ÉCOLE POLYTECHNIQUE MONTRÉAL

École Polytechnique de Montréal

Département Génie Informatique et Génie Logiciel

INF3405 – Réseaux Informatiques

Séance de laboratoire N° 2

Analyseur de protocoles

1. Informations générales

Session	Été 2017
Public cible	Étudiants de 1er cycle en génie
Taille de l'équipe	2 étudiants
Date et lieu de réalisation	16 mai 2017 au Laboratoire L-4708
Remise	16 mai 2017 à 23h55
Pondération	5 %
Directives particulières	1. 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. 2. **Justification par copie d'écran de chaque réponse. Toute réponse non justifiée sera pénalisée**. **Une capture d'écran globale du paquet peut suffire quand les questions portent sur un paquet en particulier**. 3. Soumission du rapport (en format PDF ou Word) par ***moodle*** uniquement (http://moodle.polymtl.ca). 4. Tout retard de soumission du rapport du laboratoire sera pénalisé de **3** points par heure de retard. 5. Avant de débuter votre séance de laboratoire, **notez et inscrivez sur le rapport le nom inscrit sur votre station de travail**
Chargé de laboratoire	Fabien BERQUEZ (fabien.berquez@polymtl.ca)
Version originale : Révision :	Francis Gagnon Fabien BERQUEZ, Saida MAAROUFI, Éric FAFOLAHAN, Aurel Josias RANDOLPH.

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 disfonctionnements est inhérente 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 disfonctionnements 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 destiné 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.

6. Éléments de théorie

Voir notes de cours.

7. Préparation de l'environnement de travail client 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, conserver le nom *Clone of Windows 7* et pour la **location** choisir **c:\temp 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 *Clone of Windows 7* que vous venez de créer et cliquer sur l'option *settings* dans le menu qui apparait 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 ***VMnet0***. Cliquez sur le bouton *OK* pour sauvegarder les modifications.

B) Démarrage de l'image virtuelle.

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

- Démarrez l'image virtuelle avec l'onglet *clone of Windows 7* 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** ». S'il vous est demandé de redémarrer ou non l'image virtuelle, choisissez de redémarrez aussitôt.

C) Vérifiez que le client *clone of Windows 7* possède une adresse en 192.168.44.x. Si ce n'est pas le cas, lire le paragraphe suivant.

Il est possible que vous n'ayez pas ce type d'adresse. Généralement, c'est parce que vous avez reçu une adresse en 10.x.x.x par VMWare. Dans ce cas tentez la séquence ipconfig /release et ipconfig /renew jusqu'à obtenir l'adresse en 192.168.44.x.

Pour la partie 9, faites bien attention à sélectionner les trames DHCP correspondant à l'adresse en 192.168.44.x que vous avez obtenue.

Récapitulatif de la configuration de la machine virtuelle et du réseau

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.

- *Clone of Windows 7*
    - **Network Adapter** : VMnet0
    - **Configuration IP** : Automatique
    - **Firewall Home or work** : Off
    - **Firewall Public Network** : Off

