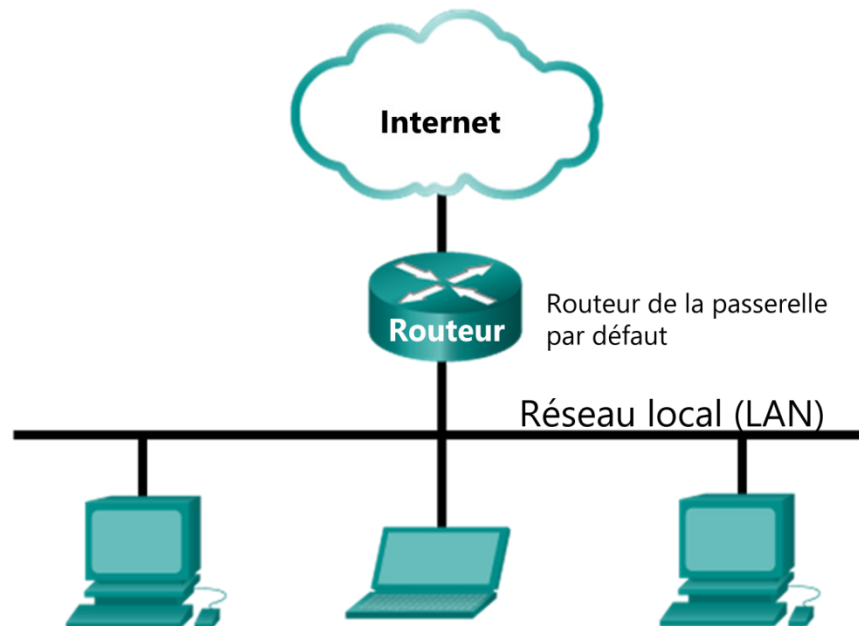


# Travaux pratiques – Protocole ARP

## Topologie



## Objectifs

### Partie 1 : Télécharger et installer Wireshark

### Partie 2 : Capturer et analyser les données ARP avec Wireshark

- Démarrez et arrêtez la capture des données du trafic de la commande ping vers les hôtes distants.
- Trouvez les informations relatives à l'adresse IPv4 et à l'adresse MAC dans les unités de données de protocole capturées.
- Analysez le contenu des messages ARP échangés entre les appareils sur le réseau LAN.

### Partie 3 : Afficher les entrées du cache ARP sur l'ordinateur

- Accédez à l'invite de commandes Windows.
- Utilisez la commande **arp** de Windows pour afficher le cache de la table ARP locale sur l'ordinateur.

## Contexte/scénario

Le protocole ARP (Address Resolution Protocol) est utilisé par TCP/IP pour mapper une adresse IPv4 de couche 3 à une adresse MAC de couche 2. Lorsqu'une trame Ethernet est transmise sur le réseau, elle doit posséder une adresse MAC de destination. Pour détecter dynamiquement l'adresse MAC d'une destination connue, l'appareil source envoie une requête ARP sur le réseau local. L'appareil auquel correspond l'adresse IPv4 de destination répond à cette requête avec une réponse ARP et son adresse MAC est enregistrée dans le cache ARP.

Tous les appareils sur le réseau LAN conservent leur propre cache ARP. Le cache ARP est une petite zone de la mémoire RAM contenant les réponses ARP. En affichant le cache ARP d'un ordinateur, vous aurez accès à l'adresse IPv4 et l'adresse MAC de tous les appareils sur le réseau LAN avec lesquels cet ordinateur a échangé des messages ARP.

Wireshark est un analyseur de protocoles (analyseur de paquets) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer. L'analyseur « capture » chaque unité de données de protocole (PDU) des flux de données circulant sur le réseau. Il permet de décoder et d'analyser leur contenu conformément aux spécifications de protocole appropriées.

Cet outil est utile pour toutes les personnes intervenant au niveau des réseaux. Vous pouvez vous en servir dans le cadre de la plupart des travaux pratiques des cours Cisco, à des fins d'analyse de données et de dépannage. Ces travaux pratiques contiennent des instructions permettant de télécharger et d'installer Wireshark, bien qu'il puisse être déjà installé. Dans le cadre de ces travaux pratiques, vous utiliserez Wireshark pour capturer les échanges ARP sur le réseau local.

### Ressources requises

- 1. Ordinateur Windows 10 avec accès Internet
- Des ordinateurs supplémentaires sur un réseau local (LAN) seront utilisés pour répondre aux requêtes **ping**. Si aucun ordinateur supplémentaire n'est disponible sur le réseau LAN, l'adresse de passerelle par défaut sera utilisée pour répondre aux requêtes **ping**.

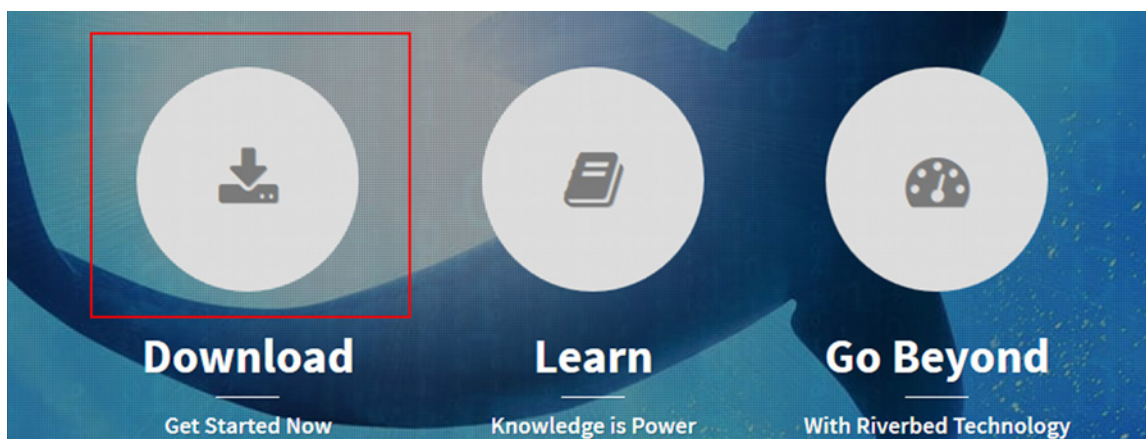
## Partie 1 : Télécharger et installer Wireshark

Wireshark est devenu le programme standard d'analyse de paquets pour les ingénieurs réseau. Ce logiciel open source est disponible pour de nombreux systèmes d'exploitation différents, y compris Windows, Mac et Linux.

