JCSA
10ÈME ÉDITION
JOURNÉE
DU CONSEIL
SCIENTIFIQUE
Afnic

JCSA
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic
10ème EDITION

BENOIT AMPEAU,
DIRECTEUR PARTENARIATS ET INNOVATION À L'AFNIC

JCSA
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic
10ème EDITION

STÉPHANE BORTZMEYER

INGÉNIEUR R&D À L'AFNIC

JCSA

JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

10ème ÉDITION

Présentation du protocole QUIC

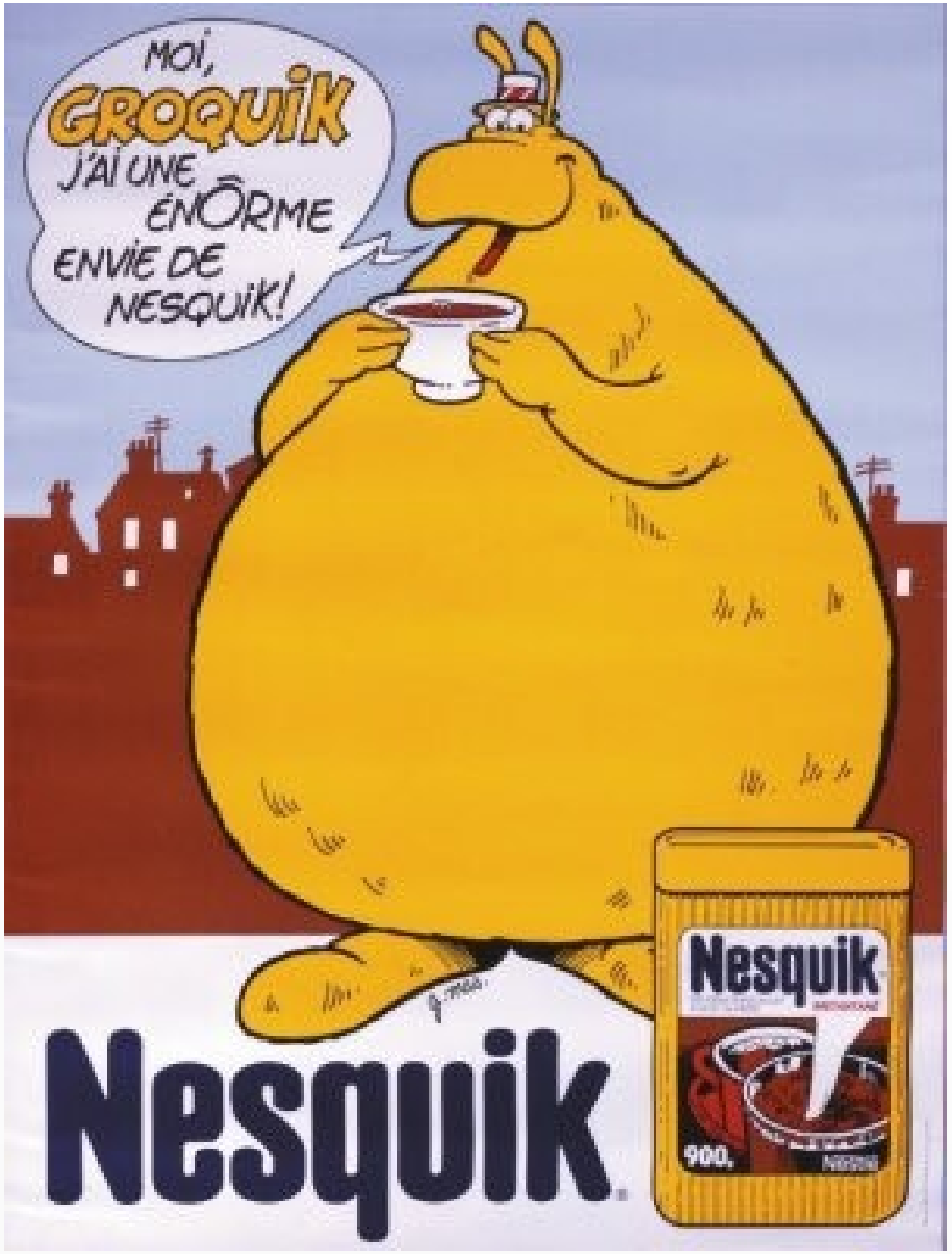
Stéphane Bortzmeyer, Afnic, bortzmeyer@afnic.fr

31 août 2021

C’est quoi, QUIC ?

