Troubleshooting with QUIC

24	1		8=	Ľ	*	33	IS	EB -	2	7	3≤	22			In C	×	33			5 87			K8- 1	1	
- 5			=8	8		38	-	8- 08	E 8	8 -		212			8 8	-	SE 2IV			8- 8		17-17_3I			
	2	8	7			2-8	5.4	<u>v= =c</u>	C I					8 -			2-8	5	٢.	7= 0	S	\$=E = 99			- 1
S	8		1			>-8	×	E KK	2.2	2.6		25	8		7 -				6.	R 174	5		L s- 4		
5		22	Σ	2		$\square = K$	- r	LL LL	<u> </u>	10		⊏8		22	66		J=K	1	r.,	ee	1		TEZ		- 1
	<u> </u>	-	a,	к	Э	IL	> 1		7 0		=	66			ii. K	Э	IC			UI L	ě.		III		
	2	8	44			9E9	8		N 6	R.		7_	5	8	4		9E9					1 J -++			I B
	Э					18		TBSKC	< k	1		=C	Э		5 2								843		. 1
			r.	8		29	2.0	CICA	Σ_{-1}	C =		38			2 8		27					3255676			
	4	2		1	2	∃Z≤		1 [>	8 C					Γ.	てア		∃Z≾			I88	I		16- L		5
80 54					8	II		CECK-	<u>v</u> E		2	重工業	ā.				II		1	CECK		66 22	>=1 1		
R 62			8			でませ	>		۲		3	1=2		e			C K C		>		5	S=E2EE	KI C		6 1
	4					> : 🚼	3		<u>e</u>			с <u>т</u>	4		U =		> 4 🖬		9	48 K S	C	K = 43	5 0 X		1
Ŧ	4	¢.				ゲービ	2		E 8			с <u>т</u>		¢.						> 2 6	2	571 99	25		K 6
22	\$	8			6	4	2	8775A	K 7		-	<u>5</u> 8		8	R.	7	4				Э	106600	<u>e-</u> =		C 7
		2	-		4	5 8		375=E	H X		8 2			¥	1 I W	5	8 6				Ι	ELBERG	KC.		•
2		2	æ.		3	25	C.	C <- 3	, e					Σ.	a		405			C <- 5		CC 学 化	8		z
25						=t.		5 850			65						# U			S 84		n 19	C8 (
70			ę			>118		3-2/5	8		1	n		U.	6		> 118			-5-6			19.6		- 5
83			ĸ			1t		8183			81	84			ĸ		It						8		
64		22				46 W	4		6	4	8x			22			264		4	100 C			3 C		
						512				5	26						512			8=0		■ 11 = 1	B =		
1					1	55		⊑ k			45					I	55			C 4		> 4 114	-4 B		I (
8 U		<u>v</u>				66		7 28	3	r	6	80		2		6	64				C,	3 1	C (6 2
43		8			A	-		83583	8					8		A	-			83543		56			1 5
						R 2		1 🕹 🗇	7								R . 4			10.2		7 . 66	6 5		5
								-3636		8											6	C 112			
					Υ.	29		6 ISU									66			18I J		3			
5						44.05		6 539				5					172			6 53		E E	6	1.0	ē.,
۳.	20					2.6		£ 154		*		x	1				28					8 =	2		
25	12				8	<u>v</u>		ų — B				-	1 A			8	<u>v</u> .					s - C	5	10.0	
						R.		IR									₹.			JII .		1 22			
					H.			13		-						8							8 5		4
										R						C.							4 -		
	t												t								П.		C 1	1	

In search of lost metrics

Alexandre Ferrieux, Isabelle Hamchaoui

Orange Innovation



What is QUIC ?

