WORKSHOP GARR 2024

NET MAKERS

The New Encrypted Protocol Stack and how to deal with it

Roberta Maglione

Principal Architect - Cisco Systems

Agenda

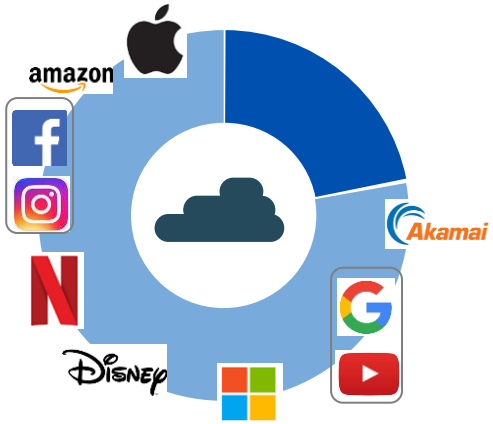
- The New Internet
- The New IP Stack and New Traffic Behaviour
- What is left?
- Summary

The New Internet

The Internet Reality – circa 2020 – Major US

>90% of
Volume: encrypted

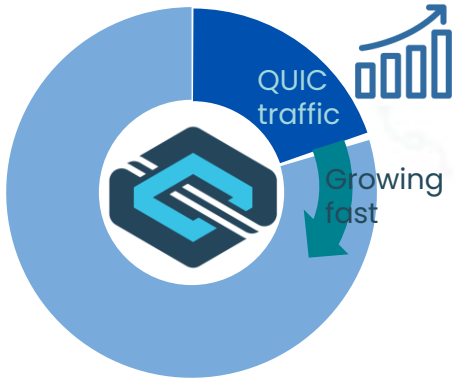
>70% of
Volume: to Cloud



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

~50% of
Flows: DNS

>20% of
Traffic: QUIC



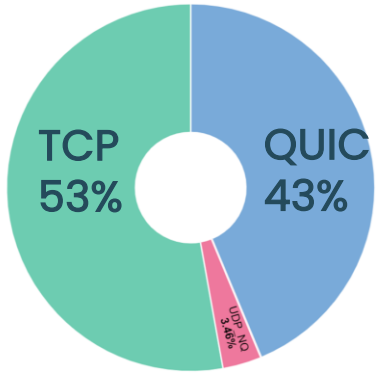
Many small
flows
Micro-sessions

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

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

Fast forward 18 months - Tier-1 EU Mobile Carrier (*)

Overall Volume

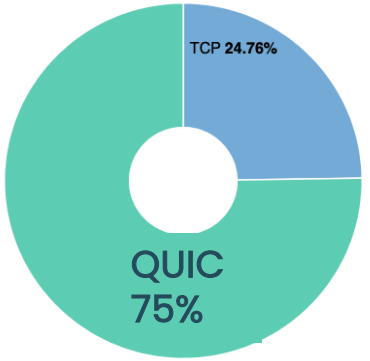


QUIC has doubled in 18 months

QUIC is 43% of total and rising

YouTube

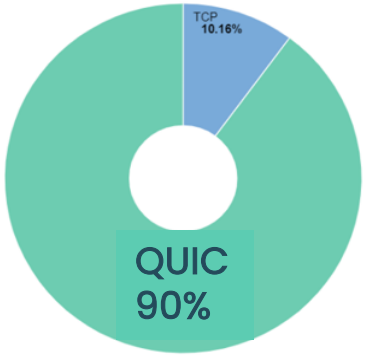
Volume



QUIC is “default”

