RFC 7594 : A framework for Large-Scale Measurement of Broadband Performance (LMAP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 septembre 2015

Date de publication du RFC : Septembre 2015

https://www.bortzmeyer.org/7594.html

Le groupe de travail LMAP <https://tools.ietf.org/wg/lmap> de l'IETF travaille sur les mesures des performances des accès Internet « haut débit ». Des mesures comme celles que fait l'ARCEP <http://www.arcep.fr/index.php?id=8571&tx_gsactualite_pi1[uid]=1744&tx_gsactualite_pi1[annee]=&tx_gsactualite_pi1[theme]=&tx_gsactualite_pi1[motscle]=&tx_gsactualite_pi1[backID]=26&cHash=b402ff4b3f44d0d1ee66194773698941> en France. Ce RFC définit le cadre conceptuel de ces mesures et leur terminologie.

Donc, d'abord, les généralités (section 1 du RFC). On veut mesurer la qualité du réseau depuis un grand nombre de points de mesure. Sur chacun de ces points se trouve un MA ("*Measurement Agent*", au passage, le vocabulaire spécifique de LMAP est en section 3 du RFC) qui peut être matériel (sondes de l'ARCEP, sondes RIPE Atlas <https://atlas.ripe.net/>, sondes Sam Knows <https://www.bortzmeyer.org/samknows.html>, etc) ou logiciel (Grenouille <http://www.grenouille.com/>, etc). Le matériel peut être un boîtier séparé ou bien être un composant dans un engin comme la "*box*". Le but de LMAP est de travailler sur des mesures à grande échelle, avec des milliers, voire des millions de MA. À qui cela va-t-il servir ?

— Aux opérateurs de réseau pour planifier les investissements et détecter des problèmes,
— Aux régulateurs des télécommunications (comme l'ARCEP déjà citée) pour comparer les opérateurs et détecter des points où de la régulation pourrait être nécessaire (par exemple en cas de violation de la neutralité du réseau).

Ces buts sont décrits plus en détail dans le RFC 7536 [1].

Outre les MA ("*Measurement Agents*", installés chez M. Michu ou dans un point de mesure dédié, et qui exécutent les mesures), le système comprend les **contrôleurs** et les **collecteurs**. Le contrôleur est celui qui dit aux MA quelles mesures faire. Dans le cas de RIPE Atlas <https://atlas.ripe.net/>,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7536.txt

le contrôleur est une machine au RIPE-NCC qui reçoit les demandes de mesures faites, par exemple, via l'API <https://www.bortzmeyer.org/ripe-atlas-api.html>, et les transmet aux Atlas « pingue donc 192.0.2.34 avec un paquet ICMP ECHO par minute pendant dix minutes ». Le collecteur reçoit les résultats de ces mesures (« premier essai, RTT de 18 ms, deuxième essai "*time out*", troisième essai, RTT de 23 ms... ») et les analyse et/ou les rend disponibles. Le collecteur doit donc gérer une belle base de donnéees ("*big data*") avec un mécanisme d'accès aux données, comme SQL. Le protocole de communication entre le contrôleur et les MA se nomme le protocole de contrôle et celui entre les MA et le collecteur le protocole de collecte ("*report protocol*"). Certains systèmes (c'est le cas des Atlas) ne font pas de différence entre contrôleur et collecteur (et donc n'utilisent qu'un seul protocole pour le contrôle et la collecte).

On souhaite évidemment que l'ensemble du système :

— Soit normalisé, afin qu'on puisse choisir indépendamment ses différents composants. Il ne s'agit pas seulement de normaliser les protocoles mais aussi le modèle de données et le format de celles-ci (description des tâches de mesure, et des données récoltées). Normaliser tout cela est le principal travail du groupe de travail LMAP <https://tools.ietf.org/wg/lmap>. (Le modèle de données a été normalisé dans le RFC 8193.)
— Passe à l'échelle comme indiqué plus haut (« des millions de MA »). Un contrôleur unique et centralisé, par exemple, pourrait avoir du mal à effectuer son travail, à devoir coordonner un million de MA bavards (cf. RFC 7398).
— Accepte la diversité des réseaux (MA connectés à des capacités <https://www.bortzmeyer.org/capacite.html> très variables, réseaux IPv4 et IPv6, tests par plusieurs moyens, par exemple traceroute avec ICMP ou UDP, de façon à maximiser les chances de passer outre les pare-feux).
— Respecter la vie privée. Certaines informations récoltées peuvent être délicates.

