Travaux pratiques - Analyse d'ARP avec la CLI de Windows, la CLI d'IOS et Wireshark

Topologie

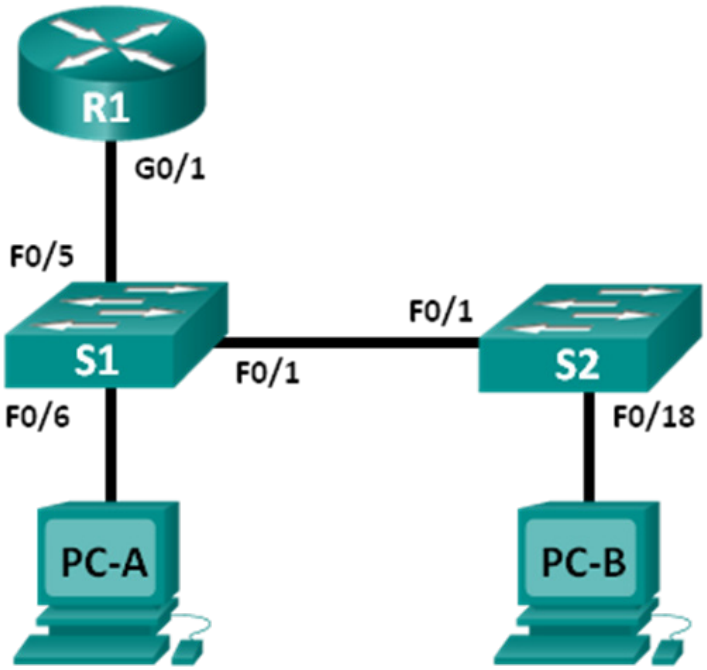


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	NA
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	Carte réseau	192.168.1.2	255.255.255.0	192.168.1.1

Objectifs

1re partie : Concevoir et configurer le réseau

2e partie : Utiliser la commande ARP de Windows

3e partie : Utiliser la commande show ARP d'IOS

4e partie : Utiliser Wireshark pour examiner les échanges ARP

Contexte/scénario

TCP/IP utilise le protocole ARP pour mapper une adresse IP de la couche 3 sur une adresse MAC de la couche 2. Lorsqu'une trame est placée du réseau, elle doit posséder une adresse MAC de destination. Pour détecter de façon dynamique l'adresse MAC d'un périphérique de destination, une requête ARP est diffusée du réseau local. Le périphérique qui contient l'adresse IP de destination répond. Ensuite, l'adresse MAC est consignée dans le cache ARP. Chaque périphérique du réseau local conserve son propre cache ARP, ou un petit espace dans la mémoire vive qui contient les résultats d'ARP. Un temporisateur de cache ARP supprime les entrées correspondantes qui n'ont pas été utilisées pendant un certain temps.

ARP constitue un parfait exemple de compromis de performances. Sans cache, ARP doit constamment demander des traductions d'adresses à chaque placement d'une trame du réseau. Ceci ajoute de la latence à la communication et peut encombrer le réseau local. Inversement, des temps d'attente illimités peuvent entraîner des erreurs avec des périphériques qui quittent le réseau ou modifient l'adresse de couche 3.

Un administrateur réseau doit tenir compte d'ARP, mais ne peut pas communiquer régulièrement avec ce protocole. ARP est un protocole qui permet aux périphériques réseau de communiquer avec le protocole TCP/IP. Sans ARP, aucune méthode n'est efficace pour créer l'adresse de destination de couche 2 du datagramme. En outre, ARP représente un risque potentiel pour la sécurité. L'usurpation ARP ou l'empoisonnement ARP est une technique utilisée par un pirate informatique pour introduire l'association d'adresses MAC incorrectes dans un réseau. Un pirate informatique usurpe l'adresse MAC d'un périphérique, et les trames sont envoyées vers la destination incorrecte. La configuration manuelle d'associations ARP statiques est un moyen d'éviter l'usurpation ARP. En fin de compte, il est possible de configurer une liste d'adresses MAC autorisées sur les périphériques Cisco pour limiter l'accès réseau aux seuls périphériques approuvés.

Au cours de ces travaux pratiques, vous utiliserez les commandes ARP à la fois sur des routeurs Windows et Cisco pour afficher la table ARP. Vous viderez également le cache ARP et ajouterez des entrées ARP statiques.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960s équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Ressources requises

- 1 routeur (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 2 ordinateurs (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal, tel que Tera Term, et de Wireshark)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet tel qu'indiqués dans la topologie

Remarque : les interfaces FastEthernet sur les commutateurs Cisco 2960 sont à détection automatique et un câble Ethernet droit peut être utilisé entre les commutateurs S1 et S2. Si vous utilisez un autre modèle de commutateur Cisco, un câble croisé Ethernet sera peut-être nécessaire.

