**Travaux pratiques : Analyse de l’activité réseau – Découverte de Wireshark**

**Objectifs**

**1) Théoriques**

* Comprendre la nécessité d'une adresse physique et d'une adresse logique
* Comprendre les concepts de trames et de paquets
* Comprendre le protocole ARP qui permet de passer d'une adresse logique IP à une adresse physique MAC (Ethernet)

Vous utiliserez l’annexe 1 (Internet une histoire d’adresses) et l’annexe 2 (adresser un poste sur le réseau)

**2) Pratiques**

* Déterminer l’adresse IP de sa machine, la partie machine de l'adresse et la partie réseau
* Déterminer l'adresse du routeur
* Déterminer l’adresse physique (MAC) de sa machine
* Déterminer si une machine est active et accessible
* Déterminer l'adresse physique (MAC) d'une machine distante
* Installer et comprendre le fonctionnement d’un analyseur de trames
* Analyser un échange ARP à l'aide de cet analyseur de trames

Vous consulterez sur l’Intranet la RFC 826 (ARP), la RFC 792 (ICMP)

**Équipements requis (Matériel, logiciel, documentation)**

* Une machine virtuelle exécutant Windows 7.
* Un accès à Internet
* Le logiciel Wireshark
* Un tutoriel d’utilisation du logiciel Wireshark (de Benoit Darties)

**Étape 1 : Tests préalables**

Pour certaines tâches vous aurez besoin de deux postes clients Windows 7. Vous travaillerez donc en collaboration avec un autre étudiant.

* Depuis un poste client Windows 7, ouvrez la fenêtre d'invite de commande et tapez **ipconfig /all**. Notez les informations fournies concernant la connexion au réseau local :
  + adresse IP,
  + masque de sous réseau,
  + adresse de passerelle,
  + adresse DNS,
  + adresse MAC.

|  |
| --- |
| 192.168.151.116  255.255.255.0  192.168.151.254  192.168.151.254  08-00-27-D9-86-3E |

Remarque : vous devez avoir une adresse IP et un masque, une adresse de passerelle par défaut et une adresse de DNS correctement configurés.

* tapez **ping 127.0.0.1** pour testez l'adresse IP de bouclage [loopback] et vérifier que les liaisons définies par TCP/IP sont correctes
* testez avec l'adresse IP de votre poste
* testez avec l'adresse IP du deuxième poste client de votre réseau
* testez avec l’adresse d’un des serveurs google : 77.153.128.27
* testez avec le nom d’hôte du serveur de google : [www.google.fr](http://www.google.fr)

**Etape 2 : Le protocole ARP**

Pour dialoguer, deux hôtes du même réseau, doivent utiliser des adresses MAC. Il faut donc un moyen pour passer de l'adresse IP à l'adresse MAC et vice versa. IP fournit pour cela le protocole **ARP** (Address Resolution Protocol) et RARP (Reverse Address Resolution Protocol).

* Affichez le cache ARP : tapez la commande arp -a à l'invite de commande. Notez le résultat

|  |
| --- |
| C:\Windows\system32>arp -a  Interface : 192.168.151.116 --- 0xb  Adresse Internet Adresse physique Type  192.168.151.6 00-d0-b8-1b-d1-62 dynamique  192.168.151.187 08-00-27-68-97-f3 dynamique  192.168.151.220 5c-f9-dd-e9-89-ae dynamique  192.168.151.254 00-14-22-76-1f-6f dynamique  192.168.151.255 ff-ff-ff-ff-ff-ff statique  224.0.0.22 01-00-5e-00-00-16 statique  224.0.0.252 01-00-5e-00-00-fc statique  239.255.255.250 01-00-5e-7f-ff-fa statique  255.255.255.255 ff-ff-ff-ff-ff-ff statique |

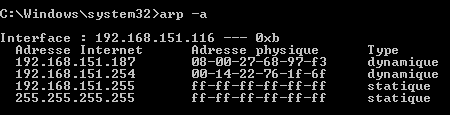
* Consultez l’aide de la commande arp (arp / ?) et videz le cache arp. Quelle commande avez-vous utilisée ?

|  |
| --- |
| Arp -d \* |

* Que contient désormais le cache ?

|  |
| --- |
|  |

* Réalisez un ping de l’autre poste client de votre réseau. Que contient le cache ?