La section 2 du RFC décrit à gros grains à quoi pourrait ressembler le système idéal. Le MA doit faire des mesures. Celles-ci peuvent être **passives** (le MA observe le trafic existant, sans interférer) ou **actives** (le MA envoie des paquets et observe leur effet). Notez que la plupart des systèmes existants sont purement actifs (une collecte passive soulève d'intéressants problèmes de vie privée...) mais que LMAP traite les deux cas.

Pour que les mesures soient anaysables et comparables, il vaut mieux qu'elles se réfèrent à des métriques standards et documentées (ce qui est rare, par exemple les mesures de l'ARCEP ne s'appuient pas sur les normes existantes, réinventant ainsi la roue).

Les canaux de communication (entre le MA et le contrôleur, ainsi qu'entre le MA et le collecteur) doivent évidemment être sécurisés, pour se prémunir contre des attaques comme celle d'un faux contrôleur qui essaierait d'utiliser les MA à son profit.

À noter que la configuration initiale du MA (par exemple, le nom de domaine pour contacter le contrôleur) n'est pas normalisée. Le MA peut arriver pré-configuré (c'est le cas des sondes RIPE Atlas) ou bien être configuré par un des protocoles existants comme NETCONF ou CWMP.

La section 4 de notre RFC est consacrée aux limites de LMAP. Le projet est assez ambitieux comme cela, il va donc se donner quelques restrictions (d'autres sont données en section 5.6) :

— Une seule organisation gère les MA, le contrôleur et le collecteur. LMAP ne va pas essayer de traiter le cas très difficile de mesures complètement pair-à-pair. Un tel système sans chef bien identifié serait sans doute très dangereux (risque de détournement pour faire des attaques par déni de service, risque de manipulation des données, ou de fuite de données privées).
— Chaque MA n'a qu'un seul contrôleur. Pour la résilience, il serait sans doute intéressant de pouvoir avoir plusieurs contrôleurs mais cela soulèverait le problème de quoi faire si un MA reçoit des instructions contradictoires.
— Les MA ne se coordonnent pas entre eux, on est purement "*top-¿down*".

— La relation entre le contrôleur et le collecteur n'est pas au programme. Ils vont bien sûr coopérer mais ce sera d'une manière non définie dans LMAP.
— Chaque système de mesures est indépendant des autres (pour éviter d'avoir à gérer des problèmes de coordination). Si un régulateur et un FAI ont chacun leur système LMAP, et que M. Michu a deux MA ("*Measurement Agent*") chez lui, les deux MA s'ignorent et chacun considère le trafic de l'autre comme du trafic utilisateur ordinaire.
— Il ne gère pas le problème de la triche. Si un régulateur fait des mesures, on peut imaginer que certains FAI chercheront à identifier les lignes où se fait la mesure, ce qui est facile, puis à favoriser ces lignes, pour obtenir un meilleur score. Le problème n'a pas de solution technique et n'est donc pas traité par LMAP. (Voir aussi la fin de la section 7.)

La section 5 du RFC décrit de manière abstraite le modèle des protocoles à élaborer. On y trouve notamment la liste des fonctions à mettre en œuvre comme par exemple un mécanisme de suppression des données si on découvre que certaines mesures étaient erronées (par exemple parce que l'amer `<https://www.bortzmeyer.org/amer-mire.html>` visé n'était pas joignable à ce moment).

Mais les informaticiens préféreront peut-être lire la section 6, plus concrète, qui décrit les questions pratiques de mise en œuvre et de déploiement. Par exemple, que doit faire un MA qui redémarre après un long arrêt ? Les instructions du contrôleur qu'il avait reçues et stockées peuvent être dépassées. Il doit donc tenter de re-contacter le contrôleur avant de se lancer dans les mesures.

Autre exemple de discussion pratique, la section 6.2 étudie les différentes formes de MA, et l'endroit où les placer, chaque forme et chaque endroit ayant ses avantages et ses inconvénients. Ainsi, un MA embarqué dans la "*box*" du FAI aurait des avantages (il voit tout le trafic, donc les mesures passives sont triviales à effectuer et toujours exactes, et les mesures actives peuvent être faites uniquement lorsque le trafic utilisateur est faible, alors qu'une sonde séparée risque de faire ses mesures au moment où on utilise la ligne à fond) et des inconvénients (dans le modèle classique des "*box*" imposées, les fonctions de la box ne sont accessibles qu'au FAI, pas au régulateur ou à l'utilisateur).

