École Polytechnique de Montréal
Département Génie Informatique et Génie Logiciel
INF3405 – Réseaux Informatiques

Travail pratique N° 2

Analyseur de protocoles

1. Informations générales

Session	Hiver 2019
Public cible	Étudiants de 1er cycle du cours INF3405
Taille de l'équipe	2 étudiants
Date et lieu de réalisation	À partir du 1er mars au L4708
Date de remise	Le 28 mars avant 23h55
Pondération	8 %
Directives particulières	Ce laboratoire est une préparation au laboratoire no.3 • **Toutes les manipulations doivent être faites sur les ordinateurs du L-4708**. • Tout rapport sera pénalisé de **5** points s'il est soumis par une équipe dont la taille est différente de deux (02) étudiants sans l'approbation préalable du chargé de laboratoire. • Soumission par ***moodle*** uniquement (http://moodle.polymtl.ca). • **Le rapport (en format PDF)** • Toute soumission de l'archive en retard est pénalisée à raison de 5 points par heure de retard. • **Vous devez inclure des captures d'écran en guise de justification de vos manipulations.**
Chargé de laboratoire	Émilie Dion-Paquin (emilie.dion-paquin@polymtl.ca)
Version originale : Révision :	Francis GAGNON Mehdi Kadi, Bilal Itani, Émilie Dion-Paquin

2. Connaissances préalables

- Pile de protocole TCP/IP
- Encapsulation des données
- Format des trames Ethernet (802.3)

3. Environnement et outils nécessaires

- Réseau FastEthernet (802.3u)
- Station de travail virtuelle Windows 7
- Analyseur de protocoles : WildPackets OmniPeek

4. Éléments de contexte

Les réseaux d'aujourd'hui présentent des architectures de plus en plus complexes au regard des protocoles impliqués dans leur fonctionnement. La localisation et la résolution de certains dysfonctionnements sont inhérentes à la tâche d'administration d'un réseau. L'analyseur de protocoles demeure l'un des outils les plus importants pour situer de manière précise certains dysfonctionnements identifiés.

Lors de son utilisation, l'analyseur de protocole place l'interface réseau dans un mode appelé *promiscuous* ou banalisé. Dans ce mode de fonctionnement, toute trame reçue sur la carte réseau est remontée à l'analyseur de protocoles et affichée à l'intérieur de celui-ci. Ce mode de fonctionnement diffère du fonctionnement normal, où la carte réseau rejette systématiquement toute trame qui n'est pas destinée au poste hôte (Adresse MAC et IP différents de ceux de l'interface réseau).

Ce laboratoire contient une série d'activités vous permettant de vous familiariser avec un analyseur de protocoles. Vous analyserez les échanges que l'on retrouve dans les réseaux (Ethernet) courants d'aujourd'hui ainsi que certains protocoles de la famille TCP/IP très répandus.

5. Objectifs du laboratoire

- Comprendre les divers types de paquets qui circulent dans un réseau ;
- Visualiser l'encapsulation des données;
- Analyser des échanges réseaux.

Ce travail pratique consiste, par la même occasion, à évaluer deux des 12 qualités de l'ingénieur définies par le BCAPG (Bureau canadien d'agrément des programmes de génie). Le Bureau d'agrément a pour mandat d'attester que les futurs ingénieurs ont atteint ces 12 qualités à un niveau acceptable. Les deux qualités en question sont:

Qualité 3 (Investigation) : capacité d'étudier des problèmes complexes au moyen de méthodes mettant en jeu la réalisation d'expériences, l'analyse et l'interprétation des données et la synthèse de l'information afin de formuler des conclusions valides.

Qualité 5 (Utilisation d'outils d'ingénierie) : capacité de créer et de sélectionner des techniques, des ressources et des outils d'ingénierie modernes et de les appliquer, de les adapter et de les étendre à un éventail d'activités simples ou complexes, tout en comprenant les contraintes connexes.

6. Préparation de l'environnement de travail clients virtuel

A) Copie et configuration des images virtuelles.

- Allez dans le répertoire **C:\VM\INF3405\Windows 7** et double cliquez sur le fichier **Windows 7.vmx** et attendez quelques secondes.