DIRIDAN	- き つ の フ ケ レ		=8	オイトのイ	UL LI BIN	33 38 91 2 2 8 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	HIUK-A	1 m 1 4 - 4 m m			8 コナオコッ	781日七日日本	H R L Z N SNI			J 8	#8 7	第1年1	MHID D			8- 7- 2	U 140	- 22 46	t> t _1		モルビ		
				A 8		110 77	-		1321 ()17		* 7	C.E		司品			2			コリ	-		14 E C (U > +		477775C		3		IC
-	4					JZS	ā.		PEPE		5		-1	C ECE		1 1	t			JZ:	a		88	H	893 1-	-91	5		40
5	U				ï	VEU			8 21	1 6			2			e e	8		ï	SEC	>	R	-25	5	8=E7EE	RI	ê		IU
1 1	4	-				>:8 ⊐-₹		N N	382		8			e I		4 • •			2	> - K	100		16 8	5	£9= 3 971 99	51 51	R.	2	4F 21
	4	8				5			4350		7			E 8		s 8	Ľ		5	5	x			È.	1128211	6-		ř.	73
-		×.	-		17 m	9 8 707			95≡€ 6-29	Ę.			8			×.	-		U III	3 B 777	U	콾	-3 E-1	Ι	575873	K2	-		e :
R.		ê				st.			€ 82				20	2 1		ê			1	= 12		₹	84		U# R	C8	t		
70 84			6			84< 71			9-24 818		8		8				U.			84<			2-	¥	39 E		-		24
64						54F		A	1 12		6	4	B	e (t		ĥ			SUR	4		X.	R	7	ž			-6
						≤12 ₹2			8=02			2	4							512	C			22	4 114			Ę.	
80		e			ē	10			7 28		3	,r	6			Ľ			ê	64		7	2		3	Ē	C.	ê	11
4		e			4				82:1	5	87			-	4	8			4			83	CKD.	4	7 20		2		57
									-JC1	Ē.		8											1	8	2 112			ç	t.
e						59 24			U 18			1			e l				r	99 25		5	181		2 2 3	0	-		2
e						10			5 12	1					۳. 1					E 8		5	125		8			È.	6
1	4				8	E.			e	U R						4			8	E.		e.	5		3 - 0	4		1	2
					8					3		Ξ							8				I.		-	8		4	8
	5				L,							6				× .			C.						6	4		-	

Child of the NSA scandal : Enhanced privacy, no linkability! A transport protocol similar to advanced

TCP

versions with deep encryption to avoid ossification **30%** of

Orange traffic

You Tube

Start in 2014, IETF standard in 2021



HTTP/3

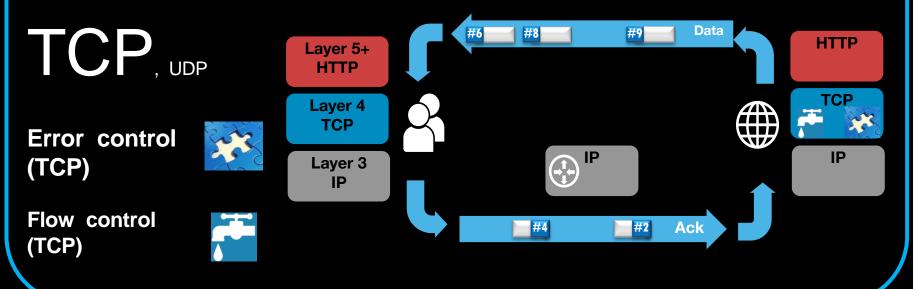


Standard Transport Layer

Layer 4 in theory

The transport layer

End-to-end connectivity



Reality check

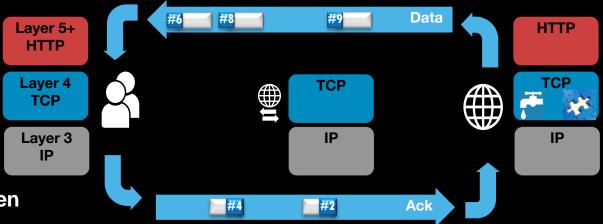
TCP transport layer

Middleboxes interfere "illegitimately" in the Transport Layer Proxy, optimizer, etc.

