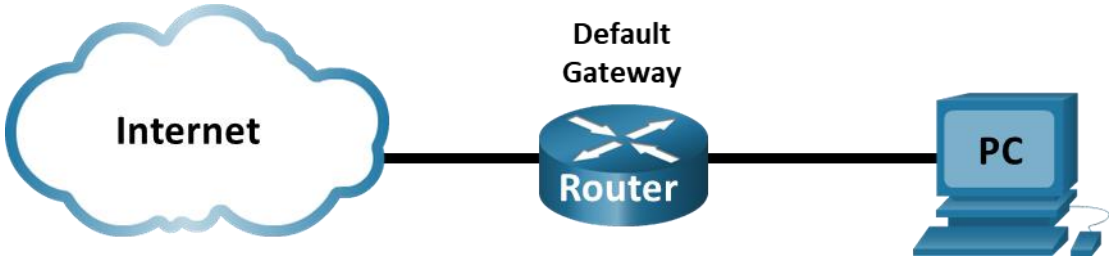
Travaux pratiques - Utiliser Wireshark pour examiner les trames Ethernet

Topologie



Objectifs

Partie 1 : Examiner les champs d'en-tête dans une trame Ethernet II

Partie 2 : Utiliser Wireshark pour capturer et analyser les trames Ethernet

Contexte/scénario

Lorsque des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI (Open Systems Interconnection) et sont encapsulées dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si les protocoles de couche supérieure sont TCP et IP et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet II. C'est généralement le cas pour un environnement de réseau local (LAN).

Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames. Dans la première partie de ce TP, vous allez examiner les champs figurant dans une trame Ethernet II. Dans la deuxième partie, vous allez utiliser Wireshark pour capturer et analyser les champs d'en-tête de trame Ethernet II pour le trafic local et distant.

Ressources requises

- 1 PC (Windows avec accès à Internet et avec Wireshark installé)

Instructions

Partie 1 : Examiner les champs d'en-tête dans une trame Ethernet II

Dans la première partie, vous allez examiner les champs d'en-tête et le contenu d'une trame Ethernet II. Une capture Wireshark sera utilisée pour examiner le contenu de ces champs.

Étape 1: Consultez les descriptions et les longueurs des champs d'en-tête Ethernet II.

Préambule	Adresse de destination	Adresse source	Type de trame	Données	FCS
8 octets	6 octets	6 octets	2 octets	De 46 à 1 500 octets	4 octets

Étape 2: Examinez la configuration réseau de l'ordinateur.

