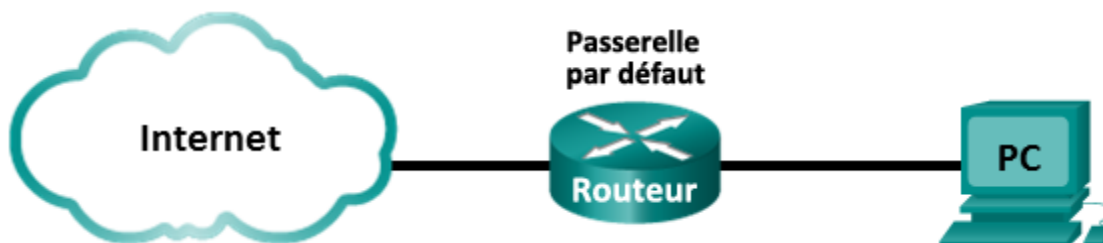


Travaux pratiques – Utilisation de Wireshark pour examiner les trames Ethernet

Topologie



Objectifs

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

2e partie : 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 sera 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 ces travaux pratiques, vous examinerez les champs figurant dans une trame Ethernet II. Dans la deuxième partie, vous utiliserez Wireshark pour capturer et analyser les champs d'en-tête de trame Ethernet II pour le trafic local et distant.

Ressources requises

- 1 ordinateur (Windows 7, Vista ou XP, doté d'un accès à Internet et sur lequel Wireshark est installé)

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

Dans la première partie, vous examinerez 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	46-1 500 octets	4 octets

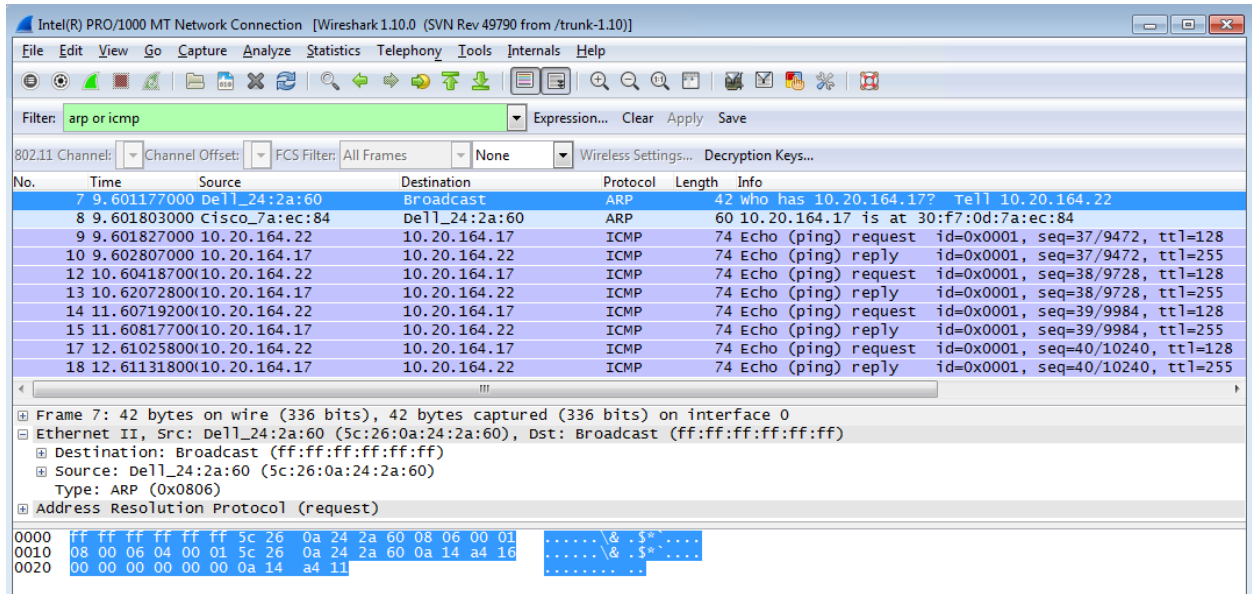
Étape 2 : Examinez la configuration réseau de l'ordinateur.

L'adresse IP de cet ordinateur hôte est 10.20.164.22 et la passerelle par défaut a l'adresse IP 10.20.164.17.

```
Carte Ethernet Connexion au réseau local :
Suffixe DNS propre à la connexion. . . : cisco.com
Adresse IPv6 de liaison locale. . . . : fe80::b875:731b:3c7b:c0b1%10
Adresse IPv4. . . . . : 10.20.164.22
Masque de sous-réseau. . . . . : 255.255.255.240
Passerelle par défaut. . . . . : 10.20.164.17
```

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

La capture Wireshark ci-dessous illustre les paquets générés par une requête ping envoyée depuis un ordinateur hôte à sa passerelle par défaut. Un filtre a été appliqué à Wireshark pour afficher les protocoles ARP et ICMP uniquement. La session commence par une requête ARP pour l'adresse MAC du routeur de passerelle, suivi de quatre requêtes ping et réponses.