Middleboxes far behind standards

→ New Transport protocols blocked

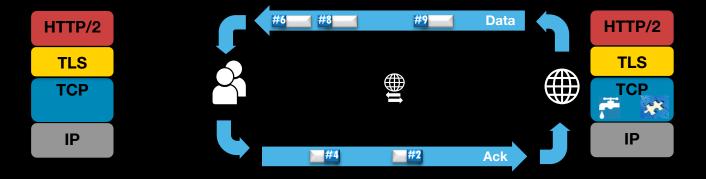
→ New TCP mechanisms blocked : e.g. TCP fast open



 \rightarrow Ossification of the Internet, innovation blocked for decades

QUIC is an answer...

TCP-like transport built over UDP + encryption



Ossification-ender

Middleboxes interference made difficult by QUIC headers encryption

QUIC is an answer...

TCP-like transport built over UDP + encryption

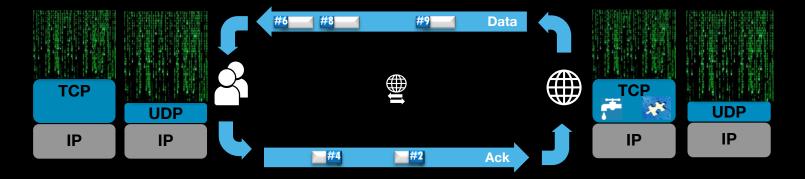


Ossification-ender

Middleboxes interference made difficult by QUIC headers encryption

QUIC is an answer...

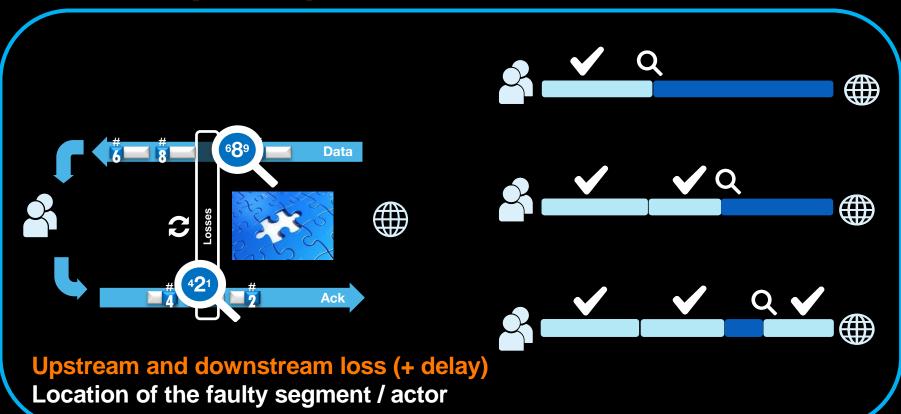
TCP-like transport built over UDP + encryption



Ossification-ender

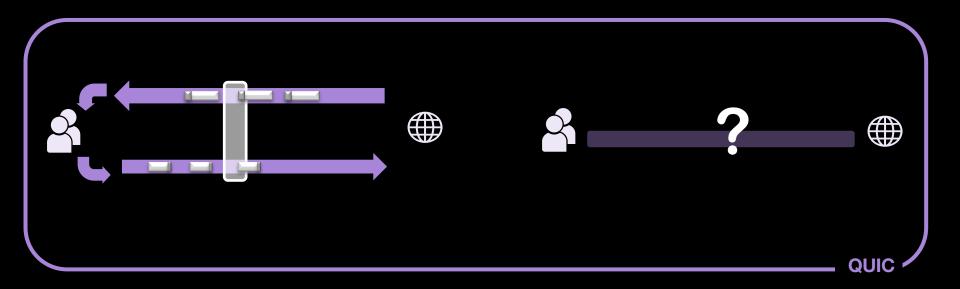
Middleboxes interference made difficult by QUIC headers encryption

TCP one point passive measurement

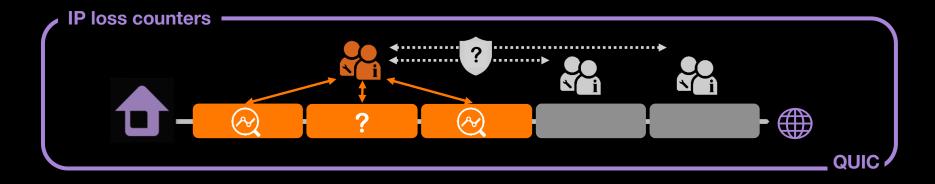


TCP

With QUIC, we're not in Kansas anymore....