Un protocole de transport (couche 4)

JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic



JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

À quoi sert un protocole de transport ?

Les datagrammes IP peuvent se perdre

- Il faut réémettre les paquets perdus
- Mais sans aggraver la congestion
- Les performances dépendent beaucoup de la couche Transport

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Ce que fait TCP

Le plus important protocole de l’Internet ?

- Établissement d’une connexion (triple poignée de mains)
- Numéros de séquence des octets, pour détecter les pertes
- Un canal virtuel ordonné d’octets offert aux applications

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Et la sécurité ?

Des méchants vous surveillent

- Il faut chiffrer les données
- Avec TCP, on doit d'abord se connecter, puis lancer TLS
- Diminuer la latence ?

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Il n’y a pas que les données

Exposer la machinerie de la couche Transport pose des problèmes

- Permet certaines attaques par déni de service
- Donne accès à des informations comme le RTT
- Contribue à l’ossification (tout ce qui est en clair s’ossifie)

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

La solution QUIC

Un autre protocole de transport est possible

- Remplace TCP
- Fournit les mêmes services + la sécurité
- En raison de l’ossification, doit tourner sur UDP et pas IP

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Et le parallélisme ?

Le Web demande du parallélisme

- Une page Web contient plein d'objets
- Plusieurs connexions TCP ? Égoïste, et empêche le partage des mesures
- Une connexion TCP ? Un datagramme perdu et tous les transferts freinent

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

QUIC

- Moins de latence à la connexion
- Fusionne transport et chiffrement
- Des ruisseaux (sortes de connexions virtuelles légères dans la session QUIC) pour le parallélisme
- Sessions indépendantes de l’adresse IP

JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Gagner quelques millisecondes

- Connexions 0-RTT si on a mémorisé le jeton

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Toujours chiffré

Plus de mode en clair dans l'Internet post-Snowden

- Utilise la négociation TLS (authentification, échange de clés)
- Mais pas son chiffrement
- Une partie de la couche Transport est chiffrée
- Un observateur extérieur ne peut plus calculer RTT ou taux de pertes

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Les petits ruisseaux font les grandes rivières

- Plusieurs ruisseaux au sein de la connexion
- Faciles à créer et à détruire
- Il y a un contrôle de flux pour la session et un par ruisseau
- La perte d'un datagramme IP n'affecte que les ruisseaux qui l'utilisaient
- L'ordre des octets est maintenu dans chaque ruisseau

JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Qu’est-ce qui définit une session ?

Le *Connection ID*

- Chez TCP et UDP, la connexion est identifiée par le tuple {protocole, addr. source, addr. destination, port s., port d.}
- L’ordiphone passe de 4G en WiFi ⇒ connexion cassée
- Le routeur NAT change le port ⇒ connexion cassée
- QUIC utilise un *Connection ID* pour identifier la connexion

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Qui fait du QUIC dans la salle ?

Les mises en œuvre

- Beaucoup de bibliothèques QUIC en logiciel libre
- Mais tout ça est récent, pas forcément bien intégré et pratique
- Déjà, il faut adapter les bibliothèques TLS
- Google Chrome, Firefox et curl, dans leurs versions récentes

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Qui fait du QUIC dans l'Internet ?

- Google Search (mais pas encore Gmail)
- Cloudflare
- Facebook
- Peu d'intérêt pour le petit serveur ?
- Nginx aura bientôt QUIC (mais pas Apache)

JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Et le noyau ?

- TCP peut parfaitement tourner en mode utilisateur et des mises en œuvre existent
- Mais en général, il est dans le noyau du système
- Les noyaux évoluent lentement (et pas forcément à la demande des auteurs d'applications)
- QUIC tourne en général dans l'espace utilisateur

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Un petit problème de vie privée

Le *Connection ID* et le pistage

- Sessions de longue durée (comme avec HTTP/1.1 et HTTP/2)
- Les sessions survivent aux changements d'adresse IP => possibilités de pistage de l'utilisateur
- QUIC travaille avec un jeu de *Connection ID* ; quand on change d'adresse IP, on change l'*ID*
- Protège contre les tiers, pas contre le partenaire
- En pratique, pas le plus gros problème du Web

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Tant d’histoires pour un seul bit

La saga du *spin bit*

- Avec TCP, un observateur extérieur peut corréler octets et accusés de réception
- Ça permet d’estimer le RTT et le taux de pertes
- QUIC chiffre les numéros des octets
- Mais fournit un bit qui change à chaque RTT
- Ce *spin bit* a été très contesté