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 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	Broadcast (ff:ff:ff:ff:ff:ff)	Les adresses de couche 2 pour la trame. Chaque adresse fait 48 bits de long, ou 6 octets, exprimés sous la forme de 12 chiffres hexadécimaux, 0–9, A–F. Un format courant est 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 à monodiffusion. L'adresse source est toujours à monodiffusion.						
Adresse source	Dell_24:2a:60 (5c:26:0a:24:2a:60)							
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le 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 : <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Valeur</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0x0800</td> <td>Protocole IPv4</td> </tr> <tr> <td>0x0806</td> <td>Protocole ARP (Address Resolution Protocol)</td> </tr> </tbody> </table>	Valeur	Description	0x0800	Protocole IPv4	0x0806	Protocole ARP (Address Resolution Protocol)
Valeur	Description							
0x0800	Protocole IPv4							
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.						
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 l'ordinateur émetteur, et englobe les adresses de trames, le type et le champ de données. Elle est vérifiée par le récepteur.						

Quel élément est-il 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 fournisseur (OUI) de la carte réseau source ? _____

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

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

2e partie : Utiliser Wireshark pour capturer et analyser les trames Ethernet

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

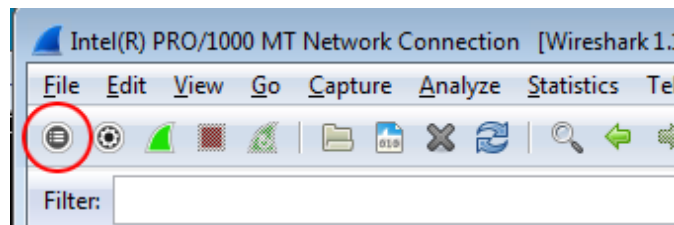
Étape 1 : Déterminez l'adresse IP de la passerelle par défaut sur votre ordinateur.

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

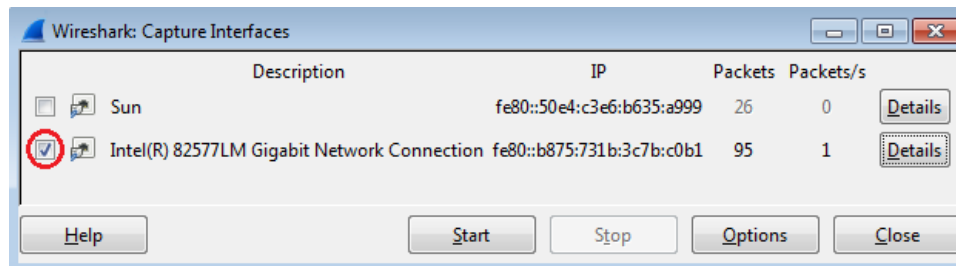
Quelle est l'adresse IP de la passerelle par défaut de l'ordinateur ? _____

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

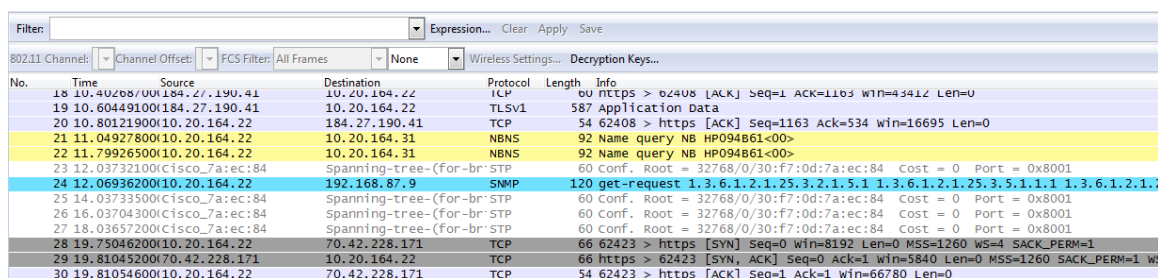
- Ouvrez Wireshark.
- Dans la barre d'outils de l'outil d'analyse de réseaux Wireshark, cliquez sur l'icône **Interface List (Liste d'interfaces)**.



- Dans la fenêtre Wireshark: Capture Interfaces (Wireshark : interfaces de capture), sélectionnez l'interface pour commencer la capture du trafic en activant la case à cocher appropriée, puis cliquez sur **Démarrer**. Si vous n'êtes pas sûr de l'interface à vérifier, cliquez sur **Détails** pour plus d'informations sur chaque interface répertoriée.



- Observez le trafic qui apparaît dans la fenêtre Packet List (Liste de paquets).

