Protocoles des Services Internet I

Juliusz Chroboczek

30 septembre 2021

En L3 et en M1, vous avez suivi des cours de réseau qui présentaient une pile de protocoles théorique qui avait la structure suivante :

NTP, DNS, WebRTC, FTP, SMTP, HTTP, Bittorrent etc.	(7)
UDP, TCP, etc.	(4)
IP	(3)
SLIP, PPP, Ethernet, 802.11 etc.	(2)
RS-232, 10Base2, 100BaseTX, radio 2,4 GHz, etc.	(1)

Cette pile a une structure fort propre : aux extrémités, une multitude de protocoles de couche application sont implementés au dessus d'une pléthore de technologies de couche physique. Au milieu, la couche réseau (3) est une couche de convergence, qui factorise l'interaction entre les applications et les technologies de couche physique. Deux couches intermédiaires, lien et transport, factorisent des fonctionnalités communes à plusieurs technologies physiques et applications respectivement.

Si cette vision n'est pas trop distante de la réalité aux couches basses, elle ne la représente plus aux couches hautes. Le « etc. » de la couche 4 est en fait une fiction : il n'est aujourd'hui plus possible de déployer des protocoles de couche transport autres que TCP et UDP. C'est l'*ossification de l'Internet*.

1 Ossification de l'Internet

Un des principes de la pile TCP/IP est que les couches 4 et 7 sont strictement de bout-en-bout : elles ne sont implémentées que dans les hôtes, pas dans l'intérieur du réseau. En d'autres termes, une entité se trouvant à l'intérieur du réseau n'a pas le droit de regarder à l'intérieur d'un paquet IP, où se trouvent les données de couche supérieure, et c'est pour cela qu'un protocole de couche transport devrait être facile à déployer.

De fait, il existe de nombreuses entités à l'intérieur du réseau qui regardent à l'intérieur d'un paquet : c'est les *middleboxes*. Les plus notables sont :

– les *pare-feu (firewalls)*, qui inspectent l'intérieur des paquets pour jeter les paquets malicieux [1] ;

1. Voyez la RFC 3514.

– les *NAT*, qui modifient les entêtes de couche réseau et transport pour multiplexer plusieurs hôtes sur une seule adresse IP ;
– les *optimiseurs* et *accélérateurs*, qui modifient le traffic pour le rendre plus efficace, par exemple sur les liens satellite ;
– les *caches*, qui répondent localement à des requêtes destinées à des hôtes distants.

Tous ces *middleboxes* ne savent interpréter que TCP et UDP, et jettent typiquement les paquets contenant d'autres protocoles de couche transport, qu'ils ne savent pas interpréter. Il n'est généralement pas possible de mettre à jour les *middleboxes* : l'utilisateur d'un réseau mobile (par exemple LTE ou « 4G ») n'a aucun contrôle sur le lien à travers lequel il se connecte à l'Internet, sans même parler des routeurs de l'infrastructure de son fournisseur.

Nous espérions jadis que la transition à IPv6 résoudrait le problème ; nous savons aujourd'hui que ce n'est pas le cas, et que les réseaux IPv6 utilisent des *middleboxes* tout aussi restrictifs que les réseaux IPv4.

Ossification des systèmes d'exploitation Outre la difficulté de mettre à jour le réseau, il est récemment devenu impossible de mettre à jour certains systèmes d'exploitation. S'il est relativement facile d'ajouter un nouveau protocole de couche transport à un noyeau Linux ou à un Unix BSD, c'est presque impossible sous Windows ou Mac OS. Android est certes une version modifiée de Linux, mais difficile à modifier du fait des différents composants propriétaires que chaque variante d'Android utilise. Quand à iOS (le système d'exploitation des iObjets brillants), il est complètement verrouillé, et Apple se permet même d'interdire l'utilisation de certaines applications utilisateur sous iOS [2].

Cette ossification des systèmes d'exploitation s'ajoute à l'ossification de l'Internet, et rend le déploiement de nouveaux protocoles de couches transport encore plus irréaliste.

