RFC 7558 : Requirements for Scalable DNS-SD/mDNS Extensions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 juillet 2015

Date de publication du RFC : Juillet 2015

https://www.bortzmeyer.org/7558.html

Pour résoudre des noms de domaine en informations (comme l'adresse IP) sur le réseau local, sans configurer de serveur DNS, nous avons mDNS (RFC 6762 [1]). Pour découvrir des services (par exemples les imprimantes) avec ce mDNS, nous avons DNS-SD (RFC 6763). Mais ces deux techniques, mDNS et DNS-SD, ne fonctionnent que sur un seul segment du réseau, à l'intérieur d'un domaine de diffusion. Il serait bien pratique de pouvoir les utiliser dans un réseau étendu (comme l'Internet...). Ce RFC décrit le problème, les souhaits et établit une liste d'exigences pour cette extension de mDNS et DNS-SD « au-delà du lien local ». (À l'heure actuelle, on n'a pas encore de solution satisfaisant ces exigences.)

C'est par conception que mDNS (RFC 6762) ne passe pas les routeurs IP. Ce protocole marche par diffusion. On crie à la cantonade « qui connait iPhone-de-Jean-Bernard ? » et la machine qui se reconnait répond. mDNS s'appuie donc sur un service de couche 2, la diffusion, et ne fonctionne donc pas sur un réseau composé de plusieurs segments L2 reliés par des routeurs.

Or, il y a évidemment des cas où on voudrait des services comme ceux fournis par mDNS et DNS-SD au-delà du lien local. Parce que le campus ou l'entreprise où on travaille a plusieurs segments L2 (par exemple un pour le filaire et un pour le WiFi), ou bien parce qu'on travaille avec une association située à des centaines de kilomètres, mais joignable par l'Internet. Il n'existe pas actuellement de solutions standard pour cela. Et pas encore de consensus sur la façon la plus propre de le faire.

Autre cas où on se retrouve facilement coincé, celui de réseaux ad hoc comme les 6LowPAN (RFC 6568) où chaque machine ou presque peut devenir routeur (RFC 4903).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6762.txt

D'ailleurs, même en l'absence de ce problème multi-segments, la technique de mDNS, la diffusion (globale, ou bien restreinte) n'est pas idéale dans tous les cas. Sur de l'Ethernet filaire, la diffusion consomme relativement peu de ressources. Mais, sur certains segments, la diffusion coûte cher. En WiFi, elle peut vite mener à consommer une bonne partie de la capacité, d'autant plus qu'il faut ralentir au niveau du récepteur le plus lent (cf. section 2.2). Au passage, autre problème de 802.11 : il n'y a pas d'accusé de réception des trames diffusées et donc des pertes peuvent se produire.

La section 2 de notre RFC décrit le problème qu'on veut résoudre. D'abord, on voudrait pouvoir découvrir des ressources distantes (comme des imprimantes ou des serveurs de fichier) même si elles ne sont pas sur le même segment L2. Actuellement, la seule solution standard est le DNS classique. Cela nécessite soit une configuration manuelle par l'administrateur système, ce qui fait du travail, surtout en cas de changement (on modifie l'adresse IP de l'imprimante mais on oublie de changer la base DNS : tous les sites n'ont pas forcément un IPAM intégré qui prend en charge tout cela et tous les réseaux ne sont pas centralement gérés). Autre solution avec le DNS classique, autoriser les mises à jour dynamiques du DNS, ce qui implique qu'on configure les imprimantes pour faire ces mises à jour.

Et la solution à ce problème doit marcher pour des cas où on a des centaines ou des milliers de machines, et à un coût raisonnable (y compris le coût pour le réseau en terme de trafic).

Les réseaux contraints (LLN pour "*Low power and Lossy Networks*", cf. RFC 7102) posent des défis particuliers. Ils sont souvent multi-segments, avec des nœuds devenant routeurs pour prolonger la portée des ondes radio, et ne peuvent donc pas se contenter des actuels mDNS et DNS-SD. Mais ils connectent souvent des machines peu dotées en ressources. Celles-ci sont parfois injoignables (hibernation ou déconnexion) et on ne peut donc pas compter sur leur présence permanente. Ainsi, mDNS assure l'unicité des noms par la vérification, par une nouvelle machine, que le nom n'était pas déjà présent sur le réseau. Si le possesseur de ce nom hiberne, il ne pourra pas « défendre » son nom.

La section 3 du RFC présente ensuite quelques scénarios d'usage concrets, pour qu'on se fasse une meilleure idée de cas où mDNS et DNS-SD ne suffisent pas. D'abord, un cas de base, le PAN ("*Personal Area Network*", qui regroupe les machines d'un seul utilisateur, par exemple, dans un cas trivial, son PC portable et son imprimante). Pas de routeur présent, mDNS et DNS-SD suffisent bien et résolvent tous les problèmes. On passe ensuite à un cas un peu plus riche : une maison, avec un routeur qui connecte à un FAI et un réseau local d'un seul segment (il peut y avor plusieurs segments physiques, par exemple filaire et WiFi, mais le routeur, qui fait également point d'accès WiFi, les présente comme un seul réseau L2. C'est le réseau de M. Michu aujourd'hui et, là encore, mDNS et DNS-SD marchent bien.

On passe ensuite au réseau SOHO ou bien à la maison « avancée ». Cette fois, on introduit plusieurs routeurs (RFC 7368). Un tel réseau peut s'auto-organiser (il n'y a typiquement pas d'administrateur réseaux professionnel) mais la résolution de noms devient difficile, mDNS ne fonctionnant plus (il ne passe pas les routeurs).