Meta

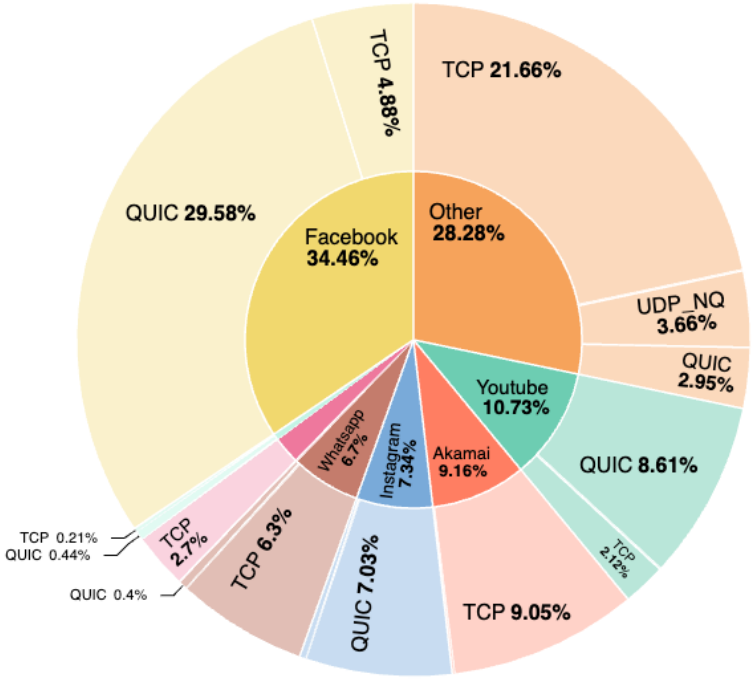
Volume



Meta has gone full QUIC

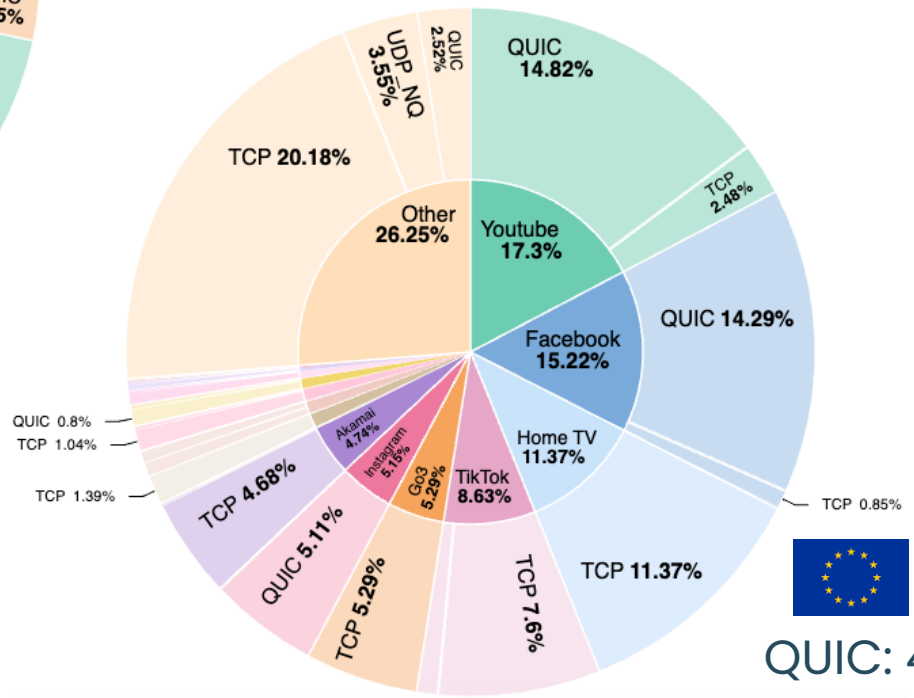
(*) snapshot 11/2/2022

Early 2024 Data: QUIC still going strong



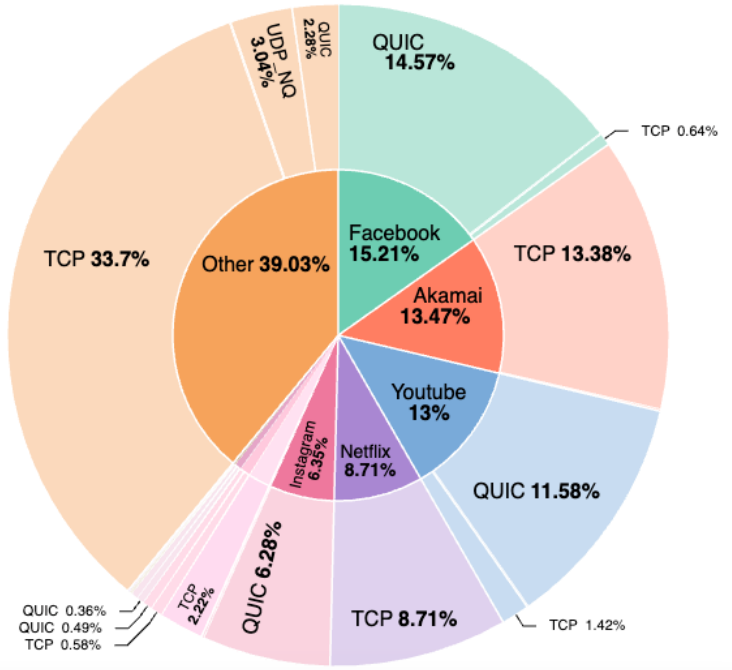
LATAM

QUIC: 47.31%



EU

QUIC: 41.98%

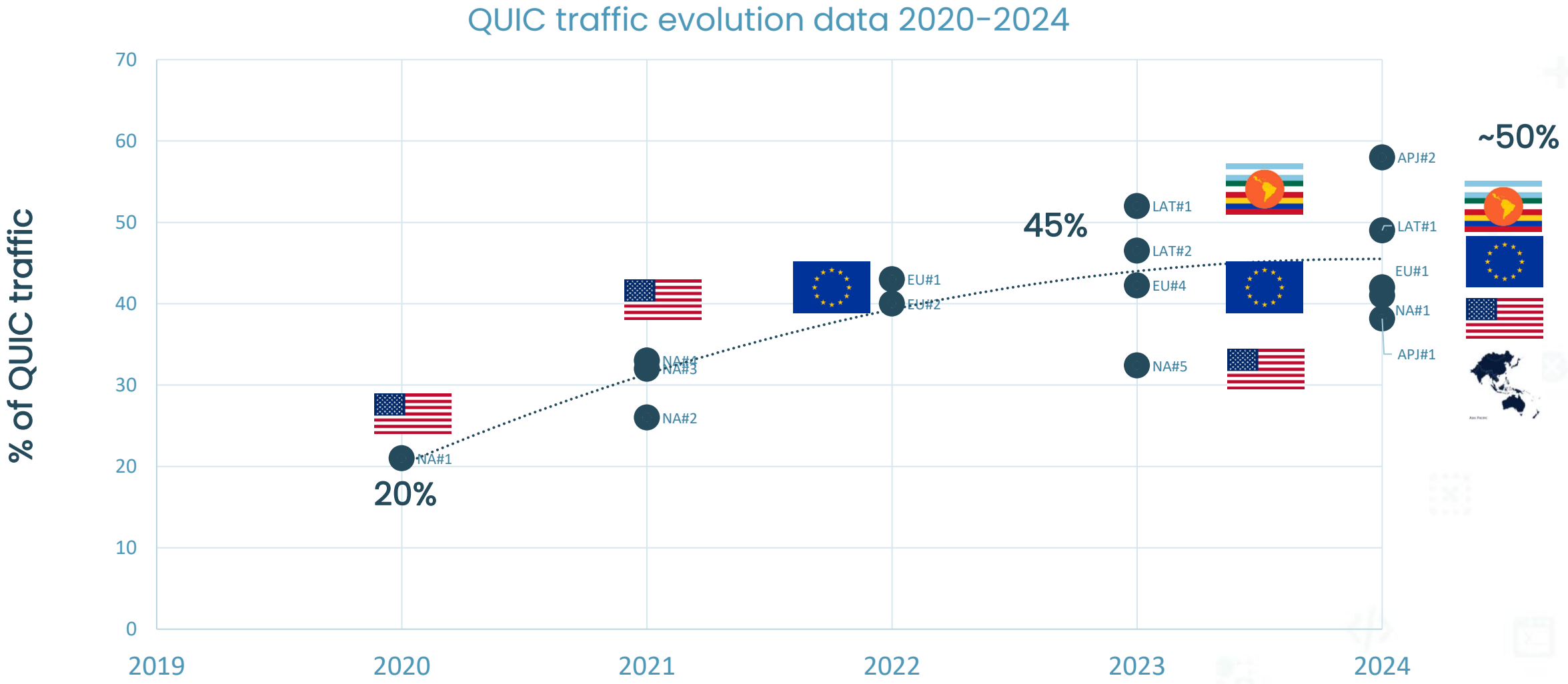


USA

QUIC: 41.5%

QUIC is growing across the world

Various snapshots – Approaching 50% WW



The New IP Stack and New Traffic Behaviour

An application driven global transition

HTTP/3 Stack = UDP+QUIC+TLS 1.3

Old App Stack

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

New App Stack

QUIC – RFC 9000
HTTP/3 – RFC9114

- HTTP/3
- QUIC + TLS 1.3
- UDP
- IP

+ **DoH**
DoT – RFC7858
DoH – RFC8484

+ **eSNI / ECH**
RFC8744

Application Controlled DNS
DNS Traffic not observable

Target Domain is opaque / unobservable

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