2 Piles de protocoles

S'il est impossible de déployer de nouveaux protocoles de couche de transport, la couche 3 cesse d'être une couche de convergence utile. La couche de convergence migre vers le haut, et le modèle change. Dans mon analyse, il y a deux modèles utilisés sur l'Internet actuel : un qui est centré sur HTTP, et un qui est centré sur UDP. Ces deux modèles sont utilisés simultanément, parfois même dans la même application.

2.1 HTTP comme protocole de convergence

HTTP est un protocole de couche application qui a initialement été conçu pour la distribution d'articles scientifiques, mais qui a ensuite évolué pour servir d'abord à la distribution de « pages web » arbitraires, puis est devenu un protocole d'application générique (« Web 2.0 »).

Du fait de la popularité du *Web*, tout réseau IP, aussi restrictif soit-il, permet d'utiliser HTTP [3]. Il est donc naturel de vouloir utiliser HTTP comme couche de convergence, et de construire nos

2. Par exemple, il est interdit d'utiliser un navigateur autre que *Safari* sous iOS — Firefox pour iOS n'est guère plus qu'une interface utilisateur alternative pour Safari.
3. Sauf le réseau de nos salles de TP.

applications au-dessus de HTTP. On arrive alors à la pile suivante :

Gmail, Facebook, Matrix, Github etc.	(7)
HTTP	(7) (ou 6 ?)
TCP	(4)
IP	(3)
SLIP, PPP, Ethernet, 802.11 etc.	(2)
RS-232, 10Base2, 100BaseTX, radio 2,4 GHz, etc.	(1)

Outre le fait de traverser les pare-feu avec aisance, HTTP a l'avantage d'être une technologie connue et implémentée partout (notamment dans 10 milliards de navigateurs web), et d'être facilement cachable. Par contre, HTTP a plusieurs limitations graves : c'est strictement un protocole client-serveur requête-réponse (il n'est pas possible au serveur de faire une notification asynchrone), les messages HTTP sont coûteux (au moins 200 octets d'entêtes), et HTTP n'a pas de facilités pour gérer les sessions. Nous verrons dans la suite de ce cours comment construire des protocoles qui contournent ces difficultés.

2.2 UDP comme protocole de convergence

UDP est une couche très fine au-dessus de IP : essentiellement, UDP n'ajoute que les numéros de ports à IP. UDP est capable de traverser la plupart des pare-feu, il est implémenté dans tous les systèmes d'exploitation, et, à la différence de HTTP, il n'impose ni *overhead* ni latence supplémentaire. Les protocoles de couche transport récents, tels que QUIC (utilisé par HTTP/3), RTP ou SCTP (utilisés par WebRTC) sont généralement implémentés au-dessus de UDP. On arrive donc à la pile suivante :

HTTP/3, WebRTC, BitTorrent etc.	(7)
QUIC, SCTP, RTP, µTP	(4)
UDP	(4) (ou 3 ?)
IP	(3)
SLIP, PPP, Ethernet, 802.11 etc.	(2)
RS-232, 10Base2, 100BaseTX, radio 2,4 GHz, etc.	(1)

Si UDP est implémenté sur tous les systèmes d'exploitation, il existe de nombreaux réseaux qui le bloquent ; c'est notamment le cas de certains réseaux d'entreprise et, tristement, de beaucoup de réseaux universitaires. Une application implémentée au-dessus de UDP va donc devoir implémenter des techniques pour utiliser TCP lorsque UDP est bloqué, ou alors accepter que quelques pourcents des utilisateurs ne pourront pas l'utiliser [4]. Par exemple, les clients HTTP/3 sont capables d'utiliser HTTP/1.1 lorsque UDP est bloqué. De même, WebRTC essaie d'abord de communiquer directement en UDP, puis, en cas d'échec, utilise le protocole TURN qui est conçu pour ressembler autant que possible à HTTP (sans cependant être aussi inefficace).