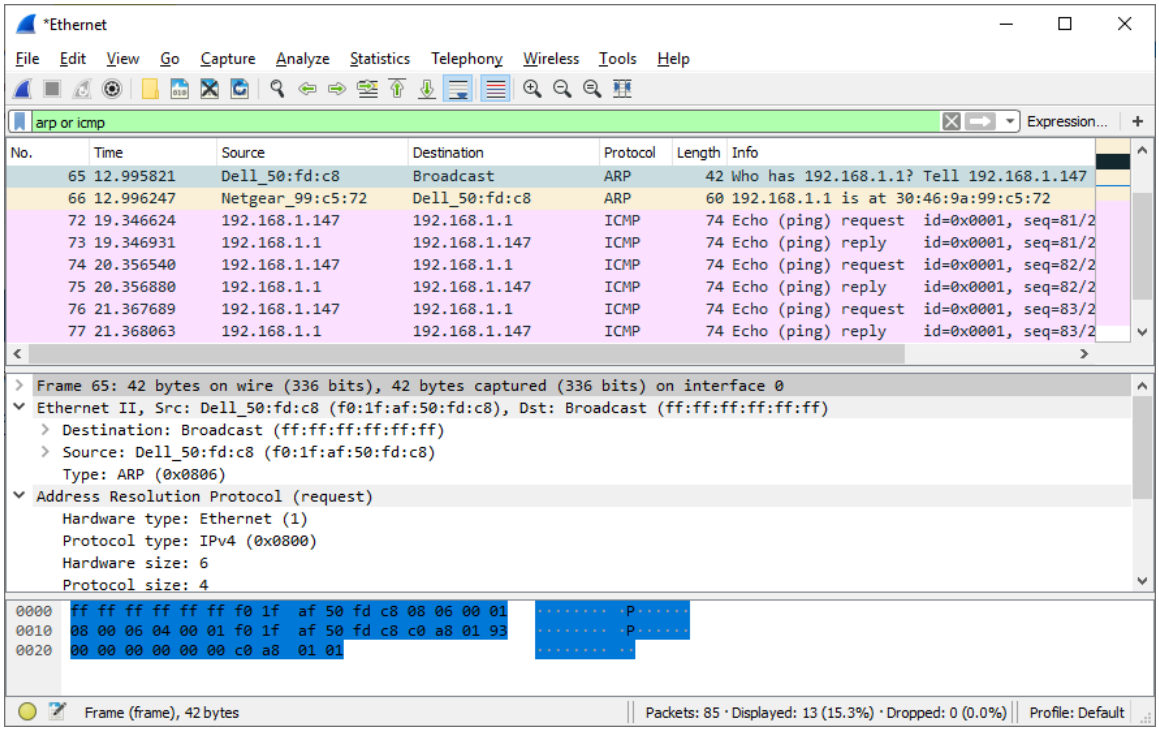
Dans cet exemple, l'adresse IP de l'hôte du PC est 192.168.1.147 et la passerelle par défaut a une adresse IP de 192.168.1.1.

```
C:\ ipconfig /all


Adaptateur Ethernet :

   Suffixe DNS propre à la connexion . :
   Description . . . . . . . . . . . : Connexion de réseau Intel(R) 82579LM Gigabit
   Physical Address. . . . . . . . .  : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80 : :58c 5:45 f 2:7 e5e:29c 2% 11 (Préféré)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147 (Préféré)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, September 6, 2019 11:08:36 AM
   Lease Expires . . . . . . . . . . : Saturday, September 7, 2019 11:08:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

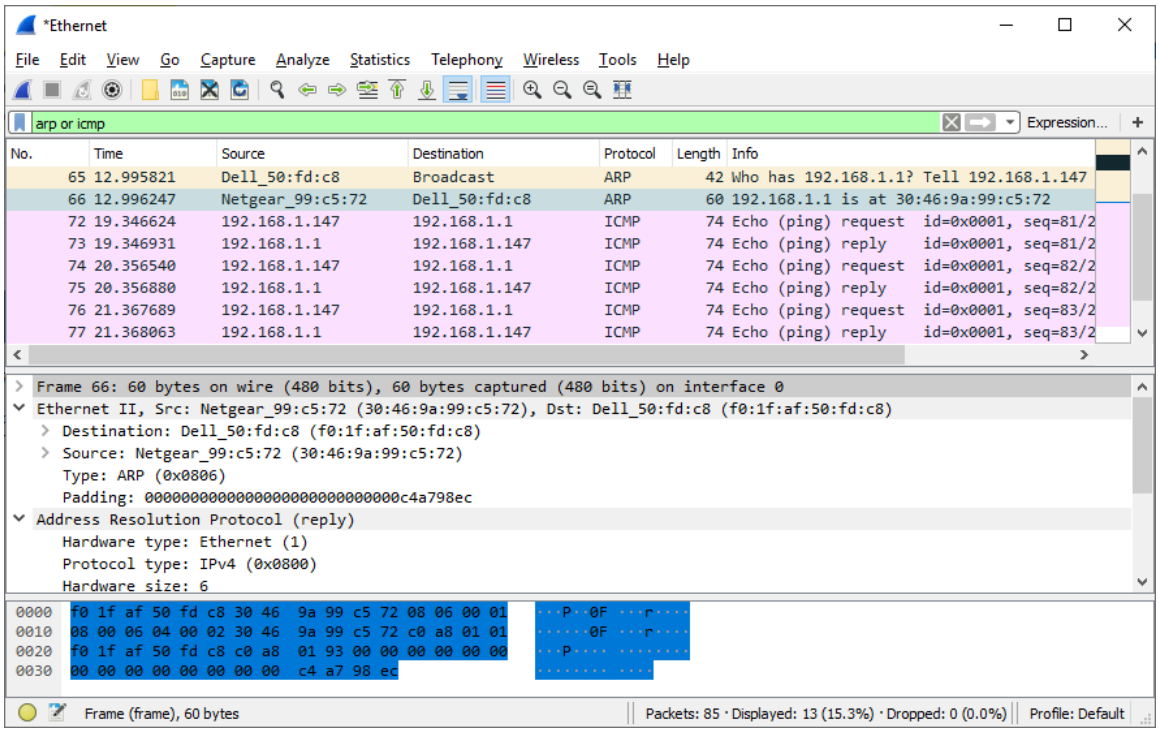
Étape 3: Examinez les trames Ethernet dans une capture Wireshark.

Les captures d'écran de la capture Wireshark ci-dessous montrent les paquets générés par un ping émis depuis un PC hôte vers sa passerelle par défaut. Un filtre a été appliqué à Wireshark pour afficher les protocoles ARP et ICMP uniquement. ARP signifie protocole de résolution d'adresse. ARP est un protocole de communication utilisé pour déterminer l'adresse MAC associée à l'adresse IP. La session commence par une requête ARP pour l'adresse MAC du routeur de passerelle, suivie de quatre requêtes ping et réponses.

Cette capture d'écran met en évidence les détails du trame pour une requête ARP.



Cette capture d'écran met en évidence les détails du trame pour une réponse ARP.



Étape 4: Examinez le contenu d'en-tête Ethernet II d'une requête ARP.

Le tableau suivant prend la première trame dans la capture Wireshark et affiche les données présentes dans les champs d'en-tête Ethernet II.

Champ	Valeur	Description
Préambule	Non affichée dans la capture	Ce champ contient des bits de synchronisation traités par la carte réseau.
Adresse de destination Adresse source	Diffusion (ff:ff:ff:ff:ff:ff) NetGear_99:c 5:72 (30:46:9 a:99:c 5:72)	Les adresses de couche 2 pour la trame. La longueur de chaque adresse est de 48 bits, ou 6 octets, exprimés en 12 chiffres hexadécimaux, `de 0 à 9 et de A à F`. Le format suivant est courant : `12:34:56:78:9A:BC`. Les six premiers chiffres hexadécimaux indiquent le fabricant de la carte réseau, les six derniers chiffres hexadécimaux correspondent au numéro de série de la carte réseau. L'adresse de destination peut être une adresse de diffusion, qui ne contient que des 1, ou une adresse de monodiffusion. L'adresse source est toujours à monodiffusion.
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le type de protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet II. Deux types de trame standard sont : Valeur Description `0x0800` IPv4 Protocol `0x0806` Protocole ARP (Address Resolution Protocol)
Données	ARP	Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1 500 octets.

Champ	Valeur	Description