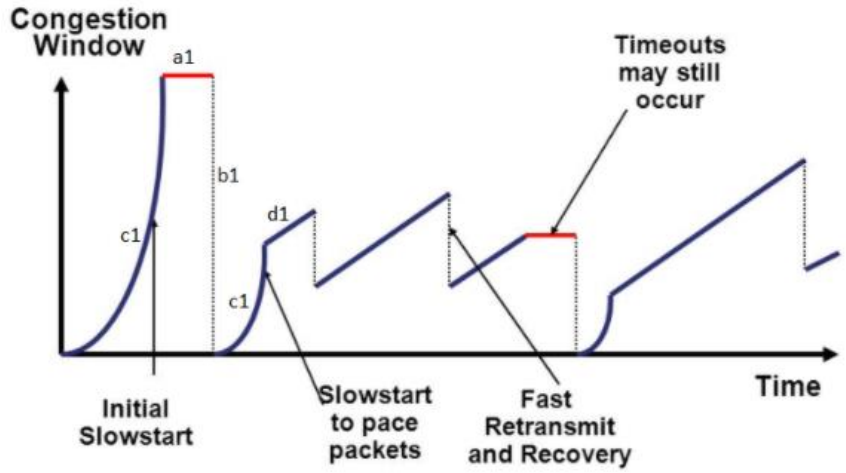
- *Improved Security*
- *Multi-session*
- *Improved QoE*
- *APP friendly design*

Large Scale Adoption

DoT: DNS over Transport Layer Security
DoH: DNS over HTTPS
eSNI: Encrypted Server Name Identification
ECH: Encrypted Client Hello

DPI Ineffective
including alternative hints e.g. DNS or SNI analysis

Challenging old network design assumptions



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)

TCP goal is network fairness

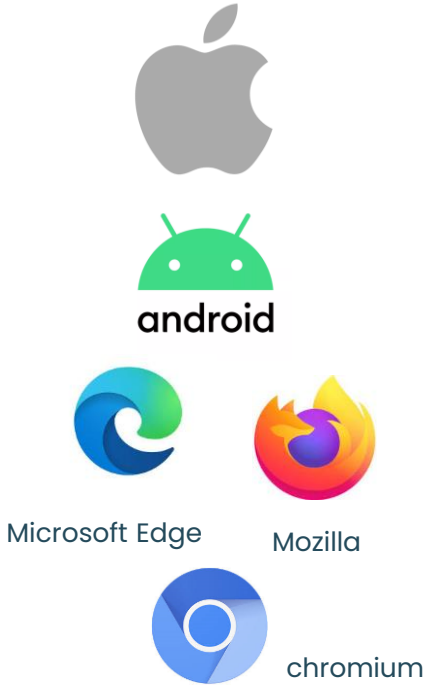
QUIC goal is "MY App" performance

Today IP Networks are architected with TCP behaviour as implicit assumption

So when packets are dropped TCP will take care of it at a higher layer

What are the new IP Network Design assumptions wrt QUIC?

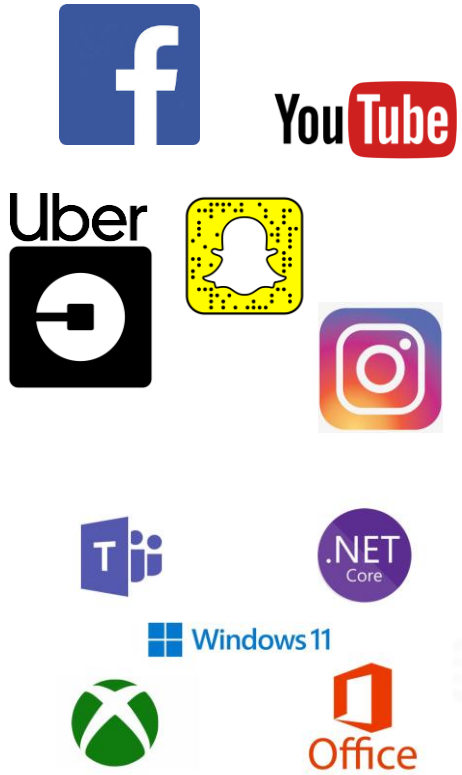
QUIC/HTTP3/DoH stack is in business
At scale, in production