* Réalisez un ping du serveur internet de votre choix (ex google). Que contient le cache ?

|  |
| --- |
|  |

* Comment expliquez-vous la dernière entrée du cache ?

|  |
| --- |
| C'est l'adresse SSDP du routeur |

* Videz de nouveau votre cache arp et vérifiez son contenu. Il doit être vide !

Nous allons créer une entrée (donc statique) dans le cache arp en indiquant la correspondance entre l’adresse IP et l’adresse mac de l’autre poste client.

* Demandez (à votre binôme) et notez l'adresse Ethernet (mac) de l’autre poste client.

|  |
| --- |
| 08-00-27-68-97-F3 |

* Créez l’entrée arp en utilisant la commande suivante :

**netsh interface ipv4 add neighbors "connexion au réseau local" adresse-IP-poste adresse-mac-poste**

**Remarque :**

**Netsh** (network shell : *shell réseau*) est un utilitaire en [ligne de commande](https://fr.wikipedia.org/wiki/Ligne_de_commande) inclus dans la gamme des systèmes d'exploitation [Windows NT](https://fr.wikipedia.org/wiki/Windows_NT) (NT, 2000, XP, 2003 Serveur, Vista) à partir de Windows 2000. Il permet la configuration du [réseau](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique), localement ou à distance. (*Source : Wikipédia*)

(Pour plus d’info : <https://technet.microsoft.com/fr-fr/library/cc731521%28v=ws.10%29.aspx>)

* Vérifiez la nouvelle entrée en visualisant le cache arp.
* Testez cette entrée avec ping. Le test de connectivité doit fonctionner
* Réalisez un ping d’un hôte externe à votre réseau IP afin d’obtenir une entrée correspondant à la passerelle. Vérifiez en affichant le cache arp.
* Trompez votre cache arp en associant une mauvaise adresse mac à la passerelle par défaut.

Donnez par exemple l’adresse : ca-fe-ca-fe-ca-fe ou 00-11-22-33-44-55. Notez la (ou les) commande(s) utilisée(s) pour le faire :

|  |
| --- |
| **netsh interface ipv4 add neighbors "connexion au réseau local"**  192.168.151.254 55-44-66-88-12-37 |

* Faites un ping sur la passerelle (notez le résultat et expliquez-le)

|  |
| --- |
|  |

* Faites un ping au delà de la passerelle (notez le résultat et expliquez-le)

|  |
| --- |
|  |

* Supprimez cette entrée incorrecte et refaites les deux tests de connectivité précédents. Donnez la commande :

|  |
| --- |
| Arp -d \* puis ping 8.8.8.8 ---> Resultat OK |

* Trouvez les commandes « **netsh** » permettant d’afficher et de supprimer le cache arp :

|  |
| --- |
|  |

**Etape 3 : Capturer les trames**

Nous allons utiliser le logiciel Wireshark.

* Videz le cache arp et vérifiez son contenu. Attention, cette étape est très importante ! Elle vous permettra de générer les trames ARP nécessaires à la suite de l’atelier.
* Démarrez une capture sur la carte réseau de votre machine virtuelle
* Réalisez un ping de l’autre poste client

Vérifiez que la commande PING a généré 10 trames Ethernet : (2 trames ARP et 8 trames ICMP).

* Repérez chacune de ces trames (donc 10 au total) et mettant en évidence les données capturées (utilisez un filtre si nécessaire)
* Analysez la **première trame ARP (request)** en retrouvant les informations suivantes :