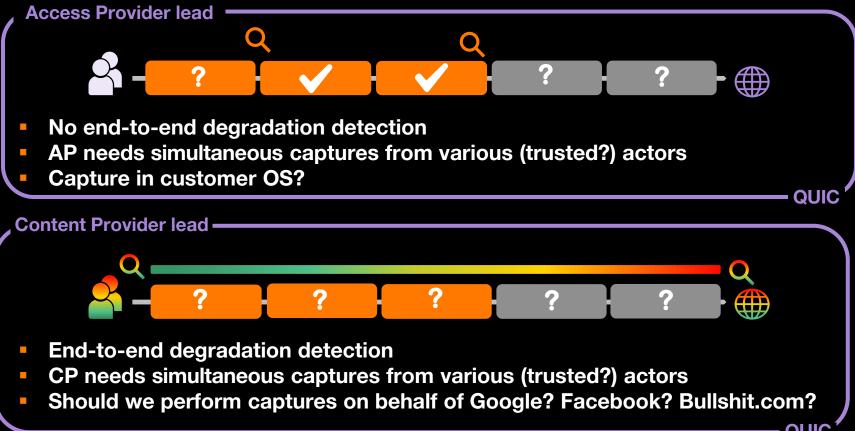
What else then? Packet drop counters?



Poor and cumbersome diagnosis

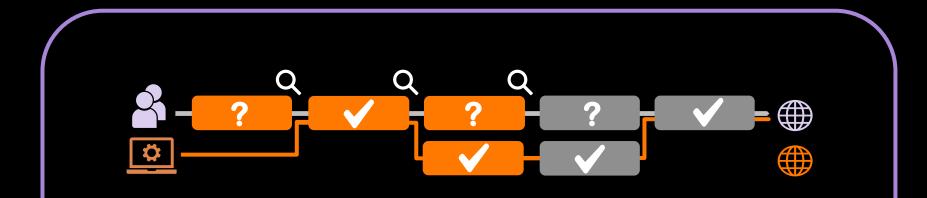
- Counters not available in all nodes => no exhaustivity
- No upstream/downstream loss: where is the faulty segment / actor?

2-points measurements?



QUIC

Active measurement



QUIC

Representativity (UE/server configuration, multipath) → For specific investigations only

Key disclosure



QUIC

The dream solution!

- Key disclosure by client or server
- Awesome! Back to TCP debug
- Any chance to get it?

The Loss bits mechanism

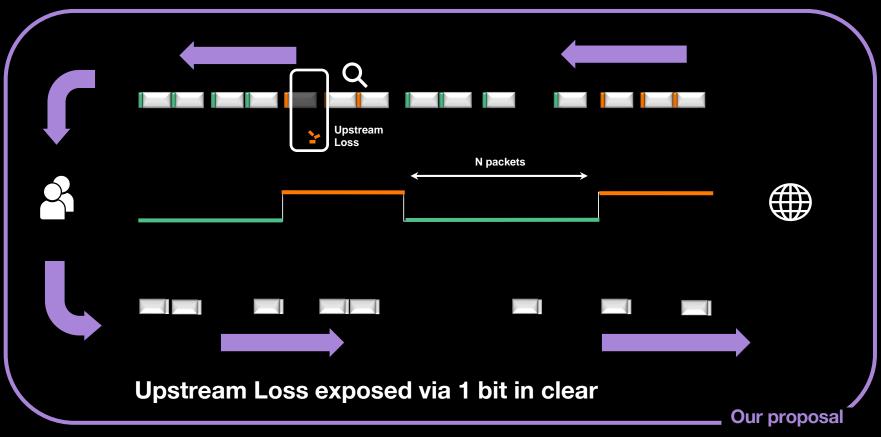
What?

