. DNS or SNI analysis

*DOH = DNS over HTTPS

So how do we deal with this Internet evolution?

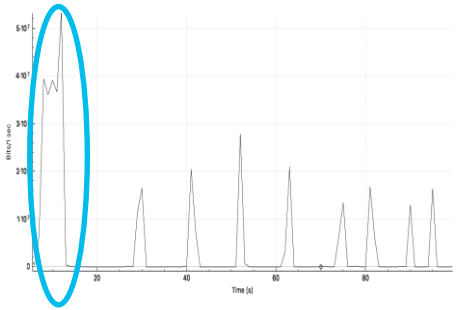
App (e.g. Video) Behavior varies by protocol and use case

TCP Video Stream Detection



TCP based ABR video players prefer **larger, sustained downloads** due to high cost of establishing the TCP session and reducing time spent in TCP slow start.
Often use HTTP/2 connection. (DASH/HLS) to fix HOL.

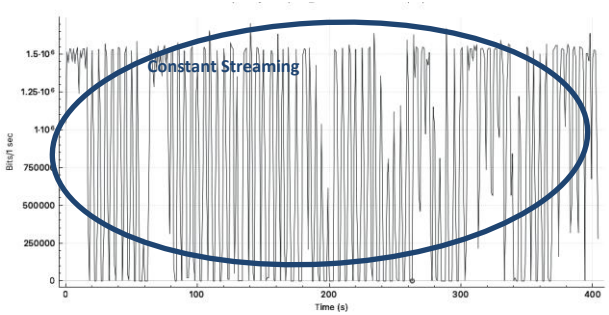
QUIC Video Stream Detection



QUIC based ABR video players prefer requesting **video in smaller chunks**.

Multiple QUIC Streams in many cases to (different) servers

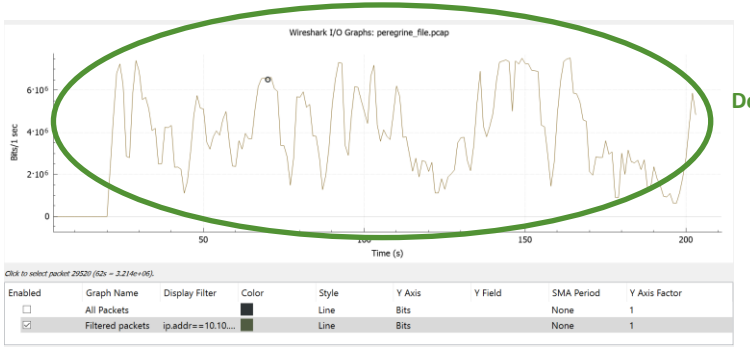
UDP Video Live Stream Detection



UDP based video players are extremely reliant on consistent network performance. Small buffer, sustained troughput
Applications: YouTube Live, WebEx, Microsoft Teams, Zoom

