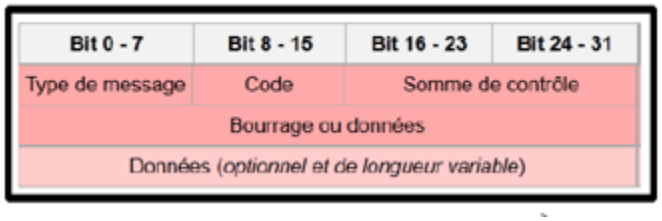
M2102-- TD 3

Le protocole ICMP

Le protocole ICMP (Internet Controle Message Protocol) est responsable pour la gestion d'erreurs qui peuvent parvenir dans un réseau. Ce protocole fait partie de la couche IP. Les erreurs gérées par ICMP ont de divers types et catégories, y compris des erreurs de correspondance (destinataire non-trouvé), erreurs pertinentes pour un message périmé, etc.

Dans un paquet IP le code utilisé pour le protocole ICMP est 0x01.

L'entête spécifique au protocole ICMP est le suivant :



Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
Type de message	Code	Somme de contrôle	
Bourrage ou données			
Données (*optionnel et de longueur variable*)			

Les configurations permanentes

Jusqu'au présent nous avons utilisé les commandes ifconfig et route pour mettre en place une configuration sur une machine. Cependant il faut savoir que mettre en place la configuration de cette façon est temporaire, on peut facilement le perdre. Une alternative pour faire une configuration à longue durée est d'utiliser le fichier etc/network/interfaces. Ce fichier nous permet une configuration à la fois des interfaces réseau (avec des adresses IP statiques ou dynamiques) et à la fois des passerelles à utiliser.

Un exemple d'un fichier etc/network/interfaces qui fait seulement la configuration d'une seule interface (eth0) avec une configuration statique serait :

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.56.11
netmask 255.255.255.0
gateway 192.168.56.1
```

Nous pouvons également utiliser une configuration dynamique, par DHCP. Nous allons voir cela en plus de détail dans un TD suivant. La syntaxe si on voulait par exemple ajouter un adressage par DHCP sur l'interface eth1 serait :

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.56.11
netmask 255.255.255.0
gateway 192.168.56.1

auto eth1
iface eth1 inet dhcp
```

Pour mettre en place les modifications indiquées par le fichier interfaces, on peut utiliser la commande `ifup` avec la syntaxe :

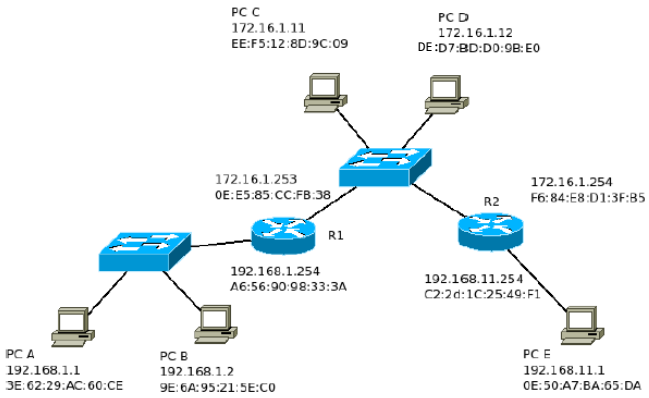
```
ifup eth0
```

On a également la possibilité de forcer un redémarrage du service en utilisant la commande :

```
/etc/init.d/networking restart
```

Exercice 1

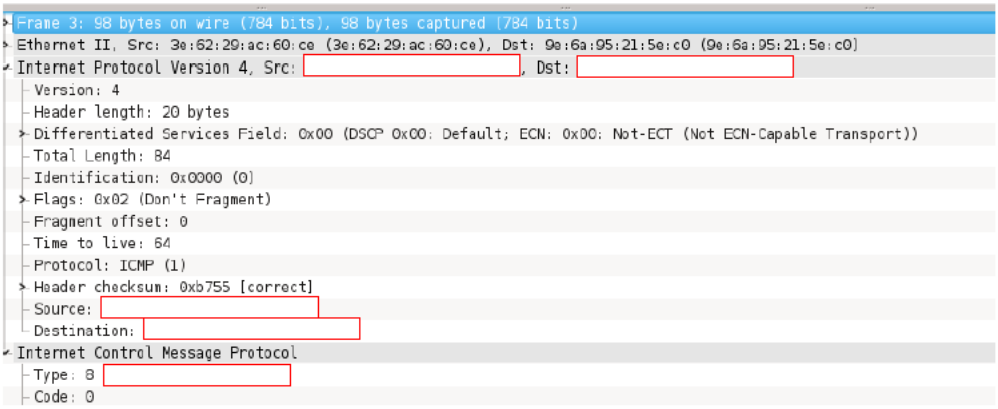
Cet exercice concerne le réseau dont la topologie est dans la figure ci-dessous :



