Laboratoire RSE 3

HUBs, Switches et ARP

Objectif

Capturer, filtrer et analyser de trames Ethernet avec le logiciel Wireshark, utiliser des HUBs et des Switchs, apprendre le fonctionnement de base du protocole ARP.

Durant ce TP, nous allons :

* Lancer le programme Wireshark
* Capturer et analyser des trames Ethernet
* Définir des filtres pour la capture et la visualisation des trames
* Observer les différences entre les HUBs et les Switches
* Observer le fonctionnement du protocole ARP

Matériels/Logiciels

* HUBs et Switches
* Wireshark

Rendu

Le rapport devra être envoyé par e-mail à [edward.ransome@heig-vd.ch](mailto:edward.ransome@heig-vd.ch) avec copie à

[marcos.rubinstein@heig-vd.ch](mailto:marcos.rubinstein@heig-vd.ch) une semaine après la fin du labo au plus tard. Le rapport

devra être rendu au format PDF, avec le nom du cours, le numéro du laboratoire et vos

noms dans le nom du fichier (en remplaçant les termes en gras) :

AP-RSE-LaboHubsSwitches\_NOM1\_NOM2\_NOM3.pdf

Questions théoriques

1. Quelle est l’origine du nom Ethernet ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Comment un Switch apprend-il quels nœuds sont connectés à quels ports ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Donnez deux avantages de l’utilisation de Switches par rapport à l’utilisation de HUBs

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Quelle est la différence principale entre le comportement d’un hub et celui d’un Switch ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Au niveau de quelle couche du modèle OSI un HUB fonctionne-t-il ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Au niveau de quelle couche du modèle OSI un Switch fonctionne-t-il ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. A quoi le protocole ARP sert-il ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Donnez la commande utilisée en ligne de commande pour visualiser la table ARP d’une machine :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