Clients

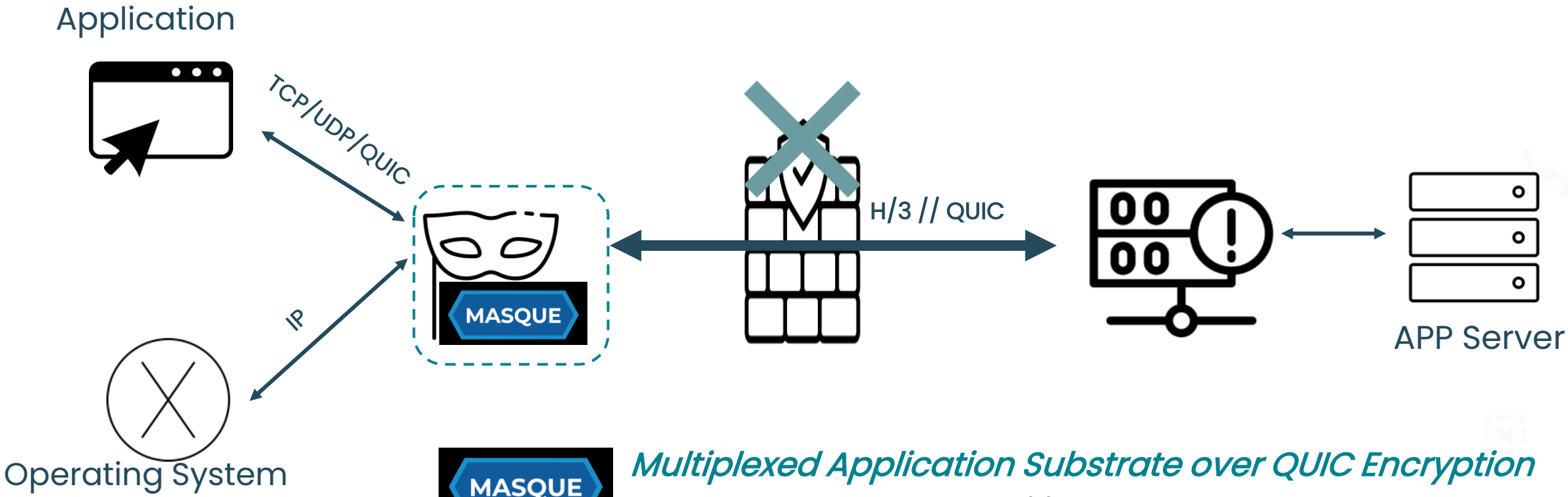
Content Delivery

Cloud providers



Applications

Tunneling is a new threat vector



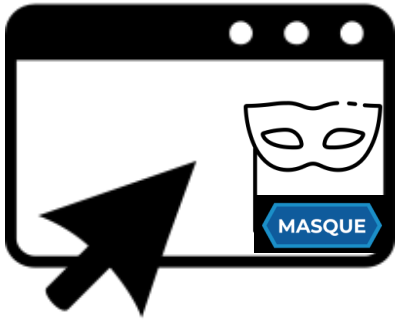
MASQUE

Multiplexed Application Substrate over QUIC Encryption

Goal is to develop mechanism(s) that allow configuring and concurrently running multiple proxied stream- and datagram-based flows inside an HTTP connection

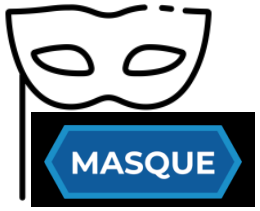
https://datatracker.ietf.org/wg/masque/about/