1. Indiquez les machines qui servent comme des routeurs dans cette figure, en donnant :
    - Leurs adresses IP et MAC
    - Les réseaux qu'elles connectent

2. Indiquez les réseaux présentes dans la figure ci-dessus et indiquez quelles machines correspondent à chaque réseau.

3. Regardez le message suivant, représentant le détail d'un message capturé sur Wireshark.



Pour ce message :

- Trouvez les deux machines qui communiquent

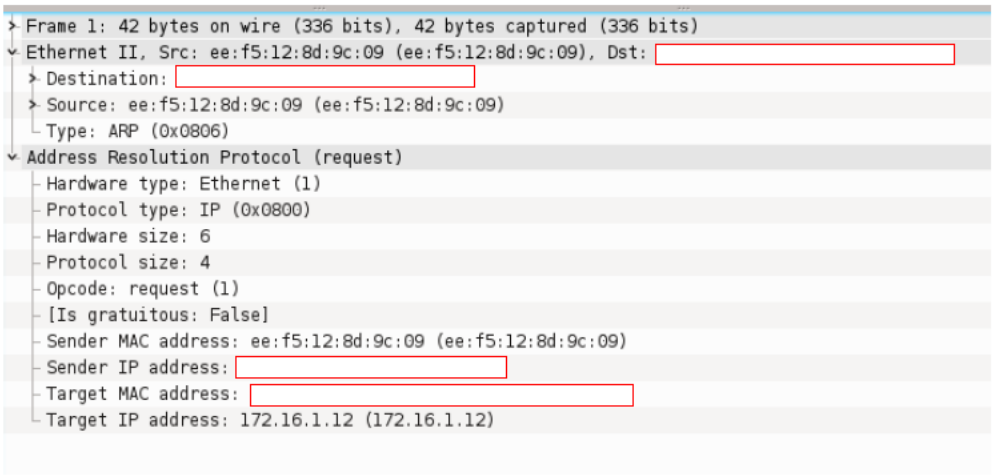
- Complétez les éléments manquants

- Quel est le protocole du niveau au plus haut utilisé par ce message (le protocole de la couche la plus haute) ?

- Donnez l'encapsulation complète de ce protocole

4. Quelle a été la commande qui a eu comme résultat le message de la figure précédente ?

5. Nous avons maintenant la trame suivante :



Pour le message donné dans la figure ci-dessus :

- Relevez le type exact de ce message (quel est son rôle, quel protocole(s) sont utilisés)

- Quelle est la structure de ce message ?

- Relevez les machines concernées

- Quelle serait une réponse probable à ce message ? (indiquez la source de la réponse, la destination, le type de message, ainsi que son contenu)

6. Le message de la question précédente est capturé lorsqu'on tape une certaine instruction sur la machine PC A. Quelle est la commande tapée ?

Exercice 2

On va utiliser la même topologie que celle dans l'exercice 1. Cette fois-ci on considère la transmission de messages entre les divers réseaux. On va supposer qu'on a déjà mis en place la configuration de chaque interface réseau sur chaque machine.

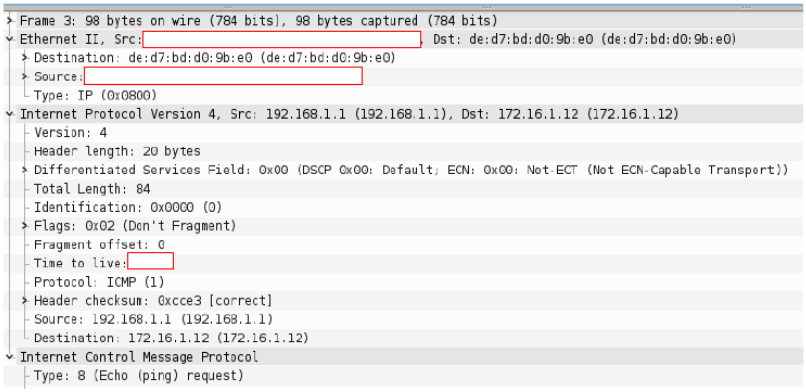
1. Quelles commandes faut-il taper (et sur quelles machines) pour s'assurer qu'un message passe de la machine PC A vers la machine PC D ?