1re partie : Créer et configurer le réseau

Étape 1 : Câblez le réseau conformément à la topologie.

Étape 2 : Configurez les adresses IP pour les périphériques selon la table d'adressage.

Étape 3 : Vérifiez la connectivité du réseau en envoyant une requête ping à tous les périphériques à partir de PC-B.

2e partie : Utiliser la commande ARP de Windows

La commande **arp** permet à l'utilisateur d'afficher et de modifier le cache ARP dans Windows. Vous accédez à cette commande à partir de l'invite de commandes Windows.

Étape 1 : Affichez le cache ARP.

a. Ouvrez une fenêtre de commande sur PC-A et saisissez **arp**.

```
C:\Users\User1> 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.
```

b. Examinez le résultat.

Quelle commande est utilisée pour afficher toutes les entrées dans le cache ARP ?

Quelle commande est utilisée pour supprimer toutes les entrées du cache ARP (vider le cache ARP) ?

Quelle commande est utilisée pour supprimer l'entrée du cache ARP pour 192.168.1.11 ?

c. Tapez **arp – a** pour afficher la table ARP.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Remarque : la table ARP est vide si vous utilisez Windows XP (comme illustré ci-dessous).

```
C:\Documents and Settings\User1> arp -a
No ARP Entries Found.
```

d. Envoyez une requête ping de PC-A vers PC-B pour ajouter dynamiquement des entrées dans le cache ARP.

```
C:\Documents and Settings\User1> ping 192.168.1.2

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
```

Quelle est l'adresse physique de l'hôte avec l'adresse IP 192.168.1.2 ?

Étape 2 : Modifiez manuellement les entrées dans le cache ARP.

Pour supprimer des entrées dans un cache ARP, exécutez la commande **arp –d {inet-addr | *}**. Il est possible de supprimer les adresses individuellement en indiquant l'adresse IP. Vous pouvez aussi supprimer toutes les entrées avec le caractère générique *.

Vérifiez que le cache ARP contient les entrées suivantes : la passerelle par défaut R1 G0/1 (192.168.1.1), PC-B (192.168.1.2) et les deux commutateurs (192.168.1.11 et 192.168.1.12).

a. À partir de PC-A, envoyez une requête ping à toutes les adresses de la table d'adresses.

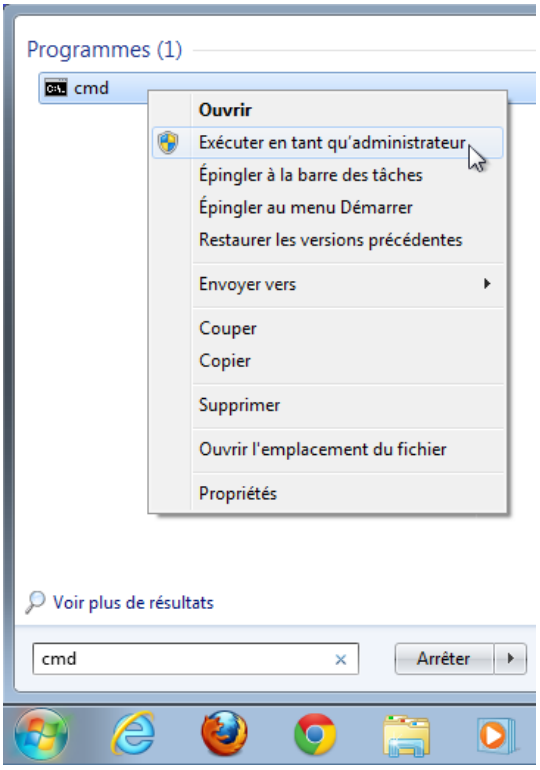
b. Vérifiez que toutes les adresses ont été ajoutées dans le cache ARP. Si l'adresse ne figure pas dans le cache ARP, envoyez une requête ping à l'adresse de destination et vérifiez que l'adresse a été ajoutée dans le cache ARP.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.2           00-50-56-be-f6-db     dynamic
```

