

Vidéo - Exemples d'en-têtes IPv6 dans Wireshark (6 min)

Cet écran illustre une capture de paquets dans Wireshark ainsi que les informations de la couche réseau d'une conversation IPv6. Examinons la capture d'écran. Comme vous pouvez le voir, le paquet mis en surbrillance est le numéro 46 et l'adresse source précisée ici dans la liste des paquets est une adresse de monodiffusion globale IPv6 puisqu'elle commence par 2001:6f8. L'adresse de destination est aussi une adresse de monodiffusion globale 2001:6f8:900. Si nous examinons le champ du protocole, nous voyons qu'au niveau des couches supérieures, il s'agit d'un paquet TCP et d'une tentative visant à établir une communication initiale avec un serveur Web HTTP. Dans les informations de la couche réseau plus bas, vous pouvez voir que les informations IPv6 sont développées. Examinons de plus près certaines informations des champs du protocole IPv6. Tout d'abord, vous pouvez voir que la quantité d'informations dans l'en-tête IPv6 est bien plus limitée que dans l'en-tête IPv4.

Cela dit, certaines sont très intéressantes. D'abord, vous constatez que le champ de la version est identique. Dans cet exemple, il indique 6, puisqu'il s'agit d'un paquet IPv6. Le chiffre binaire 6 apparaît également ici. Le champ suivant est le champ de la classe de trafic. Ce champ a une fonction identique à celle du champ des services différenciés dans un paquet IPv4. Il gère la hiérarchisation du trafic et l'encombrement. La section suivante concerne l'indicateur de flux, ou Flowlabel. Le champ Flowlabel est un nouveau champ du protocole IPv6. Son objectif est de conserver les mêmes flux de paquets sur les routeurs et les commutateurs pour faciliter la tâche des applications en temps réel qui ont besoin que les paquets arrivent dans le même ordre. Le champ suivant indique la longueur des données utiles. Il correspond au champ de la longueur totale de l'en-tête IPv4. Ce champ indique la taille totale du paquet, dans ce cas-ci 40 octets. Le champ de l'en-tête suivant a la même fonction que le champ du protocole d'un paquet IPv4. Vous voyez qu'il identifie TCP, ou 6, comme la partie données de la couche supérieure de ce paquet. La limite de sauts a une fonction identique à celle du champ TTL dans un paquet IPv4. Vous voyez qu'actuellement la limite définie est de 64 sauts. Une fois cette valeur revenue à 0, le paquet est abandonné. Ensuite, nous avons l'adresse IPv6 source, l'adresse IPv6 de destination puis, au niveau de la couche supérieure, nous voyons qu'il s'agit d'un paquet TCP avec des informations d'en-tête TCP. Examinons à présent la capture d'écran suivante. Sur cet écran, vous voyez que le paquet 49 est à présent en surbrillance.

Et qu'une connexion a été établie avec le serveur web. Ce paquet est une requête GET envoyée au serveur web. Si nous examinons la fenêtre de détails du paquet IPv6 à présent agrandie, nous voyons que les données utiles sont bien plus longues. Au-dessous, nous voyons les informations IPv6, les informations TCP mais aussi les informations du protocole HTTP contenues dans la requête GET. Cette requête GET permet d'accéder à une page web. Passons à l'écran suivant. Cette dernière capture affiche un message de sollicitation de voisin ICMP version 6. En examinant la fenêtre du paquet mis en surbrillance ici, le numéro un, nous pouvons voir que, cette fois, l'adresse source n'est pas une adresse IPv6 de monodiffusion globale, mais une adresse link-local puisqu'elle commence par fe80. Nous constatons aussi que cette adresse link-local utilise EUI-64 pour résoudre la partie ID d'interface de l'adresse. Nous pouvons le déduire de la présence de ff:fe dans l'adresse. L'adresse de destination est une adresse IPv6 ff02, indiquant qu'il s'agit d'un paquet multidiffusion. L'examen du protocole révèle qu'il s'agit d'ICMP version 6. Ensuite, les informations relatives au paquet nous indiquent qu'il s'agit d'un message de sollicitation de voisin pour le même périphérique contacté dans les captures d'écran précédentes. Pour l'essentiel, la fonction de ce paquet est identique à une requête ARP dans IPv4. Comme nous devons identifier l'adresse link-local de ce périphérique, nous envoyons un message de sollicitation de voisin ICMP v6 en mode multidiffusion en espérant obtenir en retour une adresse link-local de ce voisin. Plus bas dans la fenêtre de détails agrandie, vous voyez toutes les informations du paquet : la version 6, la classe de trafic, l'indicateur du flux, la longueur des données utiles, c.-à-d. la longueur totale du paquet. Puis nous avons le champ de l'en-tête suivant, qui est identique au champ du protocole dans IPv4, et affiche la valeur 58, indiquant que la partie données du paquet est un message ICMP v6. Vient ensuite la limite de sauts, soit 255. Ce champ est similaire au champ TTL. Et enfin l'adresse link-local source ainsi que l'adresse IPv6 de multidiffusion de destination. Tout en bas, sous les informations IPv6, une section spécifique à ICMP version 6 peut être agrandie.