RFC 8910 : Captive-Portal Identification in DHCP and Router Advertisements (RAs)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 septembre 2020

Date de publication du RFC : Septembre 2020

https://www.bortzmeyer.org/8910.html

Les portails captifs sont une des plaies de l'accès à l'Internet. À défaut de pouvoir les supprimer, ce nouveau RFC propose des options aux protocoles DHCP et RA pour permettre de signaler la présence d'un portail captif, au lieu que la malheureuse machine ne doive le détecter elle-même. Il remplace le RFC 7710[1], le premier à traiter ce sujet. Il y a peu de changements de fond mais quand même deux modifications importantes. D'abord, il a fallu changer le code qui identifiait l'option DHCP en IPv4 (du code 160 au 114). Et ensuite l'URI annoncé sur le réseau est désormais celui de l'API et pas une page Web conçue pour un humain.

On trouve de tels portails captifs en de nombreux endroits où de l'accès Internet est fourni, par exemple dans des hôtels, des trains ou des cafés. Tant que l'utilisateur ne s'est pas authentifié auprès du portail captif, ses capacités d'accès à l'Internet sont très limitées. Quels sont les problèmes que pose un portail captif ?

— Le plus important est qu'il détourne le trafic normal : en cela, le portail captif est une attaque de l'Homme du Milieu et a donc de graves conséquences en terme de sécurité. Il éduque les utilisateurs à trouver normal le fait de ne pas arriver sur l'objectif désiré, et facilite donc le hameçonnage. Au fur et à mesure que les exigences de sécurité augmentent, ces portails captifs seront, on peut l'espérer, de plus en plus mal vus.
— Le portail captif ne marche pas ou mal si la première connexion est en HTTPS, ce qui est, à juste titre, de plus en plus fréquent. Là encore, il éduque les utilisateurs à trouver normaux les avertissements de sécurité (« mauvais certificat, voulez-vous continuer ? »).
— Le portail captif n'est pas authentifié, lui, et l'utilisateur est donc invité à donner ses informations de créance à un inconnu.
— En Wifi, comme l'accès n'est pas protégé par WPA, le trafic peut être espionné par les autres utilisateurs.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7710.txt

— Spécifique au Web, le portail captif ne marche pas avec les activités non-Web (comme XMPP). Même les clients HTTP non-interactifs (comme une mise à jour du logiciel via HTTP) sont affectés.

Pourquoi est-ce que ces hôtels et cafés s'obstinent à imposer le passage par un portail captif ? On lit parfois que c'est pour authentifier l'utilisateur mais c'est faux. D'abord, certains portails captifs ne demandent pas d'authentification, juste une acceptation des conditions d'utilisation. Ensuite, il existe une bien meilleure solution pour authentifier, qui n'a pas les défauts indiqués plus haut. C'est 802.1X, utilisé entre autres dans eduroam (voir RFC 7593). La vraie raison est plutôt une combinaison d'ignorance (les autres possibilités comme 802.1X ne sont pas connues) et de désir de contrôle (≪ je **veux** qu'ils voient mes publicités et mes CGU ≫).

L'IETF travaille à développer un protocole complet d'interaction avec les portails captifs, pour limiter leurs conséquences. En attendant que ce travail soit complètement terminé, ce RFC propose une option qui permet au moins au réseau local de signaler ≪ attention, un portail captif est là, ne lance pas de tâches - comme Windows Update - avant la visite du portail ≫. Cette option peut être annoncée par le serveur DHCP (RFC 2131 et RFC 8415) ou par le routeur qui envoie des RA (RFC 4861).

Cette option (section 2 du RFC) annonce au client qu'il est derrière un portail captif et lui fournit l'URI de l'API à laquelle accéder (ce qui évite d'être détourné, ce qui est grave quand on utilise HTTPS). Les interactions avec l'API de ce serveur sont spécifiées dans le RFC 8908.