4. « Mais pourtant notre réseau n'est pas cassé, puisque Zoom marche. »

3 Techniques cryptographiques

Nous utiliserons dans ce cours un certain nombre de techniques cryptographiques : les fonctions de hachage cryptographiques et les arbres de Merkle, les codes d'authentification (MAC), qui permettent d'authentifier les messages, et le chiffrage, qui permet d'en assurer la confidentialité. Ces techniques nous serviront parfois à optimiser les protocoles (en évitant des transferts à travers le réseau), mais elles seront avant tout nécessaires pour les sécuriser.

3.1 Espionnage et surveillance

Nous savions depuis longtemps que les services de sécurité des états surveillent les échanges sur Internet, notamment dans le but de lutter contre le crime organisé, le terrorisme, ou le traffic de pornographie illégale. Depuis les révélations de Snowden en 2013, nous savons que leurs activités incluent aussi l'espionnage industriel et la surveillance de masse.

Dans beaucoup de cas, les services de sécurité font faire leur travail par des sous-traitants privés qu'ils contrôlent notamment par l'intermédiaire des lois sur la sécurité nationale. La plupart des grands services de *cloud*, tels que *Gmail*, *Outlook* ou *Facebook*, sont soumis à la loi américaine, et doivent donc accepter d'espionner leurs utilisateurs au profit des agences de sécurité américaines, généralement sans aucun contrôle juridique (tout au moins lorsqu'il ne s'agit pas de ressortissants américains). Il en est naturellement de même en France [5], et même les serveurs logés en Suisse ne sont plus à l'abri [6].

Espionnage industriel et scientifique Comme une grande part de l'activité humaine, la recherche scientifique et la R&D industrielle se font aujourd'hui à travers l'Internet. Les chercheurs ne sont pas moins paresseux que les autres, et, par facilité, passent par des services américains de *cloud* tels que *Gmail* ou *Zoom*.

Ces services de *cloud* sont soumis à la loi américaine, et se voient donc obligés de communiquer les données de leurs utilisateurs aux agences de renseignement américaines, sans contrôle juridique lorsqu'il s'agit de données de ressortissants étrangers. Ces agences sont financées par les États-Unis, il est donc parfaitement normal qu'elles avantagent les intérêts américains, et qu'ils transmettent les données confidentielles qu'ils ont obtenues aux entreprises américaines.

Il est raisonnable de supposer qu'un résultat de recherche ou de développement européen se trouve entre les mains des entreprises américaines avant même d'être publié.

Surveillance de masse Les révélations de Snowden en 2013 ont confirmé ce que beaucoup soupçonnaient depuis longtemps : que les agences de renseignement réalisent un vaste programme de surveillance de masse, et qu'elles surveillent des millions de personnes sans aucun contrôle juridique. Les révélations de Nacchio en 2007 indiquent que cette surveillance de masse a lieu depuis longtemps, et que ce n'est pas uniquement suite aux attaques terroristes de septembre 2001 qu'elle a été mise en place.

5. Loi du 24 juillet 2015 relative au renseignement.
6. `https://protonmail.com/blog/climate-activist-arrest/`

Nous ne connaissons pas les buts de cette surveillance de masse, mais nous savons qu'elle s'effectue à une échelle absolument énorme. Par exemple, la consommation (déclarée) du centre de calcul de la NSA dans l'Utah se mesure en dizaines de MW.

Il est raisonnable de supposer que chacun de nous est surveillé à un moment ou un autre de sa vie, et peut-être même en permanence.

3.2 Sécurité des protocoles

Avant les révélations de Snowden, la sécurité informatique visait avant tout à se prémunir des attaques ciblées. Une partie de la communeauté du réseau travaille aujourd'hui à se prémunir contre l'espionnage et la surveillance de masse [7], ce qui demande des techniques légèrement différentes. D'un côté, on ne peut plus faire confiance au fournisseur de service internet ou au serveur, ce qui complique les choses ; d'un autre côté, les attaques de masse sont souvent des attaques passives, dont il est relativement facile de se protéger.

Nous verrons tout au long de ce cours des techniques cryptographiques visant à assurer l'authenticité et la confidentialité des échanges, et à nous prémunir des attaques ciblées actives et des attaques de masse passives.

7. RFC 7258