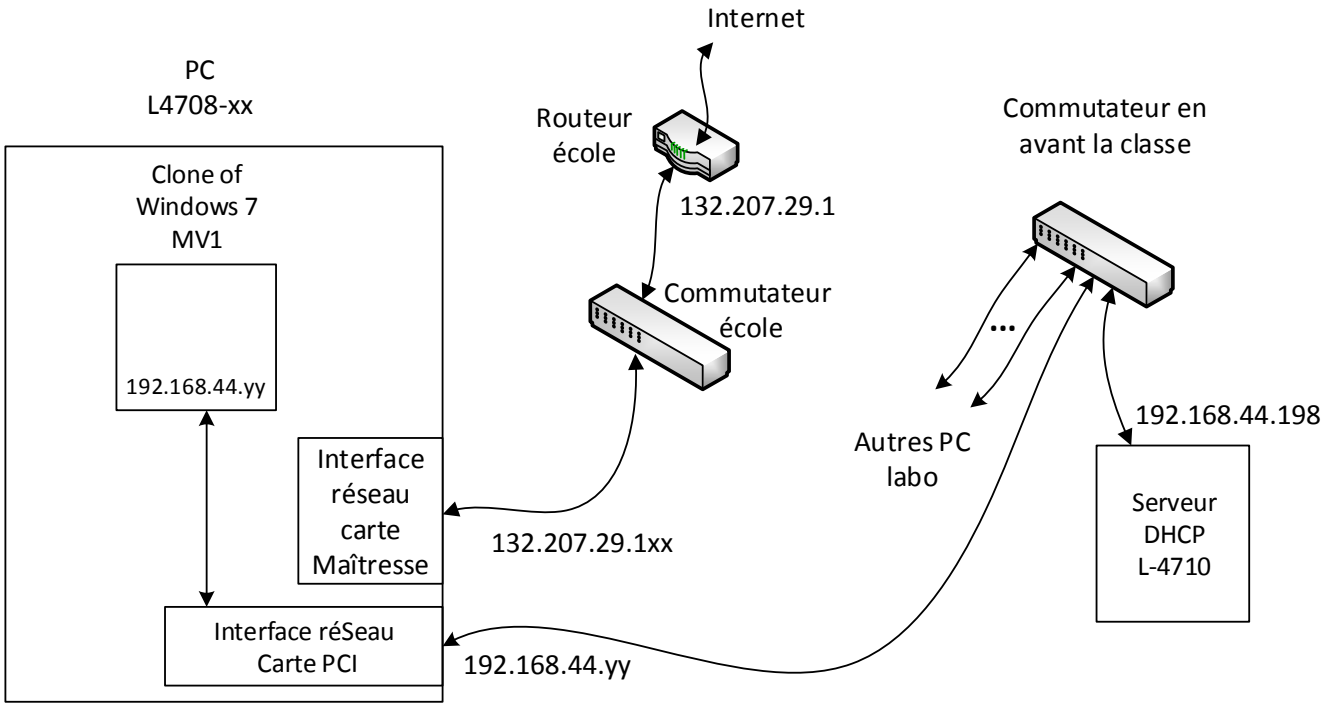

Figure 1 : Schéma récapitulatif de la configuration réseau.

8 Paramètre TCP/IP du client virtuel (0,5 pt)

8.1. Exécutez la commande *ipconfig /all* dans une fenêtre de commande (*Command Prompt*) : Menu Démarrer (*start*), cmd pour le client et start, run cmd pour le serveur. Inscrivez le nom de votre poste, l'adresse IPv4, le masque de sous-réseau, l'adresse *MAC*, la passerelle par défaut pour votre machine virtuelle. **(0,5 pt)**

Démarrez l'analyseur de protocoles sur votre client *clone of Windows 7*. Pour le démarrer, 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 saisi bien des trames.

Notez que l'on peut réinitialiser l'analyseur à partir du menu, "*Edit/Clear all packets"* sans sauver la capture précédente.

9 Partie *DHCP* (*Dynamic Host Configuration Protocol*) (8 pts)

Dans votre image virtuelle Windows 7, votre adresse IP est obtenue de façon dynamique (*DHCP*). Démarrez votre analyseur de protocole (*new capture* puis *start capture*). 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. 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. Répondez aux questions suivantes.
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.

Au besoin, vous pouvez appliquer un filtre *DHCP* sur vos données pour ne voir que les trames DHCP. Choisissez l'icône « entonnoir » en haut à gauche, puis *insert filter* et *DHCP*. Au bout de la ligne, choisissez le triangle vert *(apply filter)*. Choisissez *Hide unselected packets* afin de ne conserver que les trames DHCP qui ont été sélectionnées.

9.1. Nommez, dans leur ordre chronologique, les divers types de trames *DHCP* que vous avez dans votre analyseur de protocoles. **(1 pt)**

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

9.2. Quel est le rôle de la trame DHCP offer ? **(0,5 pt)**

Dans les questions 9.3 à 9.6, on s'intéresse à l'entête ***Ethernet.***

9.3. Nommez les champs de l'en-tête Ethernet (*Ethernet header*) **(0,5 pt)**

9.4. Quelle est la valeur du champ Source et que signifie-t-elle ? A quel poste correspond-elle ? **(0,5 pt)**

9.5. Quelle est la valeur du champ Destination et que signifie-t-elle ? A quel poste correspond-elle ? **(0,5 pt)**

9.6. Quelle est la valeur du champ Type de Protocole et que signifie-t-elle ? **(0,5 pt)**

9.7. Quelle est l'en-tête suivant de la trame (niveau 3 du modèle *OSI*) ? **(0,5 pt)**

9.8. Quelle est l'adresse *IP* source et quelle machine désigne-t-elle ? **(0,5 pt)**

9.9. Spécifiez la valeur et spécification du champ *Protocol* de cet en-tête de niveau 3. **(0,5 pt)**

9.10. Nommez le protocole de niveau supérieur (niveau 4 du modèle *OSI*) utilisé par DHCP. **(0,5 pt)**

9.11. Quel champ indique que ce message est un *DHCP offer* ? Spécifiez le champ et sa valeur. **(0,5 pt)**

9.12. Que désigne le champ ***Client IP Addr Given By Srvr*** ? Indiquez la valeur de ce champ. **(1 pt)**

9.13. Quelle est la signification du champ ***IP Address Lease Time*** ? Donnez sa valeur numérique. **(1 pt)**

9.14. Quel mécanisme introduit dans IPv6 change la nature et l'utilité du protocole DHCPv6 par rapport à DHCPv4 ? **(*Bonus* - 0,5 pt)**