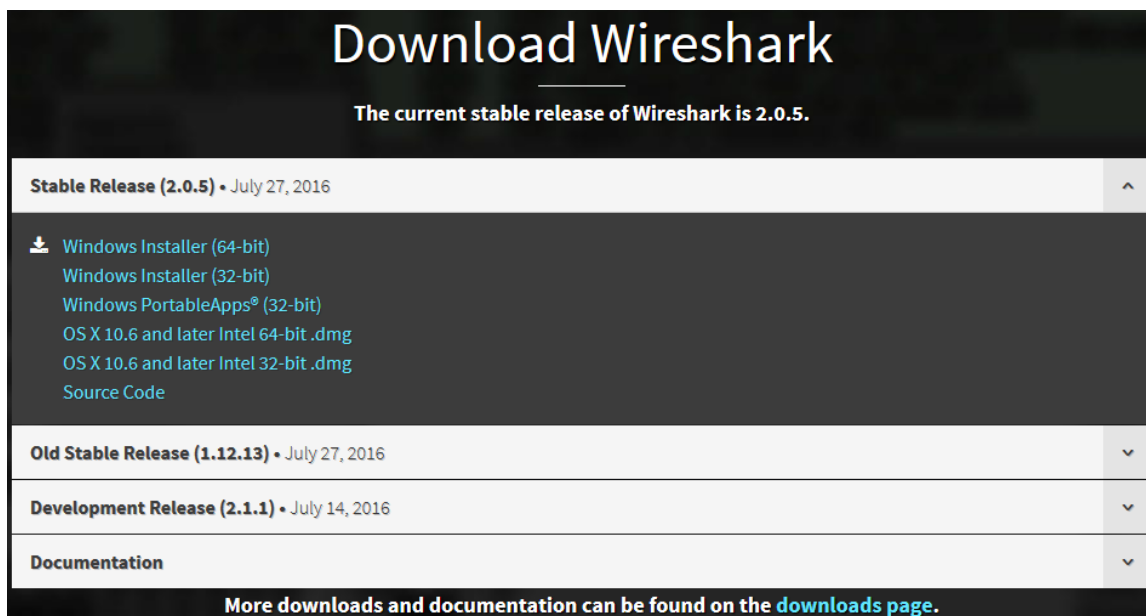
Si Wireshark est déjà installé sur votre ordinateur, vous pouvez ignorer la première partie et accéder directement à la deuxième partie. Si Wireshark n'est pas installé sur votre ordinateur, vérifiez auprès de votre formateur quelle est la politique de téléchargement des logiciels de votre école.

### Étape 1 : Téléchargez Wireshark.

- Wireshark peut être téléchargé sur [www.wireshark.org](http://www.wireshark.org).
- Cliquez sur **Télécharger**.



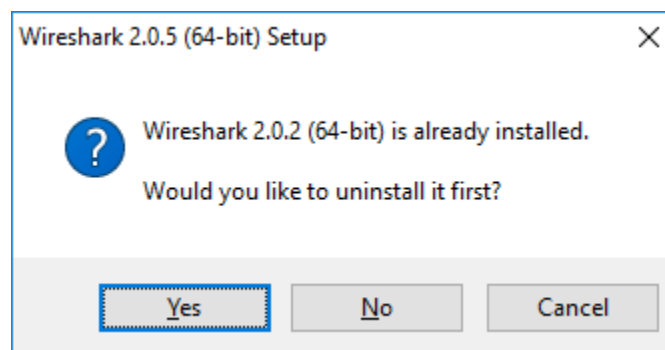
- c. Sélectionnez la version logicielle dont vous avez besoin en fonction de l'architecture et du système d'exploitation de votre ordinateur. Par exemple, si vous disposez d'un ordinateur 64 bits exécutant Windows, choisissez **Windows Installer (64-bit)** (Programme d'installation de Windows (64 bits)).



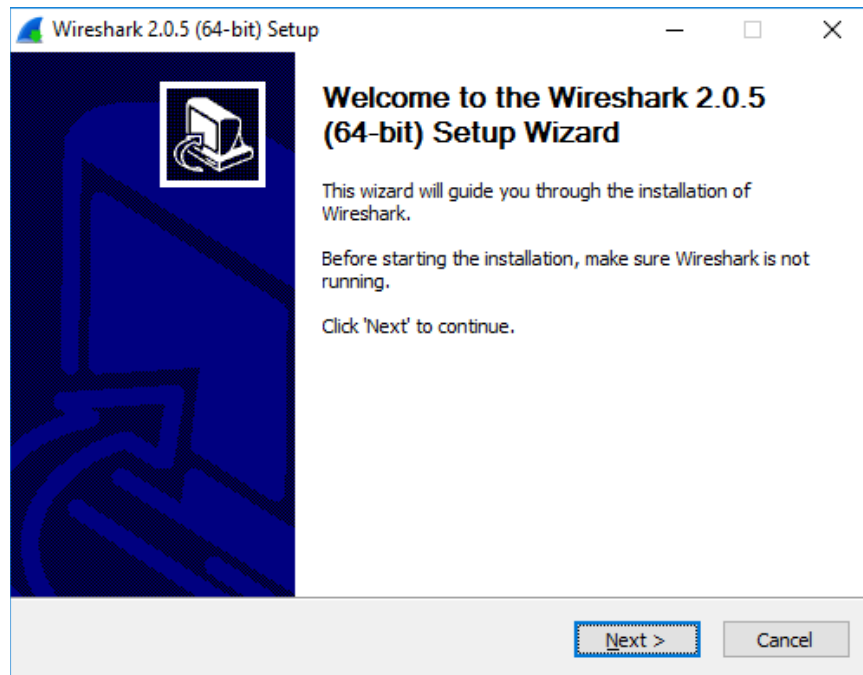
- d. Une fois que vous avez effectué votre sélection, le téléchargement doit commencer. Si vous y êtes invité, cliquez sur **Enregistrer le fichier**. L'emplacement du fichier téléchargé dépend de votre navigateur et du système d'exploitation que vous utilisez. Pour les utilisateurs Windows, l'emplacement par défaut est le dossier **Téléchargements**.

