Travaux pratiques 9.8.1 : Protocole ARP (Address Resolution Protocol)

Schéma de topologie

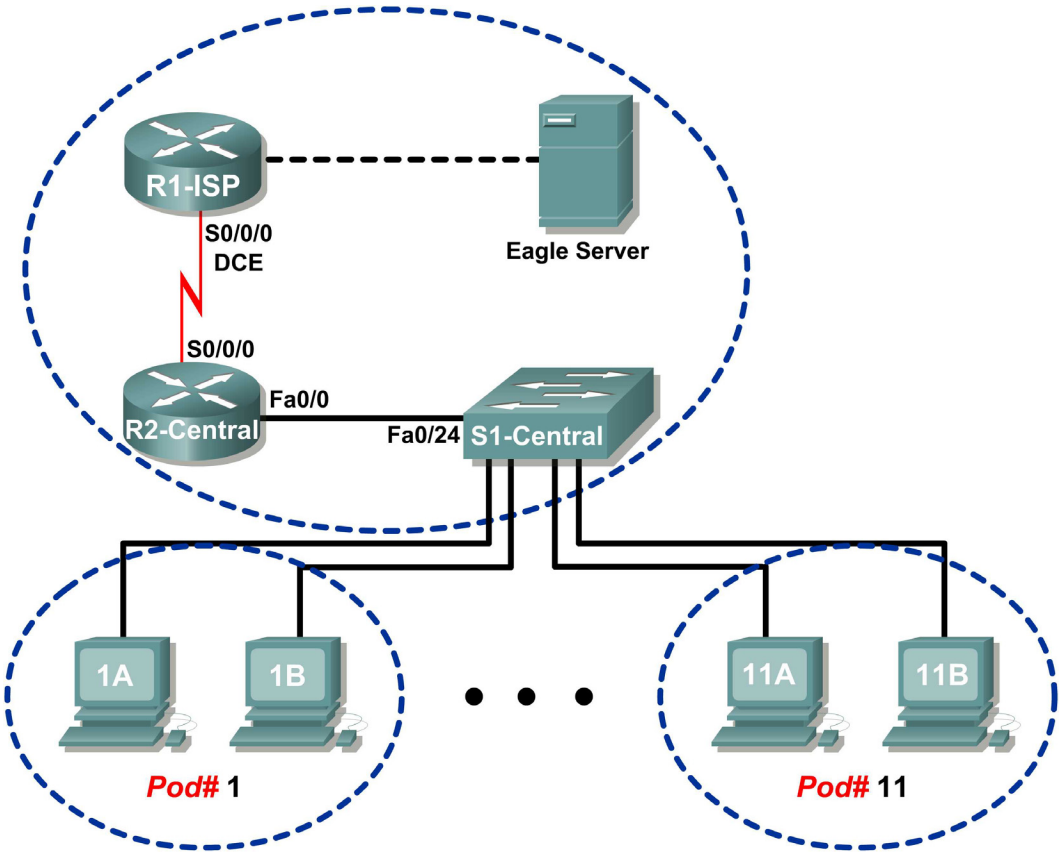

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	S/O
	Fa0/0	192.168.254.253	255.255.255.0	S/O
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	S/O
	Fa0/0	172.16.255.254	255.255.0.0	S/O
Eagle Server	S/O	192.168.254.254	255.255.255.0	192.168.254.253
	S/O	172.31.24.254	255.255.255.0	S/O
host*Pod*#A	S/O	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#B	S/O	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	S/O	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- utiliser la commande **arp** de Windows ;
- utiliser Wireshark pour examiner les échanges de ARP.

Contexte

Le protocole ARP (Address Resolution Protocol) est utilisé par TCP/IP pour mapper une adresse IP de couche 3 à une adresse MAC de couche 2. Lorsqu'une trame est placée sur le 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 sur le réseau local. Le périphérique qui contient l'adresse IP de destination répond. Ensuite, l'adresse MAC est consignée dans le cache ARP. Chaque périphérique sur le 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. Les délais diffèrent selon le périphérique utilisé. Par exemple, certains systèmes d'exploitation Windows stockent les entrées de cache ARP pendant 2 minutes. Si l'entrée est de nouveau utilisée au cours de ce délai, le temporisateur ARP de cette entrée est prolongé de 10 minutes.

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 sur le 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 ingénieur 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 pour limiter l'accès réseau aux seuls périphériques approuvés.

Scénario

Avec un ordinateur hôte pod, utilisez la commande de l'utilitaire **arp** de Windows pour examiner et modifier les entrées du cache ARP.