Options for Masque

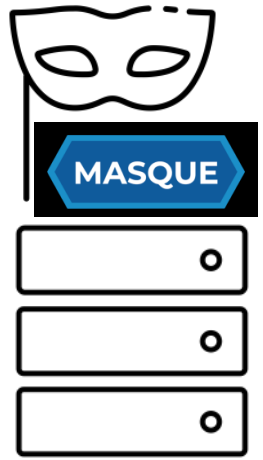


Inside the App

Inside the O/S

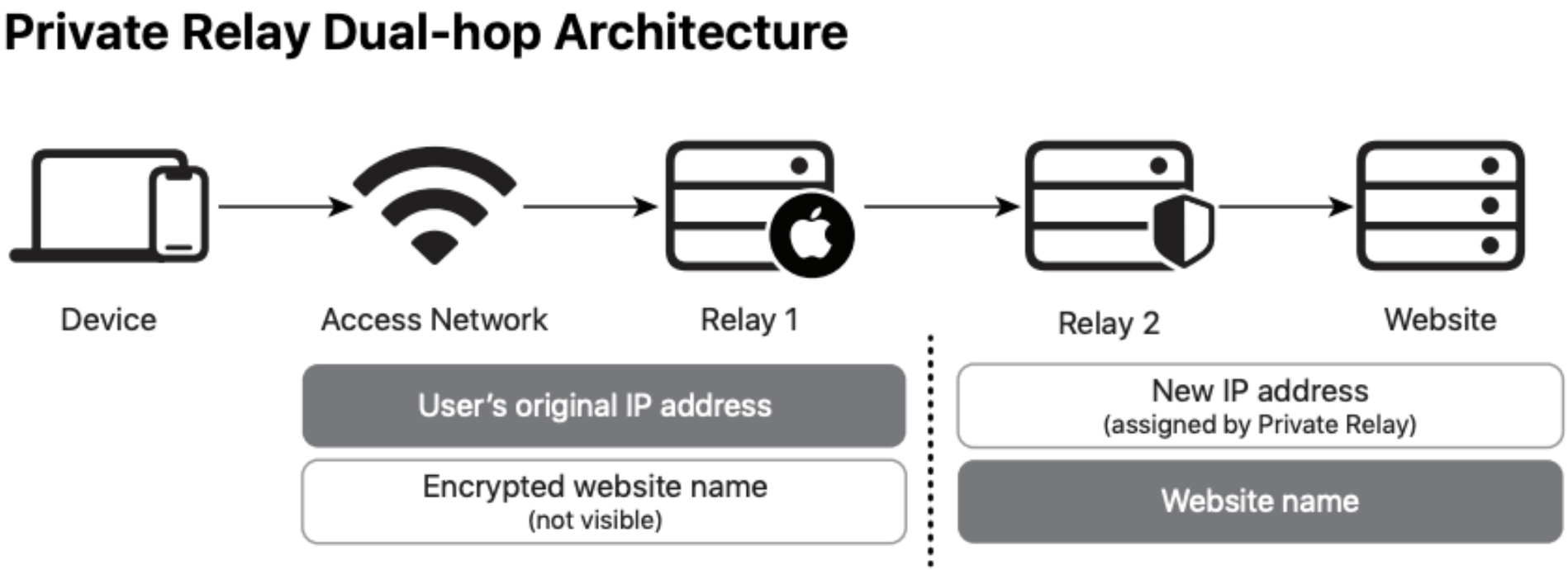


Client to O/S



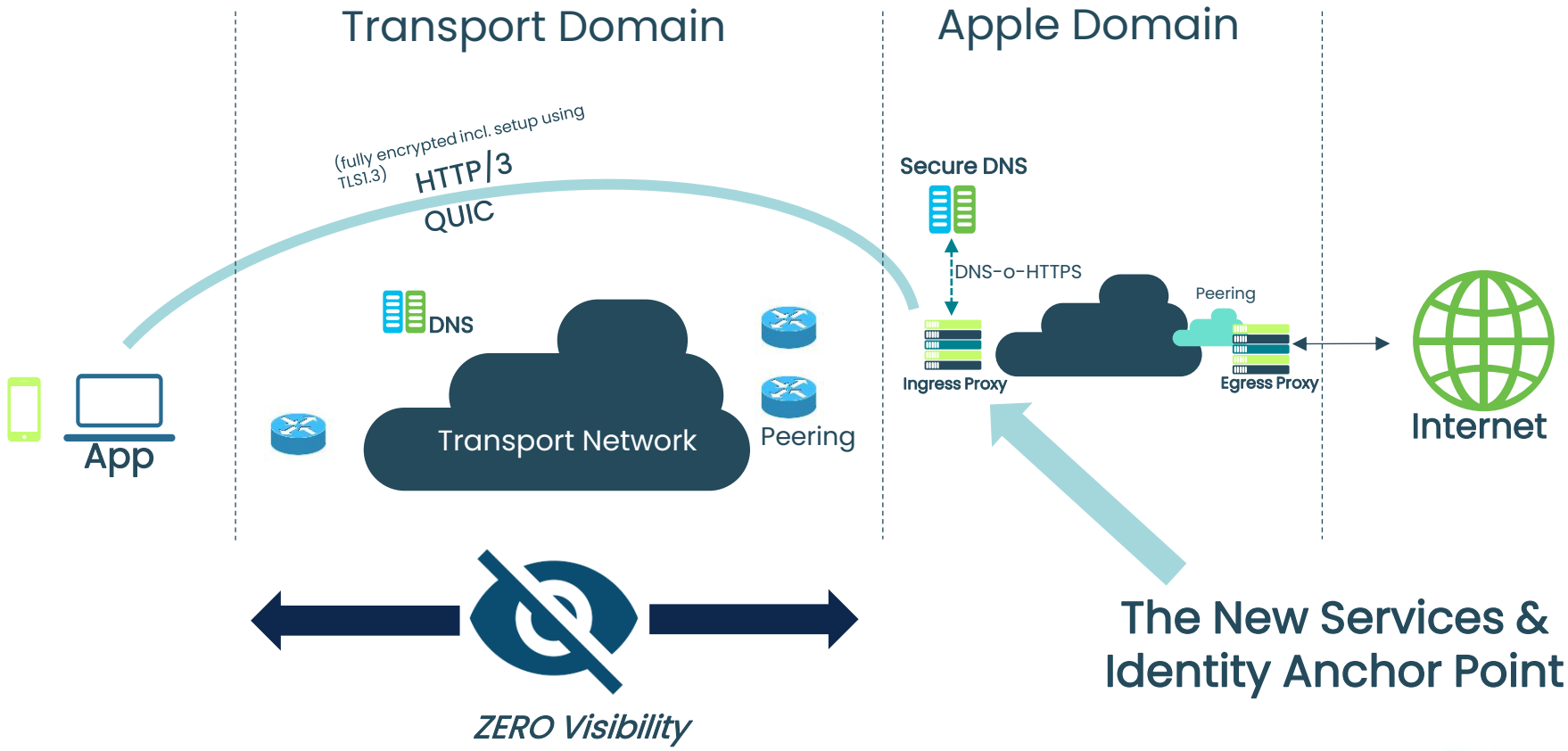
Network Appliance (tunnel IP)