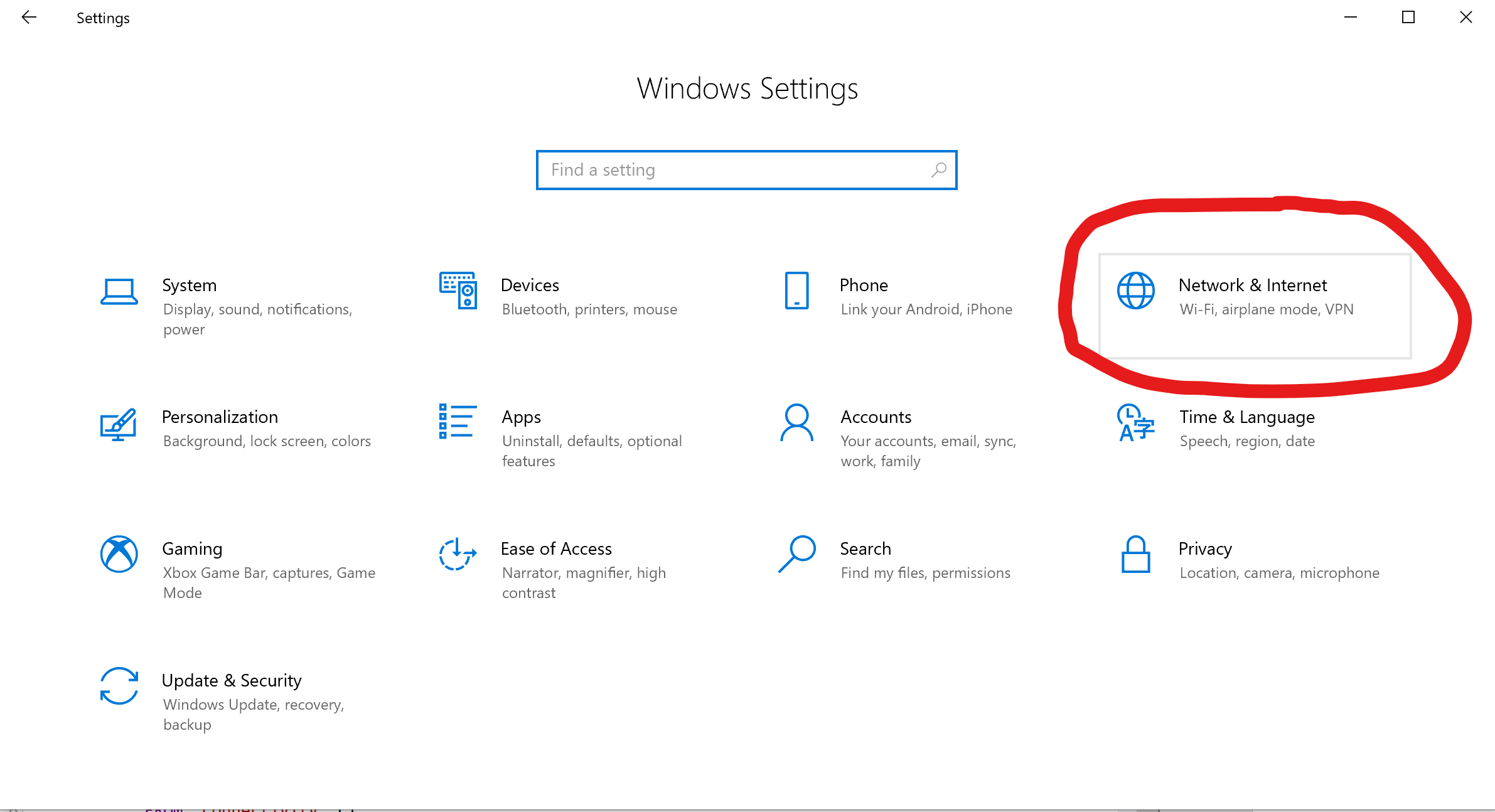
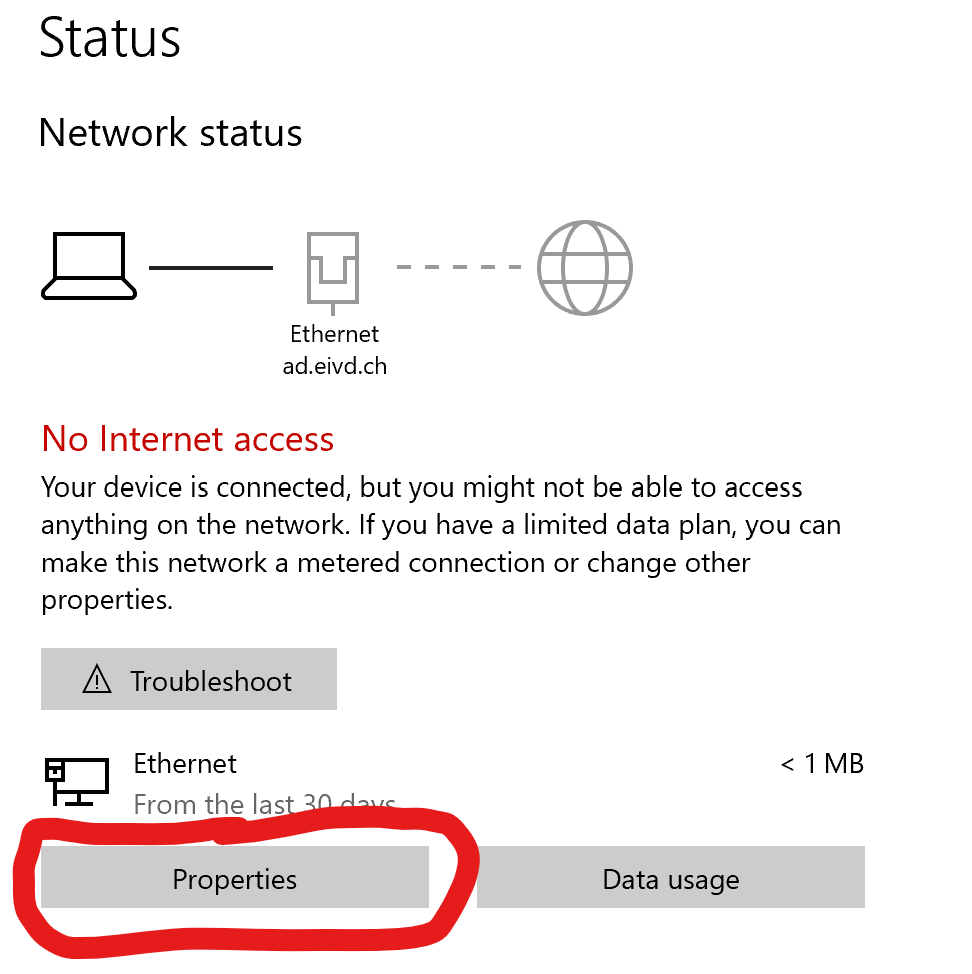
1. Donnez la commande utilisée en ligne de commande pour vider le cache ARP :