### Étape 2 : Installez Wireshark.

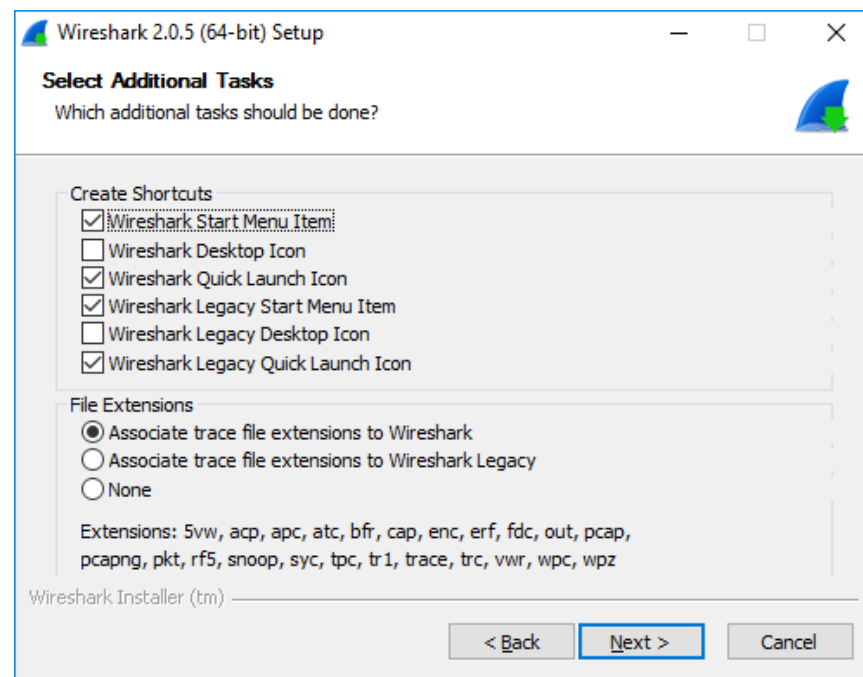
- a. Le fichier téléchargé est nommé **Wireshark-win64-x.x.x.exe**, où le symbole **x** représente le numéro de version. Cliquez deux fois sur le fichier pour lancer la procédure d'installation. Dans cet exemple, c'est la version 2.0.5 qui est utilisée.
- b. Répondez à tous les messages de sécurité qui s'affichent à l'écran. Si vous disposez déjà d'une copie de Wireshark sur votre ordinateur, vous serez invité à désinstaller l'ancienne version avant d'installer la nouvelle. Nous vous recommandons de supprimer l'ancienne version de Wireshark avant d'installer une autre version. Cliquez sur **Oui** pour désinstaller la version précédente de Wireshark.



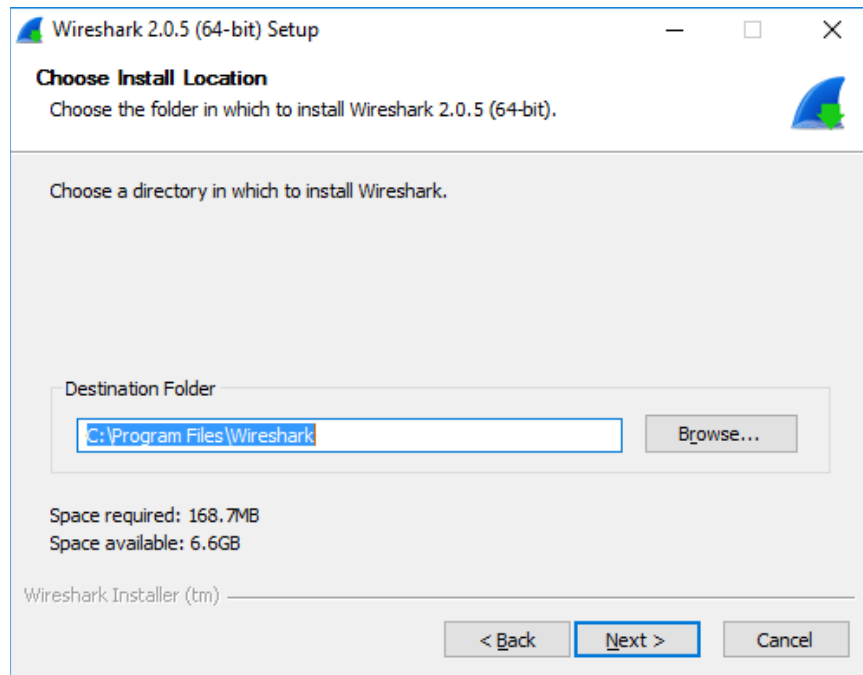
- c. Si c'est la première fois que vous installez Wireshark, ou après avoir terminé la procédure de désinstallation, accédez à l'assistant de configuration de Wireshark. Cliquez sur **Suivant**.



- d. Continuez à progresser dans la procédure d'installation. Cliquez sur **J'accepte** lorsque la fenêtre contenant la licence d'utilisation s'affiche.
- e. Conservez les paramètres par défaut dans la fenêtre Choisir les composants, puis cliquez sur **Suivant**.
- f. Choisissez les options de raccourci souhaitées, puis cliquez sur **Suivant**.

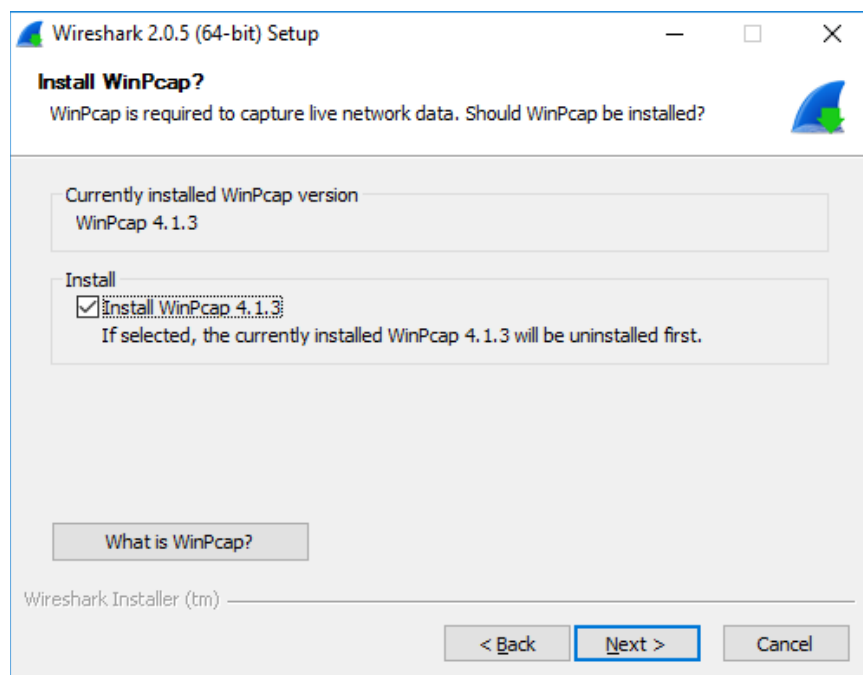


- g. Vous pouvez modifier l'emplacement d'installation de Wireshark, mais à moins que vous ne disposiez d'un espace disque limité, nous vous recommandons de conserver l'emplacement par défaut.