Apple Private Relay: Dual Hop Masque



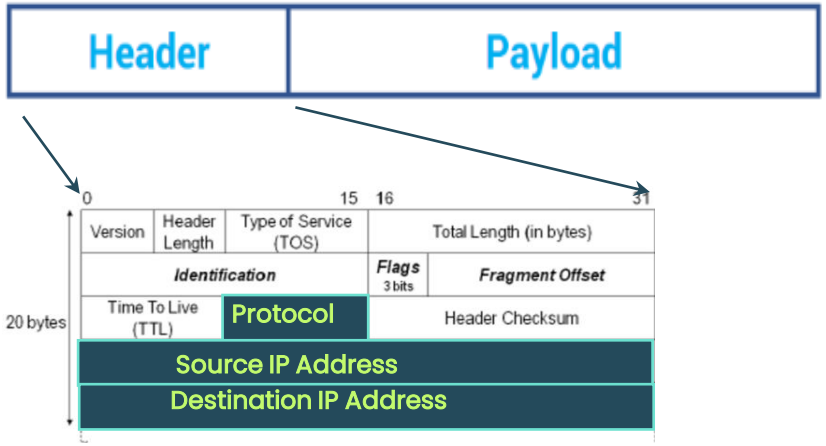
Decoupling users from content

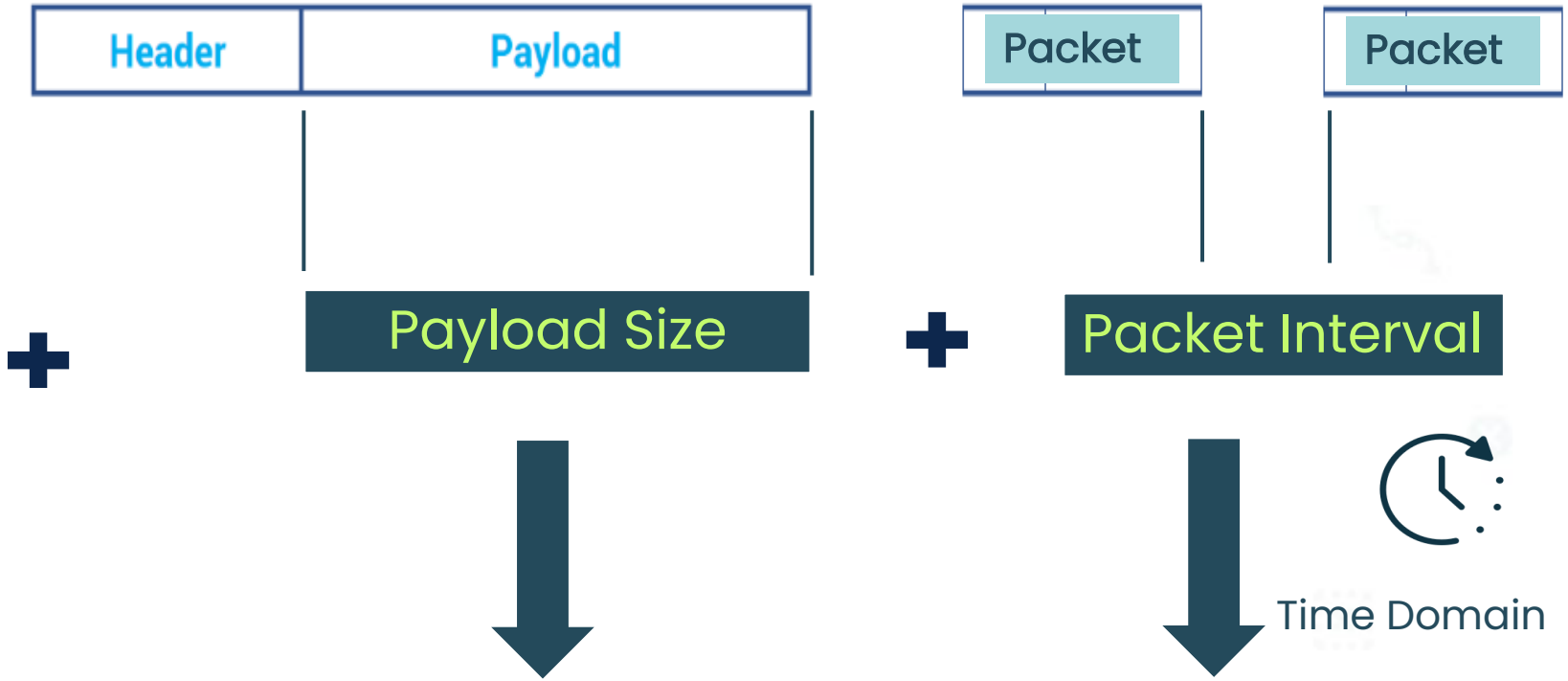
Transport Domain has less or “no” insights on traffic



What is left?

There is some information that will not go away



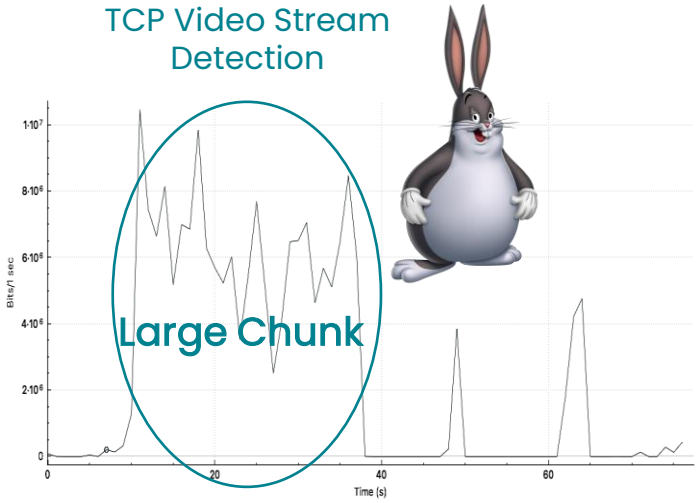


CDN Information

Traffic Volume in Time Information

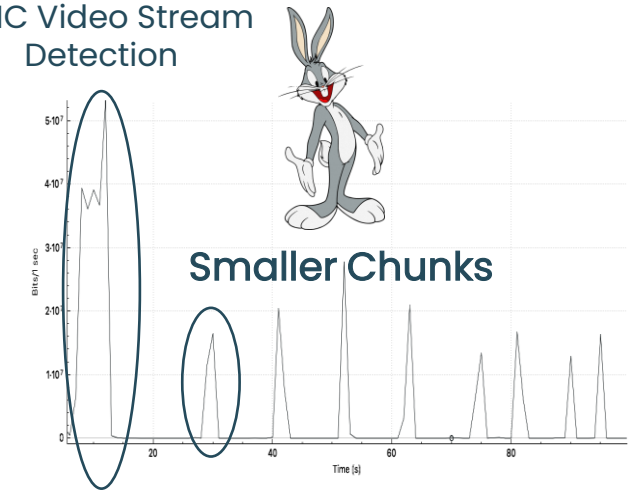
App (e.g. Video) Behavior varies by protocol and use case

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.

