École de technologie supérieure
Département de génie logiciel et des TI

Responsable du cours : Mohamed Faten Zhani
Chargé de cours : Rami Langar
Chargé de laboratoire : Firmin Mah
Session : E2024

LOG100 - Programmation et Réseautique en génie logiciel

Laboratoire 2 : Modèle en couches et encapsulation des données

Durée = 1 séance de 3 heures

Objectifs

Ce laboratoire vous permettra de comprendre l'encapsulation des données à travers les différentes couches et d'observer le format des entêtes ajoutés par les différents protocoles. Il est à noter que l'objectif n'est pas de comprendre le fonctionnement des applications mais seulement d'analyser les trames et les entêtes ajoutés par chacun des protocoles.

Montage & Outils

- Système d'exploitation : *Windows*
- Autres outils et logiciels : *Wireshark, nslookup, ping, tracert*

Notes

- Ce travail doit se faire individuellement.
- Utilisez le fichier Labo2_gabarit_rapport.docx pour compléter votre rapport de laboratoire.
- Renommez ce fichier Labo2_rapport_nom_prenom.docx (nom_prenom sont vos nom et prénom), enregistrez-le au format PDF et déposez-le dans Moodle.
- Le symbole ☛ indique la manipulation à faire pour répondre aux questions.

Introduction à Wireshark

Wireshark est un logiciel open-source qui permet de capturer les paquets sur une ou plusieurs interfaces réseaux et d'afficher des informations détaillées sur leurs contenus tels que les protocoles utilisés, les en-têtes et les données. Veuillez lire le document « Labo2-IntroductionWireshark.pdf » et consulter les 2 liens en référence pour avoir plus d'infos sur l'utilisation de Wireshark.

Commande *nslookup*

La commande *nslookup* est une commande DOS qui permet d'interroger un serveur DNS à propos d'un nom de domaine pour connaître des informations telles que son adresse IP et ses alias.

- ☛ Ouvrez une invite de commandes DOS.
- ☛ Lancez une capture *Wireshark*.
- ☛ Exécutez la commande « *nslookup montreal.ca »* dans l'invite de commandes. Une fois que vous avez la réponse, arrêtez la capture *Wireshark*.
- ☛ Utilisez le filtre d'affichage dans *Wireshark* pour ne montrer que les paquets DNS.
- ☛ Sélectionnez une trame de requête DNS et observez la pile de protocoles utilisée pour encapsuler cette trame.

1. Donnez dans le tableau fourni *(15 pts)*

    a. Dans la colonne « Nom de couche du modèle Internet » les noms de toutes les couches de la pile de protocoles du modèle Internet (toutes les couches selon les notes de cours).

    b. Dans la colonne « Nom du protocole qui encapsule la requête DNS », **s'il y a lieu**, le protocole qui a été utilisé pour encapsuler la requête DNS.

Pour les questions 2 à 4 utilisez la capture Wireshark « nslookup_amazon_ca.pcapng » fournie.

- ☛ Ouvrez le fichier « nslookup_amazon_ca.pcapng » dans Wireshark.
- ☛ Utilisez le filtre d'affichage dans Wireshark pour ne montrer que les paquets DNS.
- ☛ Sélectionnez la trame de la première requête DNS et observez la pile de protocoles.

2. Pour cette 1ière trame de requête, affichez l'entête ajouté par la couche transport. Donnez dans le tableau fourni les différents champs de cet entête, la taille en octets de chacun de ces champs et la valeur hexadécimale de chacun de ces champs. *(12 pts)*

- ☛ Pour cette 1ière trame de requête, affichez l'entête ajouté par la couche réseau.

3. Quelle est la taille de cet entête réseau ? *(1 pt)*
4. Donnez dans le tableau fourni les différents champs de cet entête et la taille **en bits** de chacun de ces champs. *(24 pts)*

Commande *Ping*

La commande *ping* permet de tester la connectivité entre deux équipements en utilisant des messages de requêtes/réponses de type Echo. La commande est lancée dans la fenêtre de commande Windows. Le protocole utilisé pour envoyer ces messages est le protocole ICMP (considéré comme protocole de la couche réseau).

- ☛ Lancez une capture *Wireshark*.
- ☛ Dans une fenêtre de commande DOS, lancez la commande « ping canada.ca » puis arrêtez la capture quand vous avez la réponse. Utilisez un filtre pour n'afficher que les paquets ICMP.