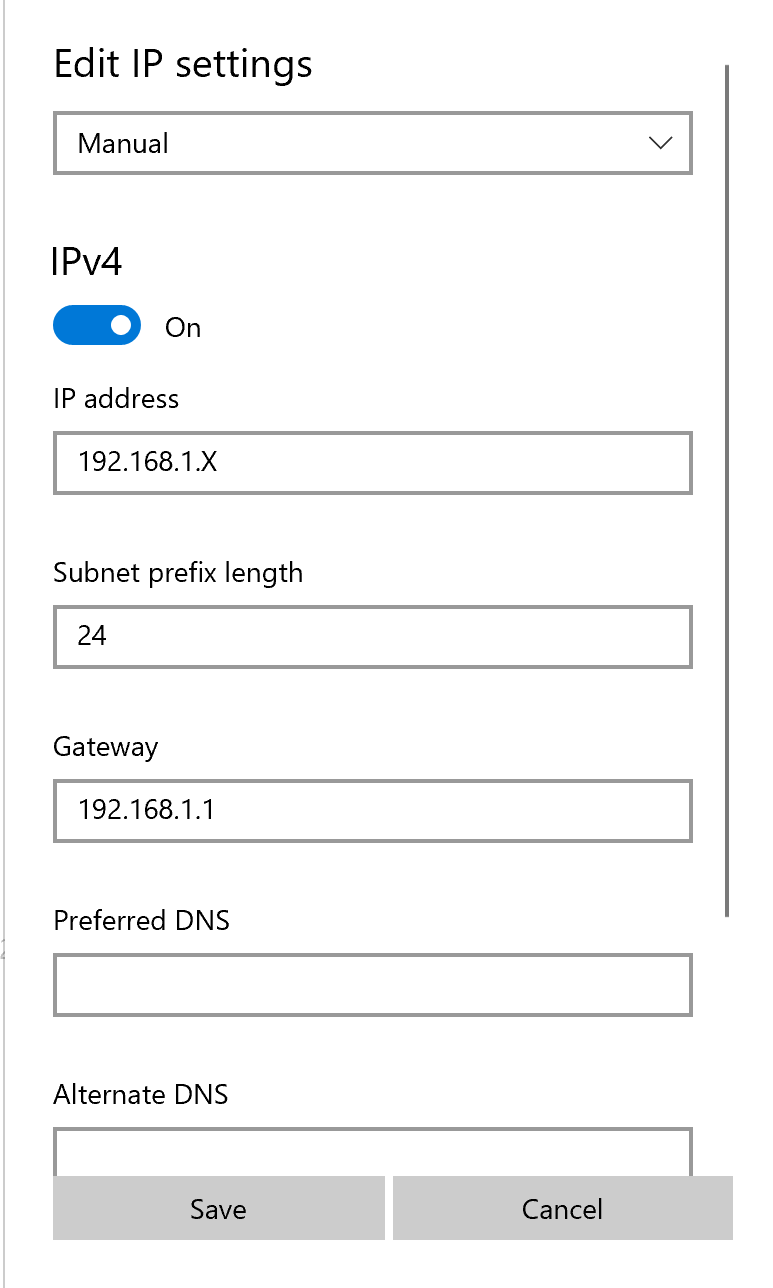
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Donnez la commande utilisée en ligne de commande pour biffer une association de la table ARP d’une machine :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mise en place

1. Branchez les ordinateurs du laboratoire sur le switch selon le schéma du point 4. Assignez leurs des addresses IP différentes selon ces instructions :
2.  
3. Sous « IP Settings », cliquez sur « Edit » et entrez les informations suivantes :



Remplacez le ‘X’ de l’addresse ip par 2, 3 ou 4 sur chaque PC. Il doivent tous avoir une adresse différente.