    - Dans VMware, sélectionner **VM, manage, clone**. À la fenêtre *Welcome*, choisir **suivant**, à la fenêtre *clone source*, choisir **suivant**, conserver *create a linked clone* et choisir suivant, nommer la machine **Windows7_A** et pour la **location** choisir **c:\temp\Windows7_A et choisir terminer**. Cette image est identique (du moins pour les fonctionnalités que vous utiliserez dans ce laboratoire) à un poste de travail Windows 7 dont vous seriez administrateur. Dans VMware, cliquez droit sur la machine virtuelle ***Windows7_A*** que vous venez de créer et cliquez sur l'option *settings* dans le menu qui apparaît pour accéder aux paramètres de la machine virtuelle. Dans l'onglet *hardware*, cliquez sur l'option *Network Adapter*. Ensuite dans *Network Connexion*, attribuez à l'option '*Custom : Specific virtual network'* la valeur ***VMnet8***. Cliquez sur le bouton *OK* pour sauvegarder les modifications.

- Effectuer de nouveau un clone de la machine Windows 7, en suivant les étapes décrite ci-haut. Changer le nom de la machine pour **Windows7_B** et placer ce deuxième clone dans le dossier **C:\temp\Windows7_B**

B) Démarrage des images virtuelles.

Aux termes de la configuration des images virtuelles, suivez les étapes ci-après:

- Démarrez l'image virtuelle avec l'onglet *Windows7_A* sélectionné et en choisissant *'Power ON this virtual machine'*. Si une boîte de dialogue vous interroge sur la copie ou le déplacement de la machine virtuelle, cliquez sur le bouton « **I copied it** ». Pour la boîte de dialogue suivante, cliquez sur « **OK** ». Si question de redémarrer ou non l'image virtuelle, choisissez de redémarrer aussitôt.

- Démarrez de la même façon *Windows7_B*.

C) Finalement pour permettre la connectivité complète entre vos clients virtuels, vous devez désactiver le firewall des deux machines Windows 7.

Sélectionnez l'*onglet **Windows7_A*** → Menu Démarrer → *Control Panel* → *System and Security* → *Windows Firewall* → *turn Windows Firewall on or off*.

Mettez les deux *pare-feux (Home or work (private) network location settings* et *Public network location settings) à Turn off Windows Firewall → OK.*
Faites de même pour la machine ***Windows7_B***

D) Vérifiez que le client ***Windows7_A*** peut joindre le client virtuel *Windows7_B* (faites un ping sur son adresse IPv4).

Pour la partie 8, faites bien attention à sélectionner les trames DHCP correspondant à l'adresse en 192.168.x.x que vous avez obtenue.

Si vous le désirez, vous pouvez aussi agrandir la fenêtre de votre client avec le bouton de droite de la souris dans l'environnement du client et choisir *screen résolution* et ensuite la résolution 1152x864 et OK deux fois.

Récapitulatif des configurations des machines virtuelles

Avant de commencer, vérifiez que vous avez bien effectué TOUTES les étapes de configuration mentionnées précédemment. Voici un petit récapitulatif des valeurs à modifier. La procédure se trouve plus haut.

- *Windows7_A*
  - **Network Adapter** : VMnet8
  - **Configuration IP** : Automatique
  - **Firewall Home or work** : Off
  - **Firewall Public Network** : Off
- *Windows7_B*
  - **Network Adapter** : VMnet8
  - **Configuration IP** : Automatique
  - **Firewall Home or work** : Off
  - **Firewall Public Network** : Off

6.1 Exécutez la commande *ipconfig /all* dans une fenêtre de commande (*Command Prompt*) : Menu Démarrer (*start*), cmd pour le client. Inscrivez le nom de votre poste, l'adresse IPv4, le masque de sous-réseau, l'adresse *MAC*, la passerelle par défaut pour vos deux systèmes virtuels. **(0.5 pt)**

7. Démarrage de l'analyseur de protocoles

Sur votre client *Windows7_A*, cliquez sur l'icône *WildPackets Omnipeek* qui se trouve sur votre bureau. Pour obtenir une fenêtre de saisie de trames, sélectionnez "*New capture*". Si demandé, cochez l'option *Continuous capture* qui permet un affichage continu en temps réel. Pour démarrer une saisie de trames, appuyez sur le bouton *Start Capture* en haut à droite de l'écran ainsi que le menu *Capture, packets,* à gauche dans la fenêtre de saisie de trames. Si aucune trame n'apparaît, assurez-vous, en faisant dans le menu "*Capture/Capture Options/Adapter*", que la carte *Local Area Connection* est bien sélectionnée dans Omnipeek. Effectuez un ping au besoin pour vérifier que votre analyseur de protocole saisit bien des trames. Notez que l'on peut réinitialiser l'analyseur à partir du menu, "*Edit/Clear all packets"* sans sauver la capture précédente.