|  |  |  |
| --- | --- | --- |
| **Partie de la trame à analyser** | **Contenu du champs/question** | **Valeur/réponse** |
| Trame complète | Combien d’octets contient la trame ? | 42 bytes = 42 octets |
| Trame complète | A quoi correspondent les 14 premiers octets ? | Adresse de Broadcast |
| Partie Ethernet | Quelle est la valeur du champ adresse de destination ? | ff:ff:ff:ff:ff:ff |
|  | A quoi correspond cette adresse mac ? | 00:00:00:00:00:00 |
| Partie Ethernet | Quelle est la valeur du champ adresse source ? | 08:00:27:d9:86:3e |
|  | A quoi correspond cette adresse mac ? | A la machine source |
| Partie Ethernet | Quelle est la partie constructeur de l’adresse physique ? | 08:00:27 |
| Partie Ethernet | Quel est la valeur (en hexadécimal) du type de trame ? | (0\*0806) |
|  | A quel protocole correspond ce type ? | ARP |
| Partie ARP | Quelle est l’adresse mac de l’expéditeur ? | 08:00:27:d9:86:3e |
| Partie ARP | Quelle est l’adresse IP de l’expéditeur ? (en hexadécimal et en décimal) | 192.168.151.116  C0:a8:97:74 |
| Partie ARP | Quelle est l’adresse mac de la cible ? | 00:00:00:00:00:00 |
|  | Pourquoi cette adresse mac contient-elle des zéros ? | C'est une adresse de Broadcast |
| Partie ARP | Quelles est l’adresse IP de la cible ? (en hexadécimal et en décimal) | 192.168.153.187  C0:A8:97:bb |

* Analysez la **deuxième trame ARP (reply)** en retrouvant les informations suivantes :

|  |  |  |
| --- | --- | --- |
| **Partie de la trame à analyser** | **Contenu du champs/question** | **Valeur/réponse** |
| Partie Ethernet | Quelle est la valeur du champ adresse de destination ? | 08:00:27:d9:86:3e |
|  | A quoi correspond cette adresse mac ? | broadcast |
| Partie Ethernet | Quelle est la valeur du champ adresse source ? | 08:00:27:d9:86:3e |
|  | A quoi correspond cette adresse mac ? | Du pc source |
| Partie ARP | Quelle est l’adresse mac de l’expéditeur ? | 08:00:27:d9:86:3e |
| Partie ARP | Quelle est l’adresse IP de l’expéditeur ? (en hexadécimal et en décimal) | 192.68.151.187 |
| Partie ARP | Quelle est l’adresse mac de la cible ? | 08:00:27:d9:86:3e |
| Partie ARP | Quelles est l’adresse IP de la cible ? (en hexadécimal et en décimal) | 192.168.151.116 |

* Comparez les deux tableaux.

|  |
| --- |
| ARP: premiere tableau: source vers destination  Deuxieme tableau: l'inverse donc les cibles et source sont inversés  ETHERNET: tableau1 : destination : broadcast pour chercher le pc destination.  Tableau2: Notre propre pc est destination de la réponse de la machine ping. |

* Analysez des trames ICMP en complétant le tableau ci-dessous :

|  |  |  |
| --- | --- | --- |
| **Partie de la trame à analyser** | **Contenu du champs/question** | **Valeur/réponse** |
| 1ère trame ICMP (echo request)  Partie ICMP | Quelle est la valeur en hexadécimal du champ type ? | 08 |
|  | Consultez la RFC 792 et expliquez à quoi correspond ce champ. | Correspond au champ ECHO |
|  | Quelle sera la valeur de ce champ si on sélectionne la deuxième trame ICMP (echo reply) ? | 0----> ECHO REPLY |
| 1ère trame ICMP  Partie ICMP | Quelle est la valeur du champ identifier ? | Identifier (BE):1 (0\*0001)  Identifier (LE): 256 (0\*0100) |
| 1ère trame ICMP  Partie ICMP | Quelle est la valeur du champ number ? | (be) 9 (0\*0009)  (le) 2304 (0\*0900) |
| 1ère trame ICMP  Partie DATA | Quelle est le contenu (en hexadécimal et en ascii) de la partie DATA ? | 6162...696a6b...6f7071...7761... |
| 2ème trame ICMP (echo reply)  Partie DATA | Quelle est le contenu (en hexadécimal et en ascii) de la partie DATA ? | 6162...696a6b...6f7071...7761... |
| 3ème trame ICMP (echo request)  Partie ICMP | Notez la valeur des champs :  - Type  - Identifier  - Sequence number | Type : 08 (Echo (ping) request)  Identifier:be 1(0\*0001)  Le 256 (0\*0100)  Number: be 10(0\*000a)  Le 2560(0\*0a00) |
|  | Qu’en concluez-vous sur la fonction des ces champs ? | Identifier et sequence number changent a chaque trame pour etre identifié dans l'ordre. |

|  |
| --- |
| **Annexe 1 : Internet, une histoire d’adresses** |

Lorsque deux ordinateurs communiquent à travers le réseau mondial Internet, cela suppose qu'ils savent s'adresser des messages.

