TD M2102 - Architecture des réseaux
Analyse de trace Ethernet – Principe d'encapsulation

Première Partie : analyse manuelle

1. Un premier exemple

Un analyseur de trame Ethernet a fourni la trace donnée en Annexe 1 (hors préambule, délimiteur, CRC, et caractères de bourrage) correspondant aux trames échangées lors de l'exécution de "`ping -c1 10.1.1.3`" sur le poste `m1.localdomain`.

1-Détaillez le contenu de chaque trame Ethernet : le type de contenu (trame ARP ou datagramme IP), adresse physique de l'émetteur et du destinataire. Sur chaque trame, notez la fin de l'entête Ethernet.
2-A quoi correspond l'adresse physique ff:ff:ff:ff:ff:ff ? Dans quel cas est-elle utilisée ?
3-Détaillez le contenu de chaque datagramme IP (type de contenu, adresse logique de l'émetteur et du destinataire). Sur chaque datagramme IP, notez la fin de l'entête IP.
4-A quoi sert la commande "`ping -c1 10.1.1.3`" ?
5-Faites un schéma représentant l'encapsulation d'une requête ARP dans une trame Ethernet.
6-Faites un schéma représentant l'encapsulation d'une requête ICMP dans une trame Ethernet.
7-Quelle est l'adresse IP de m1 ?
8-Quelle est l'adresse physique de m1 ?
9-Quelle est l'adresse physique associée à l'adresse IP 10.1.1.3 ?
10-En quoi une adresse MAC est différente d'une adresse IP ? Comment est-elle attribuée ? A quoi sert-elle ?
11-Faites un schéma représentant la pile protocolaire contenant les protocoles présents dans la trace étudiée.

2. Annexe 1

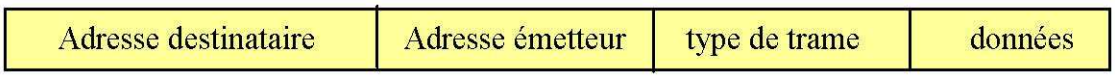
```
Trame 1:
ffff ffff ffff fefd 0000 0001 0806 0001
0800 0604 0001 fefd 0000 0001 0a01 0101
0000 0000 0000 0a01 0103

Trame 2:
fefd 0000 0001 fefd 0000 0003 0806 0001
0800 0604 0002 fefd 0000 0003 0a01 0103
fefd 0000 0001 0a01 0101

Trame 3:
fefd 0000 0003 fefd 0000 0001 0800 4500
0054 0000 4000 4001 24a4 0a01 0101 0a01
0103 0800 621b fd03 0001 a6b0 8949 75e2
0800 0809 0a0b 0c0d 0e0f 1011 1213 1415
1617 1819 1a1b 1c1d 1e1f 2021 2223 2425
2627 2829 2a2b 2c2d 2e2f 3031 3233 3435

Trame 4:
fefd 0000 0001 fefd 0000 0003 0800 4500
0054 a124 0000 4001 c37f 0a01 0103 0a01
0101 0000 6a1b fd03 0001 a6b0 8949 75e2
0800 0809 0a0b 0c0d 0e0f 1011 1213 1415
1617 1819 1a1b 1c1d 1e1f 2021 2223 2425
2627 2829 2a2b 2c2d 2e2f 3031 3233 3435
```