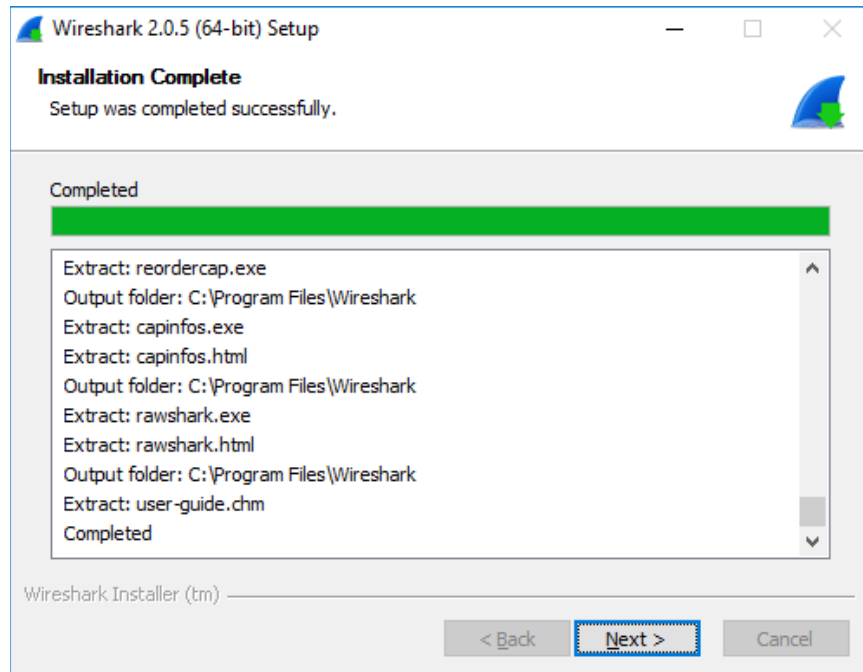
- h. Pour enregistrer des données réseau en temps réel, il faut que WinPcap soit installé sur votre ordinateur. Si WinPcap est déjà installé sur votre ordinateur, la case à cocher Installer sera désélectionnée. Si la version de WinPcap que vous avez installée est antérieure à la version fournie avec Wireshark, il est recommandé d'autoriser l'installation de la version la plus récente en cochant la case **Installer WinPcap x.x.x** (numéro de version).

Finalisez l'installation au moyen de l'Assistant si vous installez WinPcap.

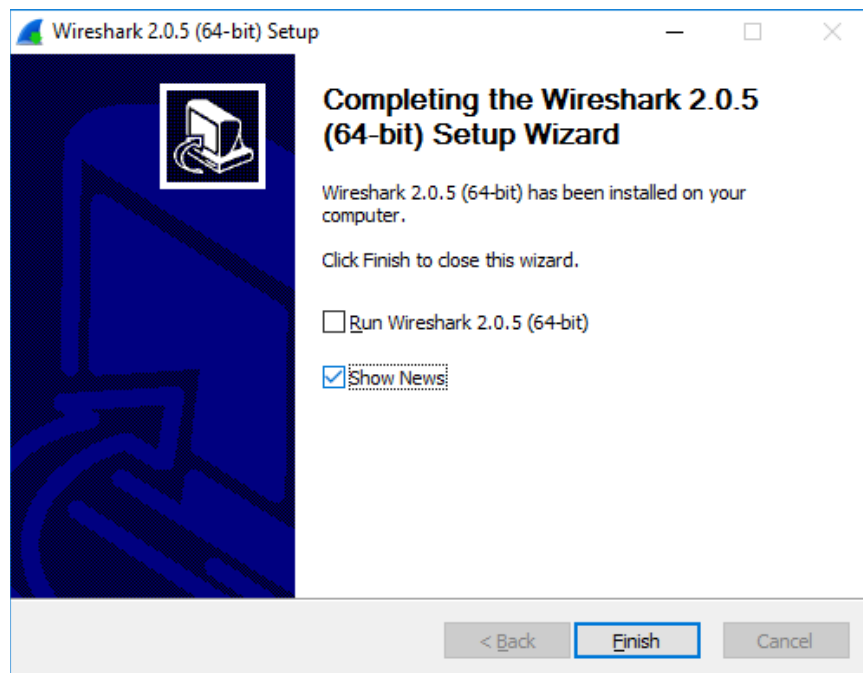


**Remarque** : il est possible que vous soyez invité à installer USBPcap. Toutefois, l'installation d'USBPcap n'est pas obligatoire.

- i. Wireshark commence à installer ses fichiers et affiche une fenêtre distincte indiquant l'état de l'installation. Cliquez sur **Suivant** une fois l'installation terminée.



- j. Cliquez sur **Terminer** pour terminer le processus d'installation de Wireshark.



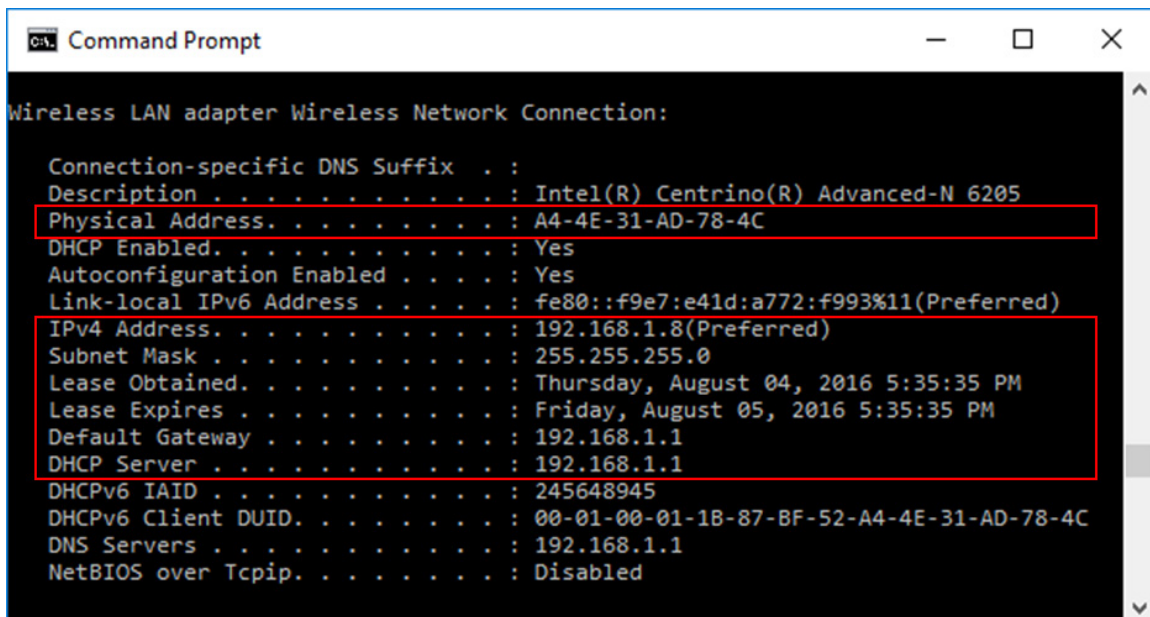
## Partie 2 : Capturer et analyser les données ARP locales avec Wireshark