2. Disons qu'on fait un ping maintenant de la machine PC A vers la machine PC D. Quel sera le résultat (en termes des messages échangés, des protocoles utilisés, etc.) ?

3. Indiquez quelles commandes il faut encore taper et sur quelles machines pour réussir le ping entre les deux machines.

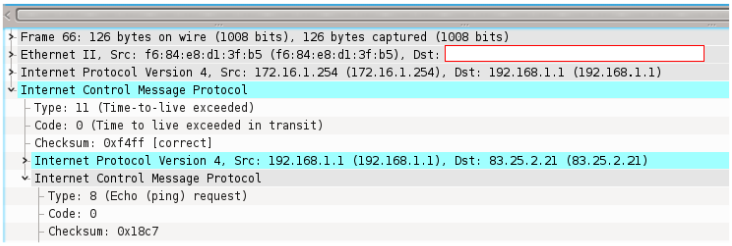
4. Disons que la machine PC A veut envoyer un message vers la machine PC D. Indiquez sa progression dans le réseau indiqué.

5. Regardez la capture suivante sur Wireshark.



En regardant les adresses IP et MAC indiquées dans cette figure, complétez les champs vides dans cette figure.

6. Analysez la capture ci-dessous.



Pour ce message :

- Relevez les adresses IP mises dans le protocole ICMP et spécifiez auxquelles machines elles correspondent.

- Relevez les adresses IP mises dans le protocole IP et spécifiez les machines concernées.

- Pourquoi ces adresses sont-elles différentes ?

- Complétez la trame ci-dessous

- Justifiez l'existence de ce message.

Exercice 3

Dans cet exercice nous allons examiner une trame Ethernet, et notamment les éléments d'un en-tête IP.

```
00 0c 29 97 68 42 f4 6d    04 1f 31 ad 08 00 45 00
00 54 0c fa 40 00 40 01    ab cf c0 a8 00 79 c0 a8
00 16 08 00 79 4a 0d 2e    00 01 00 ce 2b 55 00 00
00 00 7f 90 07 00 00 00    00 00 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d    1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d    2e 2f 30 31 32 33 34 35
36 37
```

1. Relevez les deux adresses MAC (destinataire et source)

2. En utilisant l'en-tête IP donné en CM, déchiffrez les éléments de l'en-tête IP donné ici.

3. Quel est le protocole utilisé au niveau au plus haut ? Quelle est son encapsulation ?

4. Quelle commande a dû créer ce message ?

Exercice 4

Ecrivez les configurations des machines PC A, R1 et PC D en utilisant le fichier interfaces, puis donnez pour chaque machine la ou les commandes à taper pour activer les modifications réalisées.

Exercice 5

Regardez la capture d'écran suivante :

```
Local Address         Foreign Address       state
tcp   0 0.0.:21             0.0.0.0:*             LISTEN
tcp   :::23                 :::*                  LISTEN
tcp   192.168.102.1:335     213.34.21.38:44458    TIME_WAIT
tcp   :::335                :::*                  LISTEN
tcp   192.168.102.1:21      192.168.102.18:23422  ESTABLISHED
tcp   192.168.102.1:23      182.45.47.25:24522    TIME_WAIT
tcp   192.168.102.1:23      192.168.102.34:27882  ESTABLISHED
tcp   127.0.0.1:21          127.0.0.1:12762       ESTABLISHED
tcp   127.0.0.1:12762       127.0.0.1:21          ESTABLISHED
tcp   192.168.102.1:3542    172.16.5.254:22       ESTABLISHED
```

1. Rappel : à quoi sert le protocole TCP ?

2. Donnez l'encapsulation du protocole TCP.

3. Quelle est l'adresse IP de la machine sur laquelle on a tapé cette commande ?

4. Voici quelques ports standard : 21 = FTP, 22 = SFTP, 23 = Telnet. Qu'est-ce qu'on peut dire sur la machine sur laquelle on a tapé la méthode Netstat ?