Et si le MA est (malheureusement pour lui) coincé derrière un NAT ? La principale conséquence est que le contrôleur ne pourra pas le joindre à volonté, ce sera au MA de le contacter. Une autre solution est de mettre un client PCP (RFC 6887) dans le MA.

Autre cas intéressant à considérer, celui où le MA se trouve en plein dans le réseau du FAI, et non plus chez M. Michu. (Le cas est cité dans le RFC 7398.) Cela permet au MA d'être indépendant des lubies du réseau local et de son accès et de faire des mesures dans un environnement plus contrôlé, donc plus scientifiques. Évidemment, ces mesures seront alors moins représentatives du vécu de l'utilisateur.

La section 6 discute aussi le cas où on a besoin d'une aide sur le réseau. Par exemple, si on pingue un amer `<https://www.bortzmeyer.org/amer-mire.html>` situé sur l'Internet, cet amer ne peut pas être purement passif. Ce doit être une machine allumée et qui répond aux paquets ICMP `ECHO`. Une telle aide est nommée MP pour "*Measurement Peer*". Ce rôle n'est pas évident. Par exemple, un amer peut tout à coup se mettre à limiter le trafic ICMP car il en a assez d'être pingué en permanence, faussant alors toutes les mesures. C'est encore plus vrai si on fait des tests lourds, comme de charger en HTTP un fichier de grande taille. Si on fait cela sur une machine qui n'était pas au courant de son rôle de MP, on peut se retrouver dans les ACL rapidement. S'il y a un protocole de contrôle explicite avec le MP (comme ceux des RFC 4656 ou RFC 5357), tout est plus simple, le MA négocie avec le MP le bon déroulement de la mesure. Sinon, il faut s'assurer d'abord que le MP est d'accord pour être utilisé. Heureusement, il existe des machines qui sont dédiées à ce rôle de MP, comme les Ancres `<https://atlas.ripe.net/about/anchors/>`.

La section 6.4 décrit un certain nombre de déploiements typiques. Ça peut aller de cas simples (le MA fait du HTTP avec un MP qui est juste un serveur HTTP ordinaire), à des choses plus complexes, où le MP déploie un logiciel spécifique comme iperf.

Un peu de sécurité maintenant (section 7 du RFC). La sécurité de LMAP doit protéger aussi bien le système de mesures, que le réseau mesuré (des mesures actives trop agressives pourraient sérieusement ralentir ce réseau, par exemple, voir la section 6 du RFC 4656). Plusieurs points sont donc à sécuriser. Par exemple, la mise à jour du logiciel du MA doit se faire de manière sécurisée. Imaginez des sondes dont le "*firmware*" serait mis à jour en HTTP (pas HTTPS avec vérification du certificat) : un méchant pourrait se glisser sur le trajet, leur envoyer du logiciel malveillant et se constituer ainsi un "*botnet*". Par exemple, si les MA peuvent faire des mesures passives, un tel "*botnet*" pourrait servir à faire de la surveillance massive (RFC 7258).

De la même façon, le MA ne doit pas obéir aveuglément à toute machine qui prétend être le contrôleur : il doit l'authentifier, tester l'intégrité des requêtes du contrôleur et empêcher les rejeux, qui pourraient facilement être utilisés pour des attaques par déni de service. La communication entre MA et contrôleur doit également être chiffrée : elle peut révéler des choses à un attaquant. Idem pour la communication du MA avec le collecteur : elle doit être authentifiée (imaginez un faux MA envoyant des mesures mensongères pour fausser une étude comparée sur les différents FAI) et confidentielle (les MA peuvent faire des mesures privées). À noter que, lorsque le MA est situé chez un utilisateur, on ne peut jamais être totalement sûr de son intégrité : il a pu être ouvert et modifié par l'utilisateur. (C'est encore plus vrai pour un MA logiciel.)

LMAP est prévu pour des grands systèmes de mesure. En outre, des malveillants pourraient tenter des attaques par déni de service contre le système de mesure. Notre RFC précise donc également que le collecteur doit se protéger en limitant le nombre de MA qui se connectent à lui simultanément, en limitant le débit d'envoi des données, et la taille totale des données.