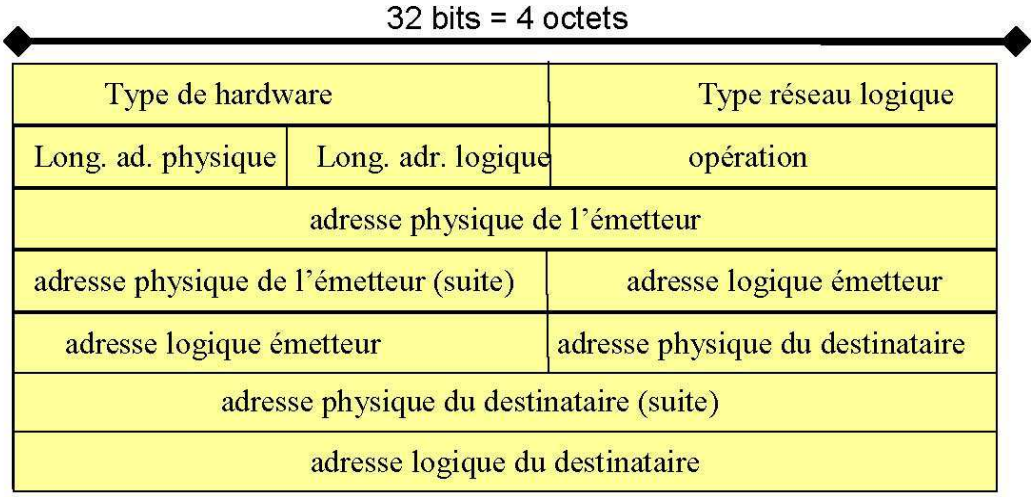
3. Format ETHERNET



Adresse sur 6 octets
Type de trame : 0x0800 = IP 0x0806 =ARP

4. **Message ARP**

ARP :



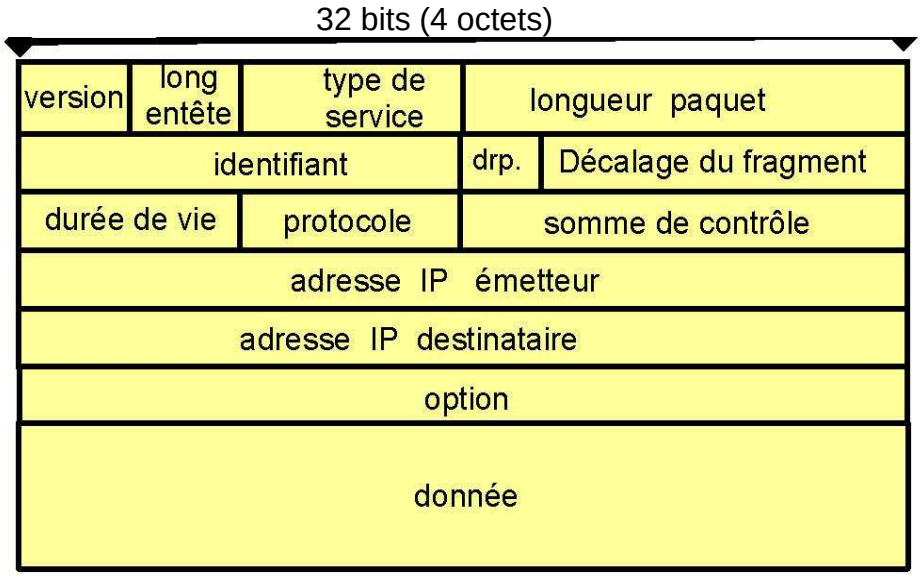
Type de hardware : 0x0001 Ethernet
Type de réseaux logique : 0x0800
Opération : 0x01 = requête, 0x02 = réponse

5. **Message ICMP**

ICMP :

(type,code) = (8,0) : requête écho (type,code) = (0,0) : réponse écho

6. **Format du datagramme IP**



Version sur 4bits.
Longueur de l'entête sur 4 bits. en mots de 4octets.
Longueur du paquet sur 2 octets en mots d'un octet.
Protocole : 0x01 = ICMP, 0x11 = UDP, 0x06 = TCP ?
Option : facultatif. Donnée correspond au protocole transporté.

Deuxième Partie : analyse informatique

Gestion du réseau virtuel

Ce TP tourne sur un réseau virtuel basé sur l'émulateur de machine virtuelle QEMU.

Michel Billaud, enseignant au département, a développé une sur-couche QS, installée dans /net/adm sur les machines du département, qui permet de configurer et manipuler de tels réseaux virtuels basés sur QEMU.

Au département, la machine virtuelle de base tourne sous une distribution allégée de debian.

Pendant la simulation :

- Vous êtes administrateur de la machine virtuelle : compte **root** et mot de passe **plop**
- La souris est parfois « capturée » par le simulateur quand vous cliquez dans une fenêtre, tapez Ctrl-Alt pour la libérer
- Vous disposez d'éditeurs de texte simples : nano ou jed (Ctrl-x s pour sauver, Ctrl-x c pour quitter)
- Redémarrez une machine par **reboot**
- Arrêtez proprement une machine par **halt**
-
- Le montage **/mnt** permet de copier des fichiers depuis/vers la racine de votre compte local
-
- Pour des manipulations avancées :
    - Démarrez l'interface graphique par **startx**
    - Par bouton droit, vous avez accès à diverses applications : interpréteur de commandes, navigateur, « sniffeur » (wireshark), etc…

Installation : exécutez le script

~/Bibliotheque/M2102 – Architecture des reseaux/installer-tp-ping.sh

(cela a pour effet de copier le fichier tp-ping.tgz dans votre répertoire ~/QS)

Simulation : exécutez la commande

qs-run tp-ping

(cela a pour effet de créer une session de travail dans le répertoire /tmp de la machine locale, et de lancer le réseau de machines virtuelles)

1. Découverte du réseau / Mise en place de l'analyseur de trames

Le réseau est un réseau local Ethernet comportant 3 machines :
- `zbox` a pour adresse IP 192.168.0.1 ; c'est elle qui sert de relais (passerelle) vers l'extérieur du réseau local,
- `alice` a pour adresse IP 192.168.0.2,
- `bob` a pour adresse IP 192.168.0.3.