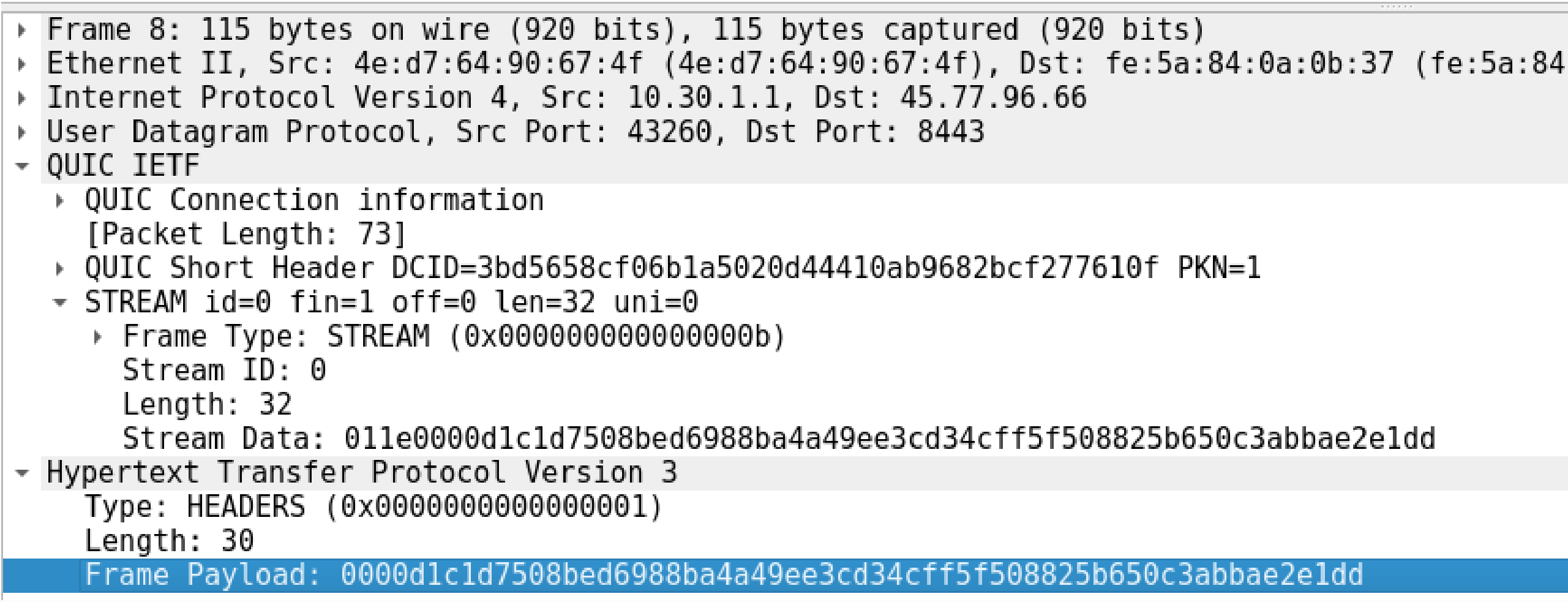
JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Vue du réseau

Ce que voit Wireshark

- RFC 8546
- Tout est chiffré, donc il faut fournir à Wireshark la clé
- Le déboguage nécessite la coopération d’un des terminaux
- Formalisme standard en cours (qlog) pour du déboguage pratique