FCS	Non affichée dans la capture	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par le dispositif d'envoi, englobant les adresses de trame, le type et le champ de données. Elle est vérifiée par le récepteur.

Quel élément est important en ce qui concerne le contenu du champ d'adresse de destination ?

Pourquoi l'ordinateur envoie-t-il une diffusion ARP avant d'envoyer la première requête ping ?

Quelle est l'adresse MAC de la source dans la première trame ?

Quel est l'ID du vendeur (OUI) du NIC source dans la réponse de l'ARP ?

À quelle partie de l'adresse MAC correspond l'identifiant OUI ?

Quel est le numéro de série de la carte réseau de la source ?

Partie 2 : Utiliser Wireshark pour capturer et analyser les trames Ethernet

Dans la deuxième partie, vous allez utiliser Wireshark pour capturer les trames Ethernet locales et distantes. Vous examinerez ensuite les informations contenues dans les champs d'en-tête de trame.

Étape 1: Déterminez l'adresse IP de la passerelle par défaut sur votre ordinateur.

Ouvrez une fenêtre d'invite de commandes et entrez la commande **ipconfig**.

Quelle est l'adresse IP de la passerelle par défaut de l'ordinateur ?

Étape 2: Commencez par capturer le trafic sur la carte réseau de votre ordinateur.

a. Ouvrez Wireshark pour lancez la capture des données.

b. Observez le trafic qui apparaît dans la fenêtre Packet List.

Étape 3: Filtrez Wireshark pour afficher uniquement le trafic ICMP.

Vous pouvez utiliser le filtre dans Wireshark pour bloquer la visibilité du trafic indésirable. Le filtre ne bloque pas la saisie de données indésirables ; il ne filtre que ce que vous voulez afficher à l'écran. Pour le moment, seul le trafic ICMP doit être affiché.

Dans la zone **Filter** (filtre) de Wireshark, saisissez **icmp**. La case devient verte si vous avez correctement tapé le filtre. Si la case est verte, cliquez sur **Apply** pour appliquer le filtre.

Étape 4: À partir de la fenêtre d'invite de commandes, envoyez une requête ping à la passerelle par défaut de votre ordinateur.

À partir de la fenêtre de commandes, envoyez une requête ping à la passerelle par défaut avec l'adresse IP que vous avez notée à l'étape 1.

Étape 5: Arrêtez la capture du trafic sur la carte réseau.

Cliquez sur l'icône **Stop Capturing Packets** pour arrêter la capture de trafic.

Étape 6: Examinez la première requête Echo (ping) dans Wireshark.

La fenêtre principale de Wireshark est divisée en trois sections : le volet Packet List (en haut), le volet **Packet Details** (au milieu) et le volet **Packet Bytes** (en bas). Si vous avez sélectionné la bonne interface pour la capture de paquets précédemment, Wireshark devrait afficher les informations ICMP dans le volet de la liste de paquets de Wireshark.

a. Dans le volet Packet List (section supérieure), cliquez sur la première trame répertoriée. **Echo (ping) request** (requête écho (ping)) devrait s'afficher en dessous de l'en-tête **Info**. La ligne doit maintenant être mise en surbrillance.