Dans la tâche 2, Wireshark permet de capturer et d'analyser les échanges ARP entre les périphériques réseau. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, fichier `wireshark-setup-0.99.4.exe`.

Tâche 1 : utilisation de la commande **arp** de Windows.

Étape 1 : accès au terminal de Windows.

```
C:\> arp
Affiche et modifie les tables de conversion d'adresses IP en adresses
physiques utilisées par le protocole ARP.
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a          Affiche les entrées ARP actuelles en interrogeant les
            données de protocole actuelles. Si inet_addr est spécifié,
            seules les adresses IP et physique de l'ordinateur spécifié
            s'affichent. Si plusieurs interfaces réseau utilisent ARP,
            les entrées de chaque table ARP s'affichent.
-g          Identique à -a.
inet_addr   Spécifie une adresse Internet.
-N if_addr  Affiche les entrées ARP de l'interface réseau spécifiée par
            if_addr.
-d          Supprime l'hôte spécifié par inet_addr. inet_addr peut
            s'utiliser avec le caractère générique * pour supprimer
            tous les hôtes.
-s          Ajoute l'hôte et associe l'adresse Internet inet_addr à
            l'adresse physique eth_addr.  L'adresse physique est
            fournie sous forme de 6 octets hexadécimaux séparés par des
            traits d'union. L'entrée est permanente.
eth_addr    Spécifie une adresse physique.
if_addr     Si présent, spécifie l'adresse Internet de l'interface dont
            la table de conversion des adresses doit être modifiée. Si
            absent, la première interface applicable est utilisée.
Exemple :
 > arp -s 157.55.85.212 00-aa-00-62-c6-09  .... Ajoute une entrée
statique.
 > arp -a                                  .... Affiche la table arp.
C:\>
```

Figure 1. Syntaxe de la commande arp

1. Ouvrez une fenêtre de ligne de commande en cliquant sur **Démarrer > Exécuter**. Tapez **cmd**, puis cliquez sur **OK**. Sans options, la commande **arp** affiche des informations d'aide utiles. Reportez-vous à la figure 1.
2. Exécutez la commande **arp** sur l'ordinateur hôte pod, et examinez les résultats.
3. Répondez aux questions suivantes sur la commande **arp** :

   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 172.16.255.254 ?

   _____

Étape 2 : utilisation de la commande `arp` pour examiner le cache ARP local.

```
C:\> arp -a
Aucune entrée ARP trouvée
C:\>
```

Figure 2. Cache ARP vide

Sans communication réseau, le cache ARP doit être vide. Ceci est illustré dans la figure 2.

Exécutez la commande qui affiche les entrées ARP. Quels sont les résultats ?

_____

_____

Étape 3 : utilisation de la commande `ping` pour ajouter de façon dynamique des entrées dans le cache ARP.

La commande **`ping`** sert à tester la connectivité réseau. En accédant à d'autres périphériques, les associations ARP sont ajoutées de façon dynamique au cache ARP.

```
C:\> ping 172.16.1.2
Envoi d'une requête sur 172.16.1.2 avec 32 octets de
données :
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Statistiques Ping pour 172.16.1.2 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte
0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 3. Commande `ping` vers un ordinateur hôte pod

1. Utilisez la commande **`ipconfig /all`** pour vérifier les données de la couche 2 et couche 3 de l'ordinateur hôte pod.
2. Exécutez la commande **`ping`** vers un autre ordinateur hôte, illustré à la figure 3. La figure 4 illustre la nouvelle entrée du cache ARP.

```
C:\> arp -a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f
dynamique
C:\>
```

Figure 4. Affichage du cache ARP

Comment l'entrée ARP a-t-elle été ajoutée au cache ARP ? Conseil : consultez la colonne Type.

_____

Quelle est l'adresse physique de l'ordinateur hôte pod de destination ?

_____

Quelle est l'adresse physique de l'ordinateur hôte pod de destination ?

Adresse IP	Adresse physique	Mode de détection ?

3. N'envoyez pas de trafic vers l'ordinateur auquel l'accès a eu lieu auparavant. Attendez 2 à 3 minutes, et vérifiez à nouveau le cache ARP. L'entrée du cache ARP a-t-elle été effacée ?
   _____
4. Exécutez la commande **ping** vers la passerelle, R2-Central. Examinez l'entrée du cache ARP. Quelle est l'adresse physique de la passerelle ? _____

Adresse IP	Adresse physique	Mode de détection ?

5. Exécutez la commande **ping** vers Eagle Server, eagle-server.example.com. Examinez l'entrée du cache ARP. Quelle est l'adresse physique d'Eagle Server ? _____
   _____
   _____

Étape 4 : modification manuelle des 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 deux entrées : une pour la passerelle et une pour l'ordinateur hôte pod de destination. L'exécution d'une commande ping vers les deux périphériques plusieurs fois peut s'avérer plus simple. Ce qui permet de conserver l'entrée du cache pendant environ 10 minutes.