**Adresser des messages qu'est ce que ça veut dire ?**

Comparons avec la poste. Lorsque vous écrivez à un correspondant, vous devez connaître l'adresse de celui-ci, et l'écrire sur l'enveloppe. Pourquoi l'écrire ?

Parce que ce courrier ce n'est pas vous qui allez le transporter. Vous allez le remettre à un service postal qui va se charger de son acheminement.

Cet acheminement peut-être direct ou indirect.

Direct quand votre correspondant dépend du même bureau de poste, indirect autrement.

Dans ce dernier cas, votre courrier passera successivement dans différents bureaux de postes. Chaque bureau de poste s’adresse au suivant jusqu'au bureau de poste dont dépend votre correspondant. Votre courrier peut aussi être transporté par différents moyens, du plus rapide (l'avion) au plus lent (le vélo du facteur).

La suite des bureaux de postes qui ont traité votre courrier constitue la route empruntée par celui-ci.

Cette route a été déterminée par l'adresse de départ mais en même temps, il a fallu déterminer toute une série d'adresses intermédiaires, les adresses des bureaux de postes traversés.

Entre vous et votre correspondant, il n'y avait pas de relation physique, sinon vous lui auriez parlé ou bien remis votre lettre en main propre.

La relation physique s'est établie entre vous et la boite aux lettres où vous avez remis votre courrier, puis entre les différents bureaux de postes, enfin entre le dernier bureau de poste et la boite aux lettres de votre correspondant.

Une fois la lettre remise par le dernier bureau de poste il n'y a pas pour autant de relation physique entre vous et votre correspondant, par contre celui-ci lira certainement votre courrier et donc, d'une certaine façon, que nous appellerons logique, vous êtes entré en communication avec lui.

**Posons-nous maintenant différents problèmes ?**

Comment être sûr que notre courrier est bien arrivé ?

Il n'y a pas trente six solutions, il faut que notre correspondant nous le confirme, cela s'appelle un accusé de réception, et pour que celui-ci nous arrive, il faut qu'il nous soit adressé. Donc on aura pris soin avec notre courrier de transmettre notre adresse.

**L'adresse suffit-elle à déterminer le correspondant ?**

Notre correspondant habite peut-être un immeuble. La seule adresse ne suffira donc pas pour identifier à qui doit être remis le courrier, il faut en plus nommer la personne destinataire.

On l'aura compris pour que nos bureaux de postes fonctionnent correctement, il faut que le système d'adressage permette d'identifier un correspondant de façon unique.

**Notre comparaison s'arrêtera là. Que retenir de celle-ci ?**

Pour qu'une communication puisse s'établir à distance, il faut un système d'adressage.

Ce système d'adressage doit permettre deux choses :

- identifier de manière unique un correspondant

- déterminer la route pour l'atteindre physiquement

Eventuellement il doit garantir que les messages ne se perdent pas en route.

L'objectif de ce système d'adressage est la communication logique entre deux correspondants, à travers l'établissement d'une succession de relations physiques entre services intermédiaires chargés d'acheminer les messages.

Bon maintenant on va essayer d'imaginer ça pour des machines qui communiquent entre elles.

**D'abord qui communique ?**

La machine c'est la carcasse, ce qui communique ce sont les programmes qui s'exécutent. Un programme qui s'exécute s'appelle un processus. Dans une machine plusieurs processus peuvent s'exécuter simultanément (principe du multitâche), on adressera la machine et le processus dans la machine.

Une machine pour communiquer doit disposer d'un moyen pour le faire. De même que vous disposez de jambes pour aller poster ou relever votre courrier, une machine doit disposer d'un organe pour émettre ou recevoir des messages. Ce moyen c'est la carte réseau dans ce qu'on va détailler, mais ça peut être aussi le modem, la carte X25... etc...