```
192.168.1.11          0c-d9-96-e8-8a-40     dynamic
192.168.1.12          0c-d9-96-d2-40-40     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
```

c. En tant qu'administrateur, accédez à l'invite de commandes. Cliquez sur l'icône **Démarrer** et dans la zone *Rechercher les programmes et fichiers*, tapez **cmd**. Lorsque l'icône **cmd** s'affiche, cliquez avec le bouton droit de la souris sur l'icône et sélectionnez **Exécuter en tant qu'administrateur**. Cliquez sur **Oui** pour permettre à ce programme d'effectuer des modifications.

Remarque : pour les utilisateurs de Windows XP, il n'est pas nécessaire de disposer de privilèges d'administrateur pour modifier les entrées du cache ARP.



d. Dans la fenêtre d'invite de commandes de l'administrateur, saisissez **arp –d ***. Cette commande supprime toutes les entrées du cache ARP. Vérifiez que toutes les entrées du cache ARP sont supprimés en entrant la commande **arp – a** à l'invite de commandes.

```
C:\windows\system32> arp -d *
C:\windows\system32> arp -a
No ARP Entries Found.
```

e. Attendez quelques minutes. Le protocole NDP (Neighbor Discovery Protocol) démarre pour remplir à nouveau le cache ARP.

```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
```

```
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Remarque : le protocole NDP n'est pas mis en œuvre dans Windows XP.

f. À partir de PC-A, envoyez une requête ping à PC-B (192.168.1.2) et aux commutateurs (192.168.1.11 et 192.168.1.12) pour ajouter les entrées ARP. Vérifiez que les entrées ARP ont été ajoutées dans le cache.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

g. Notez l'adresse physique du commutateur S2

h. Supprimez une entrée de cache ARP spécifique en entrant la commande **arp –d *inet-addr***. À l'invite de commandes, tapez **arp -d 192.168.1.12** pour supprimer l'entrée ARP pour S2.

```
C:\windows\system32> arp –d 192.168.1.12
```

i. Entrez **arp –a** pour vérifier que l'entrée ARP pour S2 a été retirée du cache ARP.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

j. Vous pouvez ajouter une entrée de cache ARP spécifique en tapant **arp –s *inet_addr mac_addr***. L'adresse IP et l'adresse MAC pour S2 seront utilisées dans cet exemple. Utilisez l'adresse MAC enregistrée à l'étape g.

```
C:\windows\system32> arp –s 192.168.1.12 0c-d9-96-d2-40-40
```

k. Vérifiez que l'entrée ARP pour S2 a été ajoutée au cache.

3e partie : Utiliser la commande show ARP d'IOS

Cisco IOS peut également afficher le cache ARP sur des routeurs et des commutateurs avec la commande **show arp** ou **show ip arp**.

Étape 1 : Affichez les entrées ARP sur le routeur R1.

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            0   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            0   0050.56be.768c  ARPA   GigabitEthernet0/1
R1#
```

Remarquez qu'il n'y a pas de valeur Age (-) pour la première entrée, l'interface de routeur G0/1 (la passerelle par défaut du réseau local (LAN)). La valeur Age correspond au nombre de minutes (min) pendant lequel l'entrée a résidé dans le cache ARP. Ce nombre est incrémenté pour les autres entrées. Le protocole NDP remplit les entrées ARP des adresses MAC de PC-A et PC-B IP.

Étape 2 : Ajoutez les entrées ARP sur le routeur R1.

Vous pouvez ajouter des entrées ARP à la table ARP du routeur en envoyant une requête ping à d'autres périphériques.

a. Envoyez une requête ping au commutateur S1.

```
R1# ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

b. Vérifiez qu'une entrée ARP pour le commutateur S1 a été ajoutée à la table ARP de R1.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            6   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            6   0050.56be.768c  ARPA   GigabitEthernet0/1
Internet  192.168.1.11           0   0cd9.96e8.8a40  ARPA   GigabitEthernet0/1
R1#
```

Étape 3 : Affichez les entrées ARP sur le commutateur S1.

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1           46   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2            8   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3            8   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11           -   0cd9.96e8.8a40  ARPA   Vlan1
S1#
```

Étape 4 : Ajoutez les entrées ARP sur le commutateur S1.

En envoyant une requête ping à d'autres périphériques, les entrées ARP peuvent également être ajoutées à la table ARP du commutateur.

a. À partir du commutateur S1, envoyez une requête ping au commutateur S2.

```
S1# ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
```

b. Vérifiez que l'entrée ARP pour le commutateur S2 a été ajoutée à la table ARP de S1.