Reste la question de la vie privée (section 8), qui fut le gros sujet de discussion au sein du groupe de travail à l'IETF. La vie privée de qui ? Eh bien, on cherche à protéger aussi bien les utilisateurs, que les FAI et les régulateurs. En cas de mesures passives, l'information sur le trafic Internet des utilisateurs est certainement très sensible et on ne veut pas qu'elle soit diffusée partout. Tout MA qui observe le trafic va donc accéder à ces informations qui peuvent menacer la vie privée. (Le RFC note qu'IPFIX a le même problème, cf. section 11.8 du RFC 7011.) Ainsi, même si la sonde Sam Knows <https://www.bortzmeyer.org/samknows.html> ne fait que des mesures actives, a priori moins sensibles, sa documentation recommande de brancher la sonde en coupure du réseau local, de manière à voir passer tout le trafic de l'utilisateur. C'est pour pouvoir ne déclencher les mesures actives que lorsque le trafic utilisateur est faible ou nul. Mais brancher un engin dont on n'a pas le source de manière à ce qu'il puisse voir tout le trafic est assez dérangeant. En outre, quelqu'un qui observerait les communications de la Sam Knows avec son contrôleur, même sans les comprendre, pourrait savoir quand l'utilisateur est en train d'utiliser son réseau : le MA n'a rien à communiquer dans ce cas (section 8.5.1 de notre RFC).

Même en l'absence de mesures passives du trafic, les MA peuvent avoir accès à des informations confidentielles : SSID du WiFi local, adresses MAC repérées lors des requêtes ARP, etc. Certaines informations sont rentrées explicitement par l'utilisateur et peuvent être sensibles : le contrôleur des sondes Atlas <https://atlas.ripe.net/> connait ainsi la longitude et latitude de la sonde donc la position de la maison (la précision est volontairement réduite lors de la saisie, précisément pour cette raison).

Quand aux données du FAI, qui peuvent être révélées indirectement via les systèmes de mesure, elles sont nombreuses : topologie exacte du réseau, trafic effectif dans les tuyaux, informations commerciales (type d'abonnements souscrits), etc.

Et le régulateur ? Oui, lui aussi a de la vie privée à défendre car il possède des infos confidentielles aussi bien sur les utilisateurs que sur les FAI, et n'a typiquement pas le droit de les diffuser.

Parmi les méchants qui seraient intéressés par cette information, on peut trouver les concurrents (le chiffrement est alors la protection minimale), l'organisation qui fait tourner les mesures (il est donc souhaitable de réduire la confiance qu'il faut lui faire, par exemple en mettant le MA derrière le port d'un commutateur, ce qui le rend difficilement capable de faire des mesures passives), ou bien sûr les organes de surveillance (RFC 6973, notamment section 5.1.1).

Outre le chiffrement des communications entre le MA et ses contrôleurs et collecteurs, solution déjà citée, il va être préférable de minimiser les données récoltées et transmises. Le chiffrement n'est pas une solution parfaite (notamment, il ne protège pas contre l'organisation qui fait fonctionner le collecteur), et il doit être complété par la **minimisation**, composante cruciale de tout projet de protection de la vie privée (RFC 6973, section 6.1, et notre RFC 7594, section 8.6.1). Les données doivent être agrégées, résumées, réduites à ce qui est strictement nécessaire pour la tâche en cours.

Les organisations qui collectent et traitent des grandes quantités de données essaient souvent de rassurer les utilisateurs en promettant que les données sont « anonymisées ». La section 8.6.2 de notre RFC rappelle que l'anonymisation est très difficile à faire correctement et que les techniques modernes d'analyse de données peuvent souvent dé-anonymiser et donc retrouver les individus dans la masse des données (cf. RFC 6235 et l'étude de Burkhart, M., Schatzmann, D., Trammell, B., et E. Boschi, « "*The Role of Network Trace anonymisation Under Attack*" <http://www.sepia.ee.ethz.ch/publications/ccr2010-burkhart.pdf> » en 2010).

L'anonymat ne doit pas être réduit au simple pseudonymat, (section 6.1.2 du RFC 6973) où il y a un identificateur stable des activités, même s'il n'est pas relié à une identité du monde extérieur. Dans le vrai anonymat (très difficile à obtenir, malgré les promesses des commerciaux du "*big data*"), il n'y a pas de traçabilité.

D'ou la conclusion de cette section, qu'un accord explicite d'un utilisateur informé et conscient est nécessaire, si on fait des mesures chez lui. (Cela peut d'ailleurs être un argument pour des points de mesures créés spécialement pour la mesure, comme dans les tests ARCEP. Il n'y a alors pas de problème de vie privée.)