Dans la partie 2 de ces travaux pratiques, vous exécuterez une commande ping sur un autre ordinateur du réseau local (LAN) et capturerez des requêtes et des réponses ARP dans Wireshark. Vous examinerez également les trames capturées pour obtenir des informations spécifiques. Cette analyse devrait vous aider à mieux comprendre la façon dont les en-têtes de paquet sont utilisés pour transporter les données vers leur destination.

### Étape 1 : Récupérez les adresses d'interface de votre ordinateur.

Pour réaliser ces travaux pratiques, vous devrez récupérer l'adresse IPv4 et l'adresse MAC de votre ordinateur.

- Ouvrez une fenêtre de commandes, tapez **ipconfig /all**, puis appuyez sur Entrée.
- Identifiez la carte réseau utilisée par l'ordinateur pour accéder au réseau. Enregistrez l'adresse IPv4 et l'adresse MAC (adresse physique) de l'interface de votre ordinateur.



```
Command Prompt

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Physical Address. . . . . : A4-4E-31-AD-78-4C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, August 04, 2016 5:35:35 PM
Lease Expires . . . . . : Friday, August 05, 2016 5:35:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 245648945
DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Disabled
```

- Demandez à un membre de l'équipe de vous communiquer l'adresse IPv4 de son ordinateur et donnez-lui l'adresse IPv4 du vôtre. Ne lui fournissez pas votre adresse MAC pour le moment.

Notez les adresses IPv4 de la passerelle par défaut et des autres ordinateurs présents sur le réseau LAN.

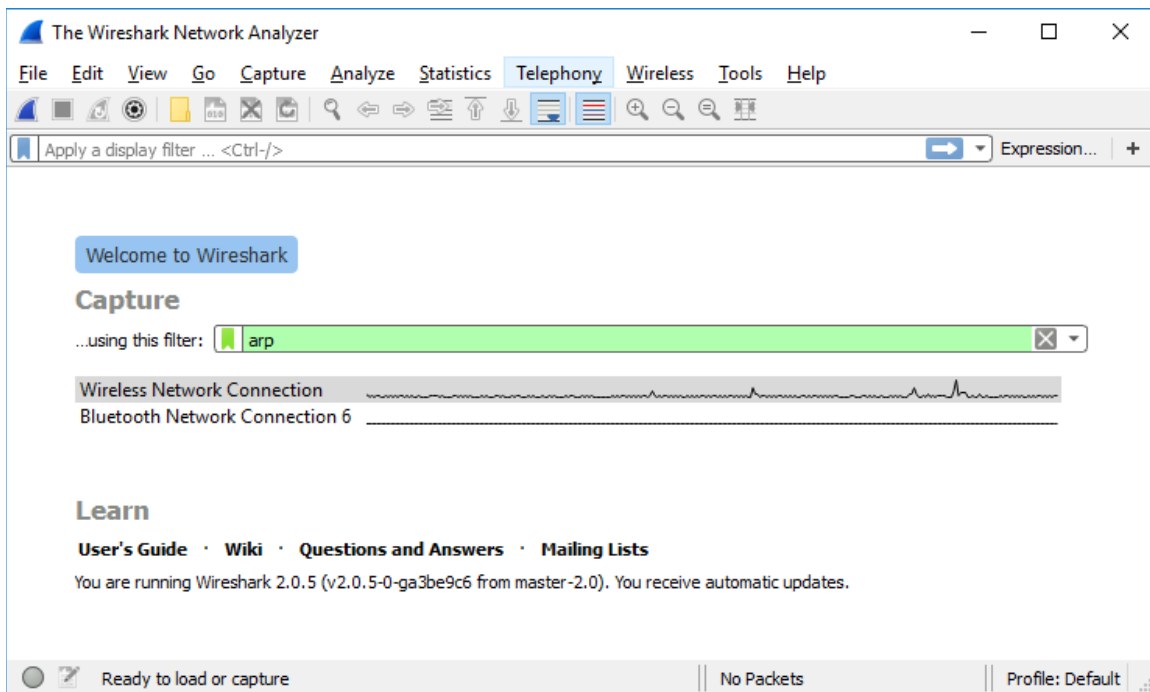
### Étape 2 : Démarrez Wireshark et commencez à capturer des données.

- Sur votre ordinateur, cliquez sur **Démarrer** et tapez **Wireshark**. Cliquez sur **Application de bureau Wireshark** lorsqu'elle apparaît dans la fenêtre des résultats de recherche.


**Remarque** : il est également possible que votre installation de Wireshark propose une option Wireshark héritée. Wireshark s'affiche alors dans une interface graphique plus ancienne, mais très connue. La fin de ces travaux pratiques a été traitée en utilisant une interface graphique de l'application de bureau plus récente.