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            5   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2           11   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3           11   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11           -   0cd9.96e8.8a40  ARPA   Vlan1
Internet  192.168.1.12           2   0cd9.96d2.4040  ARPA   Vlan1
S1#
```

4e partie : Utiliser Wireshark pour examiner les échanges ARP

Dans la quatrième partie, vous examinerez les échanges ARP en utilisant Wireshark pour capturer et évaluer l'échange ARP. Vous étudierez également la latence du réseau due aux échanges ARP entre les périphériques.

Étape 1 : Configurez Wireshark pour les captures de paquets.

a. Démarrez Wireshark.

b. Choisissez l'interface réseau à utiliser pour la capture des échanges ARP.

Étape 2 : Capturez et évaluez les communications ARP.

a. Commencez la capture des paquets dans Wireshark. Utilisez le filtre pour afficher uniquement les paquets ARP.

b. Videz le cache ARP en entrant la commande **arp –d *** à l'invite de commandes.

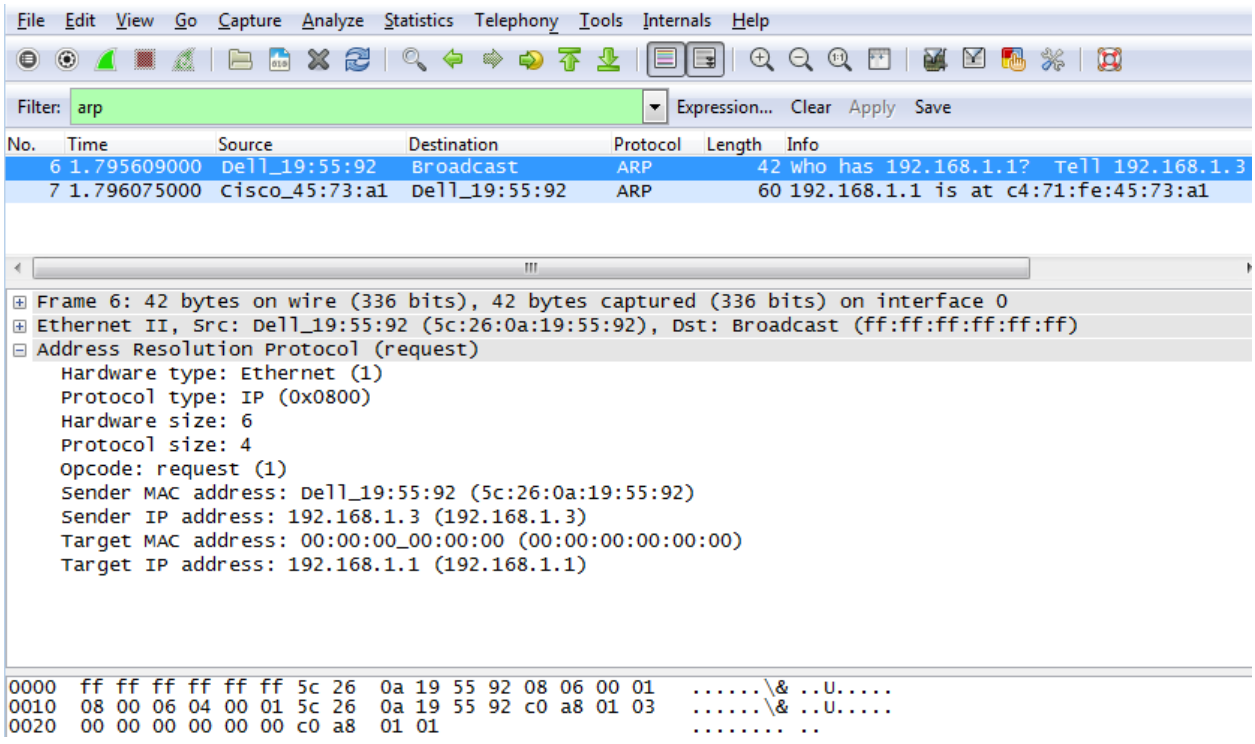
c. Vérifiez que le cache ARP a été effacé.

d. Envoyez une requête ping à la passerelle par défaut, à l'aide de la commande **ping 192.168.1.1**.