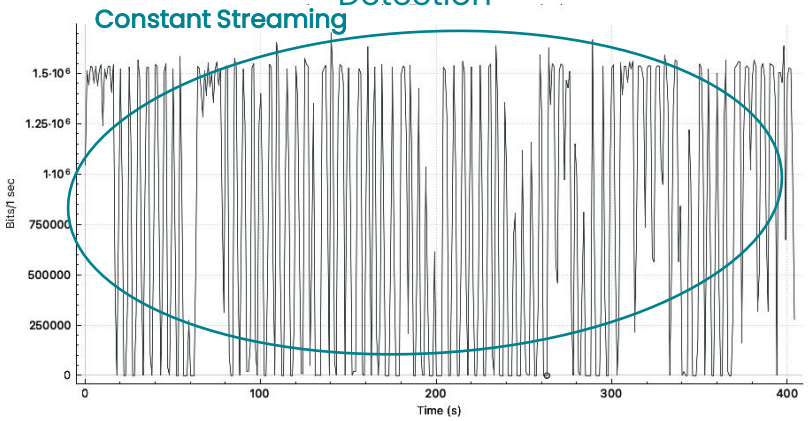
QUIC Video Stream Detection



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 T'put

Applications: YouTube Live, WebEx, Microsoft Teams, Zoom

Download Stream Detection

Premium

NETFLIX

Time Domain Flow recognition

Observe all flows

Profile per flow (Time domain matched)

The resulting profile will allow to distinguish the nature of the flow

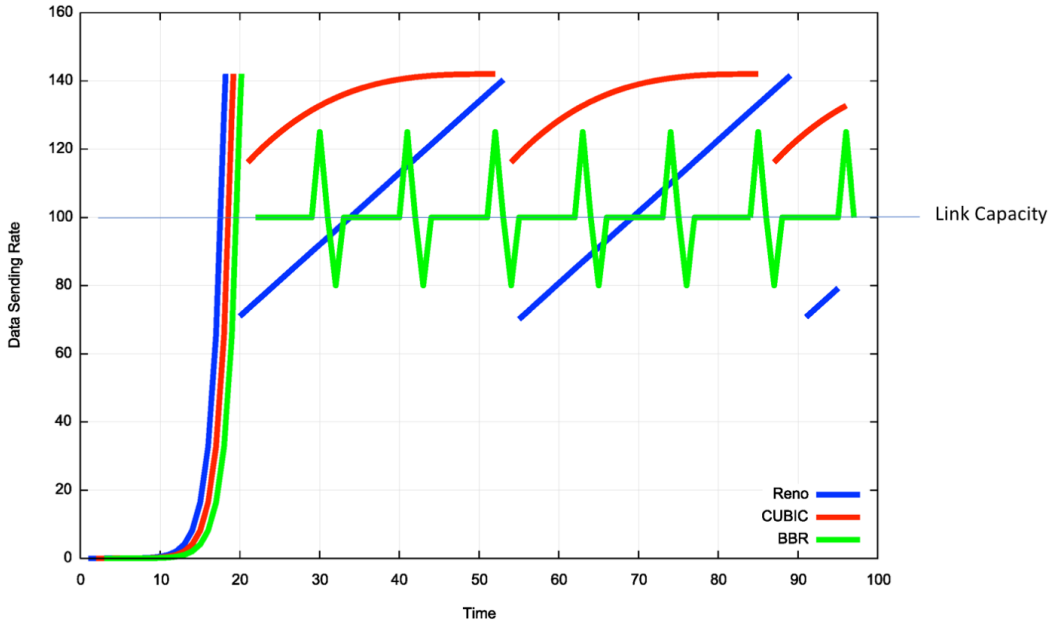
- Content Download
- (x-Form) Streaming content
- Real time 2 way communication
- Video/non-video
- Short lived flows

Inferring congestion

Different congestion algo's have different behaviour

Time-domain observation + anomaly detection -> congestion inference

Reno vs CUBIC vs BBR behaviour*



- Assessment of various flows in parallel
- Understand Protocol behaviour: congested or not
- This serves as input for Policy Application

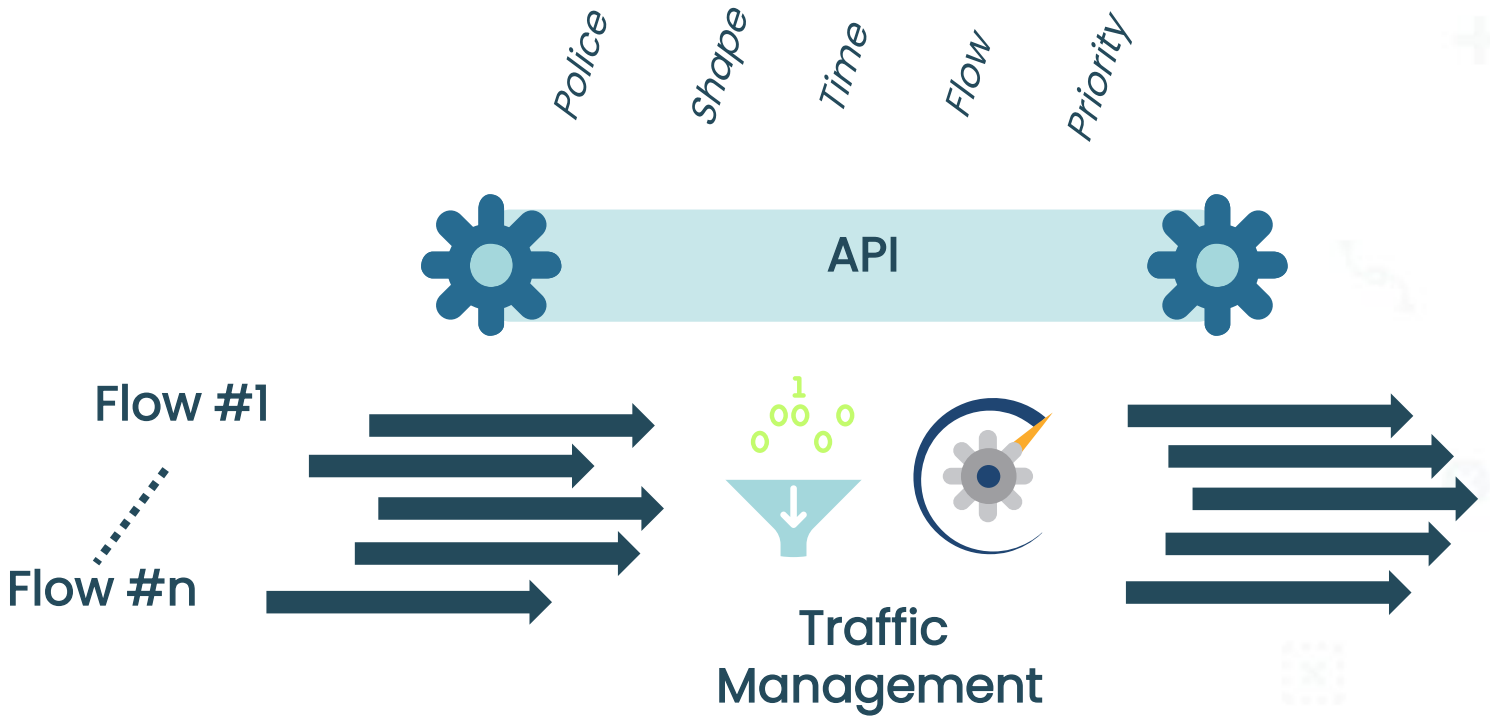
* https://blog.apnic.net/2017/05/09/bbr-new-kid-tcp-block/