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic



JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

4	0.167987	10.168.234.1	138.91.188.147	QUIC	1514	Protected Payload (KP0), DCID=d9e7940a80b4975407, PKN: 1, PING, PADDING
5	0.168550	10.168.234.1	138.91.188.147	HTTP3	225	Protected Payload (KP0), DCID=d9e7940a80b4975407, PKN: 2, STREAM(2), SETTINGS, STREAM(6), STREAM(10), STREAM(0)
6	0.332156	138.91.188.147	10.168.234.1	QUIC	1294	Protected Payload (KP0), DCID=f50587894e0cd26c, PKN: 3, ACK, DONE, NCI, NCI, PADDING
7	0.332361	138.91.188.147	10.168.234.1	QUIC	1482	Protected Payload (KP0), DCID=f50587894e0cd26c, PKN: 4, PING, PADDING
8	0.332372	138.91.188.147	10.168.234.1	HTTP3	1294	Protected Payload (KP0), DCID=f50587894e0cd26c, PKN: 5, ACK, STREAM(7), STREAM(0), HEADERS
9	0.332375	138.91.188.147	10.168.234.1	HTTP3	177	Protected Payload (KP0), DCID=f50587894e0cd26c, PKN: 6, STREAM(0), DATA
10	0.332841	10.168.234.1	138.91.188.147	QUIC	77	Protected Payload (KP0), DCID=d9e7940a80b4975407, PKN: 3, ACK, CC
11	0.487969	138.91.188.147	10.168.234.1	QUIC	80	Protected Payload (KP0), DCID=f50587894e0cd26c, PKN: 7, ACK, CC

```
Frame 5: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
Ethernet II, Src: 3e:d7:a5:38:5c:25 (3e:d7:a5:38:5c:25), Dst: fe:45:e7:7c:5a:6f (fe:45:e7:7c:5a:6f)
Internet Protocol Version 4, Src: 10.168.234.1, Dst: 138.91.188.147
User Datagram Protocol, Src Port: 56785, Dst Port: 443
QUIC IETF
▸ QUIC Connection information
  [Packet Length: 183]
▸ QUIC Short Header DCID=d9e7940a80b4975407 PKN=2
▸ STREAM id=2 fin=0 off=0 len=7 uni=1
▸ STREAM id=6 fin=0 off=0 len=1 uni=1
▸ STREAM id=10 fin=0 off=0 len=1 uni=1
▾ STREAM id=0 fin=1 off=0 len=31 uni=0
    ▸ Frame Type: STREAM (0x000000000000000b)
      Stream ID: 0
      Length: 31
      Stream Data: 011d0000d1d7510b2f696e6465782e68746d6c500a6d73717569632e6e6574
▸ PADDING Length: 104
Hypertext Transfer Protocol Version 3
Hypertext Transfer Protocol Version 3
Hypertext Transfer Protocol Version 3
Hypertext Transfer Protocol Version 3
   Type: HEADERS (0x0000000000000001)
   Length: 29
   Frame Payload: 0000d1d7510b2f696e6465782e68746d6c500a6d73717569632e6e6574
```

```
010  00000001 00000011 00001011 00000000 00011111 00000001 00011101 00000000
```

rame (225 bytes) | Decrypted QUIC (156 bytes)

Stream ID (quic.stream.stream_id), 1 byte(s) | Packets: 11 · Displayed: 11 (100.0%) | Profile:

Conséquences politiques et objections

- Moins d'information pour les intermédiaires
- Et moins de possibilités d'actions pour eux
- RFC 9065 (et 8404)
- Une nouvelle vision du déboguage, orientée terminal et plus réseau
- Remet une pièce dans les débats sur le chiffrement
- Qui a encore les moyens de développer et de promouvoir un protocole ?

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Les inconvénients de QUIC

- Trop sécurisé ?
- Trop compliqué ?
- Pas si rapide que ça ?

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

La belle histoire de QUIC

- 2012, projet Google
- 2016, passage à l'IETF
- Mai 2021, RFC 8999 à 9002, normalisant QUIC

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

HTTP/3

QUIC pour le Web

- QUIC est un protocole de Transport (couche 4)
- Il peut servir à toutes sortes d'applications (couche 7)
- Mais le principal usage est HTTP
- HTTP/1.1 et HTTP/2 utilisaient TCP
- HTTP/3, c'est la sémantique de HTTP et l'encodage de HTTP/2 sur QUIC
- Un ruisseau par couple requête/réponse

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

Que voit l'utilisateurice ?

Rien ; aucun changement

- (À part le gain en performances)
- QUIC est un protocole de Transport (couche 4)
- L'utilisateurice des applications est loin au-dessus
- Les URL sont les mêmes

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Tu QUIC ou tu QUIC pas ?

Comment le client HTTP sait-il que le serveur fait du QUIC ?

- Méthode la plus répandue : redirection HTTP par l'en-tête Alt-Svc:

```
alt-svc: h3=":443"; ma=2592000
```

JCSA 10e EDITION
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

DNS sur QUIC

DoQ

- En cours de normalisation draft-ietf-dprive-dnsoquic
- Et un groupe de travail IETF prépare VPN sur QUIC, MASQUE

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

De bonnes lectures

Pour en savoir plus

- Le livre libre de Daniel Stenberg « HTTP/3 Explained »

https://http3-explained.haxx.se/

JCSA 10e édition
JOURNÉE DU CONSEIL SCIENTIFIQUE
Afnic

JCSA

JOURNÉE DU CONSEIL SCIENTIFIQUE

Afnic

10ÈME ÉDITION

Merci !

Des questions, critiques ou remarques ?