e. Arrêtez la capture Wireshark une fois que l'envoi des requêtes à la passerelle par défaut est terminé.

f. Recherchez les échanges ARP dans les captures Wireshark à partir volet Packet Details (Détails des paquets).

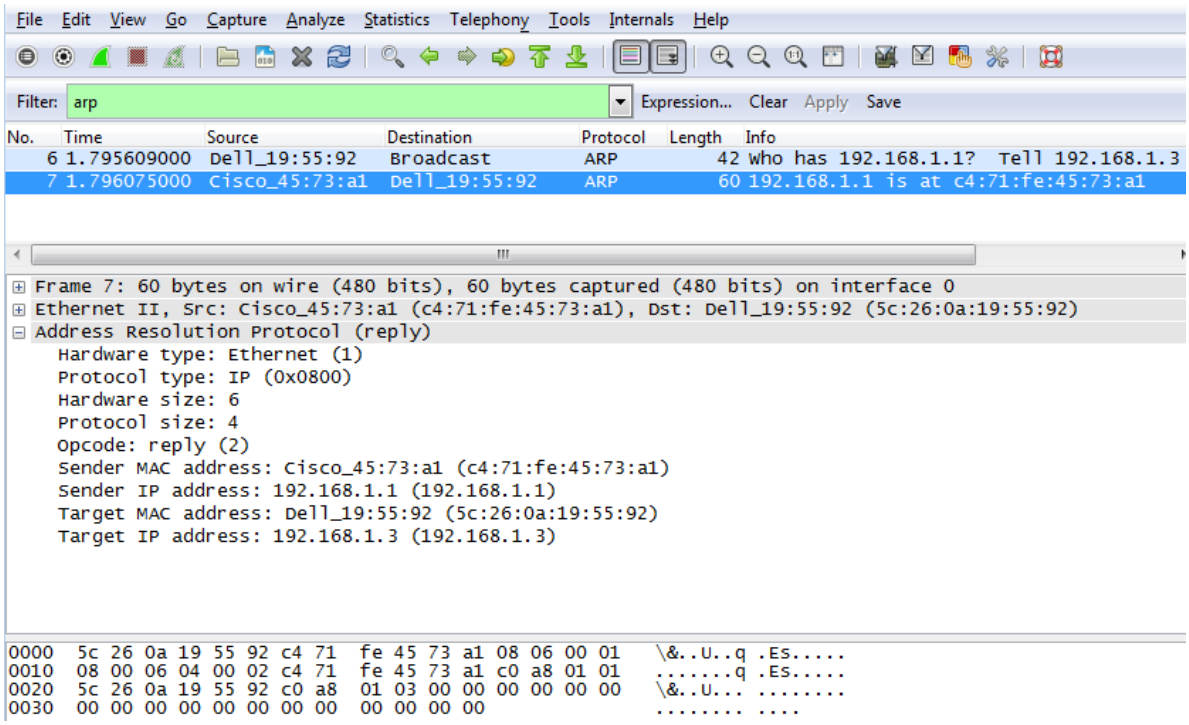
Quel était le premier paquet ARP ?



Complétez la table suivante avec les informations issues du premier paquet ARP que vous avez capturé :

Champ	Valeur
Adresse MAC de l'expéditeur	
Adresse IP de l'expéditeur	
Adresse MAC cible	
Adresse IP cible	

Quel était le deuxième paquet ARP ?



Complétez la table suivante avec les informations issues du deuxième paquet ARP que vous avez capturé :

Champ	Valeur
Adresse MAC de l'expéditeur	
Adresse IP de l'expéditeur	
Adresse MAC cible	
Adresse IP cible	

Étape 3 : Examinez la latence du réseau due au protocole ARP.

a. Effacez les entrées ARP sur PC-A.

b. Démarrez une capture Wireshark.

c. Envoyez une requête ping au commutateur S2 (192.168.1.12). La commande ping doit réussir après la première requête Echo.

Remarque :si toutes les requêtes ping ont réussi, S1 doit être redémarré pour que la latence du réseau avec le protocole ARP puisse être observée.

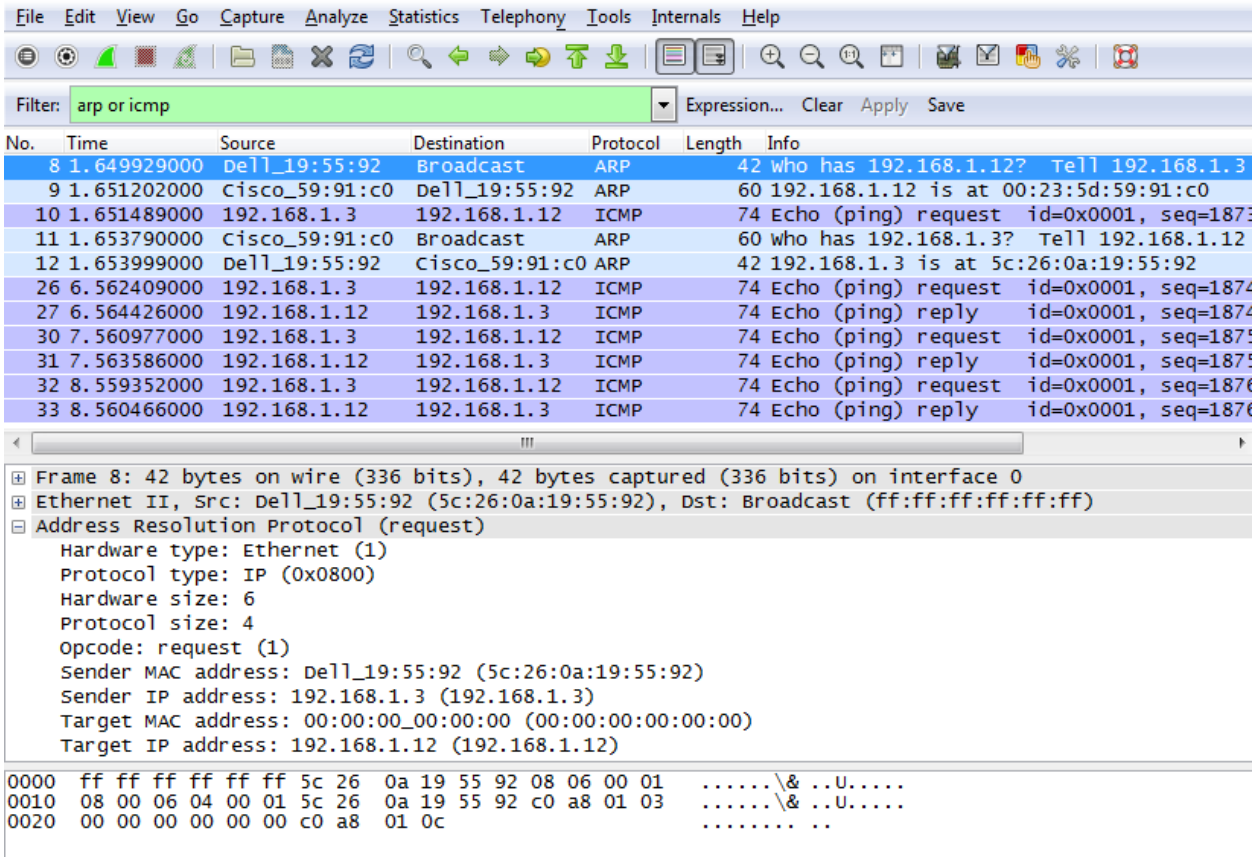
```
C:\Users\User1> ping 192.168.1.12
Request timed out.
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