Un processus élabore son message puis le remet à la carte réseau pour le transmettre. De même une carte réseau reçoit un message et le transmet au processus destinataire.

**Mais comment la carte réseau sait-elle que le message est destiné à un processus sur sa machine?**

Parce que la carte réseau est identifiée par une adresse. Un message circulant sur un réseau contient l’adresse de la carte réseau destinataire. Lorsqu’une carte reconnaît son adresse, elle récupère le message et le transmet aux processus supérieurs sur sa machine. Mais si elle reçoit un message c'est qu’une autre carte lui a transmis et que cette carte connaissait son adresse.

**Comment cette carte émettrice connaît-elle l’adresse de la carte destinataire ?**

On peut imaginer que des machines reliées à un même câble s’échangent leurs adresses respectives. C’est une hypothèse vraisemblable. Même si nous reviendrons dessus ultérieurement.

Mais comment communiquent deux machines qui ne sont pas reliées physiquement ?

Elles vont passer par des machines intermédiaires, qui bout à bout formeront un chemin physique emprunté par les messages.

Dans ce cas l’émetteur doit non seulement adresser le destinataire réel mais aussi la machine intermédiaire.

**Cela veut-il dire que les messages vont comporter l'ensemble des adresses des cartes réseaux des machines intermédiaires ?**

Non c'est impossible, ce serait trop important, cela sous-entendrait que la machine émettrice connaisse l'ensemble de ces adresses non seulement pour un correspondant mais pour l'ensemble des correspondants potentiels, que ces adresses soient immuables...etc... on voit bien évidemment qu'un tel système n'est pas viable.

Donc dès que deux machines ne sont pas reliées physiquement, il faut un système d'adressage de niveau supérieur à celui des cartes réseaux, mais qui permette cependant d'établir un chemin physique à travers l'ensemble des cartes réseaux interconnectés.

Nous dirons que nous avons besoin d'une adresse physique pour faire dialoguer physiquement 2 cartes réseaux reliés à un même câble, et d'une adresse logique permettant de faire dialoguer 2 machines reliés entre elles par une succession de machines intermédiaires.

Puis, pour ces machines, nous avons besoin d'une adresse qui nous permet d'identifier les processus émetteurs et récepteurs des messages.

Nous sommes dans le mondes des machines, ces adresses prendront forcément la forme de numéros peu compréhensibles et peu pratiques à manipuler par l'esprit humain. Celui-ci préfère manipuler des abstractions plus significatives qu'une simple suite de chiffres, il préfère utiliser des noms. Il faudra alors en plus un mécanisme qui permettra de passer d'un nom à une suite de chiffres.

**Résumons-nous :**

Deux processus qui communiquent sur des machines distantes sont identifiés par des noms logiques, qui sont traduits en adresses logiques, permettant d'établir un chemin physique qu'emprunteront les messages échangés.

Bien sûr tout cela reste un peu schématique et très approximatif, il nous faut l'approfondir, c'est ce que nous nous proposons de faire dans cette suite d’atelier et de cours dont le thème central sera "l'adressage de processus entre deux machines sur Internet".

|  |
| --- |
| **Annexe 2 : Adresser un poste sur un réseau** |

Ce cours précise les notions d'adresse physique et logique sur un réseau, le rôle de l'une et de l'autre ainsi que le passage de l'une à l'autre.

**Notion d'adresse Physique et de trames**

* Deux cartes réseaux qui communiquent s'échangent des messages (suite d'octets) appelés trames (frame).
* Tous les postes connectés au même câble reçoivent le message, mais seul celui à qui il est destiné le lit.
* Comment sait-il que cette trame lui est adressée ?
* Car il reconnaît l'adresse de destination, contenu dans la trame comme étant la sienne.
* Comment sait-il qui lui a envoyé la trame ?
* Car la trame contient aussi l'adresse de l'émetteur.
* L'adresse correspond à l'adresse de la carte réseau. On parle d'adresse physique, d'adresse MAC (Medium Access Control) ou d'adresse de couche 2 (référence au modèle OSI).
* Cette adresse est identique pour les réseaux Ethernet et FDDI. Sa longueur est de 48 bits. Elle identifie de manière unique un nœud dans le monde. Elle est physiquement liée au matériel (écrite sur la PROM), c'est à dire à la carte réseau.