5. Combien de messages de requête Echo ont été envoyés ? *(1 pt)*

Pour les questions 6 à 13 utilisez la capture Wireshark « ping_quebec_ca.pcapng » fournie.

- ☛ Ouvrez le fichier « ping_ quebec _ca.pcapng » dans Wireshark.
- ☛ Utilisez le filtre d'affichage dans Wireshark pour ne montrer que les paquets ICMP.
- ☛ Sélectionnez dans Wireshark la première trame contenant la requête Echo.

6. Quelle est la taille de cette trame (en octets) ? *(1 pt)*
7. Donnez dans le tableau fourni les noms des couches de la pile de protocoles de l'Internet (toutes les couches selon les notes de cours). Pour chaque couche donnez, **s'il y a lieu**, le protocole utilisé pour encapsuler la requête Echo. *(15 pts)*

- ☛ Accédez à l'entête de la couche liaison de données de la première requête Echo.

8. Quelle est la taille de cet entête ? *(1 pt)*
9. Donnez dans le tableau fourni les noms des différents champs de l'entête de la couche liaison de données pour la première requête Echo ainsi que les tailles de ces champs. *(6 pts)*
10. Quelle est la valeur hexadécimale du champ « type » dans cet entête ? *(1 pt)*

- ☛ Accédez à l'entête de la couche réseau de la première requête Echo.

11. Donnez les informations ci-dessous pour l'entête de couche réseau. *(3 pts)*
    - Taille de l'entête de la couche réseau
    - Adresse IP de destination
    - Nom de la machine qui a l'adresse IP destination

☛ Accédez au message ICMP.

12. Donnez les informations ci-dessous pour ce message ICMP. *(8 pts)*

- Taille du message ICMP
- Valeur du champ « Type » de cette requête
- Valeur du champ « Code » de cette requête
- Valeur de l'identificateur dans ce message (notation BE)
- Valeur de l'identificateur dans ce message (notation LE)
- Numéro de séquence de cette requête (notation BE)
- Numéro de séquence de cette requête (notation LE)
- Taille du champ de données (data)

☛ Sélectionnez la réponse à la première requête Echo et accédez au message ICMP.

13. Quelles sont les valeurs des deux champs « Type » et « Code » dans ce message ? *(2 pts)*

Commande *Tracert*

La commande *tracert* permet de déterminer le chemin suivi par les paquets pour se rendre vers une machine de destination en dressant la liste des routeurs traversés. *tracert* envoie une série de messages ICMP avec des valeurs de TTL (*Time To Live*) incrémentées de 1 à chaque fois. Le TTL est initialement à 1. Sachant qu'à chaque passage par un routeur, le TTL est décrémenté de 1 et si sa valeur devient nulle, le routeur envoie un message d'erreur de type « Temps de vie (TTL) dépassé » à la source. Cette dernière inscrit ce routeur sur la liste avant d'incrémenter le TTL et d'envoyer une autre requête ICMP et ce jusqu'à arriver à la destination. Vous pouvez voir les significations des valeurs des champs « Type » et « Code » à https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

Analyse de la capture *Wireshark* obtenue avec la commande *tracert* vers le site revenuquebec.ca. Pour les questions 14 à 19 utilisez la capture Wireshark « tracert_revenuquebec_ca.pcapng» fournie.

☛ Ouvrez la capture Wireshark « tracert_revenuquebec_ca.pcapng».

14. Répondez aux questions ci-dessous : *(2 pts)*

- Combien de routeurs ont été traversés avant d'arriver sur revenuquebec.ca ? Note : le dernier nœud étant la destination, il ne fait pas partie des routeurs traversés.
- Quelle est la valeur du TTL de la dernière requête ping (quand revenuquebec.ca a été atteint) ?

  (Attention à la valeur du TTL dans ces trames car 3 requêtes sont envoyées pour chaque valeur du TTL.

☛ Sélectionnez la trame de la première requête ICMP et accédez au message ICMP.

15. Quelles sont les valeurs des deux champs « Type » et « Code » dans ce message ? *(2 pts)*

16. Y'a-t-il une différence de format entre un message de requête ICMP obtenu grâce à la commande *tracert* et un message de requête ICMP obtenu grâce à la commande ping ? si oui, laquelle ? *(2 pts)*

☛ Sélectionnez la trame de réponse à la première requête ICMP et accédez au message ICMP.

17. Quelles sont les valeurs des deux champs « Type » et « Code » dans ce message ? *(2 pts)*

18. Quelle est la signification de la réponse pour les valeurs de « Type » et « Code » de la question 17 ? *(2 pt)*