YouTube TV webex by CISCO

zoom

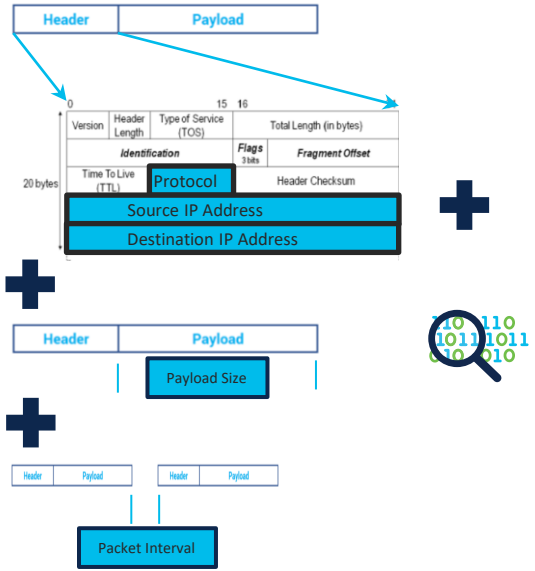


Download Stream Detection

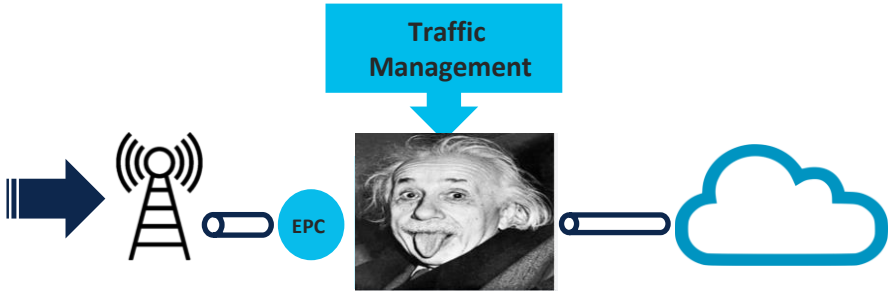
Premium

NETFLIX

The only certain data points are…

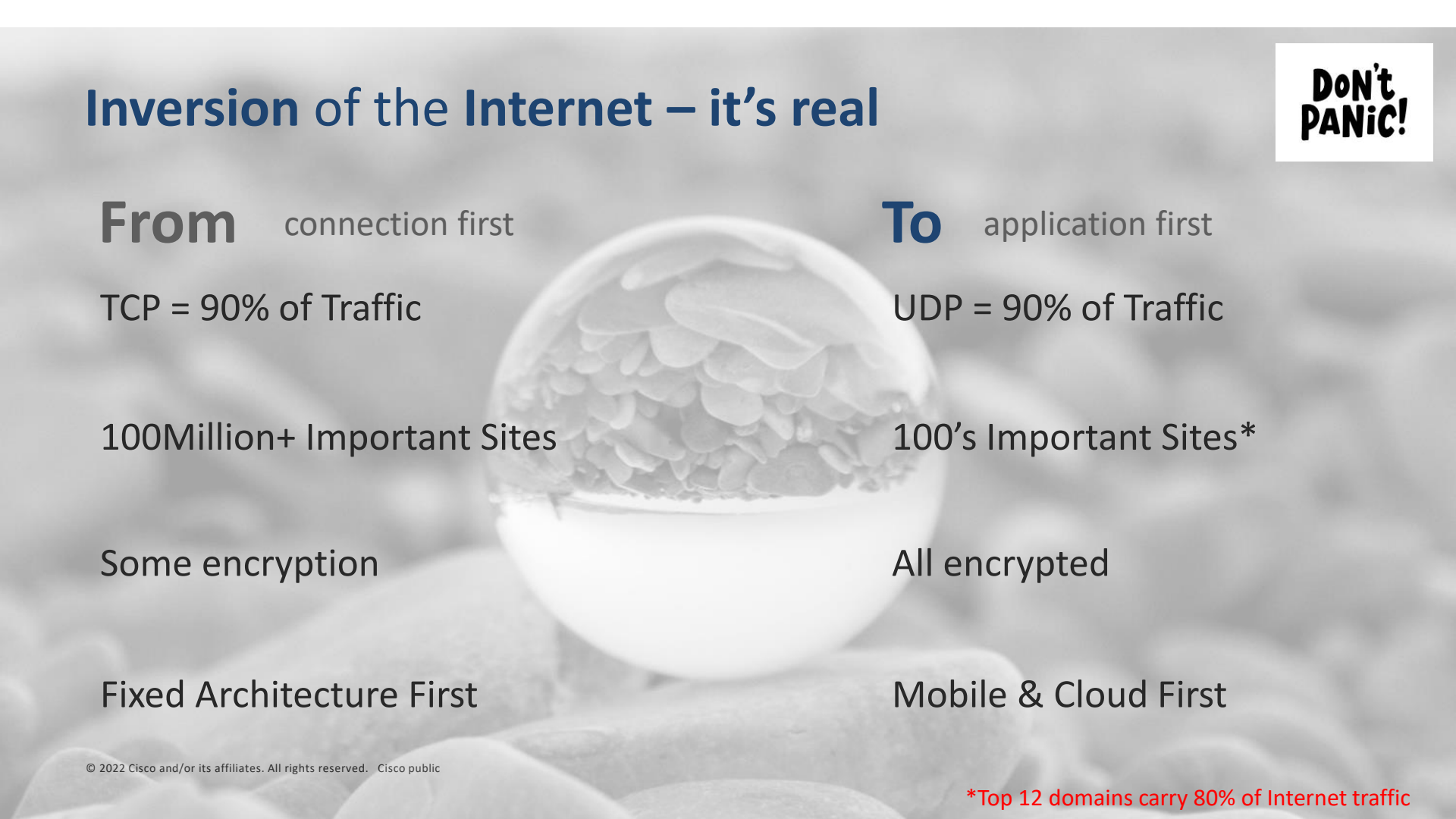


Real Time Algorithms



- Must work with encrypted traffic
- Must work with DOH/any DNS, eSNI & ECH
- Must support QUIC, UDP and TCP

Inversion of the **Internet – it's real**



From connection first	**To** application first
TCP = 90% of Traffic	UDP = 90% of Traffic
100Million+ Important Sites	100's Important Sites*
Some encryption	All encrypted
Fixed Architecture First	Mobile & Cloud First

*Top 12 domains carry 80% of Internet traffic

References...some of them ☺

- Cisco HTTP/3 QUIC measurements (thanks to Andreas and Bart)
- Cisco blogs: https://blogs.cisco.com/tag/quic
- QUIC in general: https://cloudflare-quic.com/
- QUIC use case: https://labs.apnic.net/?p=1626
- 2nd look at QUIC use case: https://blog.apnic.net/2022/09/07/a-second-look-at-quic-use/
- UCLA paper on TCP vs QUIC: https://web.cs.ucla.edu/~lixia/papers/UnderstandQUIC.pdf
- eSNI: https://www.cloudflare.com/learning/ssl/what-is-encrypted-sni/
- Speeding up HTTPS and HTTP/3 negotiation with... DNS: https://blog.cloudflare.com/speeding-up-https-and-http-3-negotiation-with-dns/
- 0-RTT: https://blog.cloudflare.com/even-faster-connection-establishment-with-quic-0-rtt-resumption/
- Uber case study: https://www.uber.com/en-HR/blog/employing-quic-protocol/
- Cloudflare Radar reports: https://radar.cloudflare.com
- …just Google for “QUIC”


Questions?


CISCO