Pour appliquer un filtre : Choisissez l'icône « entonnoir » en haut à gauche, puis *insert filter* et le type de protocole à filtrer (ex. DHCP). Au bout de la ligne, choisissez le triangle vert *(apply filter)*. Choisissez *Hide unselected packets* afin de ne conserver que les trames qui ont été sélectionnées.

Qualités évaluées :

3.5 Analyser les résultats expérimentaux

Critère d'évaluation : Qualité et exhaustivité de l'analyse des résultats obtenus à l'aide de l'outil Omnipeek. L'étudiant devra rechercher, identifier et trier l'information pertinente obtenue par l'outil. À la lumière de ses résultats, il devra formuler des conclusions.

5.2 Appliquer un outil d'ingénierie

Critère d'évaluation : Utilisation adéquate de l'outil Omnipeek afin de récupérer les données et produire des résultats.

8. Partie DHCP (Dynamic Host Configuration Protocol) (9.5 points)

Dans votre image virtuelle **Windows7_A**, votre adresse IP est obtenue de façon dynamique (*DHCP*). Démarrez votre analyseur de protocole (*new capture*, ne pas commencer la capture des paquets). Relâchez votre adresse avec *ipconfig /release*. Vérifiez que votre adresse est bel et bien relâchée en exécutant la commande *ipconfig* tant que vous n'avez pas obtenu une nouvelle adresse qui débute par 169.254. L'affichage de l'adresse 169.254 peut prendre quelques secondes, soyez patient. Une fois l'adresse IP relâchée, démarrer la capture dans le client Omnipeek. Effectuez ensuite la commande *ipconfig /renew*. Après avoir réobtenu votre adresse *IP* débutant par 192.168…. ; arrêtez l'analyseur de protocole en appuyant sur le bouton *stop capture* en haut à droite de l'écran.

8.1 Présentez une capture d'écran des paquets DHCP que vous avez capturés à l'aide de l'outil Omnipeek. À la lumière vos observations, **expliquez en détail** le mécanisme d'attribution d'une nouvelle adresse IP à un client qui veut se joindre à un réseau. **(2 pts)**

8.2 Donnez la séquence d'encapsulation des protocoles utilisés pour le paquet DHCP DISCOVER. Présentez une capture d'écran du contenu du paquet DHCP DISCOVER. **(0.25 pt)**

8.3 En se basant sur vos observations en 8.1, quelles opérations DHCP se sont effectuées en broadcast? Selon vous, pourquoi certaines de ces opérations doivent absolument être faites en broadcast? **(1.5 pts)**

8.4 Serait-il possible d'utiliser le protocole TCP de la couche 4 pour toutes requêtes DHCP? Si oui, dites comment, sinon pourquoi est-il impossible d'utiliser TCP pour les requêtes DHCP? **(1.5 pts)**

Ouvrir la trame *DHCP OFFER* pour les questions qui suivent.

8.5 Quel est le rôle de la trame DHCP offer ? **(1 pt)**

8.6 Quel champ, dans le paquet, indique que ce message est un *DHCP offer* ? Spécifiez le champ et sa valeur. **(0.25 pt)**

8.7 À quel poste correspond l'adresse MAC dans le champ Destination de l'entête Ethernet? Et celui du champ Source? **(0.5 pt)**

