

RFC 8863 : Interactive Connectivity Establishment Patiently Awaiting Connectivity (ICE PAC)

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 janvier 2021

Date de publication du RFC : Janvier 2021

<https://www.bortzmeyer.org/8863.html>

Le protocole ICE, normalisé dans le RFC 8445¹ permet de découvrir et de choisir, quand on est coincé derrière un routeur NAT, les adresses IP que vos correspondants verront. Parfois, au début du processus ICE, il n'y a pas d'adresses acceptables. Au lieu de renoncer tout de suite, ce nouveau RFC modifie le RFC 8445 pour demander qu'on patiente un peu : des adresses IP acceptables peuvent apparaître par la suite.

Résumons le fonctionnement de base d'ICE. ICE sert lorsqu'une des deux machines qui correspondent a le malheur d'être derrière du NAT : le but est de choisir une paire d'adresses IP, pour les deux machines qui correspondent. ICE compte sur des protocoles comme STUN pour la découverte d'adresses possibles. Ensuite, il teste ces adresses et réussit lorsque la communication a pu s'établir avec l'autre machine. Un effet de bord de ce processus est qu'il « crée » parfois de nouvelles adresses IP possibles, qu'il faut donc ajouter à la liste et tester. Le problème que résout notre nouveau RFC est que ces nouvelles adresses peuvent être détectées trop tard, alors qu'ICE a déjà renoncé à trouver une paire qui marche. La solution ? Attendre un peu, même si la liste des paires candidates est vide, ou qu'aucune des paires d'adresses de la liste n'a marché.

La section 3 de notre RFC note que le problème n'est pas si fréquent en pratique car ICE est **lent** ; cela prend du temps d'établir la liste des paires d'adresses IP possibles, et de les tester, d'autant plus qu'on ne reçoit pas forcément tout de suite un rejet, il faut souvent attendre la fin du délai de garde. Bref, la plupart du temps, les nouvelles adresses apparaissant en cours de route auront le temps d'être intégrées à la liste des paires à tester. Il y a toutefois quelques cas où le risque d'échec complet existe. Par exemple, si une machine purement IPv6 essaie de contacter une machine purement IPv4, aucune paire d'adresses IP satisfaisante ne sera trouvée, menant ICE à renoncer tout de suite. Or, si le réseau local de la machine IPv6 avait NAT64, la connexion reste possible, il faut juste tester et apprendre ainsi qu'une solution existe. Cela demande un peu de patience.

La section 4 formalise la solution : un chronomètre global est créé, le "*PAC timer*" (PAC pour "*Patiently Awaiting Connectivity*") et mis en route au tout début du processus ICE. ICE ne doit pas renoncer, même s'il croit ne plus avoir de solutions, avant que ce chronomètre n'ait mesuré au moins 39,5 secondes (cette durée vient du RFC 5389, section 7.2.1, mais peut être modifiée dans certains cas).

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc8445.txt>