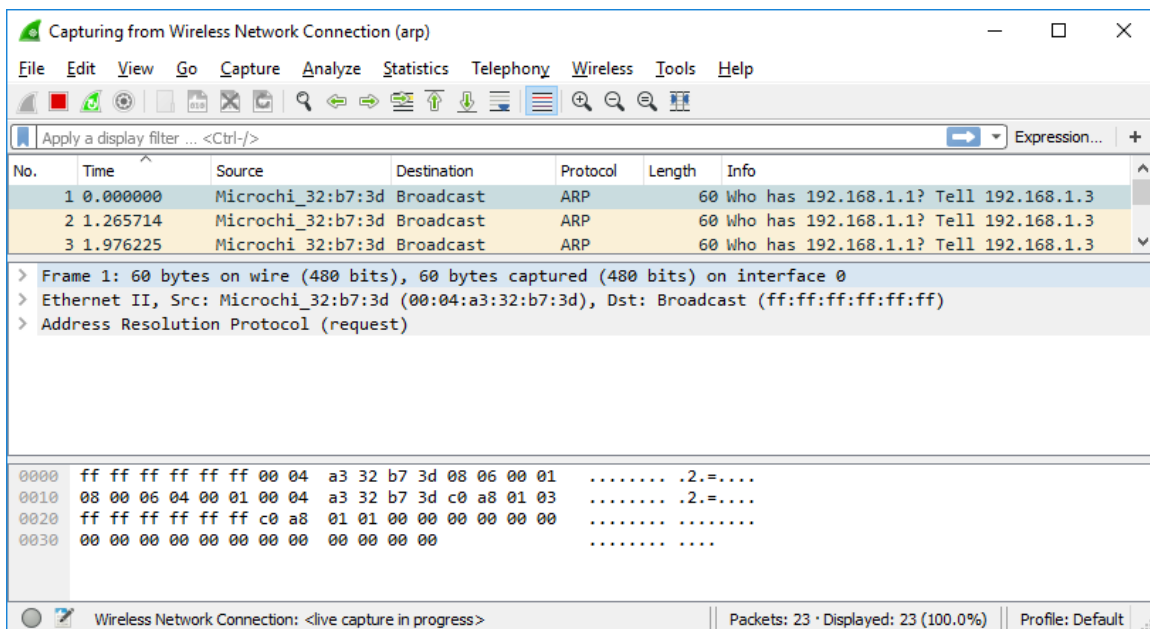


- b. Une fois que Wireshark a démarré, sélectionnez l'interface réseau que vous avez identifiée avec la commande **ipconfig**. Saisissez **arp** dans le champ de filtre. Ainsi, Whireshark n'affiche que les paquets des échanges ARP entre les appareils présents sur le réseau local.



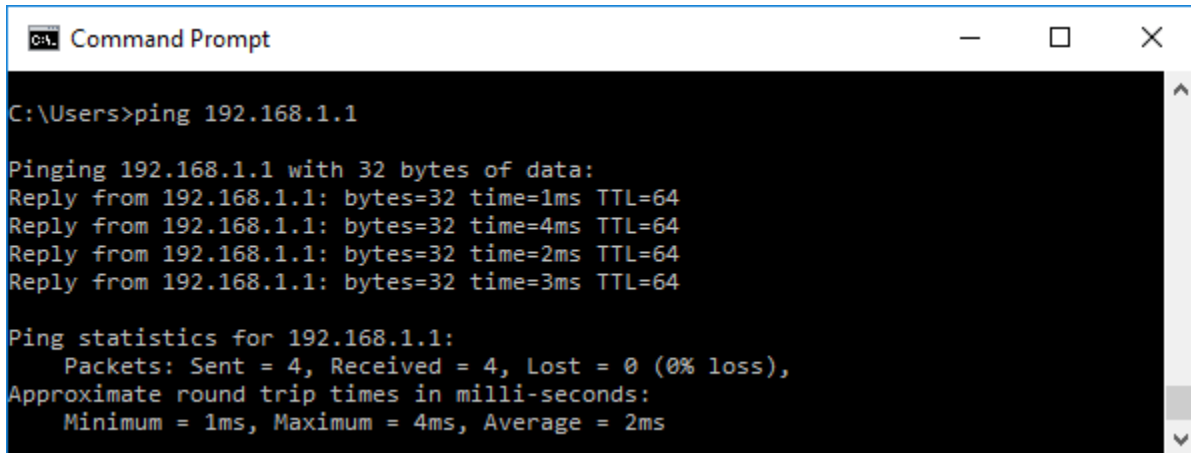
- c. Après avoir sélectionné la bonne interface et saisi les informations relatives au filtre, cliquez sur

**Démarrer** (  ) pour commencer la capture des données. Les informations commencent à défiler vers le bas à partir de la partie supérieure dans Wireshark. Chaque ligne représente un message envoyé entre un appareil source et un appareil destinataire sur le réseau.