Le format de l'adresse est le suivant :



I ou G indique si l'adresse correspond à un nœud ou à un groupe de nœuds. Quand le bit est à 1 un nœud peut adresser une trame à plusieurs nœuds simultanément (principe du multicast), si tous les bits de l'adresse sont à 1, la trame est destinée à tous les postes du réseau (broadcast)

Le second bit indique s'il est à zéro que l'adresse est universelle et respecte le format de l'IEEE (Institut of Electrical and Electronic Engineers). Dans le cas contraire le format est propriétaire (local). Une adresse universelle est attribuée par l'IEEE à chaque constructeur de matériel réseau (RFC 1700).

exemple : CISCO 00000C, 3com 0000D8 ou 0020AF ou 02608C ou 080002 , INTEL 00AA00

**Remarque** : une adresse MAC en PROM peut être ignorée et remplacée par une adresse logicielle (shell IPX de Novell).

**Notion d'adresse logique et de paquets**

L'adresse d'une carte réseau correspond à l'adresse d'un poste et d'un seul. Or les postes sont généralement regroupés en réseau. Comment identifier le réseau auquel appartient le poste ?

Il faut une adresse logique qui soit indépendante de l'adresse physique. C'est ce que proposent le protocole IP et le protocole IPX.

Ici nous ne parlons que d'IP.

**Pourquoi identifier le réseau ?**

Pour permettre à 2 postes qui ne sont pas connectés au même réseau de communiquer.

Cela est impossible avec une adresse MAC, il faut une adresse de niveau supérieur, comme nous le verrons un peu plus loin et surtout avec le routage IP.

Le message véhiculé par la trame va contenir une autre adresse destinataire dont un des objectifs sera de définir le réseau destinataire du message. On appelle le message contenu dans une trame un paquet.

Ce qu'il nous faut savoir à ce stade, c'est qu'une machine sait que le paquet n'est pas destiné au réseau si l'adresse réseau de destination est différente de la sienne, dans ce cas elle envoie le paquet à une machine spéciale dont le rôle est d'acheminer les paquets qui sortent du réseau.

Cette machine s'appelle une **passerelle** (gateway) dans la terminologie IP ou un routeur dans la terminologie OSI.

Cette adresse logique contenue dans le paquet est l'adresse IP.

**Rappel sur l'adresse IP.**

Une adresse IP a une longueur de 32 bits. Elle se compose d'une partie réseau et d'une partie adresse du poste sur le réseau.

Il existe aussi en IP des adresses de multicast et de broadcast que nous étudierons plus loin.

L'adresse IP est logique, lorsqu'on change la carte réseau, l'adresse IP du poste ne change pas.

En IP lorsqu’un poste envoie un message à un autre poste, il met son message dans un paquet précédé de l'adresse IP du destinataire et de son adresse IP d’émetteur.

Mais les carte réseaux ne lisent pas les adresse IP, elles ne lisent que les adresses MAC.

Pour pouvoir être correctement transmis, le paquet va être mis dans une trame avec une adresse MAC de destination et une adresse MAC d'émission.

On dit qu'un paquet IP est encapsulé dans une trame.

Mais pour que tout cela fonctionne, il faut un mécanisme qui permettra de passer d'une adresse logique à une adresse physique, et réciproquement

**Résolution d'adresses logiques en adresses physiques**

Toute machine sur un réseau IP et Ethernet a donc 2 adresses, une adresse MAC et une adresse IP.

Les processus de niveaux supérieurs utilisent toujours l'adresse IP et donc lorsqu'un processus communique avec un autre processus, il lui envoie un message dont l'adresse destinataire est une adresse IP, mais pour pouvoir atteindre la carte réseau du destinataire, il faut connaître son adresse MAC. Comment faire ?

C'est le rôle du protocole ARP (Address Resolution Protocol) que vous allez étudier maintenant.

Quand vous aurez terminé l’atelier vous pourrez évaluer les connaissances acquises.