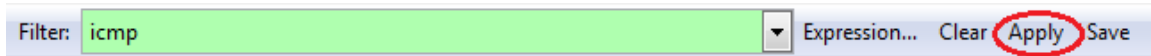


No.	Time	Source	Destination	Protocol	Length	Info
18	10.40208700	184.27.190.41	10.20.164.22	ICMP	60	icmp > 62408 [ACK] Seq=1 Ack=1163 Win=43412 Len=0
19	10.60449100	184.27.190.41	10.20.164.22	TLSv1	587	Application Data
20	10.80121900	10.20.164.22	184.27.190.41	TCP	54	62408 > https [ACK] Seq=1163 Ack=534 Win=16695 Len=0
21	11.04927800	10.20.164.22	10.20.164.31	NBNS	92	Name query NB HP094B61<00>
22	11.79926500	10.20.164.22	10.20.164.31	NBNS	92	Name query NB HP094B61<00>
23	12.03732100	cisco_7a:ec:84		Spanning-tree-(for-br) STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
24	12.06936200	10.20.164.22	192.168.87.9	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.2
25	14.03733500	cisco_7a:ec:84		Spanning-tree-(for-br) STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
26	16.03704300	cisco_7a:ec:84		Spanning-tree-(for-br) STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
27	18.03657200	cisco_7a:ec:84		Spanning-tree-(for-br) STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
28	19.75046200	10.20.164.22	70.42.228.171	TCP	66	62423 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1
29	19.81045200	70.42.228.171	10.20.164.22	TCP	66	https > 62423 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1260 SACK_PERM=1 WS
30	19.81054600	10.20.164.22	70.42.228.171	TCP	54	62423 > https [ACK] Seq=1 Ack=1 Win=66780 Len=0

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 capture des données indésirables ; il filtre uniquement ce qui doit s'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 tapé le filtre correctement. Si la case est verte, cliquez sur **Appliquer (Apply)** pour appliquer le filtre.

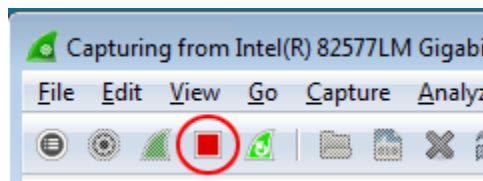


Étape 4 : À partir de la fenêtre d’invite de commandes, envoyez une requête ping à la passerelle par défaut de votre ordinateur.

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

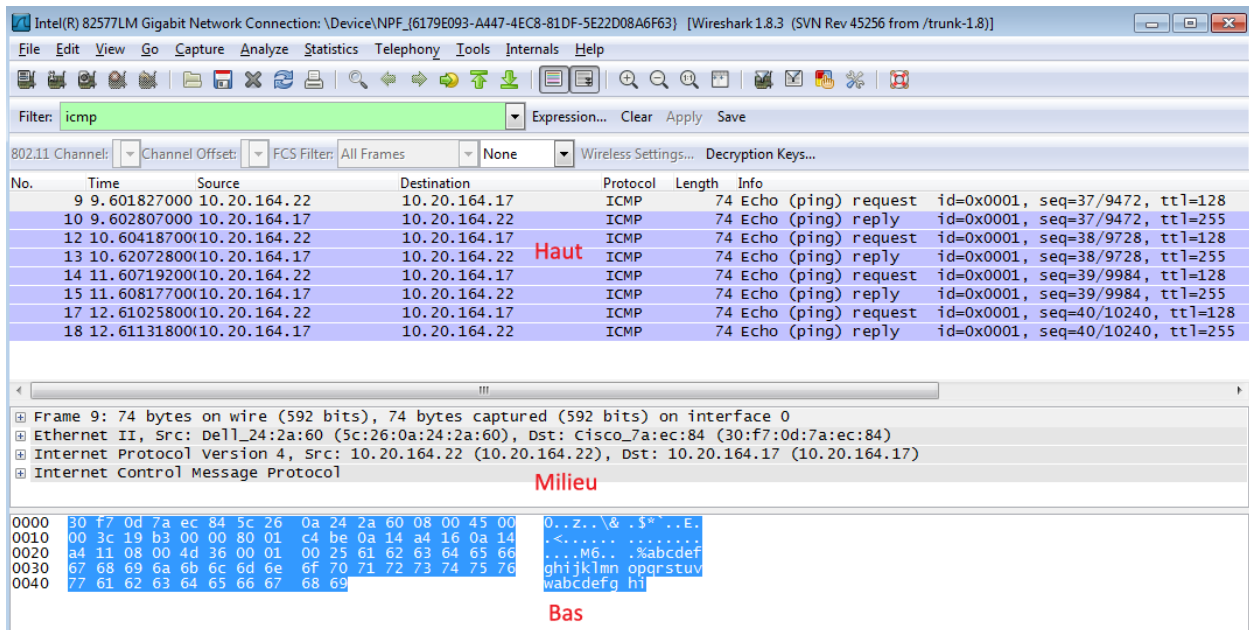
Étape 5 : Arrêtez la capture du trafic sur la carte réseau.

