



Réseaux pour ingénieurs GLO-2000

TP1 : Analyse de paquets

Professeur responsable:

Ronald Beaubrun

Ronald.Beaubrun@ift.ulaval.ca

Responsables des travaux pratiques:

Louis Fortier-Dubois et Jean-Alexandre Beaumont

glo2000a17@gmail.com

Ce premier travail pratique a pour but de vous familiariser avec les outils permettant de surveiller un réseau informatique et de comprendre des aspects pratiques en lien avec les **couches liaison et réseau**. Pour l'ensemble des questions du TP1, vous devez utiliser le logiciel *Wireshark*.

Modalités de remise

- À faire en équipe de 2 ou 3.
- Le travail doit contenir vos noms et vos numéros d'étudiant.
- Le type de fichier remis doit être un PDF (une pénalité de 10% sera attribuée dans le cas contraire).
- Nom du fichier à remettre: TP1-numero_d_etudiant_d_un_des_membres.pdf
- Remettre sur le portail des cours.
- Date limite : 27 septembre 2017
- Tout travail remis en retard se verra attribuer la note 0.

1 Trame Ethernet II (2 points)

Voici une entête de trame Ethernet II en hexadécimal :

90 06 28 5E 4C 01 64 5A 04 BA F2 31 08 00

Donnez l'adresse **MAC source**, l'adresse **MAC de destination** et le nom du **protocole de couche supérieure** encapsulé dans cette trame.

2 Adresses MAC et IP (2 points)

Expliquez en vos mots l'utilité d'avoir une adresse IP alors que chaque appareil a déjà une adresse MAC unique.

3 Address Resolution Protocol (2 points)

La trace TP1-Q3.cap contient une requête et une réponse ARP.

1. L'adresse de destination du premier paquet est FF:FF:FF:FF:FF:FF. Expliquez ce que signifie cette adresse et pourquoi elle est utilisée dans ce protocole.
2. Quelle information l'appareil à l'adresse MAC 64:5A:04:BA:F2:31 obtient-il suite à cet échange? Répondez en donnant les données reçues.
3. Pour plusieurs requêtes successives, l'appareil à l'adresse MAC 64:5A:04:BA:F2:31 doit-il exécuter ce protocole à chaque fois qu'il veut communiquer avec l'appareil ayant l'adresse IP 10.248.100.164? Expliquez en vos mots.

4 Time To Live (2 points)

1. Quel est le *Time To Live* (TTL) de chacun des 2 paquets contenus dans la trace TP1-Q4.cap? Inscrivez la valeur **décimale** et **hexadécimale** pour chaque TTL.
2. Il existe une valeur maximale pour un TTL. Sur combien de bits tient cette valeur?
3. Sachant que le deuxième paquet a été envoyé avec un TTL initial *maximal*, combien de routeurs a-t-il traversé avant d'atteindre l'adresse 10.0.9.128?

5 Ping d'un site web (2 points)

La trace TP1-Q5.cap contient le résultat d'un *ping* vers le site web *www.google.com*. Dans l'échange, il y a trois adresses IP différentes au total. Expliquez ce que représente chacune d'entre elles et leur rôle dans l'accomplissement du *ping*.

6 ICMP (2 points)

La trace TP1-Q6.pcap contient deux types de paquets ICMP. Pour les réponses reçues, identifiez le type et le code, puis donnez une cause possible expliquant la réception de ce paquet.