b. Examinez la première ligne du volet Packet Details (section centrale). Cette ligne affiche la longueur de la trame.

c. La deuxième ligne dans le volet Packet Details indique qu'il s'agit d'une trame Ethernet II. Les adresses MAC source et de destination sont également indiquées.

Quelle est l'adresse MAC de la carte réseau de l'ordinateur ?

Quelle est l'adresse MAC de la passerelle par défaut ?

d. Vous pouvez cliquer sur le signe plus grand que (>) au début de la deuxième ligne pour obtenir plus d'informations sur la trame Ethernet II.

Quel type de trame est affiché ?

e. Les deux dernières lignes figurant dans la section centrale fournissent des informations sur le champ de données de la trame. Notez que les données contiennent les informations d'adresse IPv4 de la source et de la destination.

Quelle est l'adresse IP source ?

Quelle est l'adresse IP de destination ?

f. Vous pouvez cliquer sur n'importe quelle ligne dans la section centrale pour mettre en surbrillance cette partie de la trame (hex et ASCII) dans le volet **Packet Bytes** (section inférieure). Cliquez sur la ligne **Internet Control Message Protocol** (protocole ICMP) dans la section centrale et examinez ce qui est mis en surbrillance dans le volet **Packet Bytes**.

Quelles sont les deux dernières lettres des octets mis en surbrillance ?

g. Cliquez sur la trame suivante dans la section supérieure et examinez une trame de réponse Echo. Notez que les adresses MAC source et de destination ont été inversées, car cette trame a été envoyée depuis le routeur de passerelle par défaut comme réponse au premier ping.

Quel périphérique et quelle adresse MAC s'affichent comme adresse de destination ?

Étape 7: Capturez des paquets pour un hôte distant.

a. Cliquez sur l'icône **Start Capture** (démarrer la capture) pour démarrer une nouvelle capture Wireshark. Une fenêtre contextuelle vous invite à enregistrer les précédents paquets capturés dans un fichier avant de démarrer une nouvelle capture. Cliquez sur **Continue without Saving** (continuer sans enregistrer).

b. Dans une fenêtre d'invite de commande, ping www.cisco.com.

c. Arrêtez la capture des paquets.

d. Examinez les nouvelles données dans le volet de la liste des paquets de Wireshark.

Dans la première trame de demande Echo (ping), quelles sont les adresses MAC source et de destination ?

Source:

Destination:

Quelles sont les adresses IP source et de destination figurant dans le champ de données de la trame ?

Source:

Destination:

Comparez ces adresses à celles que vous avez reçues à l'étape 6. La seule adresse qui a changé est l'adresse IP de destination. Pourquoi l'adresse IP de destination a-t-elle changé, alors que l'adresse MAC de destination est restée la même ?

Question de réflexion

Wireshark n'affiche pas le champ de préambule d'un en-tête de trame. Que contient le champ de préambule ?