Le nom de domaine de ce réseau est `mydomain`. Les noms complets des machines sont donc `zbox.mydomain`, `alice.mydomain` et `bob.mydomain`.

1-Consultez la configuration réseau de chacune des machines grâce à la commande **`ifconfig`**.
Vous pourrez vérifier leurs adresses IP énoncées ci-dessus, ainsi que leurs adresses physiques (MAC) Ethernet.

2-Dans la suite du TP, nous allons utiliser la commande ping depuis la machine `alice` et observer ce qui se passe avec un « sniffeur » = analyseur de trames, wireshark.
Démarrez le sniffeur **`sur alice`** comme suit :

- démarrez l'interface graphique par la commande **`startx`**
- lancez **`wireshark`** : bouton droit, applications / réseau / surveillance / wireshark
- démarrez la capture sur l'interface eth0
- enfin, ouvrez un interpréteur de commandes (**`XTerm`**) pour les futures commandes : bouton droit, etc…

2. Scénario ping vers l'adresse IP d'une machine locale

C'est exactement le scénario étudié dans la première partie de ce TP, l'analyse manuelle.

1-Sur la machine `alice`, faites un ping vers l'adresse IP de la machine `bob` :

ping -c1 192.168.0.3

2-Observez dans **`wireshark`** les trames échangées, les ARP puis les ICMP, comme dans la première partie du TP.

Remarque ARP :

Grâce à la commande arp, vous pouvez consulter / modifier la table cache ARP d'une machine :

- consultation : **arp –n**
- suppression d'une entrée : **arp –d <numero IP>**

3. Scénario ping vers le nom d'une machine locale

1-Avant de démarrer ce nouveau scénario ;

- nettoyez les tables cache ARP des machines (à l'aide de la commande arp)
- réinitialisez la capture dans wireshark (flèche restart)

2-Sur la machine `alice`, faites un ping vers la machine `bob` à l'aide de son nom complet :

ping -c1 bob.mydomain

3-Observez dans **`wireshark`** les trames échangées. Quelles sont les différences et les points communs avec le scénario précédent ?

4-Détaillez le contenu de chaque trame Ethernet, et de chaque datagramme IP et UDP, et leur encapsulation.

5- Faites un schéma récapitulatif des trames échangées entre les différentes machines.

6-Déduisez-en le rôle de la machine `zbox`.

7-Faites un schéma représentant la pile protocolaire contenant les protocoles présents.

4. Scénario ping vers une machine à l'extérieur du réseau

1-Avant de démarrer ce nouveau scénario ;

- nettoyez les tables cache ARP des machines (à l'aide de la commande arp)
- réinitialisez la capture dans wireshark (flèche restart)

2-Sur la machine `alice`, faites un ping vers une machine à l'extérieur du réseau :

ping -c1 www.google.fr

3-Observez dans **`wireshark`** les trames échangées. (c'est normal que le ping n'aboutisse pas complètement, déterminez ce qu'il manque)

4-Déduisez-en le**S** rôle**S** de la machine `zbox`.

5-Pour approfondir et voir ce qui se passe à la sortie du réseau, vous pouvez recommencer le scénario après avoir lancé un **`wireshark`** sur la machine `zbox` en capturant son interface eth1 (celle qui est connectée vers l'extérieur).

5. Bilan du TD :

1-Donnez la liste des trames échangées dans le cas où la commande **« ping –c1 toto.bidule.fr »** sera exécutée sur une machine du domaine `bidule.fr`.

2-Peut-on obtenir l'adresse MAC associée au nom `azure.columbia.edu` à partir d'un poste du département informatique de l'IUT de Bordeaux.

3-Dans quel cas a-t-on besoin de cette adresse MAC ?

4-Citez le protocole permettant d'obtenir une adresse physique à partir d'une adresse logique (acronyme et nom complet).