Detect and locate faulty segments without packet number

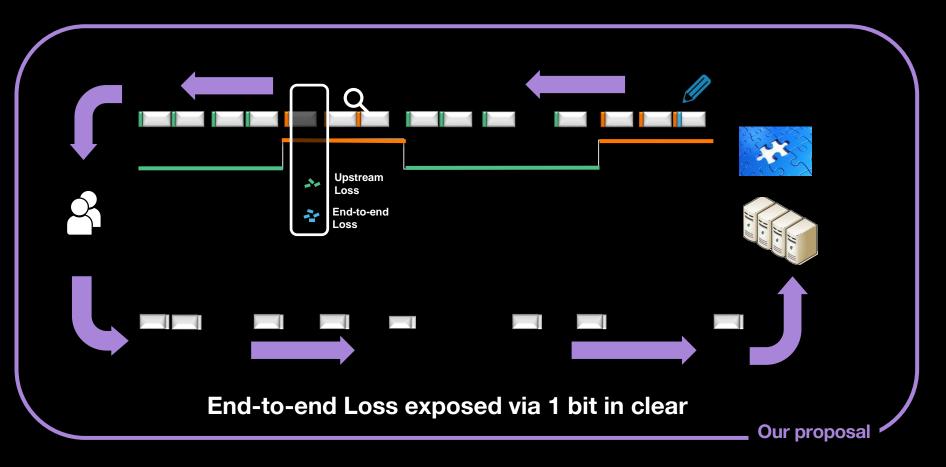
How?

Reference patterns drawn in the packet flows with 2 bits in clear in the QUIC header

The loss bits proposal (1)



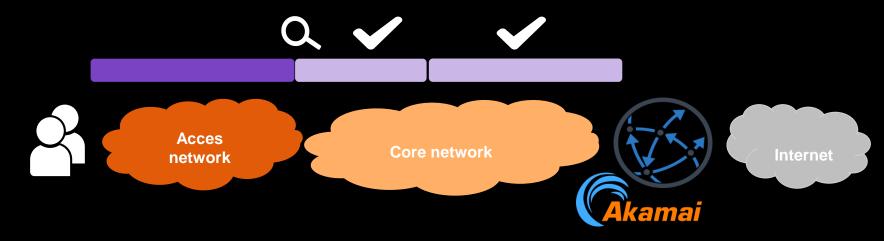
The loss bits proposal (2)



The Loss Bits in the wild

Field Trial with Akamai in 4 Orange affiliates

- Akamai CDN servers with loss bits implementation
- Thousands of Orange real clients
- Loss bits mechanism refined and validated



Additional validation by Satcom on Akamai servers and a satellite link

Wrap-up

Current Troubleshooting practices are threatened

In case of bad customer experience with QUIC, no easy way to locate faulty segment and prove actors' responsibility

New balance of power within the IETF arena

- Strong support from Akamai and CDN providers
- Very few operators expressed interest : Satcom, Telecom Italia
- Lukewarm support from Google, Microsoft, Apple
- Fierce opposition from Facebook and Mozilla

Wait... Is loss still critical?

- BBR is quite robust to mild loss
- Other Loss sensitive services ?
- Our mechanism is ultra light, energy efficienty, and still useful for strong loss

References

- First draft presented at IETF 104 (March 2019) <u>https://datatracker.ietf.org/doc/draft-ferrieuxhamchaoui-quic-lossbits</u>
- Orange-Akamai trial presented at IETF 105 (July 2019) <u>https://datatracker.ietf.org/meeting/105/materials/slides-105-maprg-packet-loss-signaling-for-encrypted-protocols-01</u>
- Akamai+lightspeed step-in at IETF 106 (November 2019) https://datatracker.ietf.org/doc/draft-ferrieuxhamchaoui-tsvwg-lossbits/
- Satcom trial presented at IETF 106 (November 2019) <u>https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-losses-in-satcom-systems-identification-and-impact</u>
- Joint draft with Telecom Italia (mars 2020) https://datatracker.ietf.org/doc/draft-mdt-ippm-explicit-flow-measurements/
- Independent evaluation from Ike Kunze et al. (Aachen university)
- L, Q, R, and T: which spin bit cousin is here to stay? (ANRW '21)

Thank you

orange[™]