Cliquez sur l’icône **Stop Capture (Arrêter la capture)** pour arrêter la capture du trafic.



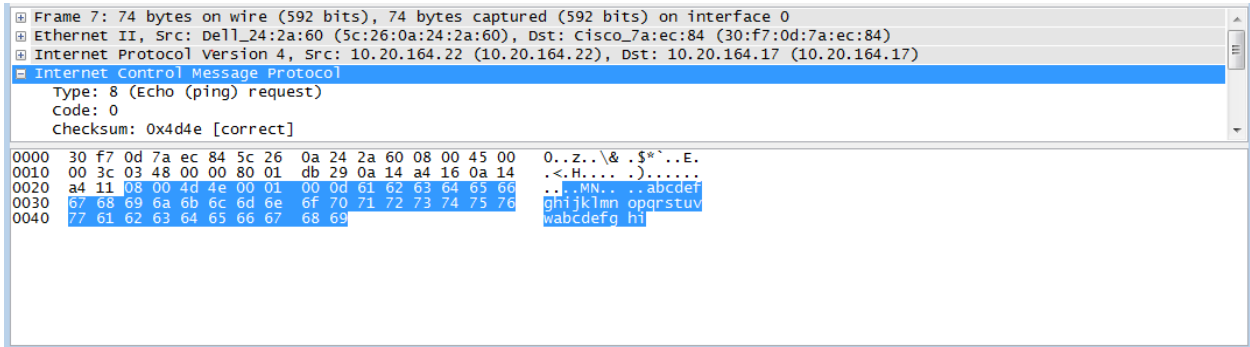
Étape 6 : Examinez la première requête Echo (ping) dans Wireshark.

La fenêtre principale de Wireshark est divisée en trois sections : le volet **Packet List** (Liste des paquets) (en haut), le volet **Packet Details** (Détails des paquets) (au milieu) et le volet **Packet Bytes** (Octets des paquets) (en bas). Si vous avez sélectionné l’interface appropriée pour la capture des paquets à l’étape 3, Wireshark doit afficher les informations ICMP dans le volet **Packet List** (Liste des paquets) de Wireshark, comme dans l’exemple suivant.



- a. Dans le volet **Packet List** (Liste des paquets) (section supérieure), cliquez sur la première trame répertoriée. **Echo (ping) request** devrait s’afficher en dessous de l’en-tête **Info**. La ligne devrait également être mise en surbrillance en bleu.

- b. Examinez la première ligne du volet Packet Details (Détails des paquets) (section centrale). Cette ligne indique la longueur de la trame : 74 octets dans cet exemple.
- c. La deuxième ligne dans le volet Packet Details (Détails des paquets) 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 (+) au début de la seconde ligne d'obtenir des informations supplémentaires sur la trame Ethernet II. Notez que le signe plus devient un signe moins (-).
Quel type de trame est affichée ? _____
- 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 (Octets des paquets) (section inférieure). Cliquez sur la ligne **Internet Control Message Protocol** dans la section centrale et examinez ce qui est mis en surbrillance dans le volet Packet Bytes (Octets des paquets).



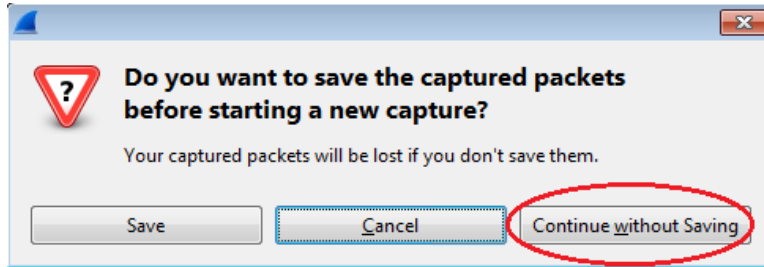
Quelles sont les deux dernières lettres des octets mis en surbrillance ? _____

- 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-ils comme adresse de destination ?

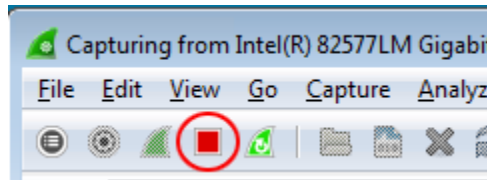
Étape 7 : Redémarrez la capture de paquets dans Wireshark.

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)**.



Étape 8 : Dans la fenêtre d'invite de commandes, envoyez une requête ping à www.cisco.com.

Étape 9 : Arrêtez la capture des paquets.



Étape 10 : 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 aux adresses que vous avez reçues à l'étape 7. 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 resté la même ?

Remarques générales

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