Questions pratiques

1. Montez un réseau comme celui de la figure (le Switch de la figure a seulement 4 ports puisque c’est seulement une illustration. Le nombre de ports peut être différent au laboratoire) :



1. Déterminez les adresses IP et MAC de chacun des nœuds et notez-les dans la tabelle ci-dessous. Pour obtenir les adresses IP et MAC, utilisez la commande « ipconfig /all » depuis un terminal (ifconfig dans les systèmes osx, Linux ou UNIX) :

|  |  |  |
| --- | --- | --- |
| Machine | Adresse IP | Adresse MAC |
| Nœud 1 |  |  |
| Nœud 2 |  |  |
| Nœud 3 |  |  |

Ping et capture

* Pour avoir une idée de ce qu’est le ping, regardez par exemple ici :

<https://www.youtube.com/watch?v=5wCTdU6rE-s>

* Lancez Wireshark dans la machine 1. Depuis une fenêtre de commande de la même machine, lancez un « ping » vers l’adresse de la machine 2 et capturez l’échange de trames. Dans un premier temps, faites une capture sans appliquer de filtre. Stoppez la capture.
* Pour afficher exclusivement le trafic ICMP, utilisez un filtre d’affichage pour ce protocole.

1. Montrez à l’aide d’une capture d’écran que vous avez capturé des ping request et des ping response.
2. Quelle machine a transmis les ping request et quelle machine a envoyé les ping response ?
3. Lancez Wireshark dans la machine 3 et refaites le ping entre la machine 1 et la machine 2. Les pings sont-ils capturés depuis la machine 3 ?

\_\_\_\_Oui \_\_\_\_\_Non

Expliquez  ce résultat :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Montez maintenant un réseau comme celui de la figure suivante :



1. Utilisant Wireshark dans la machine 3, faites de nouveau un ping depuis la machine 1 vers la machine 2. Est-ce que vous voyez les pings dans Wireshark ?

\_\_\_\_Oui \_\_\_\_\_Non

Expliquez  ce résultat :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ARP et tables de commutation dans les machines

Commencez par regarder cette vidéo pour avoir une première idée du fonctionnement du protocole ARP : <https://www.youtube.com/watch?v=2Ezyx93MkY8>

Afin de capturer les trames transmises par le protocole ARP, lancez une capture Wireshark dans la machine 3 et attendez au moins deux minutes sans rien faire (ces deux minutes sont le temps que le cache ARP garde les informations avant de les effacer). Maintenant, tout en continuant à capturer avec Wireshark au niveau de la machine 3, envoyez un ping depuis la machine 1 vers la machine 3.

1. Arrêtez la capture Wireshark et utilisez un filtre d’affichage pour montrer les trames qui correspondent au protocole ARP. Montrez les trames avec une capture d’écran.

Observez les caches arp des machines et répondez aux questions suivantes.

1. Affichez la table ARP de la machine 1. Y a-t-il une ligne qui montre correspondance entre l’adresse MAC et l’adresse IP de la machine 1 ?
2. Y a-t-il une ligne qui montre la correspondance entre l’adresse MAC et l’adresse IP de la machine 3 ?
3. Affichez maintenant la table ARP de la machine 2. Y a-t-il une ligne qui montre correspondance entre l’adresse MAC et l’adresse IP de la machine 1 ?
4. Y a-t-il une ligne qui montre correspondance entre l’adresse MAC et l’adresse IP de la machine 3 ?
5. Si les correspondances d’une ou des deux questions précédentes ont été trouvées, Comment la machine 2 a-t-elle pu mettre à jour sa table ARP avec les informations des machines 1 et 3 ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Manipulation manuelle des tables arp

Vous pouvez trouver des informations sur comment manipuler les caches ARP sur Internet.

Attention : Il est possible, pour ces questions, qu’il soit nécessaire de travailler avec une élévation des droits (c’est-à-dire par exemple sur Windows en démarrant le terminal en mode Administrateur) (clic droit : « Run as Administrator… »)

1. Affichez toutes les entrées du cache ARP de la machine 1 et montrez la commande avec une capture d’écran.
2. Effacer une des lignes du cache ARP que vous venez d’afficher et montrez la commande avec une capture d’écran.
3. Ajoutez à la main la machine 2 dans le cache ARP de la machine 1. Montrez une capture de la commande utilisée.
4. Effacez toutes les correspondances dans le cache ARP de la machine 1 avec une seule commande. Montrez la commande avec une capture d’écran.