d. Arrêtez la capture Wireshark à la fin des requêtes ping. Utilisez le filtre Wireshark pour afficher uniquement les résultats du protocole ARP et d'ICMP. Dans Wireshark, tapez **arp or icmp** dans la zone de saisie **Filter:**.

e. Examinez la capture Wireshark. Dans cet exemple, la trame 10 est la première requête ICMP envoyée par PC-A à S1. Comme il n'existe aucune entrée ARP pour S1, une requête ARP a été envoyée à l'adresse IP de gestion pour le commutateur S1 qui a demandé l'adresse MAC. Au cours des échanges ARP, la requête Echo n'a pas reçu de réponse avant l'expiration de la requête. (trames 8 à 12)

Après que l'entrée ARP pour S1 a été ajoutée au cache ARP, les trois derniers échanges ICMP ont réussi, comme illustré par les trames 26, 27 et 30 à 33.

Comme indiqué dans la capture Wireshark, ARP est un excellent exemple de compromis en matière de performances. Sans cache, ARP doit constamment demander des traductions d'adresses à chaque placement d'une trame du réseau. Ceci ajoute de la latence à la communication et peut encombrer le réseau local.



Remarques générales

1. Comment et quand les entrées ARP statiques sont-elles supprimées ?

2. Pourquoi voulez-vous ajouter des entrées ARP statiques dans le cache ?

3. Si les requêtes ARP peuvent générer une latence du réseau, pourquoi est-ce une mauvaise idée d'avoir des temps d'attente illimités pour les entrées ARP ?

Tableau récapitulatif de l'interface du routeur

Récapitulatif de l'interface du routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des combinaisons possibles des interfaces Ethernet et série dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes de Cisco IOS.