The New, Encrypted Protocol Stack & How to deal with it
Adding Real Value to Networks

Andreas Enotiadis (MIG Sales CTO)
Bart Van de Velde (Sr. Director, Engineering, Networking CTO Office)
In memory of and based on the brilliant work of Mark Gallagher
(14/09/1966-17/09/2021)
Agenda

• The New Internet
• Toolbox
• Use cases
The New Internet
The Internet Reality – circa 2020 – Major US Carrier

- >90% of Volume: encrypted
- >70% of Volume: to Cloud
- ~50% of Flows: DNS
- >20% of Traffic: QUIC

- 10 Cloud sites “Elephant destinations” not “Elephant flows”
- Many small flows Micro-sessions

- Destination: all-encrypted world
- Cloud: concentrating the Internet
- Content: DNS is the load-balancer
- QUIC: Future Protocol of choice
QUIC is growing across the world
various snapshots

QUIC traffic evolution data 2020-2023

% of QUIC traffic

© 2022 Cisco and/or its affiliates. All rights reserved.
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 targeted and high efficiency (video related behaviour)

*source EU Operator 2022
The pattern persists worldwide into 2023

LATAM
- QUIC: 46.52%

EU
- QUIC: 42.24%

US
- QUIC: 32.4%
The old network design assumptions are challenged.

The old network design assumptions are challenged.

TCP goal is network fairness

Today IP Networks are architected with TCP behaviour as implicit assumption

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

QUIC goal is “MY App” performance

What are the IP Network Design assumptions wrt QUIC ?

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

* Source: APNIC
Top 5 Apps – QUIC is dominant 80/20 rule now
An application driven global transition

HTTP/3 Stack = UDP+QUIC+TLS

Old App Stack

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

New App Stack

- 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

- Target Domain is opaque / unobservable

Large Scale Adoption

DPI Ineffective

including alternative hints e.g. DNS or SNI analysis
Packet Inspection needs different approach

Overall Volume

QUIC : 40%
TCP : 55%
UNSP : 5.36%

*source: Live Traffic USA Operator ; dd. May 2023
QUIC/H3/DoH stack is in business

Content Delivery  Security  Privacy  Loadbalancing  App Infrastructure  App Experience
Dealing with the new reality: Toolbox & Use Cases
Customers are looking for solutions
Example Use Cases Asked

Manage video downloads vs video streaming, downloads being the priority
There is some information that will not go away

<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
</tr>
</thead>
</table>

- **Protocol**
- **Source IP Address**
- **Destination IP Address**

+ 

<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
</tr>
</thead>
</table>

- **Payload Size**

+ 

<table>
<thead>
<tr>
<th>Packet</th>
<th>Packet</th>
</tr>
</thead>
</table>

- **Packet Interval**

Time Domain

**CDN Information**

**Traffic Volume in Time Information**
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 T'put Applications: YouTube Live, WebEx, Microsoft Teams, Zoom

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

TCP Video Stream Detection

Large Chunk

QUIC Video Stream Detection

Smaller Chunks

Download Stream Detection

Constant Streaming

Download Stream Detection

Netflix

YouTube TV

Webex by Cisco

Zoom

Premium

© 2022 Cisco and/or its affiliates. All rights reserved. RKSFM-2024
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

- 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
  • …

• It’s also possible to pre-compile a traffic management action based on these parameters, for constant enforcement (eg. Elephant flow management)
Overall Toolbox
Basis for building use cases

- **Header**
- **Payload**
  - Protocol
    - Source IP Address
    - Destination IP Address
  - Payload Size
  - Packet Interval
  - Time Domain

**Observe Flows**

**Inference**

**Congestion Y/N**

**Control**

**Protocol/APP Profile**

**Policy**

© 2022 Cisco and/or its affiliates. All rights reserved
Use Case: Monitoring and analytics

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 targeted and high efficiency
  (video related behaviour)

- Monitor all flows
- Infer information for Source (DNS, SNI/eSNI), CDN (ECH), Flow Type (Time domain behaviour)
- ELK (elastic Search, Logstash, Kibana) analytics engine
- Extensible to enriched CDR production
Custom Policy Enforcement
e.g. Differentiate between “download” and “streaming” (within same app)

- Same Source/Destination Address
- Differentiate between download versus streaming on the same SA/DA
- Apply Policy per flow type, e.g.
  - Download Policy: no action
  - Streaming Policy: Limit to set BW profile (police/buffer/...)

<table>
<thead>
<tr>
<th>Throughput (Mbps)</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5 Mbps</td>
<td>0</td>
</tr>
<tr>
<td>2.5 Mbps</td>
<td>25</td>
</tr>
<tr>
<td>1 Mbps</td>
<td>50</td>
</tr>
<tr>
<td>1 Mbps</td>
<td>100</td>
</tr>
<tr>
<td>0.5 Mbps</td>
<td>125</td>
</tr>
</tbody>
</table>

Throughput (Mbps) vs Time (s) chart
Time Domain shaping
User Experience optimization under congestion

Congestion inference determines which links are congested and which flows are impacted. Elephant Flow Detection identifies which (QUIC or not) Flows can be managed. Then Machine Learning determines if that Flow is being delivered during congestion (red circle) and require Flow Control or not (blue circle).
Time domain shaping
User Experience Optimization within SLA Boundaries

Situation

Broadband ISP ➔ CIR ➔ Wholesale Access Operator

Conform to SLA results in predictable cost
Violate SLA results in additional cost

Solution

CIR

Bandwidth Volume Burst ...

Monitor
Infer
Congestion Control (Pace Elephants)
Police Egress

SLA ON

Conform to SLA
Ensure QoE for every user
Fair use capability

Indiscriminate Policing leads to bad user experience
Use Case: Protecting Real-time Traffic

Observe traffic, detect videoconferencing stream, measure steady state Bandwidth usage of video conf stream, shape traffic to (total-videoconf BW)

- Real-time Video flow(s)
- Real-time collab flow(s)
- Calc Steady State For real-time flow(s)
- Traffic Management
- Nicely conditioned Real-time collab apps
Summary

- Traffic is encrypted, application controlled, and obfuscated
- H3/Quic/UDP/DOH stack is on the rise and here to stay
- Networks need an IP flow centric approach that scales
Thank you