- d. Ouvrez une fenêtre d'invite de commandes. Utilisez la commande **ping** pour tester la connectivité à l'adresse de passerelle par défaut identifiée à la partie 2, étape 1c.




```
C:\Users>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

- e. Envoyez une requête ping vers les adresses IPv4 des autres ordinateurs sur le réseau LAN qui ont été fournies par les membres de votre équipe.

**Remarque :** si l'ordinateur d'un membre de votre équipe ne répond pas à vos requêtes ping, c'est peut-être parce que le pare-feu de son ordinateur bloque ces requêtes. Si nécessaire, demandez de l'aide à votre formateur pour désactiver le pare-feu de l'ordinateur.

- f. Pour arrêter de capturer des données, cliquez sur **Arrêter la capture** (  ) dans la barre d'outils.

### Étape 3 : Examinez les données capturées.

À l'étape 3, examinez les données qui ont été générées par les requêtes **ping** de l'ordinateur du membre de votre équipe. Les données Wireshark sont divisées en trois parties :

- 1) La première partie présente la liste des trames PDU capturées, accompagnées d'un résumé des informations relatives au paquet IPv4 listées.
- 2) La partie centrale propose une liste des informations PDU pour la trame sélectionnée dans la partie supérieure de l'écran et divise une trame PDU capturée en couches de protocole.

- 3) La partie inférieure présente les données brutes de chaque couche. Les données brutes sont affichées sous forme hexadécimale et décimale.

**La partie supérieure présente les blocs d'alimentation individuels**

**La partie centrale présente les informations relatives au bloc d'alimentation en surbrillance**

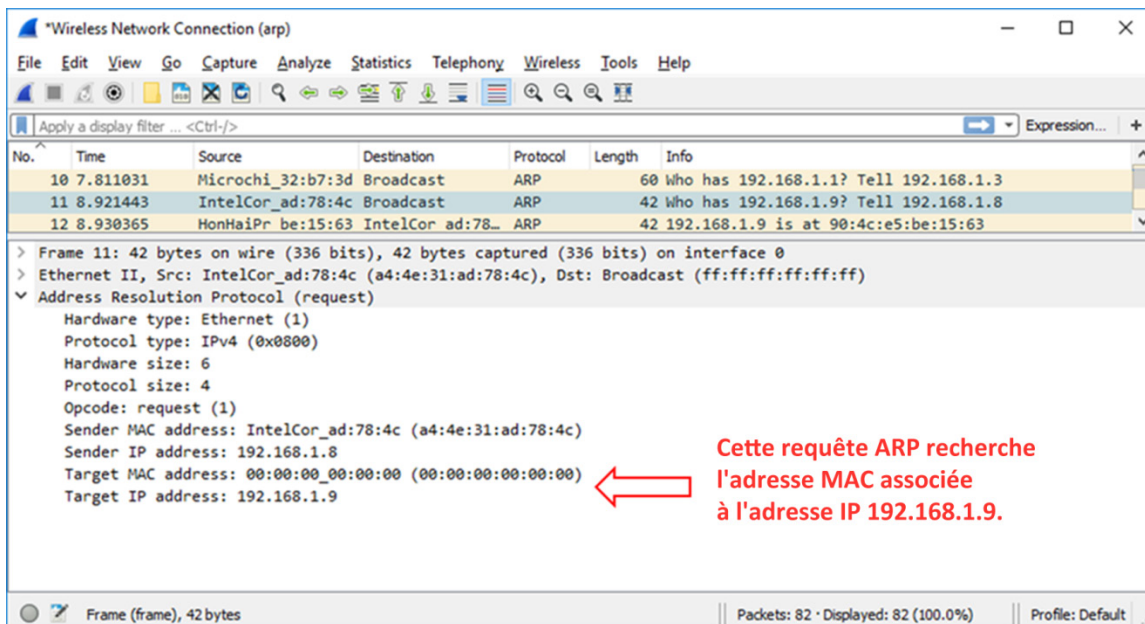
**La partie inférieure présente les données brutes**

- Dans la partie supérieure, cliquez sur l'une des trames ARP dont l'adresse source correspond à l'adresse MAC de votre ordinateur et dont la destination est « broadcast ».
- Tandis que cette trame PDU est toujours sélectionnée dans la partie supérieure, accédez à la partie centrale. Cliquez sur la flèche à gauche de la ligne Ethernet II pour afficher les adresses MAC de la destination et de la source.

**Cette section présente les informations figurant dans l'en-tête de la trame de couche 2.**

L'adresse MAC de la source correspond-elle à l'interface de votre ordinateur ? \_\_\_\_\_

- c. Cliquez sur la flèche à gauche de la ligne ARP (requête) pour afficher le contenu de la requête ARP.



### Étape 4 : Repérez la trame de la réponse ARP correspondant à la requête ARP que vous avez mise en surbrillance.

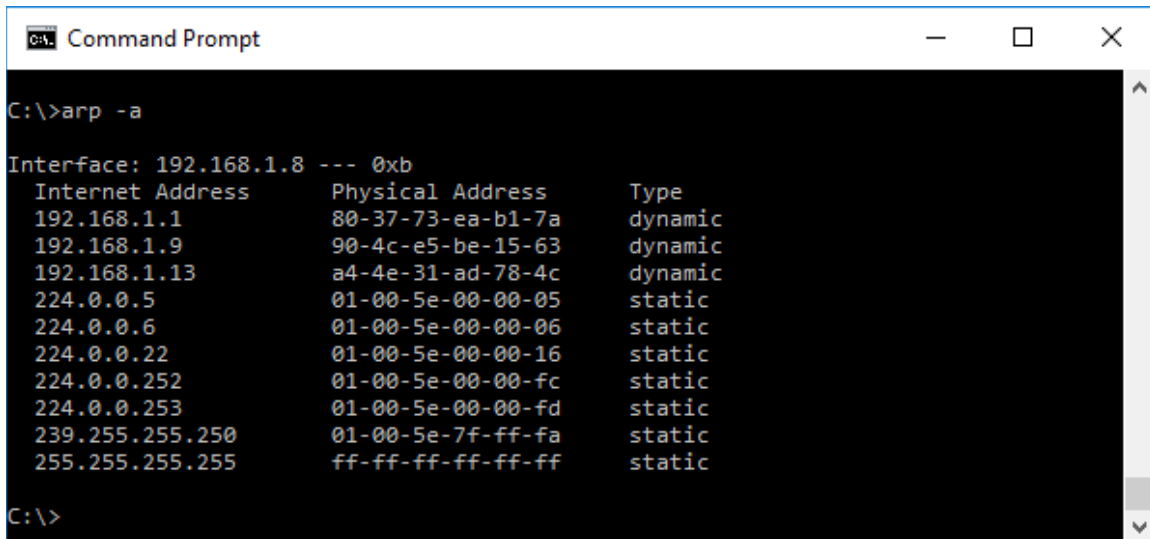
- a. À l'aide de l'adresse IPv4 cible de la requête ARP, repérez la trame de la réponse ARP dans la partie supérieure de l'écran de capture de Wireshark.
- Quelle est l'adresse IPv4 de l'appareil cible dans votre requête ARP ? \_\_\_\_\_
- b. Mettez en surbrillance la trame de réponse dans la partie supérieure de l'interface Wireshark. Vous devrez peut-être faire défiler la fenêtre pour trouver la trame de réponse correspondant à l'adresse IPv4 identifiée à l'étape précédente. Développez les lignes Ethernet II et ARP (réponse) dans la partie centrale de l'écran.
- La trame de réponse ARP est-elle une trame de diffusion ? \_\_\_\_\_
- Quelle est l'adresse MAC de destination de la trame ? \_\_\_\_\_
- S'agit-il de l'adresse MAC de votre ordinateur ? \_\_\_\_\_
- Quelle est l'adresse MAC à la source de la trame ? \_\_\_\_\_
- c. Vérifiez auprès du membre de votre équipe que l'adresse MAC correspond à celle de son ordinateur.

### Partie 3 : Examinez les entrées du cache ARP sur l'ordinateur.

Une fois que l'ordinateur a reçu la réponse ARP, l'association de l'adresse MAC à l'adresse IPv4 est stockée dans la mémoire cache de l'ordinateur. Ces entrées seront stockées sur la mémoire cache pendant une très courte durée (de 15 à 45 secondes), puis, si elles ne sont pas utilisées, elles seront supprimées.

## Étape 1 : Consultez les entrées du cache ARP sur un ordinateur Windows.

- Ouvrez une fenêtre d'invite de commandes sur l'ordinateur. À l'invite, saisissez **arp -a**, puis appuyez sur Entrée.