Ensuite viennent les réseaux d'« entreprise » (en fait, de n'importe quelle grande organisation, entreprise à but lucratif ou pas). Plusieurs routeurs, des réseaux compliqués mais, cette fois, on a des administrateurs réseaux professionnels pour s'en occuper. À noter que les grands réseaux des conférences (comme le réseau WiFi des réunions IETF) rentrent dans cette catégorie. mDNS ne marche plus mais on peut désormais avoir des serveurs DNS administrés sérieusement.

Le RFC cite un cas encore plus élaboré, avec les NREN, qui mèlent administration centrale du réseau national, avec des équipes qui gèrent des réseaux régionaux ou de campus.

Et les réseaux « "*mesh*" » ? Ils sont multi-segments mais en général pas administrés, ils posent donc le plus de problèmes.

Bon, assez de préliminaires, les exigences maintenant, le vrai cahier des charges. Il figure en section 4. Les exigences sont notées REQn où N est un numéro de 1 à 15. REQ1, par exemple, dit qu'il faut un mode d'auto-configuration permettant à la future solution de marcher toute seule, pour le cas des réseaux non administrés. Mais attention, le RFC précise aussi que les objectifs de sécurité, de passage à l'échelle, de facilité et de déployabilité sont souvent contradictoires et qu'il ne faut pas prendre les exigences isolément mais en groupe (il faudra parfois en sacrifier une pour atteindre l'autre).

REQ2, complémentaire de REQ1, dit que pour les réseaux administrés, il faut pouvoir configurer le mécanisme de manière à partitionner le réseau, pour éviter qu'une requête ne voyage partout (voir aussi REQ15). REQ3 demande que cette possibilité de partition ne se fasse pas sur des critères topologiques (si on a deux segments dans un même bâtiment et un troisième dans un autre bâtiment, il faut pouvoir faire une partition regroupant un des segments du bâtiment et le segment de l'autre bâtiment, voir aussi REQ7).

Parmi les autres exigences, le fait (REQ5) de réutiliser les protocoles existants, notamment mDNS (RFC 6762) et DNS-SD (RFC 6763), l'obligation de fonctionner sur des réseaux où la consommation électrique est un facteur crucial (REQ10, qui dit en gros que le protocole ne doit pas réveiller toutes les machines toutes les cinq minutes), la nécessité de marcher correctement sur des réseaux de plusieurs milliers de machines (REQ11), l'importance de fournir aux utilisateurs un vécu identique que les ressources qu'ils cherchent soient locales au lien ou au contraire distantes (REQ12), le souhait que l'information présentée audit utilisateur ne soit pas dépassée (pas question de lui montrer les services tels qu'ils étaient il y a deux heures, ou même simplement deux minutes, REQ13), etc.

Après cette liste d'exigences, la section 5 de notre RFC se penche sur un problème délicat, la coexistence de plusieurs espaces de noms. En effet, si on utilise le DNS « normal », les noms sont uniques, et c'est une des propriétés les plus essentielles du DNS (RFC 2826). Mais si on utilise mDNS, chaque segment réseau a ses propres noms, sous le TLD `.local`. On peut parfaitement avoir une `Imprimante-Couleur.local` dans un bâtiment et voir une toute autre imprimante sous le même nom dans un autre bâtiment. Les noms ne sont plus mondialement uniques. Comme beaucoup d'engins seront livrés avec des noms par défaut identiques, ces « collisions » seront fréquentes. Le problème reste ouvert (voir aussi la section 6.2).

Enfin, la section 6 du RFC se préoccupe de la sécurité. Bien sûr, l'exigence d'un service automatique et efficace ne va pas forcément dans le sens de la sécurité (difficile d'authentifier sans ennuyer les utilisateurs, par exemple). Mais il y a aussi d'autres pièges. Par exemple, avec le mDNS traditionnel, les requêtes et les réponses ont une portée limitée (au seul segment de réseau local). Si on donne un nom à sa machine, le nom ne sera vu que localement et l'utilisateur peut donc donner un nom ridicule ou grossier sans trop de risques. Avec le projet d'étendre cette résolution de noms plus loin que le réseau local, le nom donné aura davantage de conséquences. Sans même parler du cas de noms à problèmes, une extension de la découverte de services peut faciliter la tâche d'un attaquant (imaginez ce que Shodan ferait d'un tel service) et/ou permettre/faciliter l'accès à des ressources qu'on pensait privées (une imprimante, par exemple). Bien sûr, la découverte d'un service n'implique pas son accessibilité mais le risque est quand même là.

Autre problème, la vie privée. Déjà, aujourd'hui, une technologie comme Bonjour est très bavarde. Un Mac ou un iPhone diffusent à tout le réseau local en donnant le nom de l'utilisateur ("l'iPhone de Jean Durand"). Mais le problème ne peut que s'aggraver si on va plus loin que le réseau local. Ce n'est sans doute pas une bonne idée qu'une machine arrivant dans un réseau inconnu annonce le nom de son propriétaire immédiatement. À noter que, en juillet 2015, une expérience de collecte du trafic diffusé <http://net.hs-augsburg.de/projects/2015/07/09/ietf-broadcast-analysis.html> à la réunion IETF de Prague <http://www.ietf.org/meeting/93/index.html> a suscité de nombreuses discussions <http://mailarchive.ietf.org/arch/msg/93attendees/88H9vnO2MNzhMJiwBtaxj6PnK