8.8 À quelle machine appartient l'adresse IP source? **(0.25 pt)**

8.9 Quelle est la taille de l'entête Ethernet que vous observez? **(0.25 pt)**

8.10 Quelle est la valeur du champ Protocole Type et que signifie-t-elle ? **(0.25 pt)**

8.11 Dans l'entête DHCP, quelle est la signification du champ ***IP Address Lease Time*** ? **(0.25 pt)**

8.12 Que désigne le champ ***Client IP Addr Given By Srvr***? Quelle est l'utilité de ce champ? **(0.25 pt)**

8.13 Quelle est l'entête suivante de la trame (niveau 3 du modèle *OSI*) ? **(0.25 pt)**

8.14 Quelle est la taille de l'entête de niveau 3 du modèle OSI que vous observez? **(0.25 pt)**

8.15 Nommez le protocole de niveau supérieur (niveau 4 du modèle *OSI*) utilisé par DHCP. **(0.25 pt)**

8.16 Quelle est la taille de l'entête de niveau 4 du modèle OSI que vous observez? **(0.25 pt)**

8.17 Dans combien de temps la machine Windows 7 doit-elle revalider avec le serveur DHCP son adresse IP? **(0.25 pt)**

9. Partie ARP (Address Résolution Protocol) (4 points)

9.1 Quelle est l'utilité de la cache ARP? **(1 pts)**

9.2 Dans votre client ***Windows7_A***, et dans une fenêtre de commande (*DOS*), exécutez la commande *arp –a* qui permet d'afficher le contenu de votre cache *ARP* ? Si l'adresse de ***Windows7_B*** y apparaît, enlevez-la avec la commande *arp –d 192.168.xx.xxx*. Vérifiez qu'elle n'y est plus. **(0.25 pts)**

Démarrez l'analyseur de protocole.

9.3 Lancez une commande qui permet de vérifier votre connectivité avec ***Windows7_B***. Arrêtez l'analyseur de protocole et sauvegardez la capture réalisée. Lancez à nouveau la commande arp -a. Que remarquez-vous ? **(0.25 pt)**

9.4 Dans l'analyseur de protocole, cliquez avec le bouton droit de votre souris sur un paquet dont le champ 'protocole type' indique *ARP request* ou *ARP Response*. Sélectionnez ensuite l'option '*Make Filter'*. Dans la boîte de dialogue qui apparaît, cliquez sur le bouton **Protocol** et choisissez l'option **ARP.** Cliquez ensuite sur le bouton ***Both Direction*** et choisissez l'option *both directions.* Dans le champ address 1, vérifiez que l'adresse est la MAC de votre client (***Windows7_A***). Si ce n'est pas le cas, remplacez la valeur du champ par la MAC de votre client. Dans le champ ***address 2*** cochez l'option *Any Address***.** Dans le champ **Filter** inscrivez *filtre_ARP*. Cliquez sur le bouton **OK** pour valider les opérations effectuées. En suivant les étapes indiquées juste avant la question 8.1, appliquez le fitre *filtre ARP* à votre nouvelle capture.

Dans l'analyseur de protocole, quelle est la longueur (*size*) des trames *ARP* ? **(0.25 pt)**

9.5 Quelle est la valeur numérique du champ Protocol type de l'en-tête Ethernet (Ethertype) d'une trame ARP ? Que signifie-t-elle ? **(0.5 pt)**

9.6 En se basant sur le contenu d'un paquet ARP Request et ARP Response, qu'est-ce qui différencie une requête ARP d'une réponse ARP dans le protocole ARP ? **(0.25 pt)**

9.7 À quel nœud réseau correspond l'adresse MAC de la source de la réponse ARP? **(0.25 pt)**

9.8 À quel nœud réseau correspond l'adresse MAC de la destination de la réponse ARP? **(0.25 pt)**

9.9 Quelle est la séquence d'encapsulation d'une requête ARP ? **(0.25 pt)**

9.10 Quel champ de la réponse ARP possède l'information recherchée par la requête ARP lancée par un client d'un réseau? **(0.25 pt)**

9.11 Qu'est-ce qu'il y a de particulier à la fin des données d'une trame ARP juste avant le champ FCS (CRC de 32 bits) ? Quel pourcentage de la taille de la trame ce champ occupe-t-il? Pourquoi ce champ est-il nécessaire dans les requêtes ARP? **(0.5 pt)**

10. Partie PING (2 points)

Toujours dans l'analyseur de protocoles avec les mêmes données de capture pour la partie *ARP*, appliquer le filtre ICMP aux paquets de la capture sauvegardée afin de conserver uniquement les paquets de type PING.