10 Partie *ARP* (Address Résolution Protocol) (8 pts)

10.1. Dans votre client *clone of Windows 7*, et dans une fenêtre de commande (*DOS*), exécutez la commande *arp –a* qui permet d'afficher le contenu de votre cache *ARP*. Présentez le résultat et expliquez la ligne correspondant à l'IP 192.168.44.198. **(0,5 pt)**

Avant de passer à la suite, enlevez cette adresse avec la commande `arp –d 192.168.44.198`. Vérifiez qu'elle n'y est plus.

Démarrez l'analyseur de protocole.

10.2. Lancez la commande `ping 192.168.44.198`. Arrêtez l'analyseur de protocole et sauvegardez la capture réalisée. Lancez à nouveau la commande qui permet d'afficher le contenu de votre cache *ARP*. Que remarquez-vous ? **(0,5 pt)**

10.3. Dans l'analyseur de protocole, cliquez droit sur un paquet dont le champ 'protocole type' indique *ARP request* ou *ARP Response*. Sélectionnez ensuite l'option '*Make Filter'*. Dans la boite de dialogue qui apparait, 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 (*Clone of Windows 7*). 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 9.1, appliquez le fitre *filtre_ARP* à votre nouvelle capture.

Dans l'analyseur de protocole, quelle est la longueur (*size*) des trames *ARP* ? Pourquoi cette taille est-elle particulière ? **(1 pt)**

10.4. 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)**

10.5. Qu'est-ce qui différentie une requête *ARP* d'une réponse *ARP* dans le protocole *ARP* ? **(0,5 pt)**

10.6. Quelle est l'adresse MAC destination de la requête *ARP* ? Que signifie cette adresse ? **(0,5 pt)**

10.7. Quelle est la séquence d'encapsulation d'une requête *ARP* ? **(1 pt)**

10.8. Qu'y-a-t-il de particulier à la fin des données d'une trame *ARP* juste avant le champ *FCS* (*CRC* de 32 bits) ? Quantifiez en pourcentage de la taille de la trame. A quoi ceci sert-il ? **(0,5 pt)**

10.9. Quelle est l'adresse *MAC* de la destination de la réponse *ARP* ? À quel nœud réseau correspond cette adresse ? **(1 pt)**

10.10. Quelle est l'adresse *MAC* de la source de la réponse *ARP* ? À quel nœud réseau correspond cette adresse ? **(1 pt)**

10.11. Quel champ de la réponse *ARP* possède l'information recherchée par la requête *ARP* ? Expliquez pourquoi. **(1 pt)**

11 Partie PING (3 pts)

Avec votre capture précédente, cliquez dans le menu sur *Edit* puis sur *Unhide all packets* (Vous pouvez aussi utiliser le raccourci Ctrl + U). Tous les paquets apparaîtront à nouveau.

11.1. Toujours dans l'analyseur de protocoles avec les mêmes données de capture pour la partie *ARP*, quelle est la séquence d'encapsulation d'une trame *PING* ? **(1 pt)**

NB : Vous pouvez appliquer le filtre ICMP aux paquets de la capture sauvegardée afin de conserver uniquement les paquets de type PING.

11.2. Quelle est la version du protocole *IP* utilisée ? **(0,5 pt)**

11.3. Dans l'en-tête Ethernet, quelle est la valeur du champ *Protocol type* et sa signification ? **(0,5 pt)**

11.4. Quelle est la valeur du champ TTL (Time To Live). A quoi sert ce champ ? **(0,5 pt)**

11.5. Quel est le champ *ICMP* qui différencie les requêtes par rapport aux réponses PING et quelles sont les valeurs impliquées ? **(0,5 pt)**

12 Partie RFC (0,5 pt)

Le site www.rfc-editor.org vous permet de consulter les RFC qui ont été proposées depuis 1969. En utilisant l'outil de recherche du site, trouvez la RFC 826, et ouvrez la en format *Plain Text*. Nous allons nous intéresser à la section ***Motivations***

12.1. Quelles étaient les 2 alternatives envisagées par le RFC 826 à l'époque, en novembre 1982 pour résoudre le problème de résolution d'adresse MAC et IP ? **(0,5 pt)**