```
C:\> arp –a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamique
  172.16.255.254        00-0c-85-cf-66-40     dynamique
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamique
C:\>
```

Figure 5. Suppression manuelle d'une entrée de cache ARP

Reportez-vous à la figure 5, qui illustre la méthode de suppression manuelle d'une entrée de cache ARP.

1. Sur votre ordinateur, vérifiez d'abord que les deux entrées sont disponibles. Sinon, exécutez une requête ping vers l'entrée manquante.
2. Ensuite, supprimez l'entrée pour l'ordinateur hôte pod.
3. Finalement, vérifiez vos modifications.

4. Consignez les deux entrées du cache ARP.

Périphérique	Adresse IP	Adresse physique	Mode de détection ?

5. Indiquez la commande qui permet de supprimer l'entrée pour l'ordinateur hôte pod :
_____

6. Exécutez la commande sur l'ordinateur hôte pod. Consignez l'entrée restante du cache ARP :

Périphérique	Adresse IP	Adresse physique	Mode de détection ?

7. Simulez la suppression de toutes les entrées. Indiquez la commande qui permet de supprimer toutes les entrées dans le cache ARP : _____
8. Exécutez la commande sur votre ordinateur hôte pod, et examinez le cache ARP avec la commande **`arp -a`**. Toutes les autres entrées doivent être supprimées.
_____
9. Prenez par exemple un environnement sécurisé où la passerelle contrôle l'accès à un serveur Web qui contient des informations classées « top secret ». Quelle fonction de sécurité, pouvant aider à neutraliser l'usurpation ARP, peut être appliquée à des entrées du cache ARP ?
_____
10. Indiquez la commande qui ajoute une entrée ARP statique au cache ARP pour la passerelle :
_____
11. Examinez à nouveau le cache ARP, et renseignez le tableau suivant :

Adresse IP	Adresse physique	Type

Pour la tâche suivante, Wireshark est utilisé pour capturer et examiner un échange ARP. Ne fermez pas le terminal Windows. Il sera utilisé pour afficher le cache ARP.

Tâche 2 : utilisation de Wireshark pour examiner les échanges de ARP.

Étape 1 : configuration de Wireshark pour les captures de paquets.

Préparez Wireshark pour les captures.

1. Cliquez sur **Capture > Options**.
2. Sélectionnez l'interface qui correspond au réseau local.
3. Cochez la case pour mettre à jour la liste de paquets en temps réel.
4. Cliquez sur **Démarrer**.

Ceci permet de commencer la capture des paquets.

Étape 2 : préparation de l'ordinateur hôte pod aux captures ARP.

1. Si ce n'est pas déjà fait, ouvrez une fenêtre de terminal Windows en cliquant sur **Démarrer > Exécuter**. Tapez **cmd**, puis cliquez sur **OK**.
2. Videz le cache ARP, afin qu'ARP détecte à nouveau les mappages d'adresses. Indiquez la commande que vous avez utilisée : _____

Étape 3 : capture et évaluation de la communication ARP.

Dans cette étape, une requête ping est envoyée à la passerelle, et l'autre à Eagle Server. Ensuite, la capture Wireshark est stoppée et la communication ARP évaluée.