10.1 Quel est le champ ICMP qui différencie les requêtes par rapport aux réponses PING et quelles sont les valeurs impliquées ? **(0.5 pt)**

10.2 Quelle est la version du protocole IP utilisée ? **(0.5 pt)**

10.3 Quelle est la valeur du champ TTL (Time To Live). À quoi sert ce champ ? **(0.5 pt)**

10.4 Quelle est la séquence d'encapsulation d'une trame *PING* ? **(0.5 pt)**

11. Partie théorique (4 points)

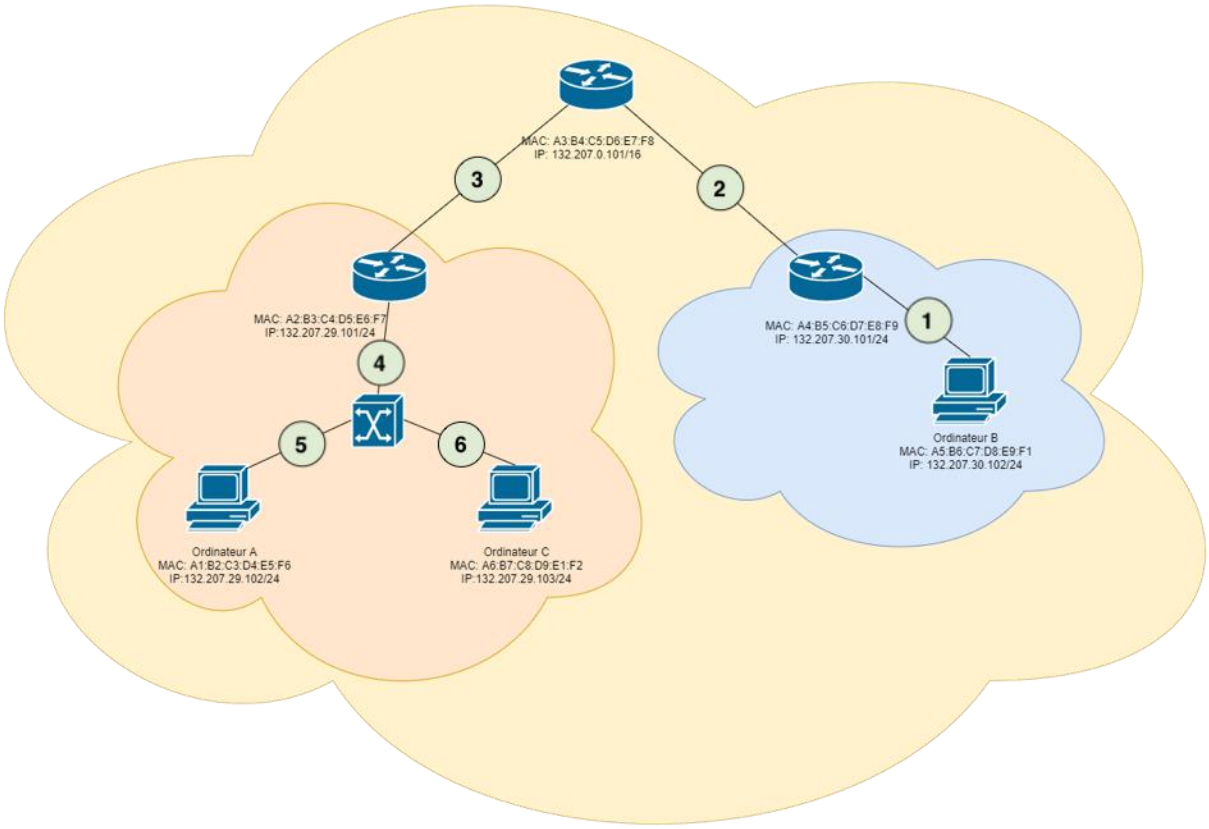

Fig.1 : Schéma d'une configuration réseau quelconque

11.1. Un ingénieur travaillant sur l'ordinateur « A » décide d'envoyer une requête PING vers l'ordinateur « C » afin de vérifier si l'ordinateur « C » est accessible sur le réseau. Sachant que le réseau en entier est câblé, donner l'état de l'entête Ethernet et IP du paquet contenant la requête PING à chaque lien (4, 5 et 6). Utiliser le format de paquet ci-dessous. **(2 pts)**

MAC Destination	MAC Source
IP source	IP destination

11.2. Ce même ingénieur, toujours depuis l'ordinateur « A » décide d'envoyer une requête PING vers l'ordinateur « B » pour vérifier si lui aussi est accessible sur le réseau. Donner l'état de l'entête Ethernet et IP du paquet contenant la requête PING à chaque lien (5, 4, 3, 2 et 1). Utiliser le même format de paquet qu'en 2.1 **(2 pts)**