```
Command Prompt

C:\>arp -a

Interface: 192.168.1.8 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1           80-37-73-ea-b1-7a     dynamic
192.168.1.9           90-4c-e5-be-15-63     dynamic
192.168.1.13          a4-4e-31-ad-78-4c     dynamic
224.0.0.5             01-00-5e-00-00-05     static
224.0.0.6             01-00-5e-00-00-06     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\>
```

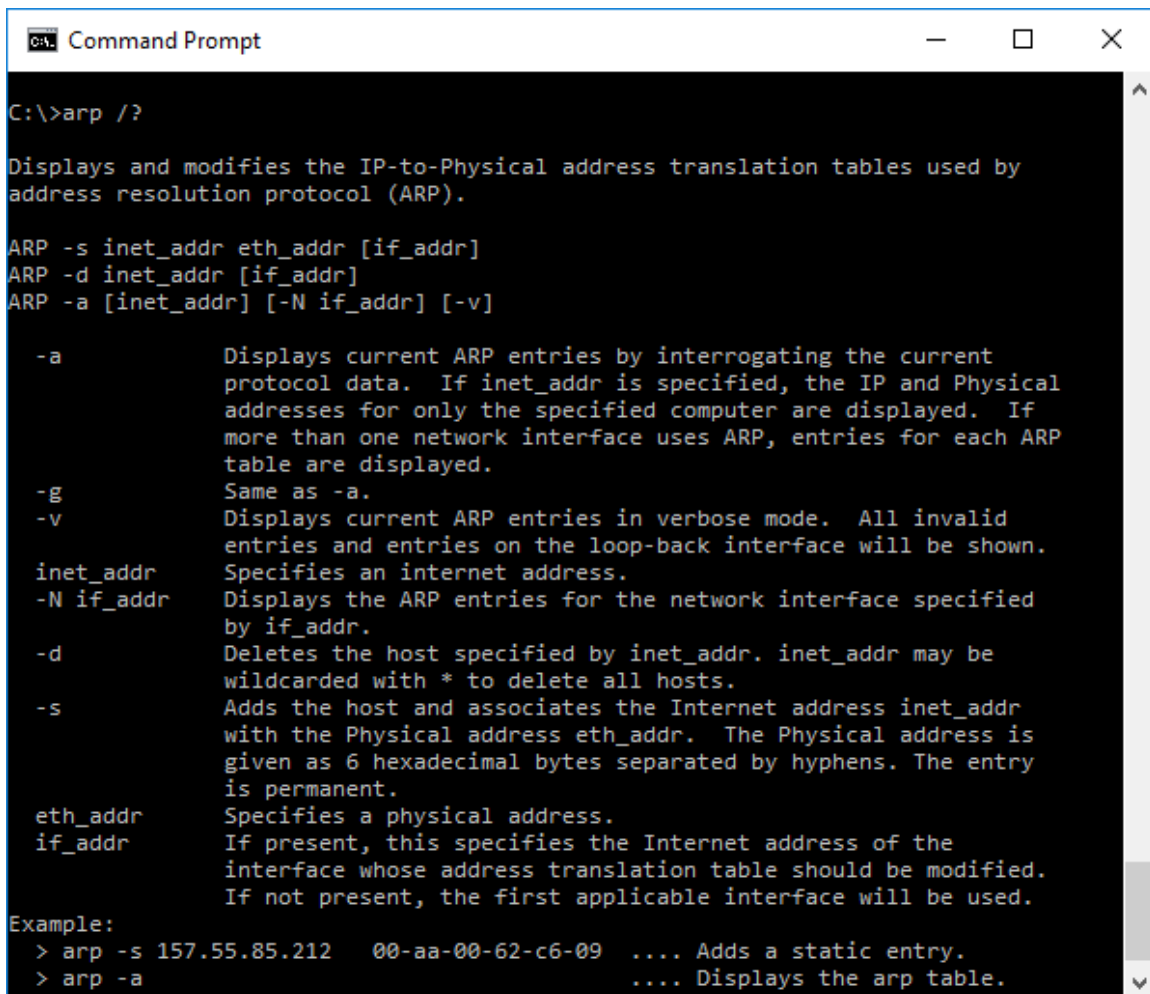
La commande **arp -a** affiche les entrées placées dans la mémoire cache de l'ordinateur. Dans l'exemple, l'ordinateur présente des entrées pour la passerelle par défaut (192.168.1.1) et pour les deux ordinateurs sur le même réseau LAN (192.168.1.9 et 192.168.1.13).

Que se passe-t-il lorsque vous exécutez la commande **arp -a** sur votre ordinateur ?

---

---

- b. La commande **arp** a d'autres utilités sur un ordinateur Windows. Saisissez **arp /?** dans l'invite de commandes et appuyez sur Entrée. Les options de commande **arp** vous permettent d'afficher, d'ajouter ou de supprimer des entrées de la table ARP si nécessaire.



```
Command Prompt

C:\>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

    -a          Displays current ARP entries by interrogating the current
                  protocol data.  If inet_addr is specified, the IP and Physical
                  addresses for only the specified computer are displayed.  If
                  more than one network interface uses ARP, entries for each ARP
                  table are displayed.
    -g          Same as -a.
    -v          Displays current ARP entries in verbose mode.  All invalid
                  entries and entries on the loop-back interface will be shown.
inet_addr      Specifies an internet address.
-N if_addr     Displays the ARP entries for the network interface specified
                  by if_addr.
-d            Deletes the host specified by inet_addr.  inet_addr may be
                  wildcarded with * to delete all hosts.
-s            Adds the host and associates the Internet address inet_addr
                  with the Physical address eth_addr.  The Physical address is
                  given as 6 hexadecimal bytes separated by hyphens.  The entry
                  is permanent.
eth_addr       Specifies a physical address.
if_addr        If present, this specifies the Internet address of the
                  interface whose address translation table should be modified.
                  If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a          .... Displays the arp table.
```

Quelle option permet de supprimer une entrée du cache ARP ? \_\_\_\_\_

Quel sera le résultat de l'envoi d'une commande **arp -d \*** ? \_\_\_\_\_

### Observations

1. Quel est le bénéfice de conserver des entrées de cache ARP dans la mémoire de l'ordinateur source ?

---

---

2. Si l'adresse IPv4 de destination n'est pas située sur le même réseau que l'hôte source, quelle adresse MAC sera utilisée comme adresse MAC cible de destination dans la trame ?

---

---