1. Envoyez une requête ping à la passerelle, à l'aide de la commande **ping –n 1 172.16.255.254.**.
2. Envoyez une requête ping à Eagle Server, à l'aide de la commande **ping –n 1 192.168.254.254**.

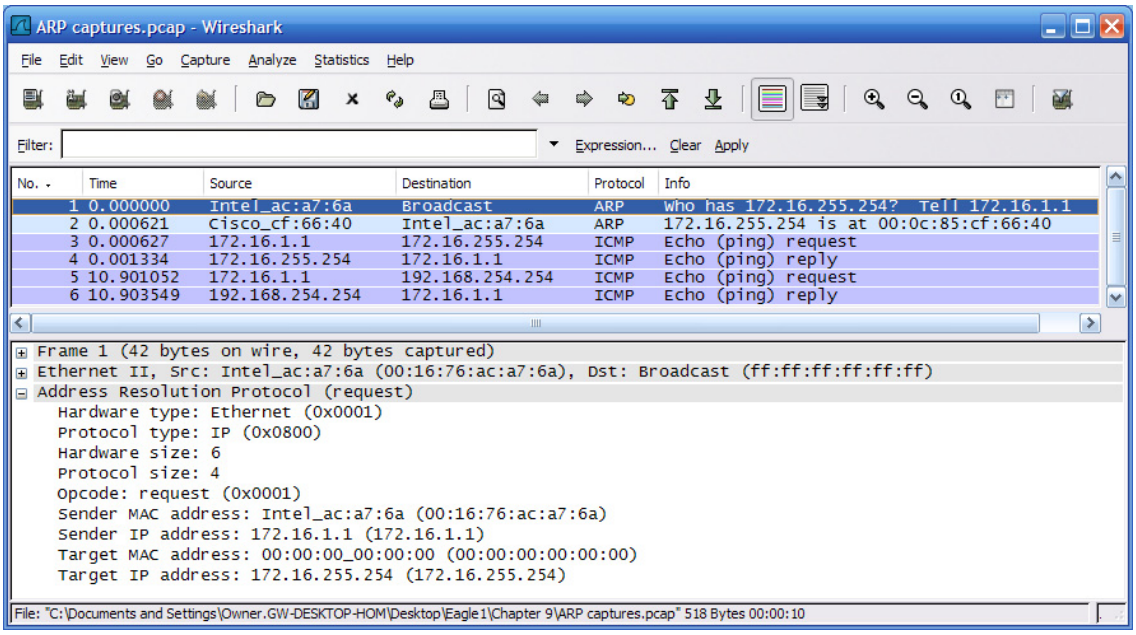

Figure 6. Capture Wireshark d'une communication ARP

3. Arrêtez Wireshark et évaluez la communication. Un écran Wireshark semblable à celui illustré à la figure 6 doit s'afficher. La fenêtre Packet list de Wireshark affiche le nombre de paquets capturés. La fenêtre Packet Details affiche le contenu du protocole ARP.
4. À l'aide de votre capture Wireshark, répondez aux questions suivantes :

   Quel était le premier paquet ARP ? _____

   Quel était le deuxième paquet ARP ? _____

   Renseignez le tableau suivant avec les informations issues du premier paquet ARP :

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

Renseignez le tableau suivant avec les informations issues du deuxième paquet ARP :

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

Si la trame Ethernet II pour une requête ARP est une diffusion, pourquoi l'adresse MAC cible ne contient que des 0 ? _____

Pourquoi n'y avait-t-il pas de requête ARP pour la commande ping envoyée à Eagle Server ?

_____

_____

_____

Combien de temps le mappage de la passerelle doit-il être stocké dans le cache ARP de l'ordinateur hôte pod ? Pourquoi ?

_____

_____

Tâche 3 : remarques générales

Le protocole ARP mappe les adresses IP de couche 3 aux adresses MAC de couche 2. Si un paquet doit parcourir des réseaux, l'adresse MAC de couche 2 change avec chaque saut sur un routeur. Cependant, l'adresse de couche 3 reste la même.

Le cache ARP stocke les mappages d'adresses d'ARP. Si l'entrée a été étudiée de façon dynamique, elle est supprimée du cache. Si elle a été manuellement insérée dans le cache ARP, il s'agit d'une entrée statique. Ainsi, elle reste disponible jusqu'à la mise hors tension de l'ordinateur ou le vidage manuel du cache ARP.

Tâche 4 : confirmation

À l'aide des ressources externes, effectuez une recherche sur l'usurpation ARP. Abordez les différentes techniques pour neutraliser ce type d'attaque.

La majorité des routeurs sans fil prennent en charge l'accès au réseau sans fil. À l'aide de cette technique, les adresses MAC qui disposent de l'accès au réseau sans fil sont ajoutées manuellement au routeur sans fil. À l'aide des ressources externes, abordez les avantages de la configuration de l'accès au réseau sans fil. Discutez des moyens dont disposent les pirates informatiques pour contourner cette sécurité.

Tâche 5 : nettoyage

Wireshark a été installé sur l'ordinateur hôte pod. Si Wireshark doit être désinstallé, cliquez sur **Démarrer > Panneau de configuration**. Ouvrez **Ajout/Suppression de programmes**. Sélectionnez Wireshark, puis cliquez sur **Supprimer**.

Supprimez tout fichier créé sur l'ordinateur hôte pod au cours des travaux pratiques.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