Les sections 2.1, 2.2 et 2.3 de notre RFC donnent le format de l'option en DHCP v4, DHCP v6 et en RA. Le code DHCP v4 est 114 <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml#options> (un changement de notre RFC), le DHCP v6 est 103 <https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2> et le type RA est 37 <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-5>. Pour la création d'options DHCPv6 avec des URI, voir le RFC 7227, section 5.7.

Un URI spécial, `urn:ietf:params:capport:unrestricted` est utilisé pour le cas où il n'y a **pas** de portail captif. (Cet URI spécial est enregistré à l'IANA <https://www.iana.org/assignments/params/params.xml#params-1>, avec les autres suffixes du RFC 3553.)

Bien que la première version de ce RFC date de plus de quatre ans, la grande majorité des réseaux d'accès avec portail captif n'annoncent toujours pas la présence de ce portail et il faudra encore, pendant de nombreuses années, que les machines terminales ≪ sondent ≫ et essaient de détecter par elles-même s'il y a un portail captif ou pas. Elles font cela, par exemple, en essayant de se connecter à une page Web connue (comme avec Firefox). Ici, en cas de vrai accès Internet :

```
%  curl http://detectportal.firefox.com/
success
```

Et ici lorsqu'il y a un portail captif qui détourne le trafic :

```
% curl -v http://detectportal.firefox.com/
> GET / HTTP/1.1
> Host: detectportal.firefox.com
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 302 Moved Temporarily
```

```
< Server: nginx
< Date: Mon, 27 Jul 2020 18:29:52 GMT
...
< Location: https://wifi.free.fr/?url=http://detectportal.firefox.com/
<
<html>
<head><title>302 Found</title></head>
<body bgcolor="white">
<center><h1>302 Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

La section 5 de notre RFC étudie les conséquences de cette option pour la sécurité. Elle rappelle que DHCP et RA ne sont pas sécurisés, de toute façon. Donc, un méchant peut envoyer une fausse option « il y a un portail captif, allez à cet URI pour vous authentifier » mais le même méchant peut aussi bien annoncer un faux routeur et ainsi recevoir tout le trafic... Si on n'utilise pas des précautions comme le "*RA Guard*" (RFC 6105) ou le "*DHCP shield*" (RFC 7610), on ne peut de toute façon pas se fier à ce qu'on a obtenu en DHCP ou RA.

Il est même possible que cette option nouvelle améliore la sécurité, en n'encourageant pas les utilisateurs à couper les mécanismes de validation comme la vérification des certificats, contrairement à ce que font les portails captifs actuels, qui se livrent à une véritable attaque de l'Homme du Milieu.

Pour DHCP, la plupart des serveurs permettent de servir une option quelconque, en mettant ses valeurs manuellement et une future mise à jour ne servira donc qu'à rendre l'usage de cette option plus simple. (Pour RA, c'est plus complexe, cf. l'expérience lors d'une réunion IETF <https://tickets.meeting.ietf.org/wiki/CAPPORT>.) Autrement, je ne connais pas encore de mise en œuvre côté clients DHCP ou RA, mais il semble (je n'ai pas testé personnellement) que ça marche sur iOS à partir de la version 14 <https://mailarchive.ietf.org/arch/msg/captive-portals/QoR4xbHFIgKZxMbCjK-2Muh9J>.

L'annexe B de notre RFC cite les changements depuis le RFC 7710. Les principaux :

— L'ajout de l'URN `urn:ietf:params:capport:unrestricted` pour le cas où il n'y a pas de portail captif,
— le changement de l'option DHCP en IPv4, suite à la collision avec les produits Polycom <https://community.polycom.com/t5/VoIP-SIP-Phones/DHCP-Standardization-160-vs-66/td-p/72577>,
— l'URI envoyée désigne désormais une API et plus una page Web ordinaire (contrairement à ce que dit l'annexe B de notre RFC, il ne s'agit pas d'une clarification mais d'un vrai changement),
— les noms (et plus seulement les adresses IP) sont acceptés dans l'URI,
— et plusieurs éclaircissements et précisions.