Programmable Traffic Management

Traffic can be controlled in various ways:

- Buffer
- Discard
- Flow control
- …

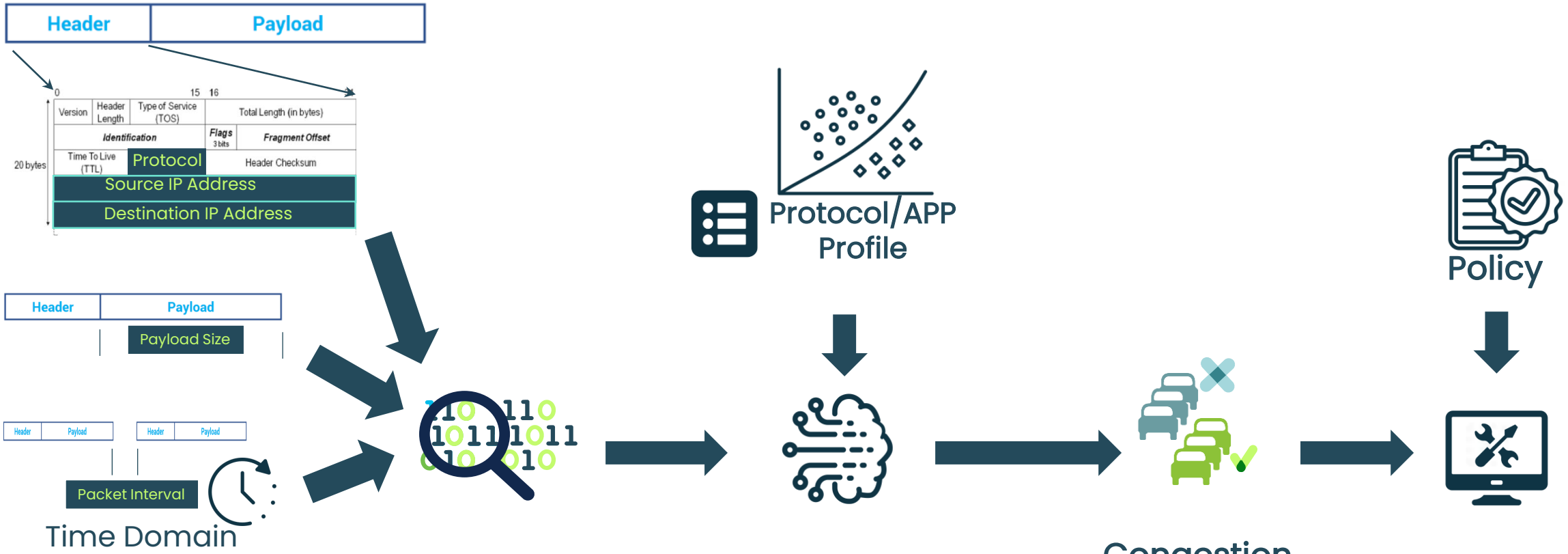
e.g. CUTO(*) is a pre-compiled example where the parameters are implicitly configured



* CUTO: Cisco Ultra Traffic Optimization

Overall System Logic

Basis for building use cases



Examples of use cases

Non-exhaustive list

Passive traffic monitoring
Real Time Passive IP flow Monitoring and enrichment with Access Network data
Visibility and analytics
Real Time Traffic Analytics QoE derivation and monitoring
Policy Enforcement
Dynamic Congestion Alleviation by Elephant Flow Shaping Interconnect link bandwidth management while maintaining and enhanced User Experience
Protection for Real-Time Traffic
Manage overall link congestion dynamically to protect RTP traffic (videoconf, collaboration, etc)

Summary

In summary

- The user Quality of Experience (QoE) is substantially improved
- Security is enhanced with TLS 1.3 improvements

But..

- Traffic is encrypted and obfuscated
- Quality of Experience is controlled by the applications
- Traditional DPI approaches won't work
- Traditional traffic management techniques are compromised

New approaches are needed:

- Traffic management: an IP Flow centric methodology is feasible and addresses several use cases (flows visibility, flows monitoring, protection of real time traffic, etc.)
- Security considerations: security at the endpoints needs to be substantially beefed up both against malicious acts and data exfiltration prevention

WORKSHOP GARR 2024

NET MAKERS

Thank you