Vidéo - Exemples d'en-têtes IPv4 dans Wireshark (6 min)

Nous allons voir comment afficher et analyser les informations de la couche réseau dans une capture de paquets Wireshark. Vous voyez ici une capture de paquets Wireshark. Comme vous pouvez le constater, le deuxième paquet capturé est mis en surbrillance et, dans la fenêtre de détails du paquet, les informations de la couche réseau sont développées pour montrer tout ce qui se passe au niveau de la couche réseau.

Examinons à présent les informations relatives au paquet en question. Avant toute chose, nous pouvons voir que le protocole de couche réseau, ou protocole de couche Internet, de ce paquet est le protocole IP version 4, ou IPv4. Nous pouvons également voir que l'adresse IP source est 192.168.1.109. Notez qu'elle est également mise en surbrillance plus haut dans la liste de paquets. L'adresse IP de destination est 192.168.1.1. Elle figure également dans la liste de paquets. Enfin, nous voyons qu'au niveau de la couche supérieure, il s'agit d'un paquet du protocole TCP. Mais si nous nous limitons aux seuls champs IPv4, donc aux informations IPv4, nous pouvons voir les différents types d'informations de contrôle contenues dans chaque paquet IPv4.

Par exemple, le numéro de version, ici 4, qui l'identifie comme un paquet IPv4 et non comme un paquet IPv6. La longueur de l'en-tête qui représente la taille minimale d'un en-tête IPv4. Le champ des services différenciés, qui sert à hiérarchiser les paquets et sert à des applications telles que la voix sur IP. Nous avons la longueur totale du paquet et le numéro d'identification utilisé pour la fragmentation. Les indicateurs : vous voyez ici que le bit DF a été défini. DF signifie « don't fragment », ou « ne pas fragmenter ». En d'autres termes, le paquet n'est pas suffisamment grand ou n'est pas identifié comme étant fragmentable. Ici, nous avons le décalage du fragment, puis le TTL, ou la durée de vie, dont la valeur est 128. Chaque fois qu'un paquet est acheminé d'un tronçon à un autre, la valeur TTL est décrémentée. Lorsqu'elle passe à 0, le paquet est abandonné pour éviter que les paquets circulent en boucle sans fin sur Internet. La valeur TTL est également utilisée dans les requêtes traceroute et ping ICMP. Le champ du protocole indique le type d'informations auquel s'attendre dans la partie données du paquet. La valeur 6 identifie la partie données de ce paquet comme un paquet TCP. Le champ de la somme de contrôle d'en-tête permet aux routeurs de vérifier la présence d'erreurs ou d'incohérences dans l'en-tête IP. Si c'est le cas, le paquet est abandonné.

Enfin, nous avons les adresses IP source et de destination, qui représentent les informations les plus importantes du paquet IPv4. Examinons à présent deux autres écrans illustrant des captures de paquets Wireshark. Ils présentent des similitudes et des différences avec le précédent. La capture d'écran suivante illustre le huitième paquet capturé. L'adresse IP source du paquet est toujours 192.168.1.109 et l'adresse IP de destination 192.168.1.1., mais il s'agit cette fois d'une requête HTTP GET. C'est une requête envoyée à un serveur Web dont l'adresse IP est 192.168.1.1. Vous constatez que les informations de la couche réseau, ou couche Internet, sont développées. Il s'agit également du protocole IP version 4 et nous avons des informations similaires dans les différents champs.

Notez toutefois que ce paquet a une longueur totale de 411 octets alors que le paquet précédent ne faisait que 52 octets. Ce paquet contient donc bien plus d'informations ou est beaucoup plus grand que le précédent. Si nous examinons les informations du protocole IPv4 plus bas, nous voyons que ce paquet contient des informations TCP, mais aussi des informations du protocole de transfert hypertexte, ou protocole HTTP, juste au-dessous. Passons ensuite au paquet suivant. Comme vous pouvez le voir dans le haut de l'écran, il s'agit du seizième paquet capturé. Il est aussi transmis par l'hôte 192.168.1.109 à l'hôte 192.168.1.1, sauf que là il s'agit du protocole ICMP. Dans les informations de la liste des paquets, vous voyez qu'il s'agit d'une requête echo, ou ping. Les informations du protocole IPv4 affichées dans la section de détails révèlent quelques différences mineures. Il s'agit toujours de la version 4 et l'en-tête a toujours une longueur de 20 octets. Mais les indicateurs sont légèrement différents et le champ de protocole a désormais la valeur 1, indiquant que la partie données du paquet est un message du protocole ICMP. Notez qu'une section est développée dans le bas de la fenêtre de détails pour pouvoir examiner les informations d'en-tête spécifiques au protocole ICMP.